Citrix Receiver für Linux 13.10

Contents

Neue Features

February 22, 2019

Neue Features in 13.10

Verbesserungen bei der Protokollierung

Die Funktion zur Verbesserung der Protokollierung ist eine Erweiterung der besseren Protokollierung. Die Protokollierung für den Einzelhandel wird für die Module Connection Center, Graphics (Thinwire) und End User Experience Monitoring (EUEM) eingeführt. Diese Verbesserung hilft Benutzern bei der Problembehandlung und erleichtert bei komplizierten Problemen die Arbeit des Supportteams dank detaillierter Protokolle.

Informationen zum Aktivieren der Protokollierung für Retailbuilds finden Sie unter Aktivieren der Protokollierung für Retailbuilds.

Kryptographische Aktualisierung

Mit diesem Feature ändert sich das Protokoll zur sicheren Kommunikation grundlegend. Verschlüsselungssammlungen mit dem Präfix **TLS_RSA_** bieten **Forward Secrecy** nicht. Diese Verschlüsselungssammlungen werden von der Branche mittlerweile allgemein als veraltet eingestuft. Um die Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop zu unterstützen, kann die Citrix Workspace-App für Linux diese Verschlüsselungssammlungen aktivieren. Weitere Informationen finden Sie unter Konfigurieren von veralteten Verschlüsselungssammlungen.

Layoutspeicherung im Multimonitormodus

Mit dieser Funktion können Sie die Position einer Desktopsitzung speichern, um diese dann an derselben Position neu starten. Dadurch müssen Sitzungen nicht aufwändig bei jedem Start neu positioniert werden. Sie können die Layoutinformationen über Endpunkte hinweg dynamisch anpassen und speichern und so die Endbenutzererfahrung in Multimonitorumgebungen optimieren. Weitere Informationen finden Sie unter Konfigurieren der Layoutspeicherung im Multimonitormodus.

Aktualisierung von SoC SDK

Kunden, die das SoC SDK verwenden, müssen u. U. die Plug-Ins für H.264-basierte Sitzungsgrafiken aktualisieren.

V3 Authentifizierungsprotokoll

Die V3-Authentifizierung bezeichnet die dritte Hauptdefinition eines Anmeldeprotokolls für NetScaler Gateway, das von der Citrix Workspace-App für Linux unterstützt wird.

V3 ist das Standardanmeldeprotokoll für NetScaler Gateway in Kombination mit dem Authentifizierungsrichtlinien-Framework "N-Factor", mit dem Authentifizierungsschritte und zugehörige Formulare zur Anmeldedatenerfassung vollständig konfigurierbar sind. Die systemeigene Citrix Workspace-App kann dieses Protokoll über die unterstützten Anmeldeformulare nutzen, die bereits für StoreFront implementiert sind. Die webbasierte Anmeldeseite für virtuelle NetScaler Gateway- und Traffic Manager-Server verwendet ebenfalls dieses Protokoll mit Code, der auch von der Citrix Workspace-App für Linux verwendet wird.

Weitere Informationen finden Sie unter SAML-Authentifizierung und im Knowledge Center-Artikel Netscaler Authentication.

Neue Features in 13.9.1

Die Citrix Workspace-App für Linux enthält nun GStreamer 1.0-Dateien. Diese Dateien sind in den Citrix Workspace-App für Linux 13.9-Paketen nicht verfügbar.

Neue Features in 13.9

Umleitung des Browserinhalts

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dadurch wird die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder Flash-Videos, verbessert. Die Browserinhaltsumleitung wird auf den x86-, x64- und ARM-Hardfloat-Plattformen (armhf) unterstützt.

Weitere Informationen finden Sie unter Umleitung des Browserinhalts und Richtlinieneinstellungen für die Umleitung des Browserinhalts in der Dokumentation von XenApp und XenDesktop.

Bessere Protokollierung

Der Retailbuild der Standardversion der Citrix Workspace-App für Linux kann jetzt Protokolle über Syslog generieren und senden. Dieses Feature ermöglicht es, die Verarbeitung von Nachrichten basierend auf ihrer Protokollebene und Herkunft zu steuern. Die Protokollierung für Retailbuilds wird für die Verbindungssequenz (WD, PD, TD, Proxy) und Druckkomponenten eingeführt. Dies hilft

Benutzern bei der Problembehandlung und die verfügbaren detaillierten Protokolle erleichtern bei komplizierten Problemen die Arbeit des Supportteams. Die Protokollausgabe ähnelt dem aktuellen Debuggingmodus.

Protokollierungsparameter, Protokollebene, Protokolldatei, Protokollierungsmethode (Sequenz, Mehrfachsequenz, Zyklus) und das zu protokollierende Modul können mithilfe von Konfigurationsdateien konfiguriert werden. Informationen zum Aktivieren der Protokollierung für Retailbuilds finden Sie unter Aktivieren der Protokollierung für Retailbuilds.

Unterstützung für Citrix Ready Workspace Hub

Citrix Ready Workplace Hub bietet eine sichere Verbindung zu autorisierten Apps und Daten. In dieser Version erweitert die Citrix Workspace-App für Linux die Implementierung des Plug-Ins für Workspace Hub, das Unterstützung für das Citrix HDX RealTime Optimization Pack und zwei mit einem Workspace Hub verbundene Bildschirme bietet.

Behobene Probleme

January 22, 2019

Citrix Workspace-App für Linux 13.10

Die folgenden Probleme wurden seit Version 13.9.1 behoben:

Seamlessfenster

- Wenn Sie mit Citrix Workspace im Seamlessmodus auf veröffentlichte Anwendungen zugreifen, werden die Anwendungen möglicherweise als Anwendungsgruppe mit einer Tag-Beschränkung veröffentlicht. Daher wird folgende Fehlermeldung in XenApp und XenDesktop 7.15 Long Term Service Release (LTSR) Cumulative Update 1 (CU1) angezeigt.
  “Die X-Anforderung 55.0 verursachte den Fehler: “9: BadDrawable (Invalid Pixmap or Window Parameter)”.” [#LC9437]

Sitzung/Verbindung

- Die automatische Proxyerkennung funktioniert möglicherweise nicht mit der Citrix Workspace-App. Daher wird die Anwendung nicht gestartet und folgende Fehlermeldung wird angezeigt: “Verbindung mit “0.0.0.129 - Anwendungsname” kann nicht hergestellt werden.” [#LC8101]

- Wenn Sie eine Benutzersitzung im Vollbildmodus starten, die auf zwei verschiedenen Monitoren ausgeführt wird, kann das Trennen eines Monitors zu der folgenden Fehlermeldung führen: "11: BadAlloc (insufficient resources for operation)" [#LC8522]
- Wenn Sie die Citrix Workspace-App verwenden, funktioniert die Option "Zeiger automatisch auf die Standardschaltfläche in einem Dialogfeld verschieben" möglicherweise nicht, wenn sie auf dem VDA aktiviert ist. [#LC8845]
- Wenn Sie Anwendungen über die Citrix Workspace-App starten, wird diese Fehlermeldung möglicherweise angezeigt:
  "BadWindow (ungültiger Window-Parameter)" [#LC9447]
- Wenn Sie bestimmte Vorgänge ausführen, z. B. Anmeldungen oder Übertragungen von Clientlaufwerkszuordnungen, werden die Benutzersitzungen, die über NetScaler verbunden sind, möglicherweise getrennt, wenn die Citrix Workspace-App verwendet wird. [#LC9574]
- Der StoreFront-Store verfügt über zwei Delivery Controller, von denen einer offline ist. Wenn Sie den Befehl storebrowse –killdaemon oder storebrowse -K verwenden, werden die zuletzt verwendeten Anmeldeinformationen, die im SSO-Cache gespeichert sind, möglicherweise nicht entfernt. Aus diesem Grund kann sich storebrowse weiterhin beim Delivery Controller authentifizieren, ohne dass nach Anmeldeinformationen gefragt wird. [#LC9611]
- Beim Starten einer Citrix Workspace-App-Sitzung aus der TAR-Datei tritt ein Fehler auf. Die Datei All_Regions.ini unter linuxx64-13.x.tar\linuxx64\linuxx64\linuxx64.cor\config\usertemplate\All_Regions.ini enthält in einigen Fällen doppelte Einträge (LocaleKeyMapping=*,SuperMetaToWinKeys=* & RightSuperMetaToWinKey=*). [#LC9765]

Benutzererfahrung

- Wenn Sie eine veröffentlichte Microsoft PowerPoint-Präsentationsfolie im Vollbildmodus auf einem Ubuntu-Client öffnen, können bestimmte Abschnitte der Folien fehlen oder verschoben sein. [#LC8734]
- Wenn Sie eine Desktopsitzung mit zwei Monitoren in der Citrix Workspace-App starten, wird die Windows-Taskleiste möglicherweise als weißer Bildschirm angezeigt. [#LC9021]

Citrix Workspace für Linux 13.9.x

Die folgenden Probleme wurden seit Version 13.8 behoben:

Server- /Siteverwaltung

- Wenn Sie den Befehl "storebrowse -killdaemon" verwenden, werden Sie u. U. unter Verwendung der im Cache gespeicherten Anmeldeinformationen direkt bei einer Sitzung angemeldet,

was zu einem ungültigen Benutzer führt. Stattdessen muss die Eingabeaufforderung für Benutzername und Kennwort für den aktuellen Benutzer angezeigt werden. Das Problem tritt auf, wenn der Befehl "storebrowse -killdaemon" die zwischengespeicherten Anmeldeinformationen des StoreFront-Servers seit der letzten Anmeldung des Benutzers nicht gelöscht hat. [#LC8707]

Sitzung/Verbindung

- Bei Verwendung der Citrix Workspace-App können Versuche fehlschlagen, Audio mit einem Eingabegerät aufzuzeichnen, das in einem VDA für Serverbetriebssysteme ist. [#LC8072]
- Versuche, eine Verbindung zu veröffentlichten Anwendungen oder Desktops herzustellen, schlagen bei Verwendung von TLS 1.0 und TLS 1.2 möglicherweise fehl. [#LC8122]
- Das Maximieren von veröffentlichten Anwendungen, die auf einem Xubuntu-Betriebssystem ausgeführt werden, schlägt u. U. fehl. Das Problem tritt auf, wenn Sie die Taskleiste über mehrere Monitore anzeigen. [#LC8436]

Citrix Workspace für Linux 13.8

Die folgenden Probleme wurden seit Version 13.7 behoben:

Drucken

- Beim Drucken eines Dokuments leitet die Citrix Workspace-App den Druckauftrag ungeachtet des ausgewählten Druckers an den Standarddrucker um. [#LC8221]

Server- /Siteverwaltung

- Wenn Sie den Befehl "storebrowse -killdaemon" verwenden, werden Sie u. U. unter Verwendung der im Cache gespeicherten Anmeldeinformationen direkt bei einer Sitzung angemeldet, was zu einem ungültigen Benutzer führt. Stattdessen muss die Eingabeaufforderung für Benutzername und Kennwort für den aktuellen Benutzer angezeigt werden. Das Problem tritt auf, wenn der Befehl "storebrowse -killdaemon" die zwischengespeicherten Anmeldeinformationen des StoreFront-Servers seit der letzten Anmeldung des Benutzers nicht gelöscht hat. [#LC8707]

Sitzung/Verbindung

- Wenn Sie Citrix Workspace mit Cisco VXME-Plug-Ins verwenden, wird Microsoft Windows Server möglicherweise beim Starten einer Sitzung getrennt. [#LC8496]

Smartcards

- In einem Double-Hop-Szenario können Versuche, auf eine Smartcard zuzugreifen, bei Verwendung der Citrix Workspace-App fehlschlagen. Die folgende Fehlermeldung wird angezeigt:

  “Auf dieser Smartcard wurden keine gültigen Zertifikate gefunden.”

  [#LC7424]

Citrix Workspace für Linux 13.7

In diesem Release wurden keine von Kunden gemeldeten Probleme behoben.

Citrix Workspace für Linux 13.6

Die folgenden Probleme wurden seit Version 13.5 behoben:

Drucken

- Die Citrix Workspace-App führt möglicherweise den ursprünglichen Druckauftrag aus, aber nachfolgende Druckaufträge in derselben Sitzung können fehlschlagen. [#LC7913]

Sitzung/Verbindung

- Wenn “Proxy Auto Configuration” aktiviert ist, kann der Versuch, eine Anwendung zu starten, zu einem segfault-Fehler in wfica führen. [#LC8179]

Tastatur

- Nach dem Upgrade auf die Citrix Workspace-App für Linux 13.5 funktioniert die Tastatureingabe möglicherweise nicht innerhalb einer Clientsitzung. [#LC7591]

Sitzung/Verbindung

- Folgende Fehlermeldung wird möglicherweise in der Citrix Workspace-App angezeigt:

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

  [#LC6682]

- Folgende Fehlermeldung wird möglicherweise in der Citrix Workspace-App angezeigt:

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

  [#LC6733]

Citrix Workspace für Linux 13.5

Die folgenden Probleme wurden seit Version 13.4 behoben:

HDX MediaStream Flash-Umleitung

- Wenn Sie die Größe eines Microsoft Internet Explorer-Fensters ändern, während HDX MediaStream Flash-Umleitung aktiviert ist, werden Websites mit Flash-Inhalten möglicherweise nicht an die geänderte Größe des Internet Explorer-Fensters angepasst. [#LC6126]

Sitzung/Verbindung

- Bei der Wiedergabe eines Medienclips in der Desktopsitzung auf einem HP Thin Client generiert Windows Media Player u. U. folgende Fehlermeldung:

  "Beim Wiedergeben der Datei ist in Windows Media Player ein Problem aufgetreten."

  Unter bestimmten Umständen wird ein leeres oder schwarzes Fenster angezeigt.

  [#LC5508]

- Beim Starten von der Citrix Workspace-App aus verschwinden Dropdownmenüs veröffentlichter Anwendungen möglicherweise sofort, nachdem sie angezeigt werden. [#LC5574]
- Wenn Sie eine Sitzung starten und dann die Fortschrittsanzeige für die Verbindung schließen, sendet der Prozess wfica u. U. ein SIGTERM an alle Prozesse in der Prozessgruppe. Die Prozesse dieser Prozessgruppe werden u. U. unerwartet beendet. [#LC5858]
- Wenn in einer Multimonitorumgebung eine Seamlessanwendung auf dem zweiten Monitor ausgeführt wird, kann das Wechseln zwischen Workspaces in Gnome 3 dazu führen, dass die Seamlessanwendung nicht richtig gerendert wird. Das Problem tritt auf, wenn "workspaces-only-on-primary" auf Gnome 3 aktiviert ist. [#LC5897]

- Die Tastenkombination “Strg+Alt+Entf” in der Symbolleiste von Desktop Viewer funktioniert möglicherweise nicht in Linux VDA-Sitzungen. [#LC6164]
- Wenn Sie versuchen, eine Anwendung durch Klicken auf das entsprechende Desktopsymbol zu starten, schlägt der Start der Anwendung u. U. fehl. [#LC6285]
- Das Starten einer Sitzung mit H.264-Codierung auf einem Linux VDA kann in wfica zu einem segfault-Fehler führen. [#LC6603]

Systemausnahmen

- Bei Verbindungsversuchen zu bestimmten XenApp- oder XenDesktop-Sites wird AuthManager-Daemon u. U. unerwartet beendet. [#LC6166]

Benutzererfahrung

- Beim Starten einer Seamlessanwendung, die mehrere untergeordnete Fenster enthält, können Sie bestimmte untergeordnete Fenster möglicherweise nicht verschieben. Außerdem können Sie u. U. nicht zu diesen Fenstern wechseln. [#LC4342]
- Wenn Sie sich von einem lokalen Desktop abmelden und dabei das Dialogfeld für die Self-Service-Anmeldeinformationen geöffnet ist, schlagen weitere Anmeldeversuche bei Self-Service u. U. fehl und das Authentifizierungsdialogfeld für Self-Service wird u. U. nicht angezeigt. [#LC4939]
- Beim Starten von Microsoft Excel im Seamlessmodus wechselt der Tastaturfokus manchmal nicht in das Fenster “Suchen” in der Anwendung. [#LC5964]

Benutzeroberfläche

- Die Symbole für “Sametime” werden u. U. nicht im Infobereich angezeigt, wenn die Citrix Workspace-App verwendet wird. [#LC3956]
- Wenn Sie das Microsoft Lync-Chatfenster an eine neue Position verschieben, wird das Fenster u. U. nicht vollständig neu gezeichnet. [#LC5583]
- Wenn Microsoft Excel im Seamlessmodus gestartet wurde, schlägt das Verschieben des Fensters “Suchen” u. U. fehl. [#LC5963]
- Wenn Sie ein untergeordnetes Fenster minimieren (Beispiel: das Hauptfenster von Spy++ ist das übergeordnete Fenster und das Fenster zum Erkennen von bestimmten Fenstern ist das untergeordnete Fenster), erscheint die Größe der minimierten Titelleiste möglicherweise kleiner. [#LC6210]

Citrix Workspace für Linux 13.4

Die folgenden Probleme wurden seit Version 13.3 behoben:

Probleme bei Clientgeräten

- Wenn Clientlaufwerkzuordnung aktiviert ist, dauert der Zugriff auf zugeordnete Laufwerke manchmal länger als erwartet. [#LC3930]

Verbesserung

- Durch die neu in diesem Release eingeführte Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Funktion ist für Anwendungen erforderlich, die relative Mauseingabe statt absoluter Eingabe erfordern.

> Hinweis: Dieses Feature ist nur in Sitzungen verfügbar, die unter XenApp oder XenDesktop 7.8 ausgeführt werden. In der Standardeinstellung ist das Steuerelement deaktiviert.

- Aktivieren des Features:*

  Fügen Sie der Datei $HOME/.ICAClient/wfclient.ini im Abschnitt [WFClient] folgenden Eintrag hinzu: RelativeMouse=1.
  Damit wird das Feature aktiviert, zum Verwenden müssen Sie es jedoch noch einschalten.

- Einschalten des Features:

  Drücken Sie Strg/F12.
  Wenn das Feature aktiviert ist, drücken Sie erneut Strg/F12, um die Serverzeigerposition mit dem Client zu synchronisieren. Die Server- und Clientzeigerpositionen werden bei Verwendung einer relativen Maus nicht synchronisiert.

- Deaktivieren des Features:

  Geben Sie Strg-Umschalt/F12 ein.
  Das Feature wird ebenfalls deaktiviert, wenn ein Sitzungsfenster den Fokus verliert.

  *Alternativ gibt es folgende Werte für RelativeMouse:

  RelativeMouse=2 Aktiviert das Feature und schaltet es ein, wenn ein Sitzungsfenster den Fokus erhält.
  RelativeMouse=3 Aktiviert das Feature und es bleibt immer eingeschaltet.

  Durch Eingeben folgender Einstellungen können Sie Tastaturbefehle ändern:

  RelativemouseOnChar=F11
  RelativeMouseOnShift=Shift

RelativemouseOffChar=F11
RelativeMouseOffShift=Shift

Die unterstützten Werte für RelativemouseOnChar und RelativemouseOffChar sind unter [Hotkey Keys] in der Datei config/module.ini in der Citrix Workspace-App für Linux-Installationsstruktur aufgeführt. Die Werte für RelativeMouseOnShift und RelativeMouseOffShift legen die zu verwendenden Zusatztasten fest und werden unter der Überschrift [Hotkey Shift States] aufgeführt. [#LC5000]

Anmeldung und Authentifizierung

- Version 13.3 der Citrix Workspace-App übergibt einige Befehlszeilenparameter, einschließlich der Option "-clearpassword" nicht an ältere XenApp-Versionen. Die Benutzer können sich infolgedessen nicht anmelden. [#LC4594]

Sitzung/Verbindung

- Der Versuch, eine Benutzersitzung im Vollbildmodus mit der Befehlszeilenoption "-span" zu starten, kann fehlschlagen. [#LC3394]
- Nach einer Größenänderung am zweiten Monitor in einer Konfiguration mit zwei Monitoren kann es vorkommen, dass die Windows-Taskleiste nicht an die ursprüngliche Position zurückkehrt. [#LC3856]
- Bei Anzeigeaktualisierungen aufgrund von Aktionen wie Markieren oder Scrollen kann ein segfault-Fehler in wfica dazu führen, dass die Verbindung der Sitzung getrennt wird oder die Sitzung nicht mehr reagiert. [#LC3947]
- Wird eine getrennte Sitzung mit mehreren Monitoren in Ubuntu 14.04 erneut verbunden, erscheint das Sitzungsfenster nur auf einem Monitor. [#LC4181]
- Der Versuch, eine Verbindung mit einem anonymen Store herzustellen, kann mit folgender Fehlermeldung fehlschlagen:

  "NoWebUIAuth 0" und "Anforderung kann nicht abgeschlossen werden."

  [#LC4270]
- Das Starten eines veröffentlichten Desktops kann fehlschlagen, wenn ein SSL-Proxyhost wie SSL-Relay verwendet wird. [#LC4739]
- Eine veröffentlichte Internet Explorer-Instanz kann den Fokus verlieren und verdoppelt werden, wenn ein Popupfenster im ursprünglichen Browserfenster erscheint. [#LC5066]

Smartcards

- Bei Verwendung einer Smartcard mit pnabrowse kann die PIN nicht an den VDA übergeben werden und die Authentifizierung schlägt fehl. Die Sitzung wird zwar gestartet, es wird jedoch das Anmeldefenster angezeigt. [#LC4241]

Systemausnahmen

- Nach der Wiedergabe von Medien in Windows Media Player auf einem Linux-Client mit ARM HF wird die Sitzung getrennt. [#LC4625]

Benutzererfahrung

- Die Audioqualität des Mikrofons in Sitzungen unter XenApp und XenDesktop 7.6 ist möglicherweise schlecht. [#LC3124]
- In Implementierungen mit ARM HF blinkt die Taskleiste gelegentlich nicht, wenn neue Lync 2010-Nachrichten eintreffen. [#LC3688]
- Nach dem Entsperren einer Benutzersitzung mit zwei Monitoren werden minimierte Fenster möglicherweise nicht an der richtigen Position wiederhergestellt und erscheinen abgestürzt. [#LC3984]
- Wird auf einem Gnome 3-Desktop eine Anwendung gestartet und maximiert, wird der Cursor möglicherweise um den Abstand der oberen Gnome 3-Leiste versetzt. [#LC4738]
- Die Webcam-Umleitung kann in Sitzungen auf einem VDA der Version 7.6 fehlschlagen. [#LC4751]

Benutzeroberfläche

- Kopieren und Einfügen kann zwischen Server und Server sowie Server und Benutzergerät fehlschlagen. [#LC4157]
- Der Cursor verschwindet bei der Wiedergabe eines Vollbildvideos und wird erst wieder angezeigt, wenn das Video nicht mehr im Vollbildmodus wiedergegeben wird. [#LC4428]
- Wenn bestimmte veröffentlichte Drittanbieter-Anwendungen ein Dialogfeld öffnen, kann ein Segmentfehler auftreten. Bei dem Versuch, die Verbindung mit einer unerwartet geschlossenen Anwendung wiederherzustellen, ist der Cursor nicht mehr zu sehen. [#LC4955]

Citrix Workspace für Linux 13.3

Die folgenden Probleme wurden seit Version 13.2 behoben:

Sitzung/Verbindung

- Nach der Wiederherstellung eines maximierten Seamlessfensters werden einige Bereiche des Desktops nicht automatisch aktualisiert. Dies tritt bei einigen Desktopumgebungen, wie Ubuntu 12.04 Unity 2D, auf. [#LC0602]
- Beim Verwenden des Parameters "ProxyType=Secure" kann ein Segmentierungsfehler auftreten. [#LC3396]
- Das Kopieren und Einfügen von Inhalt aus einer veröffentlichten Anwendung in eine lokale Anwendung kann dazu führen, dass der Prozess der ICA-Engine-Komponente (wfica) unerwartet mit einem Segmentierungsfehler beendet wird. [#LC3480]
- In bestimmten Situationen ist die Liste der zwischengespeicherten Anwendungen nicht synchronisiert. [#556245]

Systemausnahmen

- Manchmal führt die Smartcardauthentifizierung dazu, dass eine Sitzung unerwartet beendet wird. [#582550]

Benutzererfahrung

- Mit diesem Fix können russische Zeitzoneninformationen in der Citrix Workspace-App für Linux aktualisiert werden.

  Implementieren des Fixes:

  - Für XenApp 6.5 müssen Sie mindestens Hotfix Rollup Pack 5 oder aktuellere Rollup Pack Hotfixes installieren, damit alle Zeitzonen richtig umgeleitet werden.
  - Für den VDA auf XenApp und XenDesktop 7.6-Serverbetriebssystemen müssen Sie Hotfix ICATS760WX64014 installieren.
  - Wird auf dem Server Windows Server 2008 R2 Service Pack 1 ausgeführt, installieren Sie Microsoft Hotfix KB2870165 auf dem Server.
  - Aktualisieren Sie die Betriebssysteme des Servers und der Benutzergeräte, damit die aktuellen Zeitzoneninformationen angewendet werden.
  - Installieren Sie den Microsoft Hotfix KB2998527 für Windows und aktualisieren Sie dann die Zeitzonendaten für Linux.

[#LC1971]

Benutzeroberfläche

- Die Symbole veröffentlichter Anwendungen werden auf der Taskleiste u. U. nicht richtig angezeigt. [#LC3405]
- Symbole in Seamless-Sitzungen werden möglicherweise nicht auf der Taskleiste angezeigt, wenn ARM Hard Float-Plattformen (armhf) verwendet werden. [#LC4051]
- Eine falsche Abhängigkeitsmeldung wird angezeigt, wenn selfservice nach der Installation der Citrix Workspace-App mit einem TAR.GZ-Paket auf Fedora 21 gestartet wird. [#582071]

Citrix Workspace für Linux 13.2

Die folgenden Probleme wurden seit Version 13.1 behoben:

HDX Plug-n-Play

- Die Webcam ist möglicherweise nicht mit Citrix GoToMeeting und Cisco WebEx kompatibel, wenn Sie das HDX RealTime Optimization Pack (Linux) für Microsoft Lync 2010 verwenden. Um den gesamten Fix zu aktivieren, installieren Sie einen Citrix Workspace-Hotfix und einen HDX RealTime Optimization Pack (Linux) für Microsoft Lync 2010-Hotfix, der Fix LA0339 enthält.

  > **Hinweis**: Wenn Sie nach der Installation dieses Fixes Microsoft Lync in einer VDA-Sitzung starten, während eine Citrix GoToMeeting- oder Cisco WebEx-Videokonferenz ausgeführt wird, funktioniert die Webcam möglicherweise nicht mehr. Beenden Sie in diesem Fall die Kamera in der Videokonferenz und starten Sie sie neu. [#LC0339]

Anmeldung und Authentifizierung

- Benutzer können Anwendungen nicht enumerieren oder starten, wenn sie sich über die Unicon-Benutzeroberfläche mit Smartcards anmelden, die mehr als zwei Zertifikate enthalten, wobei nur ein Zertifikat ein Authentifizierungszertifikat ist. Wenn die Smartcard ein Clientzertifikat für die Authentifizierung enthält, können Benutzer Anwendungen enumerieren und starten. Es wird jedoch die folgende Fehlermeldung angezeigt: “Cert Client Authentication OID info set, but unexpected value:…”. [#LC2098]

Server-/Farmverwaltung

- Wenn Verbindungen mit der Citrix Workspace-App für Linux über ein virtuelles privates Netzwerk (VPN) erfolgen, schlägt die Citrix Workspace-App beim Start einer veröffentlichten Anwendung fehl. [#LC1284]
- Wenn Sie den Befehl "ctx_rehash" zum Installieren eines Stamm- oder Zwischenzertifikats auf einem Benutzergerät ausführen, schlägt das Erstellen des richtigen Hashs oder Links u. U. fehl und die Fehlermeldung "Error adding store:AM_ERROR_HTTP_SERVER_CERTIFICATE_NOT_TRUSTED[65150] wird angezeigt. In diesem Fall kann Citrix Workspace das Zertifikat nicht verwenden und Versuche, einen Store hinzuzufügen, schlagen fehl. [#LC1513]
- Wenn ein Benutzer bei Verwendung dieses Fixes mit dem Befehl "$ICAROOT/util/storebrowse –addstore < store URL>" oder mit dem Self-Service Plug-In einen Store hinzufügt und der Parameter "discovery" dabei nicht in der URL eingeschlossen wird, wird der Parameter "discovery" automatisch an die URL angehängt. [#LC1517]

Sitzung/Verbindung

- Wenn Sie das Fenster einer veröffentlichten Microsoft Office-Anwendung im Seamless-Modus maximieren, wird das Fenster maximiert, aber die Inhalte werden u. U. versetzt angezeigt und die linken und oberen Ränder werden möglicherweise nicht aufgebaut. [#LC0118]
- Wenn Sie in einer Umgebung mit mehreren Bildschirmen, in der der zweite Bildschirm gedreht wird oder eine andere Auflösung hat, eine veröffentlichte Anwendung im Seamlessmodus starten und dann das Fenster maximieren, zeigt der Server das maximierte Fenster nicht an und das Fenster kann nicht verwendet werden.

  Sie aktivieren den Fix, indem Sie in der Datei $HOME/.ICAClient/wfclient.ini im Abschnitt [WFClient] den Eintrag "TWIAvoidFullScreenWhenMaximized =True" hinzufügen.

  [#LC0354]
- Wenn in einer Umgebung mit mehreren Bildschirmen das Fenster einer veröffentlichten Anwendung im Seamlessmodus maximiert und mehrmals wiederhergestellt wird, wird u. U. im zweiten Bildschirm statt der Anwendung ein grauer Hintergrund angezeigt. [#LC0355]
- Wenn Sie in einer Umgebung mit mehreren Bildschirmen die Größe des Fensters einer veröffentlichten Anwendung im Seamlessmodus im zweiten Bildschirm ändern, schlägt dieser Vorgang möglicherweise fehl, wenn Sie clientseitige Größenänderung verwenden. [#LC0356]
- Beim Wechseln zwischen zwei veröffentlichten Remotedesktopsitzungen im Vollbildmodus, z. B. mstsc1 und mstsc2, wird der Verbindungsbalken nicht richtig aktualisiert und zeigt auch nach dem Wechsel zu mstsc1 als primäres Fenster mstsc2 an. [#LC0437]

- Das Starten einer Sitzung mit der Citrix Workspace-App kann zur Trennung der Sitzung führen, wenn Daten fortlaufend über die generische USB- oder Clientlaufwerkumleitung von Citrix übertragen werden. [#LC0522]
- Wenn Sie sich am Webinterface mit der IP-Adresse anmelden, tritt u. U. ein segfault auf und pnabrowse wird unerwartet beendet. [#LC0648]
- Wenn Benutzer beim Wechseln zwischen einer veröffentlichten Anwendung und Microsoft SQL Server 2012 Management Studio beide Fenster maximieren und dann nur das Fenster der veröffentlichten Anwendung minimieren, wird das Fenster von Microsoft SQL Server 2012 Management Studio nicht richtig aufgebaut und einige Teile des Fensters werden nicht aktualisiert. [#LC0739]
- Der Fokus bleibt auf dem Hauptfenster statt zum Dialogfeld zu wechseln. Beispiel: Wenn Sie einen veröffentlichten Editor mit dem geänderten Inhalt schließen, werden Sie in einer Meldung gefragt, ob Sie den Inhalt speichern möchten. Das Benachrichtigungsdialogfeld ist nicht das aktive Fenster. [#LC0952]
- Die Citrix Workspace-App wird möglicherweise unerwartet geschlossen, wenn Sie ein Image von einer veröffentlichten Anwendung in eine lokale Anwendung kopieren. [#LC1017]
- Das Starten einer Sitzung mit der Citrix Workspace-App über Citrix NetScaler Gateway kann fehlschlagen. [#LC1103]
- Ein leeres Fehlerdialogfeld wird u. U. angezeigt, wenn ein Benutzer eine Anwendung, die eine Webcam erfordert, in einer VDA-Sitzung öffnet und die Webcam bereits in einer lokalen Anwendung verwendet wird. [#LC1135]
- Wenn das Benutzergerät zwei Bildschirme hat und eine Verbindung zu einem XenDesktop 5.6 VDA hergestellt wird, tritt u. U. ein Problem mit dem zweiten Bildschirm auf. Außerdem wird das Fenster auf dem zweiten Bildschirm beim Maximieren u. U. nicht auf Bildschirmgröße maximiert. [#LC1148]
- Wenn eine Sitzung gestartet oder ihre Größe geändert wird, wird das Framepuffer-Plug-In möglicherweise nicht vollständig ausgeblendet. [#LC1515]
- Die Citrix Workspace-App schlägt fehl, wenn eine automatische Proxyserver-URL auf dem Benutzergerät konfiguriert wird. Der folgende Syslog-Fehler wird im Protokoll angezeigt:

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

  [#LC1584]
- Wenn die Sitzungszuverlässigkeit aktiviert ist und Daten fortlaufend über Citrix Generic USB übertragen werden, wird die vorhandene Sitzung u. U. getrennt. [#LC1588]

- Die 64-Bit-Version der Citrix Workspace-App registriert u. U. das Browser-Plug-In nicht. [#LC1712]
- Bei Systemen, auf denen Fix #LC1127 installiert ist, reagiert die Citrix Workspace-App für Linux 13.1.3 möglicherweise nicht mehr, wenn die Verbindung zu einer mit XenDesktop veröffentlichten Desktopsitzung getrennt wird. [#LC2365]
- Wenn Benutzer sich mit der Citrix Workspace-App anmelden und Inhalt in einem gehosteten und in XenApp 5.0 veröffentlichten Desktop einfügen möchten, wird die Sitzung getrennt und ein Segmentierungsfehler tritt auf, wenn Benutzer mit der rechten Maustaste klicken und mit der Maus auf die Option zum Einfügen zeigen. [#LC2467]
- Wenn bei einer Verbindung mit der Citrix Workspace-App für Linux für Web eine StoreFront Services-Provisioningdatei (.cr) heruntergeladen und dann der storebrowse-Befehl "./util/storebrowse -C /tmp/receiverconfig.cr" ausgeführt wird, wird das Dialogfeld "Add Service Record Add Store" nicht angezeigt und der Store nicht erstellt. [#LC2669]
- Wenn Benutzer der Citrix Workspace-App 13.1 mit der rechten Maustaste auf ein Symbol im Windows-Infobereich klicken, reagiert die Citrix Workspace-App-Sitzung u. U. nicht mehr und Maus und Tastatur funktionieren nicht, bis die Sitzung geschlossen und wieder geöffnet wird. [#LC2824]

Benutzererfahrung

- Beim Durchblättern eines großen Dokuments in der Citrix Workspace-App wird u. u. eine Fehlermeldung angezeigt. Benutzer müssen die Fehlermeldung bestätigen, um weiterhin in der Sitzung arbeiten zu können. [#LC1127]
- Wenn sich die ursprüngliche Bildschirmauflösung eines Benutzergeräts während einer Citrix Workspace-App-Sitzung ändert, behält die Sitzung den Vollbildmodus nicht bei. Daher ändert sich u. U. die Sitzungsgröße, sodass sie weder mit der aktuellen und noch der ursprünglichen Bildschirmauflösung übereinstimmt. [#LC1222]
- Wenn der Symbolname einen umgekehrten Schrägstrich ("\") enthält, werden Anwendungssymbole in der Citrix Workspace-App u. U. nicht ordnungsgemäß angezeigt. [#LC1364]
- Das Kopieren und Einfügen von Inhalt aus Java-Anwendungen in veröffentlichte Anwendungen schlägt u. U. fehl oder zuvor in die Zwischenablage aufgenommener Inhalt wird eingefügt. Das Problem tritt auf, wenn in der Citrix Workspace-App beim Synchronisieren der Zwischenablage des Benutzergeräts mit der Zwischenablage des Servers ein Fehler auftritt. [#LC1856]
- Auf einem Hewlett-Packard Thin-Gerät, das den Hardwaredecoder für H.264-Grafiken verwendet, schlägt in einer VDA-Sitzung und nach dem Start einer Anwendung in der Sitzung das Kopieren und Einfügen von Text in offenen Dokumenten fehl. Auch das Kopieren von Text von

einem Anwendungsfenster in ein anderes Anwendungsfenster, das in einem VDA ausgeführt wird, schlägt fehl. [#LC2985]

Benutzeroberfläche

- Wenn StoreFront mit einer Aggregationsgruppe konfiguriert ist und wenn der Anwendungsname einen umgekehrten Schrägstrich ("\") enthält, schlägt der Start von Anwendungen in der Citrix Workspace-App möglicherweise fehl. Die folgende Fehlermeldung wird angezeigt:

  "Corrupt ICA file"

  [#LC1268]

Citrix Workspace für Linux 13.1

Die folgenden Probleme wurden seit Version 13.0 behoben:

HDX MediaStream Windows Media-Umleitung

- Die Citrix Workspace-App für Linux 13.0 wählt als Ausgabeformat für die Webcam "Motion JPEG" (MJPEG), obwohl das YUYV-Ausgabeformat verfügbar ist. [#LA5740]

HDX MediaStream Flash-Umleitung

- Wenn HDX MediaStream für Flash aktiviert ist, schlägt das erneute Laden bestimmter Flash-Videos in Internet Explorer möglicherweise fehl. [#LA4345]
- Bei der Wiedergabe eines Videos auf YouTube werden Audio und Video in Internet Explorer möglicherweise nicht korrekt wiedergeben. Dieses Problem tritt auf, wenn Benutzer eine Verbindung mit der Citrix Workspace-App für Linux herstellen und HDX MediaStream Flash-Umleitung aktiviert ist. [#LA5833]
- Wenn HDX Flash-Umleitung aktiviert ist und Sie das YouTube-Steuerelement für die Videogröße verwenden, kann die Flash-Umleitung auf serverseitige Wiedergabe zurückgesetzt werden. [#LA5834]

Tastatur

- Das Drücken von Tastenkombinationen mit Alt, Umschalt oder Strg in einer Remotesitzung kann dazu führen, dass die Tasten gedrückt bleiben. [#LA5730]

- Dieser Fix behebt das folgende Problem mit der Num-Taste:

  Wenn Sie den Mauszeiger aus dem Fenster einer veröffentlichten Anwendung heraus und wieder zurück bewegen und dann bei gedrückter Num-Taste mehrere Tasten auf der Zehnertastatur drücken, wird die erste auf der Zehnertastatur gedrückte Taste nicht in der Sitzung angezeigt.

  [#LC0146]

Sitzung/Verbindung

- Bei aktivierter *Clientzwischenablagenumleitung* schlägt das Kopieren und Einfügen von Dateien in einer Clientsitzung (z. B. mit einer seamless veröffentlichten Version von Windows Explorer) möglicherweise fehl. [#LA5254]
- Veröffentlichte Anwendungsfenster ohne Taskleisteneintrag erhalten keinen Eingabefokus, wenn nicht ein weiteres veröffentlichtes Fenster für dieselbe Anwendung vorhanden ist. [#LA5617]
- Wenn Sie ein Seamless-Fenster verschieben, wird das Fenster in bestimmten Szenarios möglicherweise nicht richtig aufgebaut.

  Sie aktivieren diesen Fix, indem Sie in einer der Dateien ~/.ICAClient/wfclient.ini file oder config/All_Regions.ini im Abschnitt [WFClient] den Eintrag “TWIRedrawAfterMove=TRUE” hinzufügen.

  [#LA5669]
- Dieser Fix verbessert die Dateiübertragungsrate in Umgebungen mit geringer Latenz. [#LA5725]
- Die Citrix Workspace-App für Linux 13.0 wählt als Ausgabeformat für die Webcam “Motion JPEG” (MJPEG), obwohl das YUYV-Ausgabeformat verfügbar ist. [#LA5742]
- DNS-Abfragen, die mehrere Antworten auf eine Suche ergeben (häufig in Round-Robin-Konfigurationen), können dazu führen, dass sichere Verbindungsversuche fehlschlagen und die Citrix Workspace-App unerwartet beendet wird. [#LA5752]
- Beim Wiederherstellen eines maximierten Fensters auf dem Server wird das lokale Fenster wiederhergestellt, der Inhalt des Fensters ist jedoch nicht richtig und die Mausreaktion ist verzögert. [#LA5926]
- Wenn Sie das im Seamlessmodus geöffnete Fenster einer veröffentlichten Anwendung verschieben, wird der Inhalt des Fensters möglicherweise beschädigt. Sie vermeiden dieses Problem wie folgt:
  - Legen Sie auf dem Server für die Richtlinie “Fensterinhalt beim Verschieben anzeigen” die Einstellung “Nicht zugelassen” fest.

  - Fügen Sie auf dem Benutzergerät in der Datei $HOME/wfclient.ini im Abschnitt [WFClient] die Einträge “TWICoordinateWinPosition=True” und “TWIRedrawAfterMove=True” hinzu.

  [#LA5935]

- Wenn die Einstellung **Bildqualität** in der Richtlinie **Visuelle Anzeige** auf einen anderen Wert als den Standardwert (Mittel) festgelegt ist, reagiert die Anzeige von Sitzungen auf einem VDA der Version 7.5 u. U. ab dem Start nicht. [#LC0043]
- Verbindungsversuche mit veröffentlichten Anwendungen oder Desktops über NetScaler Gateway schlagen u. U. fehl und die folgende Fehlermeldung wird angezeigt:

  Es kann keine Verbindung zum Server für Anwendung <> hergestellt werden.
  Serverbrowser-Befehl enthält einen ungültigen Parameter.
  Der Name des Servers konnte nicht aufgelöst werden.

  Das Problem tritt auf, wenn eine zusätzliche Secure Ticket Authority für NetScaler Gateway und StoreFront konfiguriert wurde.

  [#LC0059]

- Bei dem Versuch, sich beim Webinterface mit einem Kerberos-Ticket zu authentifizieren, kann ein segfault auftreten und pnabrowse wird unerwartet beendet. [#LC0065]
- Wenn Sie Alt+Tab drücken, um zwischen den geöffneten Fenstern zu wechseln und das Fenster für die Remotedesktopverbindung zu öffnen, erhält das Fenster keinen Fokus. [#LC0069]
- Wenn der Cursor in einem Anwendungsfenster ist, wird das Fenster beim Drücken von Alt+Tab u. U. nicht in den Vordergrund verschoben. [#LC0070]
- Beim Ziehen eines Fensters in einen Desktop, der mit der Citrix Workspace-App gestartet wurde, verbleibt u. U. ein Schatten des Fensters. [#LA0128]
- Dieser Fix verhindert die gelegentliche Anzeige einer unerwarteten und ungerechtfertigten Fehlermeldung zu einem Verbindungsproblem, die Benutzern Optionen zum Beenden und Wiederholen bietet. [#LC0129]
- UDP-Audio kann ein paar Minuten nach dem Start der Sitzung unerwartet fehlschlagen. [#LC0137]
- Bei der Übertragung von Daten über einen seriellen Anschluss mit der Citrix Workspace-App für Linux reagieren XenDesktop-Sitzungen u. U. nicht mehr. [#LC0296]
- Wenn Benutzer eine Verbindung mit der Citrix Workspace-App für Linux und dem Thin Client HP t610 herstellen, der auf einem HP ThinPro 4.4-Betriebssystem ausgeführt wird, und wenn die Zeitzone für die folgenden Standorte auf GMT +8 festgelegt ist, wird die Fehlermeldung “Die aktuelle Zeitzone wird nicht erkannt” angezeigt:

  - Singapur

  - Brunei
  - Makassar
  - Kuala Lumpur
  - Kuching
  - Manila

  [#LC0299]

- Beim Wechseln zwischen Microsoft Word und dem Microsoft Terminaldiensteclient (MSTSC) können die in den Fenstern angezeigten Inhalte fehlerhaft sein. [#LC0308]
- Der Befehl pnabrowse -WT führt nicht zum Beenden einer Desktopsitzung.

  Fügen Sie zum Aktivieren des Fixes in der Datei $HOME/wfclient.ini im Abschnitt [WFClient] den Eintrag “LogoffDesktopThroTWI=True” hinzu.

  [#LC0345]

- Wenn Sie die Citrix Workspace-App verwenden, schlägt die Interaktion mit einigen Dropdownlisten möglicherweise fehl. [#LC0365]

Spiegeln

- Wenn die Auflösung des Linux-Client geändert wird und mit der Citrix Workspace-App für Linux eine veröffentlichte Anwendung vom XenApp-Server aus gestartet wird, wird die Anzeige des spiegelnden Geräts u. U. nicht richtig aktualisiert, wenn die Sitzung von der Verwaltungskonsole aus gespiegelt wird. [#LA5165]

Systemausnahmen

- Die Citrix Workspace-App schlägt möglicherweise fehl, wenn Sie PersistentCacheSize aktivieren. [#LC0528]

Sonstiges

- Aktuelle Tarball- und RPM-Pakete werden nicht mit GStreamer auf aktuellen Fedora-, Red Hat- und CentOS AMD (x86_64)-Distributionen integriert. [#LA4212]
- Wenn ein x.509 Public Key-Infrastruktur-Zertifikat mit bestimmten Richtlinienbeschränkungen auf NetScaler Gateway installiert wird, schlägt das Starten einer Anwendung mit der Citrix Workspace-App für Linux u. U. mit einem SSL-Fehler 85 fehl.

  Zum Starten von Anwendungen müssen Sie folgenden Schlüssel in der Datei All_Regions.ini festlegen:

[Network\SSL]
EnableCertificatePolicyVerification=1

[#LA5609]

- Dieser Featureerweiterung bietet Unterstützung für SHA-2-Zertifikate in der Citrix Workspace-App für Linux. [#LC0136]

Citrix Workspace für Linux 13.0

HDX MediaStream Windows Media-Umleitung

- Wenn HDX RealTime aktiviert ist, kann es beim gst_read-Prozess durch das Umleiten der Webcamdaten im Laufe der Zeit zu einem langsamen Speicherverlust kommen. [#LA1933]

Tastatur

- Wenn Sie mit der Citrix Workspace-App für Linux eine Verbindung mit einem virtuellen Windows 7-Desktop herstellen, wird in einer Meldung zum Zustand der Feststelltaste auf dem Windows 7-Anmeldebildschirm der Zustand der Feststelltaste auf dem Client möglicherweise nicht richtig angezeigt, bis eine Zeichentaste gedrückt wird. [#LA1784]
- Beim Wechseln zwischen lokalen und veröffentlichten Anwendungen wird die erste Taste ignoriert, die Sie nach dem Drücken der Strg-Taste drücken, oder es wird eine andere als die gedrückte Taste angezeigt. [#LA3397]
- **Wichtig**: Wenn Sie diesen Fix auf Systemen mit Fix #LA1965 installieren, funktioniert Fix #LA1965 nicht mehr. Installieren Sie diesen Fix nicht auf Systemen, auf denen Sie Fix #1965 installiert haben und benötigen.

  Tastenkombinationen, z. B. Alt+Tab, werden u. U. nicht an die Sitzung weitergeleitet, sondern werden vom Client interpretiert.

  Erläuterung zu Fix #LA1965:

  Bei einer Verbindung im Nicht-Seamlessmodus wird dem Benutzer der Citrix Workspace-App für Linux u. U. eine Sekunde lang ein grauer, flackernder Bildschirm angezeigt, bevor ein veröffentlichter Desktop oder eine veröffentlichte Anwendung angezeigt wird.

  [#LA3660]
- Wenn eine veröffentlichte Anwendung so konfiguriert ist, dass mit einer der LED-Tasten (Feststelltaste, Num-Taste oder Rollen) ein Makro ausgeführt wird, wird das Makro beim Drücken der Taste u. U. mehrmals ausgeführt.

Sie aktivieren diesen Fix, indem Sie im Ordner ~/.ICAClient in der Datei wfclient.ini im Abschnitt [WFClient] den Eintrag "BypassSetLED=True" hinzufügen. Wenn der Ordner ~/.ICAClient nicht vorhanden ist, ändern Sie stattdessen die Datei /opt/Citrix/ICAClient/nls/en/wfclient.ini.

[#LA3825]

- Beim Verwenden der japanischen Version der Citrix Workspace-App in einer virtuellen Desktopsitzung ist u. U. der Zustand der Feststelltaste auf der IME-Leiste falsch, wenn die Tasten Umschalt+Eisu gedrückt werden. [#LA4072]
- Wenn die Citrix Workspace-App in einer virtuellen Desktopsitzung verwendet wird und der japanische IME auf dem VDA installiert und aktiviert ist, kann es zu Inkonsistenzen zwischen dem Zustand der Feststelltaste auf der IME-Leiste und dem Endpunkt kommen, während die Tasten Umschalt+Eisu gedrückt werden. [#LA4422]

Sitzung/Verbindung

- In einer Umgebung mit mehreren Bildschirmen legt die Citrix Workspace-App die Größe eines maximierten Fensters im sekundären Bildschirm u. U. nicht richtig fest. Daher kann die Fenstergröße größer als die Bildschirmgröße sein. [#LA0663]
- Wenn IBM Lotus Notes mit einer anderen veröffentlichten Anwendung (z. B. Microsoft Excel) gestartet wird, wird beim Öffnen einer Anlage in einer Sitzung das Anlagenfenster u. U. nicht richtig aktualisiert und über anderen Fenstern angezeigt. Dies kann dazu führen, dass die Instanzen von anderen Fenstern als schwarzes oder andersfarbiges Rechteck angezeigt werden. [#LA1490]
- Wenn die Zeitzonenumleitung aktiviert ist, ist die in der Sitzung angezeigte und angewendete Zeit der Einstellung entsprechend richtig. Wenn Sie jedoch das Fenster "Datum und Uhrzeit" in der Systemsteuerung öffnen, wird die folgende Fehlermeldung angezeigt:

  "Die aktuelle Zeitzone wird nicht erkannt. Wählen Sie über den folgenden Link eine gültige Zeitzone aus."

  [#LA1828]
- Bei Systemen mit dem IceWM-Fenstermanager verteilt der Befehl **-span o** die Sitzung nicht über zwei Bildschirme. Stattdessen wird die Sitzung nur auf einem Bildschirm angezeigt. [#LA2178]
- Der Versuch, eine Datei, deren Name das 5C Yen-Symbol (Umschalt-JIS-codiert) enthält, mit einem clientseitig zugeordneten USB-Gerät zu öffnen, schlägt u. U. fehl. [#LA2183]
- Dieser Fix erweitert die SucConnTimeout-Einstellung, sodass sie von veröffentlichten Anwendungen und veröffentlichten Desktops angewendet wird. Daher wird der Start von mehreren Desktops um die durch das SucConnTimeout angegebenen Sekunden verzögert.

  So ändern Sie den SucConnTimeout-Wert:

Bearbeiten Sie den Abschnitt [WFClient] der Datei ~/.ICAClient/wfclient.ini wie folgt:

[WFClient]
Version=2

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

Wenn der Ordner ~/.ICAClient/ im Basisverzeichnis des Benutzers nicht vorhanden ist, ändern Sie die Datei /opt/Citrix/ICAClient/nls/en/wfclient.ini wie zuvor beschrieben. Die Datei wird in den Ordner ~/.ICAClient kopiert, wenn der Benutzer zum ersten Mal eine Verbindung herstellt. Zudem können Sie bei Bedarf ApplySucConnTimeoutToDesktops=True im selben Abschnitt wie SucConnTimeout hinzufügen.

[#LA2679]

- Das Starten einer veröffentlichten Anwendung aus der Citrix Workspace-App mit Domänenanmeldeinformationen mit Centrify schlägt u. U. fehl. [#LA3270]
- Durch diese Erweiterung erhält die Citrix Workspace-App Lese- und Schreibzugriff auf Dateien auf zugeordneten Clientlaufwerken, die das XFS-Dateisystem verwenden. [#LA3610]
- Beim Wechseln von Arbeitsbereich A zu Arbeitsbereich B und zurück zu Arbeitsbereich A wird der Fokus nicht auf dem Fenster wiederhergestellt, das zuletzt den Fokus in dem Arbeitsbereich hatte.

  Hinweis: Dieser Fix behebt das Problem für KDE-, Xfce- und Gnome-Desktopumgebungen. Er funktioniert nicht für Unity-Desktops.

  [#LA3432]

- Das Verwenden von pnabrowse in einer Umgebung mit mehreren Domänen schlägt u. U. fehl, wenn eine andere Domäne für die Benutzerauthentifizierung verwendet wird. Das Problem ist darauf zurückzuführen, dass die ursprüngliche Codeimplementierung Benutzernamen und Domäne separat behandelt. Daher funktioniert die Verwendung von pnabrowse mit einer anderen Domäne nicht.

  Beispiel: Auf einen Benutzer kann als user1@this.company oder als user1@this.local verwiesen werden, wobei die primäre Domäne *this.company* und die andere Domäne *this.local* ist. Der Fix stellt sicher, dass beide der folgenden Methoden funktionieren:

  > ./pnabrowse -L desk -U user1 -D this.company -P company123 <*IP-Adresse*>
  >
  > ./pnabrowse -L desk -U user1@this.local -P company123 <*IP-Adresse*>

  [#LA3551]

- Benutzerdefinierte virtuelle Kanäle werden bei einer automatischen Wiederverbindung von der Citrix Workspace-App für Linux u. U. nicht initialisiert. [#LA3572]
- Selbst wenn die Option “In Dialogfeldern automatisch zur Standardschaltfläche springen” (damit zeigt der Mauszeiger in einem geöffneten Dialogfeld automatisch auf die Standardschaltfläche) auf dem Server aktiviert ist, funktioniert das Feature in einer veröffentlichten Anwendung mit der Citrix Workspace-App u. U. nicht. [#LA4285]
- Im Seamlessmodus wird der rechte untere Rand und der untere Teil bestimmter Java-Anwendungsfenster (z. B. jEdit) u. U. nicht richtig aufgebaut, wenn sie verschoben oder wiederhergestellt werden.

  Sie aktivieren den Fix, indem Sie den Eintrag “TWISetFocusBeforeRestore=True” im Abschnitt [WFClient] der Datei $HOME/.ICAClient/wfclient.ini hinzufügen.

  [#LA4450]
- In NetScaler-Bereitstellungen kann die USB-Geräteumleitung in der Citrix Workspace-App für Linux langsam sein. [#LA4549]
- Wenn Sie das Fenster einer veröffentlichten Anwendung (z. B. Token 2) an einer anderen Stelle als der Titelleiste ziehen, wird das Seamlessanwendungsfenster möglicherweise minimiert.

  Sie aktivieren den Fix, indem Sie den Eintrag “TWIMoveResizeHideWindowType=2” im Abschnitt [WFClient] der Datei wfclient.ini hinzufügen.

  [#LA4737]

Systemausnahmen

- Bei der Einstellung von CommPollSize=On in der Datei module.ini wird der Prozess wfica.exe u. U. unerwartet beendet. [#LA2155]
- Bei dem Versuch, aus einer Java-basierten Anwendung in einem veröffentlichten Desktop heraus zu drucken, wird die Citrix Workspace-App u. U. unerwartet beendet. [#LA3321]
- Beim Einfügen einer großen Datenmenge aus der Zwischenablage wird die Citrix Workspace-App u. U. unerwartet beendet. [#LA3608]
- Die Citrix Workspace-App kann unerwartet beendet werden. Das Problem tritt u. U. auf, wenn eine veröffentlichte Anwendung mehr als 50 chinesische Zeichen in der Titelleiste enthält. [#LA4119]

Benutzererfahrung

- Wenn Sie die Alt-Taste drücken während Sie das Fenster einer veröffentlichten Anwendung an einer anderen Stelle als der Titelleiste ziehen, wird der Inhalt des Fensters nicht gemeinsam mit

dem Fensterrahmen verschoben. Wenn Sie die Maustaste loslassen, wird zudem das gerade beendete Ziehen wiederholt. [#LA0837]

- Der Mauszeiger wird u. U. an einer falschen Position angezeigt, wenn Sie das Fenster des sekundären Bildschirms maximieren. Menüs und Schaltflächen werden u. U. falsch aktiviert, wenn Sie den Mauszeiger darüber positionieren. Das Problem tritt auf, wenn der sekundäre Bildschirm eine geringere vertikale Auflösung (in Pixel) hat als der primäre Bildschirm.

  Beispiel: Die Auflösung von Bildschirm 1 ist 1920x1080 Pixel und die von Bildschirm 2 ist 1280x1024 Pixel. Wenn Sie eine veröffentlichte Anwendung auf Bildschirm 1 starten und die Anwendung dann auf Bildschirm 2 ziehen und maximieren, wird der Mauszeiger möglicherweise ca. einen Zentimeter neben einer Schaltfläche positioniert. Daher wird u. U. ein QuickInfo-Popupfenster für die Schaltfläche zum Maximieren angezeigt, wenn der Zeiger einen Zentimeter von der Schaltfläche entfernt ist.

  [#LA2071]

- Wenn ein Kontextmenü zu einem Symbol im Infobereich einer seamless veröffentlichten Anwendung geschlossen wird, wird der Bereich des Kontextmenüs nicht ordnungsgemäß neu aufgebaut und ein Teil des Menüinhalts wird weiter angezeigt. [#LA4139]

Benutzeroberfläche

- Durch diese Verbesserung des pnabrowse-Hilfsprogramms können Symbole für veröffentlichte Ressourcen mit einer höheren Auflösung angezeigt werden. [#LA1994]
- Ein Taskleisteneintrag mit dem Namen “Untitled Window” wird u. U. angezeigt, wenn Sie ein Dropdownmenü in einer veröffentlichten Anwendung erweitern. [#LA3422]

Sonstiges

- Mit dieser Verbesserung können Sie die USB-Umleitung von einem Client auf Benutzerbasis beschränken. Um die USB-Umleitung auf einen bestimmten Benutzer zu beschränken, führen Sie die folgenden Befehle auf dem Client als Root-Benutzer oder Administrator aus:

  1. Entfernen Sie den setuid-Teil aus der Binärdatei ctxusb:

     ```
     # chmod u-s /opt/Citrix/ICAClient/ctxusb
     ```

  2. Schließen Sie ein USB-Gerät an und suchen Sie das Gerät im Dateisystem mit folgendem Befehl:

     ```
     # ls -lR /dev/bus/usb
     ```


3. Weisen Sie Berechtigungen zu (z. B. User1), wobei /dev/bus/usb/001/041 als das USB-Gerät in Schritt 2 festgelegt wird:

```
# chown user1 /dev/bus/usb/001/041
```

[#LA1952]

- Die Integration von GStreamer (Anwendung eines Drittanbieters) mit der Citrix Workspace-App für Linux schlägt u. U. für Version 12.04 von Ubuntu fehl.

  [#LA2016]

- Auf 64-Bit-Systemen, wie der Ubuntu 64-Bit-Distribution, findet das Skript hdxcheck.sh nicht die 32-Bit-Versionen der folgenden Bibliotheken: libpcsclite.so, libcrypto.so, libjpeg.so, libldapsdk.so und libcap.so. Dies führt zu folgenden Warnmeldungen:

  "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!

  Das Problem tritt auf, weil das Skript die Bibliotheken nur unter /user/lib sucht. In 64-Bit Linux-Distributionen können die 32-Bit-Versionen dieser Bibliotheken unter /usr/lib/i386-linux-gnu oder /lib/i386-linux-gnu/ installiert sein. Mit diesem Fix sucht das Skript die Bibliotheken auch unter /lib. Wenn die Suche erfolgreich ist, werden die folgenden Meldungen statt der Warnungen angezeigt:

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

  [#LA2204]

- Diese Featureerweiterung bietet Unterstützung für playbin2, einem Open-Source- Multimedia-Framework auf dem HP T510. Sie aktivieren die Unterstützung für playbin2, indem Sie die folgenden Optionen in der Datei All_Regions.ini festlegen:

  SpeedScreenMMAClosePlayerOnEOS=True
  SpeedScreenMMAEnablePlaybin2=True

  [#LA2566]

- Dieser Fix behebt verschiedene Probleme, die durch #LA2566 verursacht wurden. Der Fix ist eine Featureerweiterung, die Unterstützung für das Open-Source-Multimedia-Framework playbin2 auf dem HP T510 einführt. [#LA2757]

Bekannte Probleme

February 22, 2019

Bekannte Probleme in Citrix Receiver für Linux 13.10

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Beim Upgrade von Citrix Receiver können neue Einstellungen nicht der Datei $HOME /. ICAClient/All_Regions.ini hinzugefügt werden. Das Problem tritt auf, weil die Datei $HOME /. ICAClient/All_Regions.ini des Benutzers über eine Vorlage erstellt wird, wenn der Benutzer das erste Mal eine Sitzung startet. Es gibt keinen Versuch, die persönliche All_Regions.ini-Konfiguration des Benutzers bei einem Upgrade zu ändern. Dies bedeutet, dass alle neuen Einträge, die der All_Regions.ini-Vorlage hinzugefügt werden, nicht automatisch auch der vorhandenen All_Regions.ini-Datei eines Benutzers hinzugefügt werden und neue Einträge sind standardmäßig blockiert.

  Workaround: Wenn Sie die Originaldatei nicht bearbeitet haben, löschen Sie $HOME/.ICAClient/All_Regions.i
  Ein Upgrade erstellt eine neue All_Regions.ini-Datei. Wenn Sie diese Datei bearbeitet haben, verschieben Sie zu einem Backupspeicherort. Stellen Sie eine Verbindung her, sodass All_regions.ini mit der aktuellen Vorlage generiert wird. Dann vergleichen Sie Ihre Version mit dem neuen $HOME/.ICAClient/All_Regions.ini-Datei mit einem Tools wie diff oder meld und übertragen Ihre persönliche Konfiguration.

  [RFLNX-706]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling

Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.
Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

Wiederholen Sie den Befehl für jeden Kern <c>.

[RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

  [RFLNX-1049]

- Installieren der tar.gz-Version von Citrix Receiver führt zu einem Ungültige-Gruppe-Fehler. Der Fehler tritt auf, weil das Betriebssystem keine Gruppe “sys” hat. Die folgende Fehlermeldung wird angezeigt:

  “chgrp: ungültige Gruppe: sys”

  Als Workaround führen Sie setupwfc mit HOST_SYS_GROUP_NAME aus und legen dabei die gewünschte Gruppe fest.

  HOST_SYS_GROUP_NAME = <group> ./setupwfc

  Geben Sie dann einen Gruppennamen für die installierten Dateien ein.

  [RFLNX-1377]

- Versuche, eine UDT-Verbindung herzustellen, schlagen fehl, wenn die maximale Übertragungseinheit (MTU) für Ihr Netzwerk unter 1500 liegt.

  Als Workaround reduzieren Sie die Größe der generierten UDP-Pakete. Hierfür verringern Sie die Größe von udtMSS so weit, dass die generierten UDP-Pakete über das MTU-Netzwerk gesendet werden können. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX224373.

  [RFLNX-1390]

- Die Bandbreitenschätzung wird bei Verbindungen mit adaptivem Transport möglicherweise nicht aktualisiert. Die führt zu einem Fehlverhalten von Features, für die ein korrektes Lesen der Sitzungsbandbreite erforderlich ist. Zum Beispiel:

  - Da der Sitzungsdurchsatz insgesamt niedriger als erwartet ist, oder im Fall einer Änderung der Netzwerkbedingungen nachdem die Sitzung hergestellt wurde (Reduktion der verfügbaren Bandbreite), versucht der Client möglicherweise, mehr Daten zu senden, als das Netzwerk tatsächlich verarbeiten kann.
  - Falsche oder ungeeignete codierte Bitrate von H264-Grafiken.
  - Fehlverhalten der MediaStream-Transkodierung.

[RFLNX-1408]

- Live Streamingvideos werden u. U. im Overlay-Browser nicht wiedergegeben, wenn die Browserinhaltsumleitung verwendet wird.
  Workaround: Installieren Sie die neueste Version von WebKitGTK.

  [RFLNX-1589]

- Wenn NetScaler Gateway mit SAML-Authentifizierung konfiguriert wurde, schlagen Benutzerzertifikate und Smartcard-Authentifizierung in Citrix Receiver für Linux fehl.

  [RFLNX-2085], [RFLNX-2084]

- Die Popupmeldung "Session layout saved successfully" wird bei einer Sitzung im Vollbildmodus abgeschnitten. Dieses Problem tritt in Japanisch, Französisch und Spanisch auf.

  [RFLNX-2114]

Bekannte Probleme in Citrix Receiver für Linux 13.9x

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Beim Upgrade von Citrix Receiver können neue Einstellungen nicht der Datei $HOME /. ICAClient/All_Regions.ini hinzugefügt werden. Das Problem tritt auf, weil die Datei $HOME /. ICAClient/All_Regions.ini des Benutzers über eine Vorlage erstellt wird, wenn der Benutzer das erste Mal eine Sitzung startet. Es gibt keinen Versuch, die persönliche All_Regions.ini-Konfiguration des Benutzers bei einem Upgrade zu ändern. Dies bedeutet, dass alle neuen Einträge, die der All_Regions.ini-Vorlage hinzugefügt werden, nicht automatisch auch der vorhandenen All_Regions.ini-Datei eines Benutzers hinzugefügt werden und neue Einträge sind standardmäßig blockiert.

  Workaround: Wenn Sie die Originaldatei nicht bearbeitet haben, löschen Sie $HOME/.ICAClient/All_Regions.i
  Ein Upgrade erstellt eine neue All_Regions.ini-Datei. Wenn Sie diese Datei bearbeitet haben, verschieben Sie zu einem Backupspeicherort. Stellen Sie eine Verbindung her, sodass

All_regions.ini mit der aktuellen Vorlage generiert wird. Dann vergleichen Sie Ihre Version mit dem neuen $HOME/.ICAClient/All_Regions.ini-Datei mit einem Tools wie diff oder meld und übertragen Ihre persönliche Konfiguration.

[RFLNX-706]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.
  Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

  Wiederholen Sie den Befehl für jeden Kern <c>.

  [RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

  [RFLNX-1049]

- Installieren der tar.gz-Version von Citrix Receiver führt zu einem Ungültige-Gruppe-Fehler. Der Fehler tritt auf, weil das Betriebssystem keine Gruppe “sys” hat. Die folgende Fehlermeldung wird angezeigt:

  “chgrp: ungültige Gruppe: sys”

Als Workaround führen Sie setupwfc mit HOST_SYS_GROUP_NAME aus und legen dabei die gewünschte Gruppe fest.

HOST_SYS_GROUP_NAME = <group> ./setupwfc

Geben Sie dann einen Gruppennamen für die installierten Dateien ein.

[RFLNX-1377]

- Versuche, eine UDT-Verbindung herzustellen, schlagen fehl, wenn die maximale Übertragungseinheit (MTU) für Ihr Netzwerk unter 1500 liegt.

  Als Workaround reduzieren Sie die Größe der generierten UDP-Pakete. Hierfür verringern Sie die Größe von udtMSS so weit, dass die generierten UDP-Pakete über das MTU-Netzwerk gesendet werden können. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX224373.

  [RFLNX-1390]

- Die Bandbreitenschätzung wird bei Verbindungen mit adaptivem Transport möglicherweise nicht aktualisiert. Die führt zu einem Fehlverhalten von Features, für die ein korrektes Lesen der Sitzungsbandbreite erforderlich ist. Zum Beispiel:
  - Da der Sitzungsdurchsatz insgesamt niedriger als erwartet ist, oder im Fall einer Änderung der Netzwerkbedingungen nachdem die Sitzung hergestellt wurde (Reduktion der verfügbaren Bandbreite), versucht der Client möglicherweise, mehr Daten zu senden, als das Netzwerk tatsächlich verarbeiten kann.
  - Falsche oder ungeeignete codierte Bitrate von H264-Grafiken.
  - Fehlverhalten der MediaStream-Transkodierung.

[RFLNX-1408]

- Live Streamingvideos werden u. U. im Overlay-Browser nicht wiedergegeben, wenn die Browserinhaltsumleitung verwendet wird.
  Workaround: Installieren Sie die neueste Version von WebKitGTK.

  [RFLNX-1589]

Bekannte Probleme in Citrix Receiver für Linux 13.8

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Beim Upgrade von Citrix Receiver können neue Einstellungen nicht der Datei $HOME /. ICAClient/All_Regions.ini hinzugefügt werden. Das Problem tritt auf, weil die Datei $HOME /.

ICAClient/All_Regions.ini des Benutzers über eine Vorlage erstellt wird, wenn der Benutzer das erste Mal eine Sitzung startet. Es gibt keinen Versuch, die persönliche All_Regions.ini-Konfiguration des Benutzers bei einem Upgrade zu ändern. Dies bedeutet, dass alle neuen Einträge, die der All_Regions.ini-Vorlage hinzugefügt werden, nicht automatisch auch der vorhandenen All_Regions.ini-Datei eines Benutzers hinzugefügt werden und neue Einträge sind standardmäßig blockiert.

Workaround: Wenn Sie die Originaldatei nicht bearbeitet haben, löschen Sie $HOME/.ICAClient/All_Regions.i
Ein Upgrade erstellt eine neue All_Regions.ini-Datei. Wenn Sie diese Datei bearbeitet haben, verschieben Sie zu einem Backupspeicherort. Stellen Sie eine Verbindung her, sodass All_regions.ini mit der aktuellen Vorlage generiert wird. Dann vergleichen Sie Ihre Version mit dem neuen $HOME/.ICAClient/All_Regions.ini-Datei mit einem Tools wie diff oder meld und übertragen Ihre persönliche Konfiguration.

[RFLNX-706]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.
  Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

  Wiederholen Sie den Befehl für jeden Kern <c>.

  [RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und

framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

[RFLNX-1049]

- Installieren der tar.gz-Version von Citrix Receiver führt zu einem Ungültige-Gruppe-Fehler. Der Fehler tritt auf, weil das Betriebssystem keine Gruppe “sys” hat. Die folgende Fehlermeldung wird angezeigt:

  “chgrp: ungültige Gruppe: sys”

  Als Workaround führen Sie setupwfc mit HOST_SYS_GROUP_NAME aus und legen dabei die gewünschte Gruppe fest.

  HOST_SYS_GROUP_NAME = <group> ./setupwfc

  Geben Sie dann einen Gruppennamen für die installierten Dateien ein.

  [RFLNX-1377]

- Versuche, eine UDT-Verbindung herzustellen, schlagen fehl, wenn die maximale Übertragungseinheit (MTU) für Ihr Netzwerk unter 1500 liegt.

  Als Workaround reduzieren Sie die Größe der generierten UDP-Pakete. Hierfür verringern Sie die Größe von udtMSS so weit, dass die generierten UDP-Pakete über das MTU-Netzwerk gesendet werden können. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX224373.

  [RFLNX-1390]

- Die Bandbreitenschätzung wird bei Verbindungen mit adaptivem Transport möglicherweise nicht aktualisiert. Die führt zu einem Fehlverhalten von Features, für die ein korrektes Lesen der Sitzungsbandbreite erforderlich ist. Zum Beispiel:

  - Da der Sitzungsdurchsatz insgesamt niedriger als erwartet ist, oder im Fall einer Änderung der Netzwerkbedingungen nachdem die Sitzung hergestellt wurde (Reduktion der verfügbaren Bandbreite), versucht der Client möglicherweise, mehr Daten zu senden, als das Netzwerk tatsächlich verarbeiten kann.
  - Falsche oder ungeeignete codierte Bitrate von H264-Grafiken.
  - Fehlverhalten der MediaStream-Transkodierung.

[RFLNX-1408]

- Der Citrix Receiver für Linux meldet dem VDA fälschlicherweise, dass die Clientadresse die Adresse des Servers ist.

  [RFLNX-1735]

- EDT-Sitzungen (Enlightened Data Transport) reagieren während der Abmeldung möglicherweise zeitweilig nicht.

  [RFLNX-1740]

Bekannte Probleme in Citrix Receiver für Linux 13.7

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Beim Upgrade von Citrix Receiver können neue Einstellungen nicht der Datei $HOME /. ICAClient/All_Regions.ini hinzugefügt werden. Das Problem tritt auf, weil die Datei $HOME /. ICAClient/All_Regions.ini des Benutzers über eine Vorlage erstellt wird, wenn der Benutzer das erste Mal eine Sitzung startet. Es gibt keinen Versuch, die persönliche All_Regions.ini-Konfiguration des Benutzers bei einem Upgrade zu ändern. Dies bedeutet, dass alle neuen Einträge, die der All_Regions.ini-Vorlage hinzugefügt werden, nicht automatisch auch der vorhandenen All_Regions.ini-Datei eines Benutzers hinzugefügt werden und neue Einträge sind standardmäßig blockiert.

  Workaround: Wenn Sie die Originaldatei nicht bearbeitet haben, löschen Sie $HOME/.ICAClient/All_Regions.i
  Ein Upgrade erstellt eine neue All_Regions.ini-Datei. Wenn Sie diese Datei bearbeitet haben, verschieben Sie zu einem Backupspeicherort. Stellen Sie eine Verbindung her, sodass All_regions.ini mit der aktuellen Vorlage generiert wird. Dann vergleichen Sie Ihre Version mit dem neuen $HOME/.ICAClient/All_Regions.ini-Datei mit einem Tools wie diff oder meld und übertragen Ihre persönliche Konfiguration.

  [RFLNX-706]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.

Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

Wiederholen Sie den Befehl für jeden Kern <c>.

[RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

  [RFLNX-1049]

- Installieren der tar.gz-Version von Citrix Receiver führt zu einem Ungültige-Gruppe-Fehler. Der Fehler tritt auf, weil das Betriebssystem keine Gruppe “sys” hat. Die folgende Fehlermeldung wird angezeigt:

  “chgrp: ungültige Gruppe: sys”

  Als Workaround führen Sie setupwfc mit HOST_SYS_GROUP_NAME aus und legen dabei die gewünschte Gruppe fest.

  HOST_SYS_GROUP_NAME = <group> ./setupwfc

  Geben Sie dann einen Gruppennamen für die installierten Dateien ein.

  [RFLNX-1377]

- Versuche, eine UDT-Verbindung herzustellen, schlagen fehl, wenn die maximale Übertragungseinheit (MTU) für Ihr Netzwerk unter 1500 liegt.

  Als Workaround reduzieren Sie die Größe der generierten UDP-Pakete. Hierfür verringern Sie die Größe von udtMSS so weit, dass die generierten UDP-Pakete über das MTU-Netzwerk gesendet werden können. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX224373.

  [RFLNX-1390]

- Die Bandbreitenschätzung wird bei Verbindungen mit adaptivem Transport möglicherweise nicht aktualisiert. Die führt zu einem Fehlverhalten von Features, für die ein korrektes Lesen der Sitzungsbandbreite erforderlich ist. Zum Beispiel:

  - Da der Sitzungsdurchsatz insgesamt niedriger als erwartet ist, oder im Fall einer Änderung der Netzwerkbedingungen nachdem die Sitzung hergestellt wurde (Reduktion der verfügbaren Bandbreite), versucht der Client möglicherweise, mehr Daten zu senden, als das Netzwerk tatsächlich verarbeiten kann.
  - Falsche oder ungeeignete codierte Bitrate von H264-Grafiken.
  - Fehlverhalten der MediaStream-Transkodierung.

[RFLNX-1408]

Bekannte Probleme in Citrix Receiver für Linux 13.6

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Beim Upgrade von Citrix Receiver können neue Einstellungen nicht der Datei $HOME /. ICAClient/All_Regions.ini hinzugefügt werden. Das Problem tritt auf, weil die Datei $HOME /. ICAClient/All_Regions.ini des Benutzers über eine Vorlage erstellt wird, wenn der Benutzer das erste Mal eine Sitzung startet. Es gibt keinen Versuch, die persönliche All_Regions.ini-Konfiguration des Benutzers bei einem Upgrade zu ändern. Dies bedeutet, dass alle neuen Einträge, die der All_Regions.ini-Vorlage hinzugefügt werden, nicht automatisch auch der vorhandenen All_Regions.ini-Datei eines Benutzers hinzugefügt werden und neue Einträge sind standardmäßig blockiert.

  Workaround: Wenn Sie die Originaldatei nicht bearbeitet haben, löschen Sie $HOME/.ICAClient/All_Regions.i
  Ein Upgrade erstellt eine neue All_Regions.ini-Datei. Wenn Sie diese Datei bearbeitet haben, verschieben Sie zu einem Backupspeicherort. Stellen Sie eine Verbindung her, sodass All_regions.ini mit der aktuellen Vorlage generiert wird. Dann vergleichen Sie Ihre Version mit dem neuen $HOME/.ICAClient/All_Regions.ini-Datei mit einem Tools wie diff oder meld und übertragen Ihre persönliche Konfiguration.

  [RFLNX-706]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.
Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

Wiederholen Sie den Befehl für jeden Kern <c>.

[RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

  [RFLNX-1049]

- Installieren der tar.gz-Version von Citrix Receiver führt zu einem Ungültige-Gruppe-Fehler. Der Fehler tritt auf, weil das Betriebssystem keine Gruppe “sys” hat. Die folgende Fehlermeldung wird angezeigt:

  “chgrp: ungültige Gruppe: sys”

  Als Workaround führen Sie setupwfc mit HOST_SYS_GROUP_NAME aus und legen dabei die gewünschte Gruppe fest.

  HOST_SYS_GROUP_NAME = <group> ./setupwfc

  Geben Sie dann einen Gruppennamen für die installierten Dateien ein.

  [RFLNX-1377]

- Versuche, eine UDT-Verbindung herzustellen, schlagen fehl, wenn die maximale Übertragungseinheit (MTU) für Ihr Netzwerk unter 1500 liegt.

  Als Workaround reduzieren Sie die Größe der generierten UDP-Pakete. Hierfür verringern Sie die Größe von udtMSS so weit, dass die generierten UDP-Pakete über das MTU-Netzwerk gesendet werden können. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX224373.

  [RFLNX-1390]

- Die Bandbreitenschätzung wird bei Verbindungen mit adaptivem Transport möglicherweise nicht aktualisiert. Die führt zu einem Fehlverhalten von Features, für die ein korrektes Lesen der Sitzungsbandbreite erforderlich ist. Zum Beispiel:

  - Da der Sitzungsdurchsatz insgesamt niedriger als erwartet ist, oder im Fall einer Änderung der Netzwerkbedingungen nachdem die Sitzung hergestellt wurde (Reduktion der verfüg-

baren Bandbreite), versucht der Client möglicherweise, mehr Daten zu senden, als das Netzwerk tatsächlich verarbeiten kann.
- Falsche oder ungeeignete codierte Bitrate von H264-Grafiken.
- Fehlverhalten der MediaStream-Transkodierung.

[RFLNX-1408]

Bekannte Probleme in Citrix Receiver für Linux 13.5

In diesem Release bestehen die folgenden bekannten Probleme:

- Die StoreFront-URL wird nicht hinzugefügt, wenn Citrix Receiver für Linux unter einem benutzerdefinierten lokalisierten Pfad installiert wird, der 4-Byte-Zeichen enthält.

  [RFLNX-613]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.0 aktiviert sind, verursacht OpenGL u. U. die Anzeige unerwarteter Popupfenster auf einigen Plattformen.

  [RFLNX-949]

- Wenn HDX MediaStream Windows Media-Umleitung und GStreamer 1.4 oder höher aktiviert sind, können im Fetch-Modus serverseitig einige Multimediadateien (MPG1, MPEG2 und H264) nicht wiedergegeben werden.

  [RFLNX-952]

- Wenn auf einem Gerät mit CPU-Frequenzskalierung, wie dem Raspberry Pi, bei der Audiowiedergabe Stottern oder allgemeine Leistungsprobleme auftreten, empfiehlt Citrix, für den Scaling Governor den Leistungsmodus festzulegen. Zum Anzeigen des aktuellen Performance Governors für die einzelnen Kerne führen Sie den folgenden Befehl aus, wobei <c> der jeweilige Kern ist:

  cat /sys/devices/system/cpu/cpu<c>/cpufreq/scaling_governor

  Standardmäßig ist diese Einstellung eine bedarfsgesteuerte Einstellung und nicht immer dynamisch genug, um die gewünschte Leistung in Echtzeit zu bieten.
  Führen Sie als Root-Benutzer folgenden Befehl aus, um für den Scaling Governor den Leistungsmodus festzulegen:

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

  Wiederholen Sie den Befehl für jeden Kern <c>.

  [RFLNX-1003]

- Das hardwarebeschleunigte H264-DecoderPlug-In für den HDX Ready Pi funktioniert nicht richtig, wenn Sie die Framebuffer-Auflösung mit den Parametern framebuffer_width und

framebuffer_height in der Datei /boot/config.txt ändern. Ändern Sie als Workaround die Auflösung für den Pi mit den Parametern hdmi_group und hdmi_mode.

[RFLNX-1049]

Bekannte Probleme in Citrix Receiver für Linux 13.4

In diesem Release bestehen die folgenden bekannten Probleme:

- Wenn das Argument "-span o" verwendet wird, um die Umleitung des Sitzungsfensters zu überschreiben, kann eine Sitzung nicht mit der Desktop Viewer-Symbolleiste vom Vollbildmodus in den Fenstermodus versetzt werden.

  Verwenden Sie in diesem Fall die Option "-span o" nicht. Verwenden Sie stattdessen einen Fenstermanager mit Unterstützung für _NET_WM_FULLSCREEN_MONITORS oder deaktivieren Sie Desktop Viewer.

  [#634855]

- Die sekundäre Sitzung wird u. U. nicht angezeigt, wenn Sie im Desktop Viewer auf ihren Namen unter der Schaltfläche zum Wechseln klicken.

  [#648716]

- Receiver für Linux reagiert nicht mehr, wenn Sie von der X1-Benutzeroberfläche zur klassischen Benutzeroberfläche wechseln.

  Wenn die Self-Service-Benutzeroberfläche den Fehler "NoWebUI 0" anzeigt, starten Sie den Prozess "selfservice" neu, um den normalen Zustand wiederherzustellen.

  [#652810]

- Bei Multimonitorclients verwendet die Flash-Umleitung den falschen Monitor.

  Wenn die Flash-Umleitung auf einem Client mit mehreren Monitoren verwendet wird, wird Flash-Inhalt möglicherweise auf dem falschen Monitor oder außerhalb des Bildschirms angezeigt. Sie können dies verhindern, indem Sie sicherstellen, dass die Sitzung auf allen verfügbaren Monitoren ausgeführt wird, bevor Sie die Flash-Umleitung verwenden.

  [#653550]

- Beim Update auf dieses Release können Optionen aus der Datei All_Regions.ini verschwinden, was zu Fehlern führt.

  [#654826]

- HDX-Webcam-Umleitung ist beim Start 45 Sekunden lang deaktiviert.

Sie können dies vermeiden, indem Sie im Abschnitt [wfclient] der Datei ~/.ICAClient/wfclient.ini (oder $ICAROOT/config/module.ini) folgenden Eintrag hinzufügen: HDXRTMEWebCam-LaunchDelayTime=0.

Wenn Sie das RTME-Plug-In statt HDX-Webcam-Umleitung verwenden, ändern Sie diesen Wert nicht.

Bekannte Probleme in Citrix Receiver für Linux 13.3

In diesem Release bestehen die folgenden bekannten Probleme:

- Citrix Receiver erkennt beim ersten Start eines Desktops die PIV-Smartcard nicht.

  [#491235]

- Unklare Fehlermeldungen werden angezeigt, wenn Citrix Receiver den Server nicht direkt nach dem Neustart finden kann.

  [#553886]

- Ein falsches Meldungsdialogfeld wird angezeigt, wenn der Sitzungszuverlässigkeitstimer abläuft.

  [#556899]

- Eine Fehlermeldung, z. B. “Unbekannter Fehler 1000047”) wird bei der Verbindung mit dem VDA angezeigt, wenn das SSLv3-Protokoll aktiviert ist.

  [#558641]

- Ein allgemeiner Netzwerkfehler wird angezeigt, wenn eine Verbindung zu einem StoreFront-Server mit aktiviertem SSLv3-Protokoll hergestellt wird.

  [#558653]

- Beim Ändern von “SharedUserMode” mit storebrowse, -c SharedUserMode[=value] muss für den Parameter “value” die Groß-/Kleinschreibung beachtet werden. Bei der Verwendung des Parameters “value” für storebrowse, -c SharedUserMode[=value] muss eine genaue Groß- und Kleinschreibung mit “True” oder “False” angegeben werden. Bei der Eingabe eines ungültigen Wertparameters wird keine Fehlermeldung angezeigt. Zum Beispiel: -c SharedUserMode=True.

  [#559402]

- Wenn eine Verbindung mit einem Terminalserver hergestellt wird (z. B. RDS) und nur das SSLv3-Protokoll aktiviert ist, schlägt eine Sitzung wie erwartet fehl, aber sie schlägt möglicherweise nicht mit einem SSL-Peer Handshake-Fehler fehl.

  [#567407]

- Generische USB-Webcameingabe schlägt auf 64-Bit-Systemen fehl.

  [#568556]

- Der Befehl “storebrowse –d command” löscht keine zuvor gelöschten Cachespeicherinformationen, die mit dem Befehl “selfservice” erstellt wurden. Daher wird die Self-Service-Benutzeroberfläche aus dem Cachespeicher geladen, wenn der Store hinzugefügt wird.

  [#569806]

- Bei Verwendung von selfservice/storebrowse werden neue TLS-Werte nicht auf Verbindungen mit dem StoreFront-Server angewendet, wenn TLS-Werte nach dem Akzeptieren der Lizenzvereinbarung geändert werden. Beachten Sie, dass das Ändern der TLS-Einstellung von einem ausgeführten AuthManager nicht gelesen wird.

  [#570725]

- Connection Center unterstützt IPv6 nicht.

  [#571743]

- Wenn ein negativer Wert für einen Konfigurationseintrag eingegeben wird, der eine ganze Zahl erfordert, z. B. TCPRecvBufferSize in $HOME/.ICAClient/All_Regions.ini, wird der Wert irrtümlicherweise an WFICA als positiver Wert weitergeleitet. Sie lösen das Problem, indem Sie einen negativen Wert für TCPRecvBufferSize mit $ICAROOT/config/module.ini festlegen.

  [#575474]

- GStreamer Helper-Prozesse zeigen eine Warnung in Verbindung mit einem GLIB Threading-Problem an.

  [#580753]

- Das ARMEL-Browser-Plug-In funktioniert in diesem Release nicht.

  [#588044]

- Wenn Zeitzonen nicht richtig den XenApp und XenDesktop 7.6-Sitzungen zugeordnet werden, stellen Sie sicher, dass der Hotfix installiert ist, auf den in CTX142640 verwiesen wird, und befolgen Sie die Schritte für Eintrag 7 [ab ICATS760WX64014]. Sollte das Problem nicht behoben sein, ändern Sie /etc/timezone (oder /etc/localtime, wenn /etc/timezone nicht vorhanden ist) in einen Symlink zu dem Namen einer Stadt unter /usr/share/zoneinfo/…

  Wenn die Zeitzone weiterhin nicht unterstützt wird, müssen Sie ggf. ein Supportticket öffnen, damit die Zuordnung dem Server hinzugefügt wird.

  [#LC1061, #606648]

- Im Platform Optimization SDK verursachen die Plug-Ins für nicht-X11 Umgebungen zwei Probleme:

- Sitzungen auf Windows-Servern für XenDesktop 7.x geschlagen fehl, wenn Sitzungszuverlässigkeit verwendet wird.
- Bei Sitzungen mit 16-Bit-Farbtiefe treten Videofehler auf.

Diese Probleme treten in Beispielimplementierungen des SDL-Plug-Ins auf, das auf der SDL Library basiert, und auch in dem Framebuffer-basierten Raw Kernel FB_plugin. Weitere vom Benutzer entwickelte Plug-Ins haben die gleichen Probleme.

Bekannte Probleme in Citrix Receiver für Linux 13.2.1

In diesem Release bestehen die folgenden bekannten Probleme:

- Das ARMEL-Browser-Plug-In (zum Starten von Sitzungen in einem Webbrowser) startet nicht und Benutzer können keine Sitzung starten. Sie lösen das Problem, indem Sie das Plug-In in den Browsereinstellungen deaktivieren, sodass ein Fallback stattfinden kann.

  [#580782]

- Bei der Ausführung von SLED 11sp3 kann das Starten von storebrowse oder selfservice von einem Terminal aus zu folgender Fehlermeldung bei mehreren Programmen führen: "libidn.so.11: no version information available." Dieses Problem hat kaum Auswirkungen (wenn überhaupt) auf Citrix Receiver.

  [#582512]

- Flash-Umleitung ist auf 64-Bit-Clients nicht verfügbar. Wenn diese Funktion für Ihre Umgebung wichtig ist, wenden Sie sich an das Citrix Produktverwaltungsteam oder informieren Sie sich über die Supportforen.

  [#582627]

- Wenn Sie in der Detailansicht "Favoriten hinzufügen" auswählen, fügt Receiver keine Favoritenanwendungen hinzu. Dieses Problem tritt auf, wenn Sie SuSE SLED 11sp3 ausführen, ohne Updates zu installieren. Sie vermeiden dieses Problem, indem Sie sicherstellen, dass das Paket libwebkit-1_0-2 Version 1.2.7-0.17.1 (oder höher) ist.

  [#585295]

- In Version EPEL 2.2.4 von libwebkitgtk+ tritt ein Drittanbieterproblem auf. Citrix empfiehlt die Verwendung EPEL-Repositorys (Extra Packages for Enterprise Linux) zum Abrufen der Version GTK+2 von libwebkitgtk unter Red Hat 7 und Centos 7. Es tritt jedoch ein Problem mit der angegebenen EPEL-Version auf, wenn die Namen gehosteter Anwendungen auf dem Server japanische bzw. chinesische Zeichen enthalten. Daher hat Receiver keine passende Methode zum Sichern eines stabilen libwebkitgtk-Builds unter Red Hat 7 und Centos 7, der für APAC-Zeichen geeignet ist.

  [#586967]

- Auf einigen Plattformen kann die Installation des Clients mit einer Tarball-Distribution dazu führen, dass das System hängen bleibt, nachdem Sie zur Integration mit KDE und GNOME aufgefordert wurden. Das Problem tritt bei der ersten Initialisierung von gstreamer-0.10 auf. Wenn dieses Problem auftritt, brechen Sie den Installationsvorgang mit Strg+C ab und führen Sie den folgenden Befehl aus: gst-inspect-0.10 – gst-disable-registry-fork –version. Nachdem der Befehl ausgeführt wurde, können Sie den Tarball-Setup erneut ausführen, ohne dass das System hängen bleibt.

  [#587640]

- In einigen GNOME-Desktopumgebungen kann ein Client abstürzen, wenn die Microsoft Remote Desktop-App (Mstsc) gestartet wird. Dieses Problem tritt auf, wenn eine Verbindung mit einem Remotedesktop hergestellt wird. Nach dem Eingeben der Anmeldeinformationen kann die Sitzung nicht durch Klicken auf das 'X' beendet werden, stattdessen wird die folgende Fehlermeldung angezeigt: "A problem has occurred and the system can't recover."

  [#587922]

- Windows Media Player zeigt folgende Fehlermeldung an: "Beim Wiedergeben der Datei ist in Windows Media Player ein Problem aufgetreten". Schließen Sie die Fehlermeldung und klicken Sie auf das Symbol für Wiedergabe.

  [#588009]

- Wenn Windows Media Player auf einem Windows 7-Desktop von einem 64-Bit-Receiver aus gestartet wird, schlägt die Wiedergabe von Audio/Video u. U. fehl. Dieses Problem ist auf ein bekanntes Problem mit Ubuntu 14.04 zurückzuführen. Erwartete GStreamer-Komponenten werden nicht installiert. Weitere Informationen finden Sie im Abschnitt Problembehandlung unter "Windows Media Player gibt bestimmte Dateiformate nicht wieder".

  [#588298]

- Windows Media Player gibt bestimmte Dateiformate nicht wieder

Bekannte Probleme in Citrix Receiver für Linux 13.2

In diesem Release bestehen die folgenden bekannten Probleme:

- Ein neues Skript, mit dem Dateitypzuordnungen für den Clientserver erstellt werden, wurde hinzugefügt. Das Skript, ctx_app_bind, ermöglicht die Verwendung einer veröffentlichten Anwendung zum Öffnen eines bestimmten Dateityps. Das Skript übernimmt entweder den Namen der veröffentlichten Anwendung, einer Beispieldatei oder eines MIME-Typs und ermöglicht zudem das Einschließen eines Servernamens oder einer URL.
  Zum Beispiel:

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

Verwenden Sie die Option –p, um eine Sitzung mit pnabrowse statt storebrowse zu starten.

Hinweis: Citrix empfiehlt, beim Ausführen des Skripts vorsichtig zu sein. Es wurde noch nicht mit allen Betriebssystemen getestet.

[#558649]

- Wenn ein Benutzer keine Verbindung zum Store herstellen kann, können Sie zur Problembehandlung in Receiver Verbindungsprotokolle aktivieren. Aktivieren der Sammlung von Verbindungsprotokollen in Receiver:

1. Bearbeiten Sie mit Administratorprivilegien die folgenden Parameter in der Datei /opt/citrix/ICAClient/config/AuthManConfig.xml:

   <!– TracingEnabled - true, false –>

   <key>TracingEnabled</key>
   <value>true</value>
   <!– LoggingMode - none, normal, verbose –>
   <key>LoggingMode</key>
   <value>verbose</value>

2. Halten Sie die folgenden Prozesse an: AuthManagerDaemon, selfservice, ServiceRecord, storebrowse.
3. Starten Sie Receiver und stellen Sie eine Verbindung zum Store her.
4. Überprüfen Sie die Protokolle unter $HOME/.ICAClient/logs.

Für die HDX RealTime-Webcamvideokomprimierung ist Folgendes erforderlich:

- Eine Video4Linux-kompatible Webcam
- GStreamer 0.10.25 (oder eine höhere 0.10.x-Version) einschließlich des Distributionspakets “plugins-good”

[#559817]

- Wenn Sie Linux Receiver X1 zum Entfernen einer App verwenden, bleibt die App erhalten, wenn Sie sich abmelden und zum Store zurückkehren.

  [#561719]

Bekannte Probleme in Citrix Receiver für Linux 13.1

In diesem Release bestehen die folgenden bekannten Probleme:

- Sie können die Verbindung virtueller Desktops mit Connection Center nicht trennen und diese dort nicht abmelden. Die Schaltfläche Trennen ist nicht verfügbar und die Schaltfläche Abmelden funktioniert nicht. Um dieses Problem zu umgehen, führen Sie das Trennen bzw. die Abmeldung über die Desktopsitzung und nicht Connection Center durch. Dieses Problem tritt bei virtuellen Anwendungen nicht auf.

  [#423651, #424847]

- Ein Fehler wird angezeigt, wenn ein Benutzer die Self-Service-Benutzeroberfläche öffnet, um eine Verbindung mit dem StoreFront-Store herzustellen, und dann das Receiver für Linux-Fenster schließt, wenn das Dialogfeld “Authentifizierungsmanager” geöffnet ist.

  [#430193]

- Receiver für Linux lässt keine Verbindung zu einem nicht sicheren StoreFront-Store `http://` zu. Abhängig von der Konfiguration des Stores erhält der Benutzer entweder eine Fehlermeldung, dass das Discoverydokument nicht abgerufen werden kann, oder die anfängliche Verbindung erfolgt über HTTP und spätere Kommunikationen wechseln zu HTTPS. Wenn Sie die IP-Adresse für den Hostnamen verwenden, werden u. U. Fehler zu Citrix XenApp Services (früher PNAgent) angezeigt. Verwenden Sie entweder ausdrücklich `https://` oder geben Sie bei der Eingabe der URL `http://` nicht an.

  [#473027, #478667 und #492402]

- Receiver für Linux unterstützt keine Anmeldung mit einer Smartcard, die mehrere Authentifizierungszertifikate enthält.

  [#488614]

- Falls Receiver für Linux einen Segmentierungsfehler beim Zugriff auf Smartcards anzeigt, kann das Problem in der PKCS#11-Bibliothek liegen. Sie können die Bibliothek mit dem pkcs11-Tool überprüfen. Das pkcs11-Tool ist Teil des opensc-Pakets. Ein Beispiel für den Test:

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

  Wenn der Test auch einen Segmentierungsfehler ergibt, müssen Sie sich an den Anbieter des Treibers wenden. Sie können auch einen Treiber von einer anderen Quelle für den gleichen Typ der Karte ausprobieren. Dieses Problem trat beim Gemalto .NET-Treiber in Fedora 19 und Fedora 20 auf.

  [#493172]

- Receiver für Linux unterstützt mehrere Smartcardleser, jedoch kann nur jeweils eine Smartcard verwendet werden.

  [#494524]

- Der Hostname der Linux-Maschine darf höchstens 20 Zeichen haben, damit Verbindungen funktionieren. Diese Einstellung kann überprüft und mit dem Befehl hostname eingestellt werden.

Jeder Benutzer kann den Hostnamen prüfen; für das Einstellen müssen Sie jedoch ein Root-Benutzer sein oder Administratorprivilegien haben.

[#494740]

- Beim Arbeiten in XenDesktop im Vollbildmodus in Receiver für Linux 13.x wird der lokale Bildschirmschoner u. U. nicht aktiviert. Dies ist ein Drittanbieterproblem und das Verhalten hängt vom Clientbetriebssystem ab.

  [#496398]

- Wenn Sie die falsche Smartcard bei einem Verbindungsversuch mit einem StoreFront-Store einstecken, wird u. U. eine Fehlermeldung wie "Protokollfehler" oder "Dieser Store konnte nicht gefunden werden" angezeigt, die das Problem nicht erläutert.

  [#496904]

- Bei einigen leistungsschwachen Geräten dauert die Anmeldung mit Smartcardauthentifizierung in einer Vollbildsitzung länger als erwartet und ein Timeout tritt auf. Sie können dieses Problem u. U. durch Deaktivieren von H264 vermeiden. Deaktivieren Sie die Verwendung von H624 wie folgt:

  1. Öffnen Sie die Datei wfclient.ini.
  2. Navigieren Sie auf den Abschnitt "Thinwire3.0".
  3. Fügen Sie den Eintrag "H264Enabled=False" hinzu.

Dieses Problem wurde auf Maschinen festgestellt, die auf armhf (ARM-Hardfloat) ohne hardwarebeschleunigtes H264 festgestellt.

[#497720]

- Wenn ein PNAgent-Server die benutzerseitige Änderung von abgelaufenen Kennwörtern durch direktes Kontaktieren des Domänencontrollers zulässt, können Sie dies nur mit der MIT-kompatiblen Version der Bibliothek libkcpm.so tun. Die Ursache sind Probleme mit der Heimdal-kompatiblen Version. Diese Einschränkung gilt für x86, armel und x64 (die x86 pnabrowse verwenden). Sie gilt nicht für armhf.

  [#498037]

- Receiver für Linux benötigt libpng12.so, die normalerweise nicht in den Standardrepositories für Fedora-basierte Systeme vorhanden ist. Suchen Sie in diesem Fall eine geeignete RPM für Ihr System im Internet. Für openSUSE ist libpng12.so verfügbar, muss jedoch separat installiert werden.

  [#501937]

- Ein Hotfix für 12.1 fügte einen pnabrowse-Exitcode E_SSLSDK_PASSWORD_LOCKED mit dem Wert 220 hinzu. Der Exitcode E_PASSWORD_EXPIRED wurde vom dokumentierten Wert 238 zu 239 geändert. In 13.0 wurde der Wert für E_SSLSDK_PASSWORD_LOCKED zu 240 geändert und

der richtige Wert für E_PASSWORD_EXPIRED wurde wiederhergestellt. Jedoch zeigen die von pnabrowse -errno aufgeführten Werte stets die falschen Werte für 220 bis 240 an.

[#502550]

Bekannte Probleme in Citrix Receiver für Linux 13

In diesem Release bestehen die folgenden bekannten Probleme:

Installationsprobleme

- libxerces-c 3.1 ist eine erforderliche Komponente für dieses Release. Es ist jedoch in einigen Linux-Distributionen, bei denen die RPM-Verpackung verwendet wird, nicht enthalten. Wenn diese Komponente in Ihrer Distribution fehlt, suchen Sie sie auf einer geeigneten Website und fügen Sie sie der Linux-Systeminstallation hinzu.

  [#384324]

- Auf Plattformen, die die libxerces- oder libwebkitgtk-Systemanforderung (oder beide Anforderungen) nicht erfüllen können, können Sie Receiver mit dem Tarball-Paket installieren oder die Installation des Debian- oder RPM-Pakets erzwingen und den browserbasierten Receiver für Web zum Herstellen von Verbindungen verwenden. Beispielsweise können Sie das RPM-Paket nicht auf CentOS-Systemen installieren, da es libwebkitgtk-1.0.so.0 erfordert und diese Komponente unter CentOS nicht verfügbar ist. Installieren Sie als Workaround das Paket mit –nodeps oder –force oder verwenden Sie alternativ das Tarball-Paket. Starten Sie dann einen Browser und geben Sie die URL für den Receiver für Web-Store ein.

  [#426176]

- Sie können Receiver mit dem RPM-Paket auf der 32-Bit-Version von OpenSUSE 13.1 installieren, die Ausführung schlägt jedoch fehl. Sie vermeiden dieses Problem, indem Sie erst das folgende RPM-Paket herunterladen und installieren und dann die Installation wiederholen: `ftp://rpmfind.net/linux/opensuse/factory/repo/oss/suse/i586/libpng12-0-1.2.50-7.3.i586.rpm`.

  [#429879]

- Nach der Installation von Receiver mit dem 64-Bit-RPM-Paket in einer 64-Bit-Fedora 19.1-Umgebung müssen Sie zusätzliche Schritte ausführen, bevor Sie pnabrowse oder die Clientengine wfica verwenden, um Verbindungen herzustellen. (Mit diesen Schritten werden Fehler bei storebrowse und selfservice behoben, da diese aufgrund von versionsbedingten Einschränkungen von curl in dieser Umgebung nicht funktionieren.) So umgehen Sie das Problem:

1. Installieren Sie das 32-Bit-Paket libpng12 mit dem folgenden Befehl:

   yum install libpng12.i686

2. Zur Minimierung von Audiofehlern installieren Sie das 32-Bit-ALSA-Plug-In mit dem folgenden Befehl:

   yum install alsa-plugins-pulseaudio.i686

3. Zur Minimierung von GtK-Fehlern installieren Sie die folgenden Pakete mit den folgenden Befehlen:

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

4. Damit Verbindungen über Firefox erstellt werden können, installieren Sie das Plug-In nspluginwrapper.i686 und registrieren Sie es beim Webbrowser mit den folgenden Befehlen:

   yum install nspluginwrapper.i686
   mozilla-plugin-config

[#429886]

Allgemeine Probleme

- Beim Fortsetzen einer Audiowiedergabe kann es zu Nebengeräuschen kommen. Diese treten nur auf, wenn eine Audiowiedergabe angehalten und dann fortgesetzt wird, aber nicht bei der ersten Wiedergabe. Dieses Problem wurde bei XenDesktop-Verbindungen mit dem Feature Remote-PC-Zugriff beobachtet. Für dieses Problem gibt es keinen Workaround.

  [#308772]

- Einige Medientypen können nur auf Benutzergeräten wiedergegeben werden, wenn der entsprechende Codec auf dem Server verfügbar ist, selbst wenn GStreamer eine direkte Verbindung mit der Medienquelle herstellen und diese mit den Decodern auf dem Gerät wiedergeben kann. Für dieses Problem gibt es keinen Workaround.

  [#339394]

- Unter Ubuntu 12.04 mit dem Gnome 3-Desktop werden Infobereichssymbole für veröffentlichte Anwendungen nicht in den systemeigenen Desktop integriert. Sie erscheinen stattdessen in einem separaten Infobereichsfenster. Für dieses Problem gibt es keinen Workaround.

  [#395140]

- Linux-Benutzer können ihre E-Mail-Adresse nicht verwenden, um StoreFront-Stores zu erstellen. Benutzer sollten stattdessen die URL der erforderlichen Stores mit der Seite Konten im

Dialogfeld Einstellungen hinzufügen. Alternativ können Sie auch eine Provisioningdatei mit Kontoinformationen bereitstellen, die zur Erstellung neuer Konten verwendet wird.

[#395394]

- Proxyunterstützung für die Befehle “selfservice” und “storebrowse” steht nicht standardmäßig zur Verfügung. Zur Verwendung eines Proxyservers mit einem StoreFront-Server legen Sie vor Verwendung eines dieser Befehle die Umgebungsvariable http_proxy fest. Verwenden Sie das folgende Format für die Umgebungsvariable:

  <server_name>.<domain>[:<port>]

  [#403729]

- Inhaltsumleitung vom Client zum Server (Ablegen veröffentlichten Inhalts auf ein Desktopsymbol) funktioniert bei der Self-Service-Benutzeroberfläche nicht. Für dieses Problem gibt es keinen Workaround.

  [#403739]

- Das Sicherheitsmodul Security-Enhanced Linux (SELinux) in RedHat Fedora kann die Clientlaufwerkzuordnung und die USB-Umleitung (unter XenApp und XenDesktop) beeinträchtigen. Wenn Sie eines dieser Features (oder beide) benötigen, deaktivieren Sie SELinux, bevor Sie es auf dem Server konfigurieren.

  [#413554]

- Die HDX MediaStream Flash-Umleitung wurde nicht auf der ARM Hard Float-Plattform (armhf) getestet, da in diesem Release Receiver nicht mit Flash-Plug-Ins auf dieser Plattform funktioniert.

  [#414253]

- Wenn Sie eine Webcam-Framerate konfigurieren, die nicht von der Webcam unterstützt wird, wird standardmäßig ein anderer Wert eingesetzt, der möglicherweise höher ist als erwartet.

  [#414576]

- Wenn Sie in Receiver eine nicht standardmäßige Auflösung für eine Webcam einstellen, werden von der Webcam bei ihrer ersten Verwendung für Citrix GoToMeeting keine Videodaten gestreamt. Die Webcam erscheint aktiv und gst_read wird ausgeführt aber es wird kein Bild angezeigt. Beenden Sie als Workaround die Webcam in GoToMeeting und starten Sie sie dann neu.

  [#414878]

- Gibt es in der Desktopumgebung keine Fensterdekorationen (z. B. wenn in der LXDE-Umgebung Dekorationen deaktiviert sind), können Self-Service-Dialogfelder möglicherweise nicht geschlossen werden.

[#416689]

- Bei einigen Versionen von XenApp oder XenDesktop kann nach dem Starten eines Desktops oder einer Anwendung nicht geprüft werden, welcher Server für eine Verbindung verwendet wird, da kein Server in Connection Center angezeigt wird. Um dieses Problem zu umgehen, klicken Sie auf Eigenschaften. Der Servername wird im Dialogfeld "Eigenschaften" angezeigt.

  [#417114]

- Wenn Sie bei der Anmeldung bei Receiver Ihre Anmeldeinformationen mit einer Verzögerung von etwa fünf Minuten eingeben, werden Ihre Anwendungen nicht auf der Self-Service-Benutzeroberfläche angezeigt. Wählen Sie als Workaround "Apps aktualisieren" aus dem Dropdownmenü in der Benutzeroberfläche aus und geben Sie die Anmeldeinformationen neu ein.

  [#417564]

- Ein Administrator, der eine Benutzersitzung spiegelt, bemerkt u. U. Anzeigefehler, wenn sein Bildschirm kleiner ist als der des Benutzergeräts. Beispiel: Bildlaufleisten passen möglicherweise nicht auf den Bildschirm des Administrators und es kann auf manche Bereiche des Bildschirms des Benutzers nicht zugegriffen werden. Für dieses Problem gibt es keinen Workaround. Außerdem kann eine Größenänderung der gespiegelten Sitzung auf der Maschine des Administrators zu einem Ausfall der Sitzungsanzeige auf dem Benutzergerät führen. Um dieses Problem zu umgehen, klicken Sie auf die Schaltfläche "Wiederherstellen" im Sitzungsfenster auf der Maschine des Administrators (nicht auf dem Benutzergerät).

  [#418672, #418690]

- Die Self-Service-Benutzeroberfläche und die zugehörigen StoreFront-Komponenten (Authentifizierungsmanager und Diensteintragsdaemon) werden aufgrund von Bibliotheksinkompatibilitäten unter Fedora nicht unterstützt. Receiver wird ohne Fehler installiert, funktioniert jedoch nicht. Starten Sie als Workaround Receiver über das Webinterface (eine Legacykomponente) oder Web Receiver.

  [#419662]

- Bestehen Abonnements für viele Anwendungen oder Desktops, enthält die Self-Service-Benutzeroberfläche eine Bildlaufleiste. Diese wird erwartungsgemäß ausgeblendet, wenn die Benutzeroberfläche so vergrößert wird, dass alle Anwendungs- und Desktopsymbole angezeigt werden. Die Bildlaufleiste wird jedoch nicht neu angezeigt, wenn die Benutzeroberfläche verkleinert wird. Dieses Problem wurde nur unter Ubuntu 13.04 beobachtet. Klicken Sie als Workaround auf die Menüoption "Aktualisieren", wiederholen Sie die Größenänderung einige Male oder beenden und starten Sie Receiver.

  [#422520]

- Beim Herstellen der ersten Verbindung macht sich möglicherweise eine Verzögerung bemerkbar. Diese kann je nach Netzwerk erheblich variieren. Eine 3G-Verbindung ist wahrscheinlich langsamer als eine ADSL-Verbindung.

  [#423663]

- Wenn Sie eine HTTPS-Storeadresse in der Self-Service-Benutzeroberfläche eingeben, wird folgende Fehlermeldung angezeigt, wenn kein Zertifikat vorhanden ist: Ihr Konto kann nicht mit dieser Serveradresse hinzugefügt werden. Prüfen Sie die Eingabe." Dieser Fehler wird angezeigt, wenn die Adresse richtig aber kein Zertifikat vorhanden ist. Um dieses Problem zu umgehen, installieren Sie ein Zertifikat.

  [#423757, #424674]

- Sie können eine XenDesktop-Richtlinie anwenden, um die höchste Framerate in Receiver-Sitzungen auf über 30 Frames pro Sekunde (F/s) anzuheben. Dieser Wert wird jedoch nicht berücksichtigt und die Framerate in den Sitzungen übersteigt diesen Wert nie, da sie durch das Feature Flusssteuerung begrenzt wird. Dieses Problem wurde bei XenDesktop 7 und 7.1 beobachtet. Um dieses Problem zu umgehen, deaktivieren Sie die Flusssteuerung.

  [#423950]

- Zum Wechseln von Konten (und für den Zugriff auf Desktops und Anwendungen von einem anderen Store) wird das Menü "Konten" in der Self-Service-Benutzeroberfläche verwendet. Dies ist möglicherweise für Benutzer nicht offensichtlich.

  [#424027]

- Wenn Sie storebrowse in mehreren Gebietsschemas verwenden, die nicht in UTF-8 codiert sind, können Teile des Texts im Anmeldedialogfeld fehlerhaft sein. Beispielsweise enthält im Gebietsschema Spanisch die Schaltfläche Anmelden keinen Text. Um dieses Problem zu umgehen, wechseln Sie zu einem UTF-8-Gebietsschema (z. B. durch Erstellen eines Wrapperskripts um storebrowse und die ausführbaren Dateien des Authentifizierungsmanager- und Diensteintragsdaemons).

  [#424052]

- Sie können die Verbindung virtueller Desktops mit Connection Center nicht trennen und diese dort nicht abmelden. Die Schaltfläche Trennen ist nicht verfügbar und die Schaltfläche Abmelden funktioniert nicht. Um dieses Problem zu umgehen, führen Sie das Trennen bzw. die Abmeldung über die Desktopsitzung und nicht Connection Center durch. Dieses Problem tritt bei virtuellen Anwendungen nicht auf.

  [#424847]

- Wenn storebrowse verwendet wird, um eine Sitzung mit einem virtuellen Desktop in einer Gruppe zu starten, in der alle Desktops ausgeschaltet sind, wird der Beendigungsstatus "255

EXEC_FAILED" angezeigt (manchmal verzögert). Dadurch wird angegeben, dass der Start fehlgeschlagen ist. Der Desktop wird in Wirklichkeit jedoch gestartet oder registriert und steht kurz danach zur Verfügung. Empfehlen Sie als Workaround Benutzern, bei denen dieses Problem auftritt, zu versuchen, den Desktop neu zu starten, bzw. stellen Sie sicher, dass alle Startskripts dies auch veranlassen.

[#425076, #425103]

- In der japanischen und der vereinfacht chinesischen Version von Receiver funktionieren Tastenkombinationen in einigen Dialogfeldern nicht.

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

- In der deutschen, französischen und spanischen Version von Receiver sind bei Ausführung unter Ubuntu in einigen Dialogfeldern Tastenkombinationen nicht sichtbar, sie können aber verwendet werden.

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

- In der deutschen Version von Receiver gibt es einige Tastenkombinationen in manchen Dialogfeldern doppelt.

  [#425284, #425338]

- Das openssl-Tool c_rehash wird für den Import und die Hashverarbeitung von Stammzertifikaten für den Schutz der Kommunikation mit StoreFront verwendet. Manche c_rehash-Versionen können Zertifikate mit MS-DOS-artigen Zeilenenden nicht richtig verarbeiten. Werden durch die c_rehash-Ausgabe keine symbolischen Verknüpfungen für ein Zertifikat generiert, müssen Sie die Zeilenenden möglicherweise in das UNIX-Format konvertieren. Sie können dies mit der folgenden tr-Befehlszeile tun:

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

  Anschließend führen Sie das c_rehash-Skript an dem mit diesem Befehl erstellten neuen Stammzertifikat aus.

  [#425775]

- Auf Debian-Plattformen wird der ctxusbd-Daemon nicht neu gestartet, wenn das System neu gestartet wird, wodurch die USB-Umleitung fehlschlägt. Dies liegt daran, dass das init-Skript /etc/init.d/ctxusbd die Variable ###INIT_UDEV### enthält, die auf udev erweitert werden muss. Bearbeiten Sie als Workaround das Skript /etc/init.d/ctxusbd wie nachfolgend beschrieben. Sie müssen hierfür Rootberechtigungen haben:

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

  Anschließend führen Sie insserv manuell neu aus (mit Rootberechtigung):

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

Dieses Problem wurde nur auf Debian-Plattformen beobachtet.

[#425810]

- Wenn Sie eine Verbindung mit Program Neighborhood Agent-Sites herstellen, verursachen fehlende oder abgelaufene Zertifikate möglicherweise ein Blinken der Receiver-Benutzeroberfläche, mehrfache Aufforderung an den Benutzer zur Eingabe der Anmeldeinformationen oder eine hohe CPU-Auslastung. Als Workaround empfiehlt Citrix, dass Sie die Zertifikate richtig installieren und regelmäßig pflegen. Das Problem wird bei Verbindungen mit StoreFront-Sites nicht beobachtet.

  [#425848]

- Symbole in der Self-Service-Benutzeroberfläche werden möglicherweise nicht angezeigt, wenn neue Benutzer Anwendungen oder Desktops suchen. Klicken Sie als Workaround auf "Apps aktualisieren".

  [#426364]

- Wenn Sie mit pnabrowse eine Verbindung zu mit HTTPS geschützten Program Neighborhood Agent-Sites auf bestimmten Microsoft Server 2012-Servern in Hard Float-Umgebungen (armhf) herstellen, wird eine generische Fehlermeldung angezeigt und die Verbindung schlägt fehl. Dieses Problem ist nicht vollständig untersucht. Ursache kann jedoch sein, dass die Server einen vollqualifizierten Domänennamen haben, der in ".local" endet oder dass der im Feld "Öffentlicher Schlüssel" angegebene Schlüssel 2048 Bits und nicht 1024 Bits lang ist. Dieses Problem tritt nicht bei storebrowse und nur in armhf-Umgebungen auf.

  [#426420]

- Wenn Sie sich von Receiver abmelden (durch Klicken auf "Abmelden" in der Self-Service-Benutzeroberfläche), anschließend versuchen, eine Verbindung mit einem Desktop oder einer Anwendung herzustellen, und dann den Vorgang abbrechen, wenn Sie dazu aufgefordert werden, Ihre Anmeldeinformationen einzugeben, wird die Meldung "Anforderung kann nicht verarbeitet werden" angezeigt. Sie können diese Meldung ignorieren. Die Abmeldung war erfolgreich.

  [#426424]

- Ein Segmentierungsfehler tritt auf und Receiver schlägt fehl, wenn Sie zum ersten Mal mit der Self-Service-Benutzeroberfläche eine Verbindung zu einer Program Neighborhood Agent-Site herstellen, auf Abbrechen im Anmeldedialogfeld klicken, dann auf Apps aktualisieren klicken und das Receiver-Fenster dann schließen. Für dieses Problem gibt es keinen Workaround.

  [#426625]

- Werden Datenspeicher- oder Ladeprozedurverfahren zur gleichen Zeit von mehreren Prozessen aufgerufen, kann dies zu Datenverlust in den Dateien im Arbeitsspeicher (z. B. StoreCache.xml)

führen. Die jeweils letzte Änderung an den einzelnen Dateien wird beibehalten, frühere Änderungen gehen verloren. Es besteht keine Gefahr der Dateibeschädigung.

[#426692]

- Wenn Sie einen Store entfernen und dann hinzufügen, wird der neue Store auf der Seite "Konten" im Dialogfeld "Einstellungen" nicht angezeigt, bis Sie das Dialogfeld schließen und wieder öffnen.

  [#426735]

- Wenn die Einstellung "Apps und Desktops wieder verbinden" auf "Beim Starten oder Aktualisieren von Apps" festgelegt ist und eine Verbindung mit einem Desktop oder einer Anwendung besteht, reagiert nach Auswahl von "Apps aktualisieren" im Receiver-Menü die Benutzeroberfläche erst dann wieder, wenn die Verbindung hergestellt ist.

  [#426761]

- Es wird keine Fehlermeldung angezeigt, wenn Sie versuchen, einen Store oder ein Gateway hinzuzufügen, der bzw. das bereits in Receiver aufgeführt wird. Es gibt keinen Workaround für dieses Problem, es werden jedoch keine doppelten Einträge erstellt und der vorhandene Store bzw. das vorhandene Gateway funktionieren weiterhin ordnungsgemäß.

  [#427379]

- Menüs in veröffentlichten Anwendungen verschwinden, wenn auf sie geklickt wird. Dieses Verhalten wurde bei maximierten Anwendungsfenstern in GNOME 3-Desktopumgebungen unter Ubuntu 12.04 beobachtet, jedoch nicht in Unity-Umgebungen unter Ubuntu 12.04.3.

  [#429686]

- Achtung: Eine Einschränkung in Windows führt dazu, dass die Lautstärke bei Audiowiedergabe maximiert ist, wenn eine Sitzung nach einem Netzwerkausfall automatisch wieder verbunden wird. Für dieses Problem gibt es keinen Workaround.

  [#430160]

- Receiver-Einstellungen wirken sich nur auf neue oder wiederverbundene Sitzungen aus und nicht auf getrennte Sitzungen. Beispielsweise können Sie Citrix GoToMeeting von einem virtuellen Desktop aus starten und dann die Verbindung mit der Desktopsitzung trennen (aber nicht mit GoToMeeting). Wenn Sie dann im Dialogfeld "Einstellungen" auf der Seite "Mikrofon & Webcam" die Option Mikrofon und Webcam verwenden auswählen, wird die Webcam in der GoToMeeting-Sitzung nicht gestartet. Sie vermeiden dieses Problem, indem Sie die betroffene Sitzung schließen und neu starten (in diesem Beispiel die GoToMeeting-Sitzung).

  [#430692]

- Wenn selfservice von einem Terminal ausgeführt wird und das Terminal vor selfservice geschlossen wird, wird das Standardsignal zum Beenden an alle Vordergrundprozesse

gesendet, die vom Terminal gehostet werden. Andere Linux Receiver-Prozesse, wie die Authentifizierungsmanager- und Diensteintragsdaemons, ignorieren das Signal nicht, aber selfservice ignoriert es. Dadurch kann selfservice einfrieren, denn die Prozesse, von denen es abhängig ist, werden beendet. Sie vermeiden dieses Problem, indem Sie die Daemons mit storebrowse in einem Fenster starten und dann selfservice in einem zweiten Fenster ausführen. Auf diese Weise können Sie das Terminalfenster, in dem selfservice ausgeführt wird, schließen, während die Daemons im Hintergrund weiter ausgeführt werden und die Benutzeroberfläche weiterhin funktioniert.

[#430697]

Systemanforderungen

March 11, 2019

Geräte

- Linux Kernel-Version 2.6.29 oder höher mit glibcxx 3.4.15 oder höher, glibc 2.11.3 oder höher, gtk 2.20.1 oder höher, libcap1 oder libcap2 und udev-Unterstützung
- Für die Self-Service-Benutzeroberfläche:
  - libwebkit oder libwebkitgtk 1.0
  - libxml2 2.7.8
  - libxerces-c 3.1
- ALSA (libasound2), Speex und Vorbis-Codec-Bibliotheken
- Mindestens 55 MB freier Speicherplatz für die installierte Receiver-Version. Mindestens 110 MB, wenn Sie das Installationspaket auf dem Datenträger erweitern. Sie können den freien Speicherplatz durch Eingabe des folgenden Befehls in einem Terminal-Fenster überprüfen:

  ```
  df -k
  ```

- Mindestens 1 GB RAM für SoC-Geräte (system-on-a-chip), die HDX MediaStream Flash-Umleitung verwenden.
- Farbbildschirm im 256-Farbenmodus oder höher.
- TCP/IP-Netzwerkunterstützung.

H.264

Bei x86-Geräten werden Einzelmonitorsitzungen in typischen Auflösungen (z. B. 1280 x 1024) gut angezeigt, wenn die Prozessorgeschwindigkeit mindestens 1,6 GHz beträgt. Wenn Sie HDX 3D Pro verwenden, werden ein nativer, hardwarebeschleunigter Grafiktreiber und eine Mindest-Prozessorgeschwindigkeit von 2 GHz benötigt.

Für ARM-Geräte wird ein Hardware-H.264-Decoder für die allgemeine H.264-Unterstützung und für HDX 3D Pro benötigt. Die Leistung profitiert auch von einer höheren Prozessor-Taktfrequenz.

HDX MediaStream Flash-Umleitung

Informationen zu allen Anforderungen für die HDX MediaStream Flash-Umleitung finden Sie unter CTX134786.

Citrix empfiehlt, das aktuelle Plug-In zu testen, bevor Sie eine neue Version bereitstellen, um die Vorteile der neuesten Funktionen und Sicherheitsverbesserungen auszuschöpfen.

Integration des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Damit das CEIP richtig funktioniert, sind die folgenden Bibliotheken erforderlich:

- zlib 1.2.3.3
- libtar 1.2 und höher
- libjson 7.6.1 oder eine höhere Version

HDX RealTime-Webcamvideokomprimierung

Für die HDX RealTime-Webcamvideokomprimierung ist Folgendes erforderlich:

- Eine Video4Linux-kompatible Webkamera
- GStreamer 0.10.25 (oder eine höhere 0.10.x-Version) einschließlich des Distributionspakets “plugins-good”.

  Oder

  GStreamer 1.0 (oder eine höhere 1.x-Version), einschließlich der Distributionspakete “plugins-base”, “plugins-good”, “plugins-bad”, “plugins-ugly” und “gstreamer-libav”.

HDX MediaStream Windows Media-Umleitung

Für die HDX MediaStream-Windows-Medienumleitung ist Folgendes erforderlich:

- GStreamer 0.10.25 (oder eine höhere 0.10.x-Version) einschließlich des Pakets mit den Good Plug-Ins der Distribution. In Allgemeinen ist Version 0.10.15 oder höher für die HDX MediaStream Windows Media-Umleitung ausreichend.

  Oder

  GStreamer 1.0 (oder eine höhere 1.x-Version), einschließlich der Distributionspakete "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly" und "gstreamer-libav".

  > **Hinweis:** Wenn GStreamer in Ihrer Linux-Distribution nicht enthalten ist, können Sie GStreamer auch herunterladen unter

http://gstreamer.freedesktop.org. Für die Verwendung bestimmter Codes (z. B. in "plugins-ugly") ist u. U. eine Lizenz des Herstellers der jeweiligen Technologie erforderlich. Lassen Sie sich von Ihrer Rechtsabteilung beraten, ob für die Codes, die Sie verwenden möchten, zusätzliche Lizenzen notwendig sind.

Umleitung des Browserinhalts

Die Browserinhaltsumleitung erfordert:

- Linux-Betriebssystem webkit2gtk Version 2.16.6 und glibcxx 3.4.20 oder höher.

Philips SpeechMike

Wenn Sie Philips SpeechMike-Geräte mit Receiver verwenden möchten, müssen Sie u. U. die entsprechenden Treiber auf dem Benutzergerät installieren. Auf der Philips Website finden Sie weitere Informationen und Softwaredownloads.

Smartcardunterstützung

Sie können die Smartcardunterstützung in Citrix Receiver für Linux nur konfigurieren, wenn die StoreFront Services-Site die Smartcardauthentifizierung zulässt.

> **Hinweis:**
> Smartcards werden nicht für Konfigurationen mit der XenApp Services-Site für Webinterface (früher Program Neighborhood Agent) oder mit der "Legacy-PNAgent"-Site unterstützt, die von einem StoreFront-Server bereitgestellt werden können.

Citrix Receiver für Linux unterstützt Smartcardleser, die mit PCSC-Lite kompatibel sind, und Smartcards mit PKCS#11-Treiber für die entsprechende Linux-Plattform. Standardmäßig sucht Receiver für Linux nach opensc-pkcs11.so in einem der Standardspeicherorte. Damit Receiver für Linux opensc-pkcs11.so in einem Speicherort findet, der kein Standardspeicherort ist, oder aber einen anderen PKCS#11-Treiber findet, speichern Sie den Speicherort in einer Konfigurationsdatei:

1. Suchen Sie die Konfigurationsdatei: $ICAROOT/config/AuthManConfig.xml
2. Suchen Sie die Zeile <key>PKCS11module</key> und fügen Sie den Treiberspeicherort dem Element <value> hinzu, das direkt der Zeile folgt.

   Hinweis: Wenn Sie einen Dateinamen für den Treiberspeicherort eingeben, navigiert Receiver im Verzeichnis $ICAROOT/PKCS#11 zur Datei. Sie können auch einen absoluten Pfad verwenden, der mit "/" beginnt.

Sie konfigurieren das Verhalten von Citrix Receiver für Linux, wenn die Smartcard entfernt wird, indem Sie SmartCardRemovalAction in der Konfigurationsdatei wie folgt aktualisieren:

1. Suchen Sie die Konfigurationsdatei: $ICAROOT/config/AuthManConfig.xml
2. Suchen Sie die Zeile <key>SmartCardRemovalAction</key> und fügen Sie dem Element <value> "noaction" oder "forcelogoff" hinzu, das direkt der Zeile folgt.

Das Standardverhalten ist "noaction". Keine Aktion wird zum Löschen der gespeicherten Anmeldeinformationen und Token unternommen, die hinsichtlich der Smartcard beim Entfernen der Smartcard erstellt werden. Mit der Aktion "forcelogoff" werden alle Anmeldeinformationen und Token beim Entfernen der Smartcard in StoreFront entfernt.

Citrix Server

- XenApp: Alle Versionen werden von Citrix unterstützt. Weitere Informationen finden Sie in der Citrix Produktmatrix.
- XenDesktop: Alle Versionen werden von Citrix unterstützt. Weitere Informationen finden Sie in der Citrix Produktmatrix.
- VDI-in-a-Box: Alle Versionen werden von Citrix unterstützt. Weitere Informationen finden Sie in der Citrix Produktmatrix.
- Sie können den browserbasierten Zugriff auf Citrix Receiver für Linux 1808 oder höher (mit oder ohne NetScaler Gateway-Plug-In) in Kombination mit StoreFront Receiver für Web und dem Webinterface verwenden.

  StoreFront:

  - StoreFront 3.x, 2.6, 2.5 und 2.1

    Bietet direkten Zugriff auf StoreFront-Stores.

  - StoreFront konfiguriert mit einer Receiver für Web-Site

    Bietet Zugriff auf StoreFront-Stores über einen Webbrowser. Informationen zu den Beschränkungen dieser Bereitstellung finden Sie im Abschnitt "Wichtige Überlegungen" unter Receiver für Web-Sites.

Webinterface mit dem NetScaler VPN-Client:

- Webinterface 5.4 für Windows mit Webinterface-Sites

  Bietet Zugriff auf virtuelle Desktops und Apps über einen Webbrowser.

- Webinterface 5.4 für Linux mit XenApp Services- oder XenDesktop Services-Sites

- Methoden der Bereitstellung von Citrix Receiver für Benutzer:
  - Download durch die Benutzer von receiver.citrix.com und Konfiguration unter Verwendung einer E-Mail- oder Dienstadresse mit StoreFront
  - Angebot der Installation von Citrix Receiver für Web-Site (mit StoreFront konfiguriert)
  - Angebot der Installation von Receiver von Citrix Webinterface 5.4

Browser

Citrix empfiehlt, die neueste Version von Mozilla Firefox oder Google Chrome zu verwenden.

> Hinweis:
> Weitere Informationen über Änderungen am Google Chrome NPAPI-Support finden Sie im Citrix Blog-Artikel
> Preparing for NPAPI being disabled by Google Chrome.

Konnektivität

Citrix Receiver für Linux unterstützt HTTPS- und ICA-über-TLS-Verbindungen über folgende Konfigurationen:

- LAN-Verbindungen:
  - StoreFront mit StoreFront Services- oder Citrix Receiver für Web-Sites
  - Webinterface 5.4 für Windows mit Webinterface- oder XenApp Services-Sites.
- Für sichere Remote- oder lokale Verbindungen:
  - Citrix NetScaler Gateway 12.0
  - Citrix NetScaler Gateway 11.1
  - Citrix NetScaler Gateway 11.0
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX

Weitere Informationen zu den von StoreFront unterstützten NetScaler Gateway- und Access Gateway-Versionen finden Sie unter den Systemanforderungen von StoreFront.

Hinweis: Verweise auf NetScaler Gateway in diesem Abschnitt gelten auch für Access Gateway, soweit nicht anders angegeben.

Info zu sicheren Verbindungen und Zertifikaten

Hinweis: Weitere Informationen zu Sicherheitszertifikaten finden Sie in den Abschnitten unter Sichere Verbindungen und Sichere Kommunikation.

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, muss das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installiert sein, um mit Receiver auf Citrix Ressourcen zuzugreifen.

Hinweis: Wenn das Zertifikat des Remote-Gateways beim Herstellen der Verbindung nicht verifiziert werden kann (da das Stammzertifikat nicht im lokalen Schlüsselspeicher vorhanden ist), wird ein Fehler aufgrund eines nicht vertrauenswürdigen Zertifikats angezeigt. Das Stammzertifikat muss im Zertifikatspeicher des Clients installiert werden.

Installieren von Stammzertifikaten auf Benutzergeräten

Informationen zum Installieren von Stammzertifikaten auf Benutzergeräten und zum Konfigurieren von Zertifikaten auf dem Webinterface finden Sie unter Installieren von Stammzertifikaten in der Dokumentation zur Citrix Workspace-App für Windows.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Citrix Receiver für Linux unterstützt Zertifikate mit Platzhalterzeichen. Diese sollten jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden. In der Praxis kann die Verwendung von Alternativen, z. B. von Zertifikaten mit einer Liste der Servernamen in der Subject Alternative Name-Erweiterung, in Betracht gezogen werden. Solche Zertifikate können von privaten und öffentlichen Zertifizierungsstellen ausgestellt werden.

Zwischenzertifikate und NetScaler Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem NetScaler Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter Configuring Intermediate Certificates in der NetScaler Gateway-Dokumentation.

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

Citrix Receiver für Linux hat eine strenge Validierungsrichtlinie für Serverzertifikate.

> **Wichtig**
>
> Bestätigen Sie vor der Installation dieser Version von Citrix Receiver für Linux, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:
>
> - Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
> - Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
> - Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
> - Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet Citrix Receiver für Linux jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases von Citrix Receiver für Linux wird dann auch überprüft, ob die Zertifikate vertrauenswürdig sind. Wenn nicht alle Zertifikate vertrauenswürdig sind, schlägt die Verbindung fehl.

Diese Richtlinie ist strenger als die Zertifikatrichtlinie in Webbrowsern. Viele Webbrowser enthalten eine große Anzahl Stammzertifikate, denen sie vertrauen.

Der Server bzw. das Gateway muss mit den richtigen Zertifikaten konfiguriert sein. Sind nicht die richtigen Zertifikate vorhanden, schlägt die Verbindung von Citrix Receiver für Linux u. U. fehl.

Angenommen, ein Gateway ist mit gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen. Dabei wird genau ermittelt, welches Stammzertifikat Citrix Receiver für Linux verwendet:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Beispielstammzertifikat”

Citrix Receiver für Linux überprüft, ob alle Zertifikate gültig sind. Citrix Receiver für Linux überprüft ebenfalls, ob dem “Beispielstammzertifikat” bereits vertraut wird. Wenn Citrix Receiver für Linux dem “Beispielstammzertifikat” nicht vertraut, schlägt die Verbindung fehl.

Wichtig

- Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet. Beispielsweise gibt es derzeit zwei Zertifikate (“DigiCert”/”GTE CyberTrust Global Root” und “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”), mit denen die gleichen Serverzertifikate validiert werden können. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar (“DigiCert Baltimore Root”/”Baltimore CyberTrust Root”). Wenn Sie “GTE CyberTrust Global Root” auf dem Gateway konfigurieren, schlagen Citrix Receiver für Linux-Verbindungen auf diesen Benutzergeräten fehl. Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist. Beachten Sie außerdem, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.
- Einige Server und Gateways senden nie das Stammzertifikat, selbst wenn es konfiguriert ist. Ein strengere Validierung ist dann nicht möglich.

Angenommen, ein Gateway ist mit diesen gültigen Zertifikaten konfiguriert. Wir empfehlen die folgende Konfiguration ohne das Stammzertifikat:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

Citrix Receiver für Linux verwendet dann diese beiden Zertifikate. Dann sucht die App nach einem Stammzertifikat auf dem Benutzergerät. Wird ein gültiges Zertifikat gefunden, das auch vertrauenswürdig ist (z. B. “Beispielstammzertifikat”), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt Citrix Receiver für Linux das benötigte Zwischenzertifikat zur Verfügung und ermöglicht auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

Nehmen wir nun an, ein Gateway ist mit den folgenden Zertifikaten konfiguriert:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Falsches Stammzertifikat”

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Citrix Receiver für Linux ignoriert das falsche Stammzertifikat jedoch nicht und die Verbindung schlägt fehl.

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall ist das Gateway normalerweise wie folgt mit allen Zwischenzertifikaten konfiguriert, jedoch nicht mit dem Stammzertifikat:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat 1”

- “Beispielzwischenzertifikat 2”

> **Wichtig**
>
> - Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat. Dies ist für Situationen vorgesehen, wenn mehr als ein Stammzertifikat vorhanden ist und ein früher ausgestelltes Stammzertifikat zur gleichen Zeit wie ein später ausgestelltes Stammzertifikat verwendet wird. In diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden. Beispielsweise hat das früher ausgestellte Stammzertifikat “Class 3 Public Primary Certification Authority” das entsprechende übergreifende Zwischenzertifikat “VeriSign Class 3 Public Primary Certification Authority - G5”. Ein entsprechendes später ausgestelltes Stammzertifikat “VeriSign Class 3 Public Primary Certification Authority - G5” ist ebenfalls verfügbar und es ersetzt “Class 3 Public Primary Certification Authority”. Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.
> - Das übergreifende Zwischenzertifikat und das Stammzertifikat haben den gleichen Antragstellernamen (Ausgestellt an). Das übergreifende Zwischenzertifikat hat jedoch einen anderen Ausstellernamen (Ausgestellt durch). Dadurch unterscheidet sich das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat wie “Beispielzwischenzertifikat 2”.

Normalerweise empfiehlt sich die folgende Konfiguration ohne das Stammzertifikat und das übergreifende Zwischenzertifikat:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

Konfigurieren Sie das Gateway nicht für die Verwendung des übergreifenden Zwischenzertifikats, weil es sonst das früher ausgestellte Stammzertifikat auswählt:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Übergreifendes Beispielzwischenzertifikat” [nicht empfohlen]

Es wird nicht empfohlen, das Gateway nur mit dem Serverzertifikat zu konfigurieren:

- “Beispielserverzertifikat”

In diesem Fall schlägt die Verbindung fehl, wenn Citrix Receiver für Linux nicht alle Zwischenzertifikate finden kann.

Benutzeranforderungen

Sie müssen nicht als privilegierter Benutzer (root) angemeldet sein, um Citrix Receiver für Linux zu installieren. USB-Unterstützung wird nur aktiviert, wenn Sie beim Installieren und Konfigurieren von

Receiver als privilegierter Benutzer angemeldet sind. Installationen, die von nicht-privilegierten Benutzern durchgeführt wurden, ermöglichen Benutzern mit den unterstützten Browsern über StoreFront oder über die native Receiver-Benutzeroberfläche auf veröffentlichte Ressourcen zuzugreifen.

Prüfen, ob das Gerät die Systemanforderungen erfüllt

Citrix stellt ein Skript, hdxcheck.sh, als Teil des Receiver-Installationspakets bereit. Das Skript überprüft, ob das Gerät alle Systemanforderungen erfüllt, um die gesamte Funktionalität in Receiver für Linux auszunutzen. Das Skript befindet sich im Verzeichnis “Utilities” des Installationspakets.

Ausführen des Skripts hdxcheck.sh

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie cd $ICAROOT/util ein und drücken Sie die EINGABETASTE, um auf das Verzeichnis “Utilities” des Installationspakets zu navigieren.
3. Geben Sie ./hdxcheck.sh ein, um das Skript auszuführen.

Installation und Einrichtung

February 22, 2019

Folgende Pakete sind für Citrix Receiver für Linux verfügbar. Die Pakete können im Abschnitt “Downloads” auf der Citrix Website heruntergeladen werden.

Paketname	Inhalt
Debian-Pakete (Ubuntu, Debian, Linux Mint usw.)	
icaclient_13.10.0.20_amd64.deb	Self-Service-Support, 64 Bit, x86_64
icaclient_13.10.0.20_i386.deb	Self-Service-Support, 32 Bit, x86
icaclient_13.10.0.20_armhf.deb	Self-Service-Support, ARM HF
icaclientWeb_13.10.0.20_amd64.deb	nur Web Receiver, 64 Bit, x86_64
icaclientWeb_13.10.0.20_i386.deb	nur Web Receiver, 32 Bit, x86
icaclientWeb_13.10.0.20_armhf.deb	nur Web Receiver, ARM HF
ctxusb_2.7.20_amd64.deb	USB-Paket, 64 Bit, x86_64
ctxusb_2.7.20_i386.deb	USB-Paket, 32 Bit, x86

Paketname	Inhalt
ctxusb_2.7.20_armhf.deb	USB-Paket, ARM HF
Redhat-Pakete (Redhat, SUSE, Fedora usw.)	
ICAClient-rhel-13.10.0.20-0.x86_64.rpm	Self-Service-Support, basierend auf Red Hat (einschl. Linux-VDA), 64 Bit, x86_64
ICAClient-rhel-13.10.0.20-0.i386.rpm	Self-Service-Support, basierend auf RedHat, 32 Bit, x86
ICAClientWeb-rhel-13.10.0.20-0.x86_64.rpm	nur Web Receiver, basierend auf Red Hat, 64 Bit, x86_64
ICAClientWeb-rhel-13.10.0.20-0.i386.rpm	nur Web Receiver, basierend auf RedHat, 32 Bit, x86
ICAClient-suse-13.10.0.20-0.x86_64.rpm	Self-Service-Support, basierend auf SUSE, 64 Bit, x86_64
ICAClient-suse-13.10.0.20-0.i386.rpm	Self-Service-Support, basierend auf SUSE, 32-Bit, x86
ICAClient-suse11sp3-13.10.0.20-0.x86_64.rpm	Self-Service-Support, basierend auf SUSE 11 sp3 (einschl. Linux-VDA), 64 Bit, x86_64
ICAClient-suse11sp3-13.10.0.20-0.i386.rpm	Self-Service_Support, basierend auf SUSE 11 sp3, 32-Bit, x86
ICAClientWeb-suse-13.10.0.20-0.x86_64.rpm	nur Web Receiver, basierend auf SUSE, 64 Bit, x86_64
ICAClientWeb-suse-13.10.0.20-0.i386.rpm	nur Web Receiver, basierend auf SUSE, 32 Bit, x86
ctxusb-2.7.20-1.x86_64.rpm	USB-Paket, 64 Bit, x86_64
ctxusb-2.7.20-1.i386.rpm	USB-Paket, 32 Bit, x86
Tarballs (Skriptinstallation für jede Distribution)	
linuxx64-13.10.0.20.tar.gz	64 Bit Intel
linuxx86-13.10.0.20.tar.gz	64 Bit Intel
linuxarmhf-13.10.0.20.tar.gz	ARM HF

Der Unterschied zwischen den Paketen für Web Receiver und für Self-Service ist, dass die Pakete mit Unterstützung für Self-Service die dafür erforderlichen Abhängigkeiten enthalten (zusätzlich zu den für Web Receiver erforderlichen Abhängigkeiten). Die Abhängigkeiten für Self-Service sind eine Ober-

menge der für Web Receiver erforderlichen Abhängigkeiten. Die installierten Dateien sind jedoch identisch.

Wenn Sie nur Unterstützung für Web Receiver benötigen oder Ihre Distribution nicht die erforderlichen Pakete für Self-Service umfasst, installieren Sie nur das Paket für Web Receiver.

> **Hinweis**
>
> Wenn Ihre Distribution es zulässt, installieren Sie Citrix Receiver vom Debian- oder RPM-Paket. Diese Dateien sind einfacher zu verwenden, da sie automatisch alle erforderlichen Pakete installieren. Wenn die den Installationsort steuern möchten, installieren Sie Citrix Receiver vom Tarball-Paket.
>
> Verwenden Sie nicht beide Installationsmethoden auf derselben Maschine. Wenn Sie beispielsweise Citrix Receiver für Linux mit einem Tarball-Paket auf einer Maschine installieren, auf der Citrix Receiver für Linux bereits mit einem Debian-Paket installiert wurde, treten wahrscheinlich Fehlermeldungen und unerwünschtes Verhalten auf.

Installieren von Citrix Receiver für Linux von einem Debian-Paket

Wenn Sie Receiver mit dem Debian-Paket unter Ubuntu installieren, ist es u. U. bequemer, die Pakete im Ubuntu Software Center zu öffnen.

Ersetzen Sie in den folgenden Anweisungen
packagename durch den Namen des Pakets, das Sie installieren.

Für diese Vorgehensweise werden eine Befehlszeile und der native Paketmanager für Ubuntu/Debian/Mint verwendet. Sie können das Paket auch durch Doppelklicken auf das heruntergeladene DEB-Paket in einem Dateibrowser installieren. In der Regel wird dadurch ein Paket-Manager gestartet, der fehlende erforderliche Software herunterlädt. Wenn kein Paketmanager verfügbar ist, empfiehlt Citrix
gdebi, ein Befehlszeilentool, das diese Funktion bietet.

Installieren des Pakets an der Befehlszeile

1. Melden Sie sich als privilegierter Benutzer (root) an.
2. Öffnen Sie ein Terminal-Fenster.
3. Führen Sie die Installation der folgenden 3 Pakete aus, indem Sie **gdebi packagename.deb** eingeben. Zum Beispiel:
   - gdebi icaclient_13.9.1.6_amd64.deb
   - gdebi icaclientWeb_13.9.1.6_i386.deb
   - gdebi ctxusb_2.7.6_amd64.deb

   Hinweis: Um in den obigen Beispielen dpkg zu verwenden, ersetzen Sie “gdebi” mit “dpkg -i”.

Ein Benutzer muss das icaclient-Paket oder das icaclientWeb-Paket installieren. Das ctxusb-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.

4. Wenn Sie dpkg verwenden, installieren Sie fehlende Abhängigkeiten durch Eingabe von sudo **apt-get -f install**.
5. Akzeptieren Sie die Lizenzvereinbarung.

Installieren von Citrix Receiver für Linux von einem RPM-Paket

Wenn Sie Citrix Receiver vom RPM-Paket auf SUSE installieren, verwenden Sie das Hilfsprogramm YaST oder Zypper, nicht das RPM-Hilfsprogramm. Das RPM-Hilfsprogramm installiert nur das RPM-Paket. Es lädt die benötigten Abhängigkeiten nicht herunter und installiert sie nicht. Wenn die erforderlichen Abhängigkeiten fehlen, tritt ein Fehler auf.

Hinweis: Sie können der Beispielinstallation eines RPM-Pakets im folgenden Citrix Blog-Artikel folgen: Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop.

Ersetzen Sie in den folgenden Anweisungen
packagename durch den Namen des Pakets, das Sie installieren.

Hinweis: Wenn in einer Fehlermeldung angezeigt wird, dass libwebkitgtk-1.0.so.0 für eine Installation auf Red Hat-basierten Distributionen (RHEL, CentOS, Fedora, usw.) erforderlich ist, fügen Sie das EPEL-Repository hinzu (weitere Informationen finden Sie unter https://fedoraproject.org/wiki/EPEL), das das fehlende Paket bereitstellt oder zur Webversion des Pakets wechselt.

Einrichten des EPEL-Repositorys auf Red Hat

1. Laden Sie das entsprechende RPM-Quellpaket hier herunter:

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

2. Beispiel für Red Hat Enterprise 7.x:

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

Tipp: RPM Package Manager installiert keine fehlende erforderliche Software. Citrix empfiehlt für den Download und die Installation die Verwendung von **zypper install <Dateiname>** an einer Befehlszeile unter OpenSUSE oder **yum localinstall <Dateiname>** unter Fedora/Red Hat.

Installieren Sie Receiver mit dem RPM-Paket nach dem Setup des EPEL-Repositorys.

1. Melden Sie sich als privilegierter Benutzer (root) an.
2. Führen Sie die Installation der folgenden drei Pakete aus, indem Sie “zypper” in package-name.rpm eingeben.

   Hinweis: Ein Benutzer muss das icaclient-Paket oder das icaclientWeb-Paket installieren. Das ctxusb-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.

3. Öffnen Sie ein Terminal-Fenster.

   Für SUSE-Installationen:

   zypper in ICAClient-suse-13.9.1.6-0.x86_64.rpm

   zypper in ICAClient-suse-13.9.1.6-0.i386.rpm

   zypper in ctxusb-2.7.6-1.x86_64.rpm

   Für Red Hat-Installationen:

   yum localinstall ICAClient-rhel-13.9.1.6-0.i386.rpm

   yum localinstall ICAClientWeb-rhel-13.9.1.6-0.i386.rpm

   yum localinstall ctxusb-2.7.6-1.i386.rpm

4. Akzeptieren Sie die Lizenzvereinbarung.

Installieren von Citrix Receiver für Linux von einem Tarball-Paket

Hinweis: Das Tarball-Paket führt keine Abhängigkeitenprüfung durch und installiert auch keine Abhängigkeiten. Alle Systemabhängigkeiten müssen separat gelöst werden.

1. Öffnen Sie ein Terminal-Fenster.
2. Entpacken Sie die TAR.GZ-Datei und extrahieren Sie den Dateiinhalt in ein leeres Verzeichnis. Geben Sie beispielsweise Folgendes ein: tar xvfz packagename.tar.gz.
3. Geben Sie **./setupwfc** ein und drücken Sie die Eingabetaste, um das Setupprogramm auszuführen.
4. Akzeptieren Sie den Standardwert 1 (Receiver installieren) und drücken Sie die Eingabetaste.
5. Geben Sie den Pfad und den Namen des gewünschten Installationsverzeichnisses ein und drücken Sie die Eingabetaste oder drücken Sie die Eingabetaste, um Receiver im Standardverzeichnis zu installieren.

   Das Standardverzeichnis für Installationen durch privilegierte Benutzer (root) ist /opt/Citrix/ICAClient.

   Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist $HOME/ICAClient/platform. “platform” ist ein systemgenerierter Bezeichner des installierten Betriebssystems. Beispiel: $HOME/ICAClient/linuxx86 für die Plattform Linux/x86)

   Hinweis: Wenn Sie einen anderen Speicherort als den Standardspeicherort verwenden, legen Sie ihn in $ICAROOT in $HOME/.profile oder $HOME/.bash_profile fest.

6. Geben Sie “y” ein und drücken Sie die Eingabetaste, wenn Sie zum Fortfahren aufgefordert werden.

7. Wählen Sie, ob Receiver in die Desktopumgebung integriert werden soll. Die Installation erstellt eine Menüoption, über die Benutzer Receiver starten können. Geben Sie an der Eingabeaufforderung **y** ein, um die Integration zu aktivieren.
8. Wenn Sie GStreamer installiert haben, können Sie entscheiden, ob Sie GStreamer in Receiver integrieren und damit die HDX Mediastream-Multimediabeschleunigung bereitstellen. Um Receiver mit GStreamer zu integrieren, geben Sie an der Eingabeaufforderung "y" ein.

   Hinweis: Auf einigen Plattformen kann die Installation des Clients mit einer Tarball-Distribution dazu führen, dass das System hängen bleibt, nachdem Sie zur Integration mit KDE und GNOME aufgefordert wurden. Das Problem tritt bei der ersten Initialisierung von gstreamer-0.10 auf. Wenn dieses Problem auftritt, brechen Sie den Installationsvorgang mit Strg+C ab und führen Sie den folgenden Befehl aus: **gst-inspect-0.10 – gst-disable-registry-fork –version**. Nachdem der Befehl ausgeführt wurde, sollten Sie den Tarball-Setup erneut ausführen können, ohne dass das System hängen bleibt.
9. Wenn Sie sich als privilegierter Benutzer (root) anmelden, können Sie entscheiden, ob Sie die USB-Unterstützung für mit XenDesktop und XenApp veröffentlichte VDI-Anwendungen aktivieren möchten. Geben Sie an der Eingabeaufforderung "y" ein, um die USB-Unterstützung zu installieren.

   Hinweis: Wenn Sie nicht als privilegierter Benutzer (root) angemeldet sind, wird die folgende Warnung angezeigt: "USB-Unterstützung kann nur von Root-Benutzern installiert werden. Führen Sie den Installer als root aus, um diese Option installieren zu können."
10. Nach Abschluss der Installation wird das Hauptinstallationsmenü wieder angezeigt. Geben Sie zum Beenden des Setupprogramms "3" ein und drücken Sie die Eingabetaste.

Anpassen einer Citrix Receiver für Linux-Installation

September 7, 2018

Sie können eine Konfiguration vor der Installation anpassen, indem Sie den Inhalt des Citrix Receiver-Pakets bearbeiten und die Dateien dann neu verpacken. Alle Installationen, die Sie mit diesem bearbeiteten Paket ausführen, enthalten dann Ihre Änderungen.

Anpassen einer Citrix Receiver für Linux-Installation

1. Entpacken Sie das Citrix Receiver-Paket in einem leeren Verzeichnis. Die Paketdatei heißt platform.major.minor.release.build.tar.gz (z. B. linuxx86.13.2.0.nnnnnn.tar.gz für die Plattform Linux/x86).

2. Nehmen Sie die erforderlichen Änderungen am Citrix Receiver-Paket vor. Sie können dem Paket beispielsweise ein TLS-Stammzertifikat hinzufügen, wenn Sie ein Zertifikat einer Zertifizierungsstelle verwenden möchten, die nicht Teil der standardmäßigen Receiver-Installation ist. Informationen, wie Sie dem Paket ein TLS-Stammzertifikat hinzufügen, finden Sie unter "Installieren von Stammzertifikaten auf Benutzergeräten" auf der Citrix Website mit der Produktdokumentation.
   Weitere Informationen über integrierte Zertifikate finden Sie unter "Konfigurieren und Aktivieren von SSL und TLS" auf der Citrix Website mit der Produktdokumentation.
3. Öffnen Sie die PkgID-Datei.
4. Fügen Sie folgende Zeile hinzu, um anzuzeigen, dass das Paket bearbeitet worden ist:MODIFIED=traceinfo wobei traceinfo Informationen darüber enthält, wer die Änderung vorgenommen hat und wann. Ein spezielles Format muss für diese Informationen nicht verwendet werden.
5. Speichern und schließen Sie die Datei.
6. Öffnen Sie die Dateiliste des Pakets Plattform/Plattform.psf (z. B. linuxx86/linuxx86.psf für die Plattform Linux/x86).
7. Aktualisieren Sie die Dateiliste des Pakets, um Ihre Änderungen aufzunehmen. Wenn Sie diese Datei nicht aktualisieren, können bei der Installation des neuen Pakets Fehler auftreten. Beispielsweise können Sie die Größe der geänderten Dateien aktualisieren oder neue Zeilen hinzufügen für Dateien, die Sie dem Paket hinzugefügt haben. Im Folgenden werden die Spaltentitel der Dateiliste des Pakets aufgeführt:
   - Dateityp
   - Relativer Pfad
   - Unterpaket (hierfür muss immer cor eingestellt sein)
   - Berechtigungen
   - Besitzer
   - Gruppe
   - Größe
8. Speichern und schließen Sie die Datei.
9. Erstellen Sie die Receiver-Paketdatei mit dem tar-Befehl neu, z. B.: tar czf ../newpackage.tar.gz * wobei newspackage der Name der neuen Receiver-Paketdatei ist.

Starten von Citrix Receiver für Linux

September 7, 2018

Sie können Citrix Receiver entweder an einer Terminal-Eingabeaufforderung oder von einer der unterstützten Desktopumgebungen aus starten.

Wenn Citrix Receiver nicht im Standardverzeichnis installiert wurde, muss die Umgebungsvariable ICA-

ROOT auf das richtige Installationsverzeichnis verweisen.

> **Tipp**
>
> Die folgenden Anweisungen gelten nicht für mit Webpaketen oder Tarball ausgeführte Installationen, sondern wenn die Anforderungen für den Self-Service nicht erfüllt sind.

Starten von Citrix Receiver an einer Terminal-Eingabeaufforderung

Geben Sie an der Terminal-Eingabeaufforderung /opt/Citrix/ICAClient/selfservice ein und drücken Sie die EINGABETASTE, wobei /opt/Citrix/ICAClient das Verzeichnis ist, in dem Sie Citrix Receiver installiert haben.

Starten von Citrix Receiver vom Linux-Desktop

Mithilfe eines Dateimanagers können Sie Citrix Receiver von einer Desktopumgebung für Linux aus starten.

Auf einigen Desktops können Sie Citrix Receiver auch über ein Menü starten. Receiver ist, je nach Linux-Distribution, in unterschiedlichen Menüs.

Verwenden von Citrix Receiver für Linux als ICA-zu-X-Proxy

March 11, 2019

Sie können eine Workstation, auf der Citrix Receiver ausgeführt wird, als Server verwenden und die Ausgabe auf ein anderes X11-fähiges Gerät umleiten. So können Sie Microsoft Windows-Anwendungen auch auf X-Terminals oder auf UNIX-Workstations bereitstellen, für die es Citrix Receiver nicht gibt.

> **Hinweis**
>
> Citrix Receiver-Software ist für zahlreiche X-Geräte verfügbar und in diesen Fällen ist das Installieren der Software auf diesen Geräten die bevorzugte Lösung. Das Ausführen von Citrix Receiver in dieser Weise, als ICA-zu-X-Proxy, wird auch serverseitiges ICA genannt.

Citrix Receiver kann als ICA-X11-Konverter angesehen werden, der die X11-Ausgabe auf den lokalen Linux-Desktop leitet. Natürlich können Sie die Ausgabe auch auf ein anderes X11-Display umleiten. Sie können mehrere Kopien von Citrix Receiver gleichzeitig auf einem System ausführen und dabei festlegen, dass jede Kopie die Ausgabe an ein anderes Gerät sendet.

Diese Grafik zeigt ein System, in dem Citrix Receiver für Linux als ICA-zu-X-Proxy eingerichtet ist:

Für solche Systeme benötigen Sie einen Linux-Server als ICA-zu-X11-Proxy:

- Wenn Sie bereits X-Terminals verwenden, können Sie Citrix Receiver auf dem Linux-Server ausführen, der normalerweise die X-Anwendungen für die X-Terminals bereitstellt.
- Wenn Sie UNIX-Workstations einsetzen möchten, für die es Citrix Receiver nicht gibt, benötigen Sie einen eigenen Server, der als Proxy dient. Hier wäre ein PC, auf dem Linux ausgeführt wird, denkbar.

Unterstützte Features

Anwendungen werden dem Endgerät mit X11 und den Funktionen des ICA-Protokolls bereitgestellt. Standardmäßig können Sie mit der Laufwerkszuordnung nur auf Laufwerke auf dem Proxy zugreifen. Dies ist bei Einsatz von X-Terminals kein Problem (diese haben normalerweise keine lokalen Laufwerke). Wenn Sie Anwendungen anderen UNIX-Workstations bereitstellen, können Sie Folgendes tun:

- Einhängen der lokalen UNIX-Workstation über NFS auf der als Proxy dienenden Workstation und dann Verweisen einer Clientlaufwerkzuordnung auf den NFS-Einhängepunkt (Mount Point) auf dem Proxy.
- Verwenden eines NFS-SMB-Proxys (z. B. SAMBA) oder eines NFS-Clients auf dem Server (z. B. Microsoft Services for UNIX).

Einige Leistungsmerkmale werden nicht an das Endgerät weitergeleitet:

- USB-Umleitung
- Smartcard-Umleitung
- COM-Portumleitung
- Dem X11-Gerät wird kein Audio übermittelt, selbst wenn der als Proxy dienende Server Audio unterstützt.
- Clientdrucker werden nicht an das X11-Gerät weitergeleitet. Sie müssen mit LPD-Druck manuell auf den UNIX-Drucker vom Server zugreifen oder einen Netzwerkdrucker verwenden.
- Die Umleitung von Multimedia-Eingaben funktioniert voraussichtlich nicht, da hierfür auf der Maschine, die Citrix Receiver ausführt, eine Webcam erforderlich ist. Diese Maschine ist jedoch der Server, der als Proxy fungiert. Die Umleitung von Multimedia-Ausgaben funktioniert jedoch, wenn GStreamer auf dem Server, der als Proxy fungiert, installiert ist (nicht getestet).

Starten von Citrix Receiver mit serverseitigem ICA von einem X-Terminal oder einer UNIX-Workstation

1. Stellen Sie über ssh oder Telnet eine Verbindung zum Computer her, der als Proxy dient.
2. Setzen Sie in einer Shell auf dem Proxygerät die Umgebungsvariable **DISPLAY** auf den lokalen Computer. Geben Sie z. B. in einer C-Shell Folgendes ein:

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


Hinweis: Wenn Sie mit dem Befehl ssh -X eine Verbindung zu dem Gerät, das als Proxy fungiert, herstellen, müssen Sie die Umgebungsvariable **DISPLAY** nicht einrichten.

3. Geben Sie an der Befehlszeile des lokalen Geräts Folgendes ein: xhost <Proxyservername>
4. Wenn Receiver nicht im Standardverzeichnis installiert wurde, muss die Umgebungsvariable ICAROOT auf das richtige Installationsverzeichnis verweisen.
5. Suchen Sie das Verzeichnis, in dem Citrix Receiver installiert ist. Geben Sie an einer Eingabeaufforderung selfservice & ein.

Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

January 22, 2019

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit Citrix die Qualität und Leistung seiner Produkte verbessern kann. Weitere Informationen zum CEIP finden Sie unter Citrix Programm zur Verbesserung der Benutzerfreundlichkeit.

Sie werden standardmäßig automatisch beim CEIP registriert, wenn Sie Citrix Receiver für Linux installieren. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation von Receiver. Die für aktive Benutzer gesammelten Daten werden alle sieben Tage auf den CIS-Server hochgeladen.

Registrierungseinstellung zur Steuerung der Registrierung in CEIP:

- Speicherort: <ICAROOT>/config/module.ini
- Abschnitt: CEIP
- Eintrag: EnableCeip
- Wert: Enable (Standard) / Disable

Die folgenden anonymen Informationen werden gesammelt. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren. Wenn EnableCeip auf “Disable” festgelegt ist, werden nur die Receiver-Versionsinformationen gesammelt.
Datenpunkt|Beschreibung
———-|———
Maschinen-ID|Identifiziert die Maschine, von der die Daten stammen.
Linux-Kernelversion|Die Zeichenfolge steht für die Kernelversion der Maschine.
Linux-OS-Name und -Version|Zeichenfolge, die den Linux-OS-Namen und die Linux-OS-Version der Maschine angibt.
Datum der Datensammlung|Das Datum, an dem die Datenerfassung erfolgt.

CPU-Modellname|Das CPU-Modell der Clientmaschine.
Systemspeicherinformationen|Sammelt Systemspeicherinformationen, u. a. gesamter RAM, verfügbarer RAM, Puffer-RAM, gemeinsam verwendeter RAM, gesamter Auslagerungsspeicher, verfügbarer Auslagerungsspeicher und die Anzahl der aktuellen Prozesse.
Bildschirmauflösung|Die Bildschirmauflösung der Clientmaschine.
Desktopumgebung|Informationen, ob die aktuell verwendete Desktopumgebung vom Typ - XDG_CURRENT_DESKTOP oder DESKTOP_SESSION ist.
Browserversion|Ruft Informationen über den verwendeten Browser ab: Firefox, Chrome usw.
USB-Geräteinformationen|Ruft Informationen zu den auf dem Clientsystem verfügbaren USB-Ports ab.
Flash-Version|Ruft Informationen zur verwendeten Flash-Version ab.
Gebietsschemaversion|Die Version des Gebietsschemas.
Sprachinformationen|Tastaturzuordnung und entsprechende Informationen.
Schemainformationen|Die Schemainformationen für Receiver.
Multimediaumleitung|Boolescher Wert, der anzeigt, ob dieses Feature aktiviert ist.
Webcamumleitung|Boolescher Wert, der anzeigt, ob die Webcamumleitung aktiviert ist.
Flash-Umleitung|Boolescher Wert, der anzeigt, ob die Flash-Umleitung aktiviert ist.
MediaStream|Boolescher Wert, der anzeigt, ob MediaStream aktiviert ist. Dies schließt SpeedScreen-Audio- und Videofunktionen ein.

Deinstallieren von Citrix Receiver für Linux

September 7, 2018

Dieses Verfahren wurde mit dem Tarball-Paket getestet. Entfernen Sie das RPM- und Debian-Paket mit den Standardtools des Betriebssystems.

Die Umgebungsvariable ICAROOT muss für das Installationsverzeichnis des Clients festgelegt sein. Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist $HOME/ICAClient/-platform. Die Variable “platform” ist eine vom System erstellte Kennung für das installierte Betriebssystem. Beispiel: $HOME/ICAClient/linuxx86 für die Plattform Linux/x86 Das Standardverzeichnis für Installationen durch privilegierte Benutzer ist /opt/Citrix/ICAClient.

1. Führen Sie das Setupprogramm aus. Geben Sie hierfür $ICAROOT/setupwfc ein und drücken Sie die EINGABETASTE.
2. Geben Sie zum Entfernen des Clients 2 ein und drücken Sie die EINGABETASTE.

> **Hinweis**
>
> Um Citrix Receiver für Linux zu deinstallieren, müssen Sie als der Benutzer angemeldet sein, der

> die Installation durchgeführt hat.

Verbinden

September 7, 2018

Citrix Workspace bietet Benutzern sicheren Self-Service-Zugriff auf virtuelle Desktops und Anwendungen und bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen (Software-as-a-Service). Der Benutzerzugriff wird über Citrix StoreFront oder mit Webinterface erstellte Legacywebseiten verwaltet.

Herstellen einer Verbindung zu Ressourcen mit der Citrix Workspace-Benutzeroberfläche

Die Homepage der Citrix Workspace-App zeigt virtuelle Desktops und Anwendungen an, die Benutzern basierend auf deren Kontoeinstellungen (d. h. dem Server, mit dem sie eine Verbindung herstellen) und basierend auf den von Citrix XenDesktop- oder Citrix XenApp-Administratoren konfigurierten Einstellungen zur Verfügung stehen. Mit der Seite Einstellungen > Konten können Benutzer die Konfiguration selbst vornehmen, indem sie die URL eines StoreFront-Servers oder, wenn die E-Mail-basierte Kontenermittlung konfiguriert ist, ihre E-Mail-Adresse eingeben.

> **Tipp**
>
> Wenn Sie denselben Namen für mehrere Stores auf dem StoreFront-Server verwenden, vermeiden Sie Duplikationen, indem Sie Nummern hinzufügen. Die Namen dieser Stores hängen von der Reihenfolge ab, in der sie hinzugefügt werden. Für PNAgent wird die Store-URL angezeigt, die den Store eindeutig identifiziert.

Wenn Sie die Verbindung zu einem Store hergestellt haben, zeigt Self-Service folgende Registerkarten an: FAVORITEN, DESKTOPS und APPS. Um eine Sitzung zu starten, klicken Sie auf das entsprechende Symbol. Um ein Symbol zu FAVORITEN hinzuzufügen, klicken Sie auf den Link “Details” neben dem Symbol, und wählen Sie “Zu Favoriten hinzufügen”.

Konfigurieren von Verbindungseinstellungen

Sie können einige Standardeinstellungen für Verbindungen zwischen der Citrix Workspace-App für Linux und XenApp- und XenDesktop-Servern konfigurieren. Sie können diese Einstellungen ggf. für einzelne Verbindungen ändern.

Die Informationen im übrigen Teil enthalten Verfahren für typische, von Benutzern der Citrix Workspace-App ausgeführte Aufgaben. Obwohl sich die Aufgaben und Verantwortungsbereiche von

Administratoren und Benutzern überschneiden können, wird der Ausdruck “Benutzer” in diesem Abschnitt dort verwendet, wo Aufgaben beschrieben werden, die normalerweise von Benutzern und nicht von Administratoren ausgeführt werden.

Verbinden mit Ressourcen per Eingabeaufforderung oder Browser

March 11, 2019

Verbindungen mit Servern werden hergestellt, wenn Sie auf der Receiver-Homepage auf ein Desktop- oder Anwendungssymbol klicken. Außerdem können Sie Verbindungen über eine Eingabeaufforderung oder über einen Webbrowser herstellen.

Herstellen einer Verbindung zu einem Program Neighborhood- oder StoreFront-Server mit einer Befehlszeile

Stellen Sie zunächst sicher, dass der Store Citrix Receiver bekannt ist. Falls erforderlich, fügen Sie ihn mit dem folgenden Befehl hinzu:

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

1. Rufen Sie die eindeutige ID des Desktops oder der Anwendung auf, mit dem bzw. der Sie eine Verbindung herstellen möchten. Dies ist die erste Zeichenfolge in Anführungszeichen auf einer Zeile, die über einen der folgenden Befehle aufgerufen wird:
   - Auflisten aller Desktops und Anwendungen auf dem Server:

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

   - Auflisten der Desktops und Anwendungen, die Sie abonniert haben:

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

2. Führen Sie den folgenden Befehl aus, um den Desktop oder die Anwendung zu starten:

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

Wenn Sie keine Verbindung zu einem Server herstellen können, muss der Administrator möglicherweise die Angaben für den Serverstandort oder den SOCKS-Proxyserver ändern. Weitere Informationen finden Sie unter
Herstellen von Verbindungen über Proxyserver.

Herstellen einer Verbindung mit einem Webbrowser

Die Konfiguration zum Starten von Sitzungen über einen Webbrowser erfolgt normalerweise während der Installation automatisch. Aufgrund der Vielzahl von Browsern und Betriebssystemen ist möglicherweise etwas manuelle Konfiguration erforderlich.

Wenn Sie die MAILCAP- und MIME-Dateien für Firefox, Mozilla oder Chrome manuell einrichten, führen Sie die nachfolgend aufgeführten Dateiänderungen durch, sodass die ICA-Dateien die ausführbare Receiver-Datei wfica starten. Um andere Browser zu verwenden, müssen Sie die Browserkonfiguration entsprechend konfigurieren.

1. Führen Sie die folgenden Befehle aus, wenn die Citrix Workspace-App von einem Benutzer ohne Administratorrechte installiert wird. Die Einstellungen von ICAROOT werden möglicherweise geändert, wenn sie nicht in einem Standardspeicherort installiert werden. Testen Sie das Ergebnis mit dem Befehl “xdg-mime query default application/x-ica”, der “wfica.desktop” zurückgeben muss.

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

xdg-icon-resource install --size 64  “$ICAROOT/icons/000
    _Receiver_64.png Citrix Workspace app”

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

xdg-mime default new_store.desktop application/vnd.citrix.receiver
    .configure
```

2. Erstellen oder erweitern Sie die Datei /etc/xdg/mimeapps.list (bei Installation durch einen Administrator) oder $HOME/.local/share/applications/mimeapps.list (mimeapps.list). Die Datei muss mit [Default Applications] beginnen, dann folgt:

   application/x-ica=wfica.desktop;

   application/vnd.citrix.receiver.configure=new_store.desktop;

   Möglicherweise müssen Sie in Firefox unter “Einstellungen > Anwendungen” Konfigurationen vornehmen. Wählen Sie für “Citrix ICA settings file content” in der Dropdownliste “Citrix Receiver Engine (default)”. Oder wählen Sie “Use other …” und dann die Datei /usr/share/applications/wfica.desktop (für die Administratorinstallation von Receiver) oder $HOME/.local/share/applications/wfica.desktop (für ein Installation ohne Administratorrechte).

Problembehandlung bei Verbindungen mit Ressourcen

September 7, 2018

Benutzer können aktive Verbindungen mit dem Connection Center verwalten. Dieses Feature ist ein nützliches Tool, mit dem Benutzer und Administratoren Probleme mit langsamen oder fehlerhaften Verbindungen beheben können. Mit Connection Center, können Benutzer folgende Verbindungsverwaltungsaufgaben durchführen:

- Schließen einer Anwendung
- Abmelden von einer Sitzung. Dabei wird die Sitzung beendet und alle geöffneten Anwendungen werden geschlossen.
- Trennen der Verbindung mit einer Sitzung. Mit diesem Schritt wird die ausgewählte Verbindung mit dem Server getrennt, ohne offene Anwendungen zu schließen (außer wenn der Server zum Schließen von Anwendungen bei Verbindungstrennung konfiguriert ist).
- Anzeigen der Verbindungsübertragungsstatistik

Verwalten einer Verbindung

1. Klicken Sie im Citrix Workspace-App-Menü auf “Connection Center”.

   Die verwendeten Server und die für jeden Server aktiven Sitzungen werden aufgelistet.

2. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie einen Server aus und trennen Sie die Verbindung, melden Sie sich ab oder zeigen Sie die Eigenschaften des Servers an.
   - Wählen Sie eine Anwendung aus und schließen Sie das Fenster, in dem der Desktop bzw. die Anwendung angezeigt wird.

Anpassen mit Konfigurationsdateien

November 15, 2018

Konfigurationsdateien

Zum Ändern erweiterter oder selten verwendeter Einstellungen können Sie die Konfigurationsdateien von Receiver bearbeiten. Die Konfigurationsdateien werden jedes Mal gelesen, wenn wfica gestartet

wird. Sie können mehrere Dateien bearbeiten, je nachdem welche Wirkung Sie mit Ihren Änderungen erzielen möchten.

Ist die Sitzungsfreigabe aktiviert, wird möglicherweise eine vorhandene Sitzung anstelle einer neu konfigurierten verwendet. Dies kann dazu führen, dass in einer Konfigurationsdatei vorgenommene Änderungen ignoriert werden.

Anwenden von Standardwerten auf alle Citrix Receiver-Benutzer

Wenn Sie Standardwerte für alle Citrix Receiver-Benutzer ändern möchten, bearbeiten Sie die Konfigurationsdatei module.ini im Verzeichnis $ICAROOT/config.

> **Hinweis**
>
> Für Konfigurationswerte, die aus module.ini gelesen werden sollen, müssen Sie keinen Eintrag in All_Regions.ini machen. Dies ist nur erforderlich, wenn Sie möchten, dass andere Konfigurationsdateien den Wert in module.ini überschreiben können sollen. Wenn mit einem Eintrag in All_Regions.ini ein spezifischer Wert festgelegt wird, wird der Wert in module.ini nicht verwendet.

Anwenden von Änderungen auf neue Citrix Receiver-Benutzer

Wenn die Datei $HOME/.ICAClient/wfclient.ini nicht vorhanden ist, erstellt wfica sie durch Kopieren von $ICAROOT/config/wfclient.template. Wenn Sie diese Vorlagendatei ändern, werden die Änderungen auf alle zukünftigen Citrix Receiver-Benutzer angewendet.

Anwenden von Änderungen auf alle Verbindungen bestimmter Benutzer

Wenn Ihre Änderungen für alle Verbindungen für einen bestimmten Benutzer gelten sollen, bearbeiten Sie die Datei wfclient.ini im Verzeichnis $HOME/.ICAClient des Benutzers. Die Einstellungen in dieser Datei gelten für zukünftige Verbindungen für diesen Benutzer.

Überprüfen von Einträgen in Konfigurationsdateien

Wenn Sie die Werte für Einträge in wfclient.ini beschränken möchten, können Sie die zulässigen Optionen oder Optionsbereiche in der Datei All_Regions.ini festlegen. Wenn Sie nur einen möglichen Wert angeben, wird dieser Wert verwendet. $HOME/.ICAClient/All_Regsions.ini kann nur mit den in $ICAROOT/config/All_Regions.ini angegebenen Werten übereinstimmen oder sie reduzieren. Beschränkungen können nicht aufgehoben werden. Weitere Informationen finden Sie in der Datei All_Regions.ini im Verzeichnis $ICAROOT/config.

> **Hinweis**
>
> Wenn ein Eintrag in mehr als einer Konfigurationsdatei enthalten ist, hat der Wert in wfclient.ini Vorrang vor dem Wert in module.ini.

Parameter in den Dateien

Die Parameter in jeder Datei sind in Abschnitte zusammengefasst. Jeder Abschnitt beginnt mit einem Namen in eckigen Klammern, der auf zusammengehörige Parameter hinweist. [ClientDrive] steht beispielsweise für die Parameter der Clientlaufwerkzuordnung.

Standardwerte werden, sofern nicht anders angegeben, automatisch für alle fehlenden Parameter eingesetzt. Wenn ein Parameter keinen Wert besitzt, wird automatisch der Standardwert angewendet. Beispiel: Wenn auf “InitialProgram” ein Gleichheitszeichen (=) ohne Wert folgt, wird der Standardwert (nach der Anmeldung kein Programm ausführen) angewendet.

Rangfolge

Über All_Regions.ini wird bestimmt, welche Parameter durch andere Dateien festgelegt werden können. In dieser Datei können Werte für Parameter eingeschränkt oder genau festgelegt werden.

Für jede einzelne Verbindung werden die Dateien normalerweise in der in der folgenden Reihenfolge geprüft:

1. All_Regions.ini. Werte in dieser Datei haben Vorrang vor:
   - ICA- Datei der Verbindung
   - wfclient.ini
2. module.ini Die Werte in dieser Datei werden verwendet, wenn sie nicht in All_Regions.ini, der ICA- Datei der Verbindung oder in wfclient.ini festgelegt wurden. Sie werden jedoch nicht durch die Einträge in All_Regions.ini eingeschränkt.

Wird in keiner dieser Dateien ein Wert gefunden, dann wird der Standardwert im Receiver-Code verwendet.

> **Hinweis**
>
> Es gibt Ausnahmen bei dieser Rangfolge. Beispielsweise werden vom Code aus Sicherheitsgründen gezielt einige Werte aus wfclient.ini gelesen, um sicherzustellen, dass sie nicht von einem Server festgelegt wurden.

Konfigurieren von Citrix XenApp-Verbindungen (früher PNAgent) mit dem Webinterface

September 7, 2018

Dieser Abschnitt gilt nur für Bereitstellungen, die XenApp Services auf dem Webinterface oder "legacy PNAgent" auf StoreFront verwenden.

Mit Optionen wie selfservice, storebrowse und pnabrowse können Benutzer über einen Server, auf dem eine XenApp Services-Site ausgeführt wird, eine Verbindung zu veröffentlichten Ressourcen (veröffentlichten Anwendungen und Serverdesktops) herstellen. Diese Programme können Verbindungen direkt starten oder sie können zum Erstellen von Menüelementen verwendet werden, über die Benutzer auf veröffentlichte Ressourcen zugreifen können. Mit pnabrowse können für diesen Zweck auch Desktopelemente erstellt werden.

Einstellbare Optionen für alle Benutzer, die Citrix XenApp im Netzwerk ausführen, sind in der Konfigurationsdatei config.xml festgelegt, die auf dem Webinterface-Server gespeichert ist. Wenn ein Benutzer eines dieser Programme startet, liest es die Konfigurationsdaten vom Server und aktualisiert anschließend die Einstellungen und die Benutzeroberfläche in regelmäßigen Abständen wie in der Datei config.xml festgelegt.

> **Wichtig**
>
> Die Datei config.xml gilt für alle Verbindungen, die von der XenApp Services-Site definiert werden.

Veröffentlichen von Inhalten

Eine XenApp Services-Site kann auch eine Datei und nicht nur Anwendungen oder Desktops veröffentlichen. Dieser Vorgang wird als Veröffentlichen von Inhalt bezeichnet und ermöglicht pnabrowse, die veröffentlichte Datei zu öffnen.

Die Citrix Workspace-App für Linux erkennt nicht alle Dateitypen. Das System erkennt nur dann den Dateityp der veröffentlichten Inhalte und die Benutzer können die Inhalte nur dann über die Citrix Workspace-App anzeigen, wenn eine Zuordnung zwischen einer veröffentlichten Anwendung und dem Dateityp der veröffentlichten Datei besteht. Um beispielsweise eine veröffentlichte Adobe PDF-Datei mit der Citrix Workspace-App zu öffnen, muss eine Anwendung wie z. B. Adobe PDF Viewer veröffentlicht sein. Benutzer können den veröffentlichten Inhalt nur anzeigen, wenn eine geeignete Anwendung veröffentlicht ist.

Optimieren

March 11, 2019

Durch Optimieren Ihrer Umgebung erhalten Sie die beste Leistung von Citrix Receiver und bieten die beste Benutzererfahrung. Sie können die Leistung folgendemaßen optimieren:

- Zuordnen von Benutzergeräten
- Konfigurieren der USB-Unterstützung
- Bloomberg-Tastaturumleitung
- Steigern der Leistung über Verbindungen mit geringer Bandbreite
- Steigern der Multimedialeistung
- Optimieren der Leistung für Bildschirmkacheln
- Aktivieren der Protokollierung für Retailbuilds
- Konfigurieren der Layoutspeicherung im Multimonitormodus

Zuordnen von Benutzergeräten

Citrix Receiver unterstützt Clientgerätzuordnung für Verbindungen zu XenApp- und XenDesktop-Servern. Mit der Clientgerätzuordnung kann eine auf dem Server ausgeführte Remoteanwendung auf Geräte zugreifen, die an das lokale Benutzergerät angeschlossen sind. Dem Benutzer des Benutzergeräts erscheinen die Anwendungen und Systemressourcen, als würden sie lokal ausgeführt. Vergewissern Sie sich, dass der Server die Clientgerätzuordnung unterstützt, bevor Sie diese Funktionen verwenden.

Hinweis: Das Sicherheitsmodul Security-Enhanced Linux (SELinux) kann sich auf die Clientlaufwerkzuordnung und die USB-Umleitung (unter XenApp und XenDesktop) auswirken. Wenn Sie eines dieser Features (oder beide) benötigen, deaktivieren Sie SELinux, bevor Sie es auf dem Server konfigurieren.

Zuordnen von Clientlaufwerken

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf dem XenApp- oder XenDesktop-Server auf Verzeichnisse, die auf dem lokalen Benutzergerät vorhanden sind. In einer Citrix Benutzersitzung kann beispielsweise der Laufwerk H einem Verzeichnis auf dem lokalen Computer, auf dem Receiver ausgeführt wird, zugeordnet werden.

Mit der Clientlaufwerkzuordnung werden alle auf dem lokalen Benutzergerät bereitgestellten Verzeichnisse, einschließlich CDs, DVDs oder USB-Sticks, in Sitzungen für den Benutzer verfügbar, wenn der lokale Benutzer Zugriffsrechte hat. Wenn ein Server für die Clientlaufwerkzuordnung konfiguriert ist,

können Benutzer auf lokal gespeicherte Dateien zugreifen, diese in ihren Sitzungen bearbeiten und dann entweder auf einem lokalen Laufwerk oder einem Laufwerk auf dem Server speichern.

Es gibt zwei Arten von Laufwerkzuordnung:

- Die statische Clientlaufwerkzuordnung ermöglicht es Administratoren, einen beliebigen Teil des Dateisystems auf dem Benutzergerät bei der Anmeldung einem bestimmten Laufwerksbuchstaben auf dem Server zuzuordnen. Sie können damit beispielsweise das gesamte Basisverzeichnis oder einen Teil davon sowie die Bereitstellungspunkte von Hardwaregeräten, wie CD-ROMs, DVDs oder USB-Sticks, zuordnen.
- Die dynamische Clientlaufwerkzuordnung überwacht die Verzeichnisse, in denen Hardwaregeräte wie CD-ROMs, DVDs und USB-Sticks üblicherweise auf dem Benutzergerät bereitgestellt werden. Geräte, die der Sitzung neu hinzugefügt werden, werden automatisch dem nächsten verfügbaren Laufwerksbuchstaben auf dem Server zugeordnet.

Wenn eine Verbindung zwischen Citrix Receiver und XenApp oder XenDesktop hergestellt wird, werden die Clientlaufwerkzuordnungen wiederhergestellt, es sei denn, die Clientgerätzuordnung ist deaktiviert. Sie können mit Richtlinien genauer steuern, wie die Clientgerätzuordnung angewendet wird. Weitere Informationen finden Sie in der Dokumentation von XenApp und XenDesktop.

Benutzer können Laufwerke im Dialogfeld Einstellungen zuordnen.

Hinweis: Standardmäßig wird durch das Aktivieren der statischen Clientlaufwerkzuordnung auch die dynamische Clientlaufwerkzuordnung aktiviert. Damit beim Aktivieren der statischen Clientlaufwerkzuordnung die dynamische Clientlaufwerkzuordnung nicht aktiviert wird, legen Sie “DynamicCDM” in wfclient.ini auf “False” fest.

Zuordnen von Clientdruckern

Citrix Receiver unterstützt das Drucken auf Netzwerkdruckern und auf lokal an Benutzergeräte angeschlossenen Druckern. XenApp ermöglicht Benutzern Folgendes, außer wenn Sie dies durch Richtlinien verhindern:

- Drucken auf allen Druckgeräten, die vom Benutzergerät aus verfügbar sind
- Hinzufügen von Druckern

Diese Einstellungen sind jedoch möglicherweise nicht für alle Umgebungen optimal. Beispielsweise ist die Standardeinstellung, bei der Benutzer alle Drucker verwenden können, auf die sie über das Benutzergerät zugreifen können, anfänglich die am einfachsten zu verwaltende Lösung. Die Standardeinstellung kann jedoch in manchen Umgebungen zu langen Anmeldezeiten führen. In solchen Situationen sollten Sie die Liste der auf dem Benutzergerät konfigurierten Drucker einschränken.

Die Sicherheitsrichtlinien des Unternehmens könnten es außerdem erforderlich machen, dass Sie das benutzerseitige Zuordnen lokaler Druckerports nicht zulassen. Hierfür stellen Sie auf dem Server die Citrix Richtlinieneinstellung Client-COM-Ports automatisch verbinden auf Deaktiviert ein.

Einschränken der Liste der auf dem Benutzergerät konfigurierten Drucker

1. Öffnen Sie die Konfigurationsdatei wfclient.ini in einem der folgenden Verzeichnisse:
   - Im Verzeichnis $HOME/.ICAClient, um die automatisch erstellten Drucker für einen einzelnen Benutzer einzuschränken.
   - Im Verzeichnis $ICAROOT/config, um die Drucker für alle Receiver-Benutzer einzuschränken. In diesem Fall sind "alle Benutzer" diejenigen, die das Self-Service-Programm nach der Änderung zuerst verwenden.
2. Geben Sie im Abschnitt [WFClient] der Datei Folgendes ein:

   ClientPrinterList=Drucker1:Drucker2:Drucker3

   Dabei sind Drucker1, Drucker2 usw. die Namen der ausgewählten Drucker. Trennen Sie die Einträge für die Druckernamen mit einem Doppelpunkt (:).
3. Speichern und schließen Sie die Datei.

Zuordnen von Clientdruckern auf XenApp für Windows

Citrix Receiver für Linux unterstützt den universellen Citrix PS Druckertreiber. Daher ist normalerweise keine lokale Konfiguration erforderlich, damit Benutzer mit Netzwerkdruckern oder Druckern, die an die lokalen Benutzergeräte angeschlossen sind, drucken können. Sie müssen Clientdrucker unter XenApp für Windows jedoch u. U. manuell zuordnen, wenn z. B. die Drucksoftware des Benutzergeräts nicht den universellen Druckertreiber unterstützt.

Zuordnen eines lokalen Druckers auf einem Server

1. Starten Sie eine Serververbindung von Citrix Receiver und melden Sie sich an einem Server an, auf dem XenApp ausgeführt wird.
2. Wählen Sie im Startmenü **Einstellungen > Drucker**.
3. Wählen Sie im Menü "Datei" die Option **Drucker hinzufügen**.

   Der Druckerinstallationsassistent wird angezeigt.
4. Fügen Sie mit dem Assistenten einen Netzwerkdrucker aus dem Clientnetzwerk und der Clientdomäne hinzu. Hierbei handelt es sich normalerweise um einen Standarddruckernamen, vergleichbar mit denen, die durch native Remotedesktopdienste erstellt werden, z. B. "HPLaserJet 4 von Clientname in Sitzung 3".

   Weitere Informationen zum Hinzufügen von Druckern finden Sie in der Dokumentation zum Windows-Betriebssystem.

Zuordnen von Clientdruckern auf XenApp für UNIX

In UNIX-Umgebungen werden von Citrix Receiver definierte Druckertreiber ignoriert. Das Drucksystem auf dem Benutzergerät muss in der Lage sein, das von der Anwendung erzeugte Druckformat zu verarbeiten.

Bevor Benutzer von Citrix XenApp für UNIX auf einem Clientdrucker drucken können, muss der Systemadministrator diese Funktion aktivieren. Weitere Informationen finden Sie unter "XenApp für UNIX" in der Dokumentation für XenApp und XenDesktop.

Zuordnen von Clientaudio

Die Clientaudiozuordnung ermöglicht es, dass auf XenApp-Servern oder XenDesktop ausgeführte Anwendungen Audiodaten über ein auf dem Benutzergerät installiertes Audiogerät abspielen. Sie können die Audioqualität auf dem Server auf Verbindungsbasis festlegen und Benutzer können sie auf dem Benutzergerät einstellen. Bei unterschiedlichen Einstellungen wird die niedrigere Einstellung verwendet.

Die Clientaudiozuordnung kann zu einer Überlastung der Server und des Netzwerks führen. Je höher die Audioqualität, desto größer die erforderliche Bandbreite für die Übertragung der Audiodaten. Bei der höheren Audioqualität wird außerdem auch mehr Prozessorzeit auf dem Server in Anspruch genommen.

Sie können die Clientaudiozuordnung mit Richtlinien konfigurieren. Weitere Informationen finden Sie in der Dokumentation von XenApp und XenDesktop.

Hinweis: Diese Funktion steht nicht bei einer Verbindung zu Citrix XenApp für UNIX zur Verfügung.

Festlegen eines anderen Geräts als das Standardaudiogerät

Das Standardaudiogerät ist normalerweise das Standard-ALSA-Gerät, das für Ihr System konfiguriert ist. Mit der folgenden Methode können Sie ein anderes Gerät festlegen:

1. Wählen Sie je nachdem, für welche Benutzer die Änderungen gelten sollen, die entsprechende Konfigurationsdatei aus und öffnen Sie sie. Informationen dazu, wie sich Änderungen in bestimmten Konfigurationsdateien auf bestimmte Benutzer auswirken, finden Sie unter Anpassen von Receiver mit Konfigurationsdateien.
2. Fügen Sie die folgende Option hinzu. Wenn dieser Abschnitt nicht vorhanden ist, erstellen Sie ihn.

[ClientAudio]

AudioDevice =

Die Informationen für Gerät befinden sich in der ALSA-Konfigurationsdatei auf Ihrem Betriebssystem.

Hinweis: Der Speicherort für diese Informationen ist nicht auf allen Linux-Betriebssystemen einheitlich. Citrix empfiehlt, in der Dokumentation Ihres Betriebssystems nachzulesen, wo Sie diese Informationen finden können.

Konfigurieren der USB-Unterstützung

Mit der USB-Unterstützung können Benutzer mit zahlreichen USB-Geräten interagieren, wenn sie mit einem virtuellen Desktop verbunden sind. Benutzer können USB-Geräte an ihren Computer anschließen. Diese werden dann zum virtuellen Desktop umgeleitet. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets.

USB-Umleitung erfordert XenApp 7.6 (oder höher) oder XenDesktop. XenApp unterstützt nicht die USB-Umleitung von Massenspeichergeräten. Für die Unterstützung von Audiogeräten ist eine besondere Konfiguration erforderlich. Weitere Informationen finden Sie in der XenApp 7.6-Dokumentation.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz und hoher Geschwindigkeit unterstützt. Normalerweise ist jedoch die Standardaudio- oder Webcamumleitung besser geeignet.

Die folgenden Gerätetypen werden direkt in einer XenDesktop-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards
- Headsets
- Webcams

Hinweis: USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie unter
CTX119722.

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über XenDesktop unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre in diesem Fall nicht angebracht. Die folgenden Typen von USB-Geräten können standardmäßig nicht in einer XenDesktop-Sitzung verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten

- USB-Hubs

Um die Standardliste von USB-Geräten für Remoting zu aktualisieren, bearbeiten Sie die Datei usb.conf in $ICAROOT/. Weitere Informationen finden Sie unter “Aktualisieren der für Remoting verfügbaren USB-Geräteliste”.

Um Remoting von USB-Geräten zu virtuellen Desktops zuzulassen, aktivieren Sie die USB-Richtlinienregel. Weitere Informationen finden Sie in der Dokumentation von XenApp und XenDesktop.

Funktionsweise der USB-Unterstützung

Wenn ein Benutzer ein USB-Gerät anschließt, wird es anhand der USB-Richtlinie überprüft und, sofern zulässig, an den virtuellen Desktop umgeleitet. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Bei Desktops, auf die über Desktop Appliance Mode zugegriffen wird, erfolgt die automatische Umleitung eines Geräts zum virtuellen Desktop, wenn ein Benutzer ein USB-Gerät anschließt. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.

Das Sitzungsfenster muss den Fokus haben, wenn der Benutzer das USB-Gerät für die Umleitung anschließt, es sei denn, der Desktop Appliance Mode wird verwendet.

Massenspeichergeräte

Wenn ein Benutzer die Verbindung zu einem virtuellen Desktop trennt, während ein USB-Massenspeichergerät noch am lokalen Desktop angeschlossen ist, wird das Gerät nicht an den virtuellen Desktop umgeleitet, wenn der Benutzer die Verbindung wieder herstellt. Um sicherzustellen, dass das Massenspeichergerät an den virtuellen Desktop umgeleitet wird, muss der Benutzer es entfernen und nach der Wiederherstellung der Verbindung wieder anschließen.

Hinweis: Wenn Sie ein Massenspeichergerät an eine Linux-Workstation anschließen, die Remoteverbindungen von USB-Massenspeichergeräten nicht zulässt, wird das Gerät von der Receiver-Software nicht akzeptiert. Möglicherweise wird ein separater Linux-Dateibrowser geöffnet. Aus diesem Grund empfiehlt Citrix, dass Sie die Benutzergeräte so konfigurieren, dass die Einstellung **Wechselmedien beim Einlegen einbinden** standardmäßig deaktiviert ist. Wählen Sie dazu auf Geräten mit Debian auf der Debian-Menüleiste, Folgendes: **System > Einstellungen > Wechseldatenträger und -medien**. Deaktivieren Sie auf der Registerkarte **Speichermedien** unter **Wechseldatenträger** das Kontrollkästchen **Wechselmedien beim Einlegen einbinden**.

Hinweis: Wenn die Serverrichtlinie “Client-USB-Geräteumleitung” aktiviert ist, werden Massenspeichergeräte wie USB-Geräte umgeleitet, selbst wenn die Clientlaufwerkzuordnung aktiviert ist.

Webcams

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen jedoch, müssen Benutzer Webcams mit USB-Unterstützung anschließen. Hierzu müssen Sie HDX RealTime-Webcamvideokomprimierung deaktivieren. Weitere Informationen finden Sie unter Videokonferenzen mit HDX RealTime-Webcamvideokomprimierung.

Standardmäßig zugelassene USB-Klassen

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln zugelassen:

- Audio (Geräteklasse 01)

  Umfasst Mikrofone, Lautsprecher, Kopfhörer und MIDI-Controller.

- Physikalische Schnittstelle (Geräteklasse 05)

  Diese Geräte ähneln HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Hautskelette.

- Bilder (Geräteklasse 06)

  Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen oft die Bilderklasse, in der Bilder mit den Protokollen PTP (Picture Transfer Protocol) oder MTP (Media Transfer Protocol) zu einem Computer oder zu einem anderen Peripheriegerät übertragen werden. Kameras können auch als Massenspeichergeräte angezeigt werden. Eine Kamera kann möglicherweise über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

  Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet und die USB-Unterstützung wird nicht benötigt.

- Drucker (Geräteklasse 07)

  Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. Mehrfunktionsdrucker haben ggf. einen internen Hub oder sind Composite-Geräte. In beiden Fällen verwendet das Druckerelement meistens die Druckerklasse und das Scanner- oder Faxelement verwendet eine andere Klasse, z. B. Bilder.

  Drucker funktionieren normalerweise ohne USB-Unterstützung.

- Massenspeicher (Geräteklasse 08)

  Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke sowie über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, die auch eine Massenspeicherschnittstelle darstellen, u. a. Medienplayer, digitale Kameras und Mobiltelefone. Bekannte Unterklassen:

- 01: Begrenzte Flashlaufwerke
- 02: Normalerweise CD- bzw. DVD-Geräte (ATAPI/MMC-2)
- 03: Normalerweise Bandgeräte (QIC-157)
- 04: Normalerweise Diskettenlaufwerke (UFI)
- 05: Normalerweise Diskettenlaufwerke (SFF-8070i)
- 06: Die meisten Massenspeichergeräte verwenden diese SCSI-Variante

  Der Zugriff auf Massenspeichergeräte erfolgt oft über die Clientlaufwerkzuordnung und USB-Unterstützung wird daher nicht benötigt.

  Wichtig: Einige Viren werden aktiv mit allen Typen des Massenspeichers übertragen. Überlegen Sie genau, ob die Verwendung von Massenspeichergeräten entweder über die Clientlaufwerkzuordnung oder die USB-Unterstützung im Unternehmen wirklich erforderlich ist. Zur Verringerung dieses Risikos kann auf dem Server konfiguriert werden, dass Dateien über die Clientlaufwerkzuordnung ausgeführt werden.

- Content Security (Geräteklasse 0d)

  Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.

- Personal Healthcare (Geräteklasse 0f)

  Hierzu gehören Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.

- Anwendung und herstellerspezifisch (Geräteklasse fe und ff)

  Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

In der Standardeinstellung nicht zugelassene USB-Geräteklassen

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a)

  Umfasst Modems, ISDN-Adapter, Netzwerkkarten und einige Telefone und Faxgeräte.

  Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein Gerät möglicherweise die Verbindung zum virtuellen Desktop bereitstellt.

- HID (Human Interface Devices) (Geräteklasse 03)

  Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktabletts, Sensoren, Game Controller, Tasten und Steuerfunktionen.

  Die Unterklasse 01 wird “Boot Interface”-Klasse genannt und für Tastaturen und Mäuse verwendet.

  USB-Tastaturen (Klasse 03, Unterklasse 01, Protokoll 1) oder USB-Mäuse (Klasse 03, Unterklasse 01, Protokoll 2) werden von der USB-Standardrichtlinie nicht zugelassen. Begründung: Die meisten Tastaturen und Mäuse können auch ohne USB-Unterstützung genutzt werden. Sie werden sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.

- USB-Hub (Geräteklasse 09)

  Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.

- Chipkarte (Smartcard) (Geräteklasse 0b)

  Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.

  Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.

- Video (Geräteklasse 0e)

  Die Videoklasse umfasst Geräte, mit denen Videos und mit Video zusammenhängendes Material manipuliert werden, u. a. Webcams, digitale Camcorder, analoge Videokonverter, einige Fernsehtuner und einige digitale Kameras, die Videostreaming unterstützen.

  Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung.

- Kabelloser Controller (Geräteklasse e0)

  Hierzu gehören viele kabellose Controller, u. a. Ultra-Breitband-Controller und Bluetooth.

  Einige dieser Geräte stellen u. U. wichtigen Netzwerkzugang bereit oder schließen wichtige Peripheriegeräte an, z. B. Bluetooth-Tastaturen oder -Mäuse.

  Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

Aktualisieren der für Remoting verfügbaren USB-Geräteliste

Sie können den Umfang der USB-Geräte, die für Remoting auf Desktops zur Verfügung stehen, aktualisieren, indem Sie die Liste der Standardregeln in der Datei usb.conf auf dem Benutzergerät unter

$ICAROOT/ bearbeiten.

Sie aktualisieren die Liste, indem Sie neue Richtlinienregeln hinzufügen, die USB-Geräte, die nicht Teil des Standardumfangs sind, zulassen oder ablehnen. Von einem Administrator auf diese Weise erstellte Regeln steuern, welche Geräte dem Server angeboten werden. Die Regeln auf dem Server steuern dann, welche Geräte akzeptiert werden.

Die standardmäßige Richtlinienkonfiguration für nicht zulässige Geräte lautet folgendermaßen:

DENY: class=09 # Hub-Geräte

DENY: class=03 subclass=01 # HID-Bootgerät (Tastaturen und Mäuse)

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless-Controller

DENY: class=02 # Kommunikations- und CDC-Steuerung

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC-Daten

ALLOW: # Letzter Ausweg: alles andere zulassen

Erstellen von USB-Richtlinienregeln

Tipp: Wenn Sie Richtlinienregeln erstellen, verwenden Sie die USB-Klassencodes. Sie finden sie auf der USB-Website unter http://www.usb.org/. Richtlinienregeln in usb.conf auf dem Benutzergerät haben das Format {ALLOW:|DENY:} gefolgt von einer Reihe von Ausdrücken, die auf Werten für die folgenden Tags basieren:

Tag	Beschreibung
VID	Vendor-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie eine Richtlinienregel erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen, die als Trennzeichen verwendet werden, werden ignoriert. Sie dürfen aber nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class=08 SubClass=05 eine gültige Regel; Deny: Class=0 8 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.

Beispiel

Das folgende Beispiel zeigt einen Abschnitt der Datei usb.conf auf dem Benutzergerät. Um diese Regeln zu implementieren, müssen dieselben Regeln wie auf dem Server vorhanden sein.

ALLOW: VID=1230 PID=0007 # Weitere Industrie, Weiteres Flash-Laufwerk

DENY: Class=08 SubClass=05 # Massenspeichergeräte

DENY: Class=0D # Alle Sicherheitsgeräte

Konfigurieren von Startmodi

Mit “Desktop Appliance Mode” können Sie anpassen, wie ein virtueller Desktop zuvor angeschlossene USB-Geräte behandelt. Stellen Sie auf jedem Benutzergerät in der Datei $ICAROOT/config/module.ini im Abschnitt WfClient die Option DesktopApplianceMode = Boolean wie folgt ein.

TRUE	USB-Geräte, die bereits angeschlossen sind, starten, vorausgesetzt dass das Gerät nicht durch eine Ablehnungsregel in den USB-Richtlinien auf dem Server (Registrierungseintrag) oder dem Benutzergerät (Konfigurationsdatei der Richtlinienregeln) deaktiviert ist.
FALSE	Keine USB-Geräte starten.

Bloomberg-Tastaturumleitung

Die Bloomberg-Tastaturumleitung kann über eine generische USB-Umleitung durchgeführt werden.

Konfigurieren der Bloomberg v4-Tastatur über die generische USB-Umleitung auf der Clientseite:

Als Voraussetzung muss die Richtlinie im Delivery Controller der Domäne (DDC) aktiviert sein.

1. Suchen Sie die VID und PID der Bloomberg-Tastatur. In Debian und Ubuntu führen Sie hierfür den folgenden Befehl aus:

   ```
   lsusb
   ```

2. Wechseln Sie zu $ICAROOT und bearbeiten Sie die Datei usb.conf.
3. Fügen Sie folgenden Eintrag zur Datei usb.conf hinzu, um die USB-Umleitung für die Bloomberg-Tastatur zuzulassen und speichern Sie die Datei.

   ALLOW: vid=1188 pid=9545

4. Starten Sie den ctxusbd-Daemon auf dem Client neu. In Debian und Ubuntu führen Sie hierfür den folgenden Befehl aus:

   ```
   systemctl neustart ctxusbd
   ```

5. Starten Sie eine Clientsitzung. Stellen Sie sicher, dass die Sitzung im Fokus ist, während Sie die umzuleitende Bloomberg v4-Tastatur anschließen.

Steigern der Leistung über Verbindungen mit geringer Bandbreite

Citrix empfiehlt die Verwendung der aktuellen XenApp- oder XenDesktop-Version auf dem Server und der aktuellen Receiver-Version auf dem Benutzergerät.

Wenn Sie eine Verbindung mit geringer Bandbreite verwenden, können Sie durch eine geänderte Receiver-Konfiguration und -Verwendung eine Verbesserung der Leistung erzielen.

- **Konfigurieren Sie die Receiver-Verbindung**: Konfigurieren der Receiver-Verbindungen kann die Bandbreite reduzieren, die für ICA erforderlich ist und die Leistung verbessern
- **Ändern Sie die Verwendung von Receiver**: Durch Ändern der Verwendung von Receiver können Sie die Bandbreite verringern, die für eine schnelle Verbindung benötigt wird.
- **Aktivieren Sie UDP-Audio**: Dieses Feature kann für eine gleichmäßige Latenz bei VoIP-Verbindungen (Voice over IP) in stark ausgelasteten Netzwerken sorgen.
- **Verwenden Sie die neuesten Versionen von XenApp und Receiver für Linux**: Citrix erweitert und verbessert die Leistung mit jedem Release und für viele Leistungsfeatures ist die neueste Receiver- und Serversoftware erforderlich

Konfigurieren von Verbindungen

Auf Geräten mit beschränkter Rechenleistung oder geringer Bandbreite gibt es entweder Einbußen bei Leistung oder Funktionalität. Benutzer und Administratoren können eine akzeptable Mischung

aus umfassender Funktionalität und interaktiver Leistung wählen. Wenn Sie eine oder mehrere der folgenden Änderungen – häufig auf dem Server anstatt auf dem Benutzergerät – vornehmen, kann dies die von der Verbindung benötigte Bandbreite verringern und die Leistung verbessern:

- **Aktivieren Sie die SpeedScreen-Latenzreduktion**: SpeedScreen-Latenzreduktion steigert die Leistung bei Verbindungen mit hoher Latenz, da schnell Feedback für eingegebene Daten und Mausklicks geboten wird. Aktivieren Sie dieses Feature mit dem SpeedScreen-Latenzreduktionsmanager. In der Standardeinstellung ist dies in Receiver bei Verbindungen mit hoher Latenz für die Tastatur deaktiviert und nur für die Maus aktiviert. Weitere Informationen finden Sie in der Dokumentation Citrix Receiver for Linux OEM's Reference Guide.
- **Aktivieren Sie die Datenkomprimierung**: Mit der Datenkomprimierung wird die in der Verbindung übertragene Datenmenge reduziert. Für das Komprimieren und Dekomprimieren werden zusätzliche Prozessorressourcen benötigt. Dies kann jedoch die Leistung bei Verbindungen mit eingeschränkter Bandbreite erhöhen. Verwenden Sie die Citrix Richtlinieneinstellungen Audioqualität und Bildkomprimierung, um dieses Feature zu aktivieren.
- **Reduzieren Sie die Fenstergröße**: Ändern Sie die Fenstergröße auf die kleinste Größe, mit der Sie noch gut arbeiten können. Legen Sie auf der XenApp Services-Site die Sitzungsoptionen fest.
- **Reduzieren Sie die Farbanzahl**: Reduzieren Sie die Anzahl der Farben auf 256. Legen Sie auf der XenApp und XenDesktop-Site die Sitzungsoptionen fest.
- **Verringern Sie die Audioqualität**: Wenn die Audiozuordnung aktiviert ist, verringern Sie die Audioqualität mit der Citrix Richtlinieneinstellung "Audioqualität" auf die niedrigste Einstellung.

Aktivieren von UDP-Audio

UDP-Audio kann die Qualität von Telefonanrufen über das Internet verbessern. Dabei wird UDP (User Datagram Protocol) statt TCP (Transmission Control Protocol) verwendet.

Beachten Sie Folgendes:

- UDP-Audio ist nicht für verschlüsselte Sitzungen verfügbar (solche, die TLS- oder ICA-Verschlüsselung verwenden). In solchen Sitzungen verwenden Audioübertragungen TCP.
- Die ICA-Kanalpriorität kann UDP-Audio beeinflussen.

1. Stellen Sie die folgenden Optionen in module.ini im Abschnitt ClientAudio ein:
   - Setzen Sie EnableUDPAudio auf "True". Standardeinstellung ist "False", wodurch UDP-Audio deaktiviert wird.
   - Geben Sie Minimum und Maximum für die Portnummern von UDP-Audioverkehr mit UDPAudioPortLow und UDPAudioPortHigh an. Standardmäßig werden Ports 16500 bis 16509 verwendet.
2. Stellen Sie Client- und Serveraudioeinstellungen wie folgt ein, sodass die resultierende Audioqualität "Mittel" ist (also weder hoch noch niedrig).

		Audioqualität auf dem Client	Audioqualität auf dem Client	Audioqualität auf dem Client
		Hoch	Mittel	Niedrig
Audioqualität auf dem Server	Hoch	Hoch	Mittel	Niedrig
Audioqualität auf dem Server	Mittel	Mittel	Mittel	Niedrig
Audioqualität auf dem Server	Niedrig	Niedrig	Niedrig	Niedrig

Ändern der Verwendungsweise von Receiver

Die ICA-Technologie ist äußerst optimiert und stellt normalerweise keine hohen Anforderungen an CPU und Bandbreite. Wenn Sie jedoch eine Verbindung mit sehr geringer Bandbreite verwenden, beachten Sie zur Aufrechterhaltung der Leistung Folgendes:

- **Vermeiden Sie den Zugriff auf große Dateien unter Verwendung der Clientlaufwerkszuordnung**: Wenn Sie über die Clientlaufwerkzuordnung auf eine große Datei zugreifen, wird diese über die Serververbindung übertragen. Bei langsamen Verbindungen kann dies sehr lange dauern.
- **Vermeiden Sie das Drucken von großen Dokumenten auf lokalen Druckern**: Wenn Sie ein Dokument auf einem lokalen Drucker drucken, wird die zu druckende Datei über die Serververbindung übertragen. Bei langsamen Verbindungen kann dies sehr lange dauern.
- **Vermeiden Sie das Abspielen von Multimediainhalten**. Die Wiedergabe von Multimediainhalten benötigt viel Bandbreite und kann die Leistung reduzieren.

Steigern der Multimedialeistung

Receiver enthält zahlreiche Technologien, die in den heutigen medienreichen Benutzerumgebungen eine High-Definition-Benutzererfahrung ermöglichen. Diese verbessern die Benutzererfahrung bei Verbindungen mit gehosteten Anwendungen und Desktops:

- HDX MediaStream Windows Media-Umleitung
- HDX MediaStream Flash-Umleitung
- HDX RealTime-Webcamvideokomprimierung
- H.264-Unterstützung

Konfigurieren von HDX MediaStream-Windows Media-Umleitung

Mit HDX MediaStream Windows Media-Umleitung sind keine hohen Bandbreiten mehr erforderlich, um auf virtuellen Desktops, auf die von Linux-Benutzergeräten zugegriffen wird, Multimediainhalte aufzunehmen und wiederzugeben. Mit Windows Media-Umleitung werden die Laufzeitdateien von Medieninhalten auf dem Benutzergerät statt auf dem Server abgespielt. Dies führt zu einer Reduktion der Bandbreitenanforderungen beim Abspielen von Multimediadateien.

Windows Media-Umleitung verbessert die Leistung des Windows Media-Players und anderer kompatibler Player, die auf virtuellen Windows-Desktops ausgeführt werden. Es werden eine Vielzahl von Formaten unterstützt, u. a.:

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

Citrix Receiver enthält eine textbasierte Übersetzungstabelle, MediaStreamingConfig.tbl, die Windows-spezifische Medienformat-GUIDs in MIME-Typen übersetzt, die GStreamer verwenden kann. Sie können die Übersetzungstabelle bearbeiten, um folgende Aktionen auszuführen:

- Hinzufügen bisher unbekannter oder nicht unterstützter Medienfilter/-dateiformate zur Übersetzungstabelle
- Blockieren problematischer GUIDs, um Fallback auf serverseitige Wiedergabe zu erzwingen
- Hinzufügen zusätzlicher Parameter zu vorhandenen MIME-Strings, um Probleme mit schwierigen Formaten durch Ändern der GStreamer-Parameter eines Streams beheben zu können
- Verwalten und Bereitstellen benutzerdefinierter Konfigurationen basierend auf den Mediendateitypen, die von GStreamer auf einem Benutzergerät unterstützt werden

Mit dem clientseitigem Inhaltabruf können Sie zulassen, dass das Benutzergerät Medien direkt von URLs im Format http://, <mms://> oder <rtsp://> streamt, statt die Medien über einen Citrix Server zu streamen. Der Server leitet das Benutzergerät an die Medien um und sendet Steuerbefehle (einschließlich Wiedergabe, Pause, Stopp, Lautstärke, Suchen). Der Server verarbeitet jedoch keine Mediendaten. Dieses Feature erfordert erweiterte GStreamer-Multimediabibliotheken auf dem Gerät.

Einrichten von HDX Mediastream Windows Media-Umleitung

1. Installieren Sie GStreamer 0.10, ein Open-Source-Multimedia-Framework, auf jedem erforderlichen Benutzergerät. Normalerweise installieren Sie GStreamer vor Citrix Receiver, damit der Installationsvorgang Citrix Receiver für die Verwendung von GStreamer konfiguriert.

   GStreamer ist in den meisten Linux-Distributionen enthalten. Ansonsten können Sie GStreamer auch von http://gstreamer.freedesktop.org herunterladen.

2. Um den clientseitigen Inhaltsabruf zu aktivieren, installieren Sie die erforderlichen Protocol Source-*Plug-Ins* für die Dateitypen, die Benutzer auf dem Gerät wiedergeben. Sie prüfen mit dem Hilfsprogramm gst-launch, ob ein Plug-In installiert und funktionsbereit ist. Wenn gst-launch die URL wiedergeben kann, ist das erforderliche Plug-In funktionsbereit. Führen Sie beispielsweise gst-launch-0.10 playbin2 uri=http://example-source/file.wmv aus und vergewissern Sie sich, dass das Video einwandfrei wiedergegeben wird.
3. Wählen Sie bei der Installation von Citrix Receiver auf dem Gerät die Option “GStreamer”, wenn Sie das Tarball-Skript verwenden. Für DEB- und RPM-Pakete erfolgt die Auswahl automatisch.

Beachten Sie Folgendes beim clientseitigen Inhaltsabruf:

- Standardmäßig ist dieses Feature aktiviert. Sie können es in All-Regions.ini im Abschnitt “Multimedia” mit der Option SpeedScreenMMACSFEnabled deaktivieren. Wenn Sie für diese Option “False” einstellen, wird die Windows Media-Umleitung für die Medienverarbeitung verwendet.
- Standardmäßig verwenden alle MediaStream-Features das GStreamer-Protokoll “playbin2”. Sie können auf ein früheres playbin-Protokoll für alle MediaStream-Features außer dem clientseitigen Inhaltsabruf zurückgehen, der weiter playbin2 verwendet. Stellen Sie dazu in All-Regions.ini im Abschnitt “Multimedia” die Option SpeedScreenMMAEnablePlaybin2 ein.
- Receiver erkennt nicht Playlistdateien oder Streamkonfigurationsdateien wie ASX- oder NSC-Dateien. Benutzer müssen eine Standard-URL angeben, die nicht auf diese Dateitypen verweist. Überprüfen Sie mit gst-launch, ob eine URL gültig ist.

Beachten Sie bei GStreamer 1.0:

- GStreamer 0.10 wird standardmäßig für die HDX MediaStream Windows Media-Umleitung verwendet. GStreamer 1.0 wird nur verwendet, wenn GStreamer 0.10 nicht verfügbar ist.
- Wenn Sie GStreamer 1.0 verwenden möchten, folgen Sie den nachstehenden Anweisungen:

1. Navigieren Sie zum Installationsverzeichnis der GStreamer-Plug-Ins. Der Speicherort der Plug-Ins hängt von Ihrer Distribution, der Architektur des Betriebssystems und der Installationsweise von GStreamer ab. Der Installationspfad ist normalerweise /usr/lib/x86_64-linux-gnu/gstreamer-1.0 oder $HOME/ .local/share/gstreamer-1.0.
2. Navigieren Sie zum Installationsverzeichnis von Citrix Receiver für Linux. Das Standardverzeichnis für Installationen durch privilegierte Benutzer (root) ist /opt/Citrix/ICAClient. Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist $HOME/ICAClient/platform (wobei “platform” z. B. linuxx64 sein kann). Weitere Informationen finden Sie unter Installation und Einrichtung.
3. Installieren Sie libgstflatstm1.0.so, indem Sie einen symbolischen Link im Verzeichnis der GStreamer-Plug-Ins erstellen: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflat
Für diesen Schritt sind u. U. erhöhte Berechtigungen erforderlich, z. B. mit sudo.
4. Verwenden Sie gst_play1.0 als Player: ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play.
Für diesen Schritt sind u. U. erhöhte Berechtigungen erforderlich, z. B. mit sudo.

- Wenn Sie GStreamer 1.0 HDX RealTime-Webcamvideokomprimierung verwenden möchten, verwenden Sie gst_read1.0 als Leser: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Konfigurieren der HDX MediaStream-Flash-Umleitung

HDX MediaStream-Flash-Umleitung sorgt dafür, dass Adobe Flash-Inhalte lokal auf den Benutzergeräten wiedergegeben werden. So erhalten Benutzer High Definition-Audio und -Video, ohne dass die Bandbreitenanforderungen steigen.

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt. Weitere Informationen finden Sie unter Systemanforderungen.
2. Fügen Sie in der Datei wfclient.ini im Abschnitt [WFClient] (für alle Verbindungen eines bestimmten Benutzers) oder in der Datei All_Regions.ini im Abschnitt [Client Engine\Application Launching] (für alle Benutzer in Ihrer Umgebung) folgende Parameter hinzu:
   - **HDXFlashUseFlashRemoting=Ask|Never|Always**

     Aktiviert HDX MediaStream für Flash auf dem Benutzergerät. Die Standardeinstellung ist **Never**. Benutzer werden beim Aufrufen von Webseiten mit Flash-Inhalten in einem Dialogfeld gefragt, ob sie diese optimieren möchten.
   - **HDXFlashEnableServerSideContentFetching=Disabled|Enabled**

     Aktiviert oder deaktiviert serverseitigen Inhaltsabruf für Receiver. Die Standardeinstellung ist **Disabled**.
   - **HDXFlashUseServerHttpCookie=Disabled|Enabled**

     Aktiviert oder deaktiviert HTTP-Cookie-Umleitung. Die Standardeinstellung ist **Disabled**.
   - **HDXFlashEnableClientSideCaching=Disabled|Enabled**

     Aktiviert oder deaktiviert clientseitige Zwischenspeicherung für von Receiver abgerufene Inhalte. Die Standardeinstellung ist **Enabled**.
   - **HDXFlashClientCacheSize= [25-250]**

     Definiert die Größe des Clientcaches in MB. Die Größe kann zwischen 25 MB und 250 MB liegen. Wenn die maximale Größe erreicht ist, werden bereits im Cache vorhandene Daten gelöscht, um Platz für neue Inhalte zu schaffen. Die Standardeinstellung ist **100**.
   - **HDXFlashServerSideContentCacheType=Persistent|Temporary|NoCaching**

     Definiert den Zwischenspeicherungstyp, den Receiver für mit serverseitigem Inhaltsabruf abgerufene Inhalte verwendet. Die Standardeinstellung ist **Persistent**.

Hinweis: Dieser Parameter ist nur erforderlich, wenn **HDXFlashEnableServerSideContentFetching** auf **Enabled** gesetzt ist.

3. Flash-Umleitung ist standardmäßig deaktiviert. Ändern Sie in der Datei /config/module.ini die Einstellung FlashV2=Off in FlashV2=On, um das Feature zu aktivieren.

Konfigurieren Sie HDX RealTime-Webcamvideokomprimierung

HDX RealTime bietet Webcamvideokomprimierung, mit der die Bandbreiteneffizienz während Videokonferenzen verbessert wird. So erhalten Benutzer optimale Leistung, wenn sie Anwendungen wie GoToMeeting mit HD Faces oder Skype for Business verwenden.

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt.
2. Stellen Sie sicher, dass der virtuelle Multimedia-Kanal aktiviert ist. Öffnen Sie hierzu die Konfigurationsdatei module.ini im Verzeichnis $ICAROOT/config und überprüfen Sie, ob im Abschnitt [ICA3.0] die Option “MultiMedia” auf “On” festgelegt ist.
3. Aktivieren Sie die Audioeingabe durch Klicken auf Mikrofon und Webcam verwenden auf der Seite Mikrofon und Webcam des Dialogfelds “Einstellungen”.

Deaktivieren Sie die HDX RealTime-Webcamvideokomprimierung

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen müssen Benutzer Webcams mit USB-Unterstützung anschließen. Dazu müssen Sie die folgenden Schritte ausführen:

- Deaktivieren Sie die HDX RealTime-Webcamvideokomprimierung
- Aktivieren Sie die USB-Unterstützung für Webcams

1. Fügen Sie der entsprechenden INI-Datei im Abschnitt [WFClient] den folgenden Parameter hinzu:

   HDXWebCamEnabled=Off

   Weitere Informationen finden Sie unter Anpassen von Receiver mit Konfigurationsdateien.

2. Öffnen Sie die Datei usb.conf, die normalerweise unter $ICAROOT/usb.conf ist.
3. Entfernen Sie die folgende Zeile oder kommentieren Sie sie aus:

   ```
   DENY: class=0e ## UVC (default via HDX RealTime Webcam Video Compression
   )
   ```

4. Speichern und schließen Sie die Datei.

Konfigurieren der H.264-Unterstützung

Receiver unterstützt die H.264-Grafikanzeige einschließlich der von XenDesktop 7 bereitgestellten HDX 3D Pro-Technologie. Bei dieser Unterstützung wird der standardmäßig aktivierte Tiefenkomprimierungscodec verwendet. Dieses Feature liefert im Vergleich zum JPEG-Codec eine bessere Leistung bei reichhaltigen und professionellen Grafikanwendungen in WAN-Netzwerken.

Befolgen Sie die Anweisungen in diesem Abschnitt, um das Feature zu deaktivieren und zur Grafikverarbeitung stattdessen den JPEG-Codec zu verwenden. Sie können auch die Textprotokollierung deaktivieren und gleichzeitig den Tiefenkomprimierungscodec weiterverwenden. So lassen sich CPU-Kosten während der Verarbeitung von Grafiken mit komplexen Bildern aber relativ wenig oder unwichtigem Text senken.

Wichtig: Verwenden Sie zum Konfigurieren dieses Features keine verlustfreie Einstellung in der XenDesktop-Richtlinie
“Bildqualität”. Wenn Sie eine verlustfreie Einstellung wählen, ist die H.264-Codierung auf dem Server deaktiviert und funktioniert für Receiver nicht.

Deaktivieren der Unterstützung für den Tiefenkomprimierungscodec

Legen Sie in wfclient.ini für H264Enabled die Einstellung False fest. Dadurch wird auch die Textprotokollierung deaktiviert.

Ausschließliches Deaktivieren der Textprotokollierung

Legen Sie bei aktiviertem Tiefenkomprimierungscodec in wfclient.ini TextTrackingEnabled auf False fest.

Optimieren der Leistung für Bildschirmkacheln

Sie können die Verarbeitung von JPEG-codierten Bildschirmkacheln mit den Features Bitmapdecodierung direkt zum Bildschirm, Batchverarbeitung der Kacheldecodierung und Verzögertes XSync verbessern.

1. Stellen Sie sicher, dass Ihre JPEG-Bibliothek diese Features unterstützt.
2. Setzen Sie in wfclient.ini im Abschnitt Thinwire3.0 DirectDecode und BatchDecode auf True.

   Hinweis: Aktivieren der Batchverarbeitung für die Kacheldecodierung aktiviert gleichzeitig verzögertes XSync.

Aktivieren der Protokollierung für Retailbuilds

Aktivieren der Protokollierung für Retailbuilds von Citrix Receiver für Linux

1. Laden Sie den Citrix Receiver für Linux Retailbuild herunter und installieren Sie ihn auf Ihrer Linux-Maschine. Legen Sie dabei die ICAROOT-Umgebungsvariable auf den Installationsordner fest.
2. Für Citrix Receiver für Linux ist debug.ini im Konfigurationsordner von ICAROOT vorhanden. Erstellen Sie einen Symlink dieser Datei im $ICAROOT-Pfad, indem Sie an der Befehlszeile **> ln -s config/debug.ini debug.ini** eingeben.
3. Bearbeiten Sie die Datei debug.ini unter $ICAROOT und fügen Sie die erforderlichen Traceparameter im Abschnitt [wfica] hinzu.
4. Fügen Sie in der Datei $ICAROOT/config/module.ini am Ende des Abschnitts [WFClient] Folgendes hinzu: SyslogThreshold=7. Dadurch werden Protokolle aller Ebenen erstellt. Um nur Fehler zu protokollieren, setzen Sie SyslogThreshold auf 3.
5. Um Syslog-Traces zu erhalten, bearbeiten Sie die Syslog-Konfigurationsdatei. Wechseln Sie je nach Ihrer Linux-Distribution in die Datei /etc/rsyslog.conf (oder syslog.conf) und nehmen Sie die folgenden Änderungen vor:

   Um die lokale Protokollierung von allen Facilities zu aktivieren, stellen Sie sicher, dass die Auskommentierung der Zeile **$ModLoad imuxsock.so** am Anfang der Datei aufgehoben ist.

   Die nächsten zwei Änderungen in der Konfigurationsdatei sind für die Remoteprotokollierung erforderlich, jedoch **nicht** für die lokale Protokollierung in Syslog.

   Serverseitige Konfiguration: Entfernen Sie die Kommentarzeichen für die folgenden Zeilen in der Datei rsyslog.conf des Syslog-Servers:

   $ModLoad imtcp

   $InputTCPServerRun 10514

   Clientseitige Konfiguration: Fügen Sie die folgende Zeile hinzu, indem Sie localhost durch die IP-Adresse des Remoteservers ersetzen:
   ***.* @@localhost:10514**
6. Speichern Sie die Änderungen und starten Sie den Syslog-Dienst neu, indem Sie an der Befehlszeile **sudo service rsyslog restart** eingeben.
7. Alle Syslog-Protokolle werden unter /var/log gespeichert. Sie benötigen sudo-Zugriff, um Protokolle in diesem Ordner anzuzeigen oder zu bearbeiten. Die Protokolle werden in die Datei user-all-drivers_proxy22.log geschrieben. Sie können Pfad und Namen der Protokolldatei konfigurieren, indem Sie die folgende Zeile im Abschnitt RULES in der Datei rsyslog.cong bearbeiten:

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

   Sie können den Abschnitt RULES in der Syslog-Konfigurationsdatei bearbeiten. Wenn der

Abschnitt RULES nicht in Ihrer Syslog-Konfigurationsdatei vorhanden ist, können Sie den Abschnitt RULES aus der Beispieldatei rsyslog.conf in Ihre Syslog-Konfigurationsdatei einfügen.

Hinweis: Jedes Mal, wenn Sie die Datei rsyslog.conf bearbeiten, müssen Sie den Syslog-Dienst neu starten.

8. Starten Sie den Receiver-Prozess (./selfservice unter $ICAROOT). Wenn die Sitzung beendet wurde, finden Sie die Protokolldatei unter /var/log.
   Standardmäßig werden die Protokolle bei nachfolgenden Starts an die Protokolldatei angehängt. Um jeden Start zu verfolgen, bearbeiten Sie die Konfigurationsdatei vor jedem Start, um die Protokolldatei zu ändern und den rsyslog-Dienst neu zu starten.

> **Hinweis**
>
> Um die Ablaufverfolgung zu aktivieren, ändern Sie die folgenden Parameter in der Datei **$ICAROOT/debug.ini**:
>
> - Protokollierung für Connection Center: Ändern Sie im Abschnitt [conncenter] “traceClasses” in “+TC_NCS”.
> - Protokollierung für Graphics (Thinwire): Ändern Sie im Abschnitt [wfica] “traceClasses” in “+TC_TW”.
> - Protokollierung für EUEM: Ändern Sie im Abschnitt [wfica] “traceClasses” in “+TC_CLIB”.
>
> Um die Ablaufverfolgung zu deaktivieren, ändern Sie die Einträge unter “traceClasses” in null.
>
> Beispiel:
>
> [wfica]
>
> traceFlags =
>
> traceClasses =
>
> traceFeatures =
>
> traceFile = clb.log.$$
>
> traceBufferSize = 65536

Konfigurieren der Layoutspeicherung im Multimonitormodus

Mit diesem Feature werden die Angaben zum Bildschirmlayout einer Sitzung über Endpunkte hinweg beibehalten. Die Sitzung wird dann gemäß Konfiguration stets auf dem- oder denselben Monitor(en) angezeigt.

Voraussetzung

Dieses Feature erfordert Folgendes:

- StoreFront v3.15 oder höher.
- Wenn .ICAClient bereits im Basisordner des aktuellen Benutzers vorhanden ist:

  Löschen Sie die Datei All_Regions.ini.

  oder

  Zum Beibehalten der Datei AllRegions.ini fügen Sie die folgenden Zeilen am Ende des Abschnitts [Client Engine\Application Launching] hinzu:

  SubscriptionUrl =

  PreferredWindowsBounds =

  PreferredMonitors=

  PreferredWindowState=

  SaveMultiMonitorPref=

Wenn der Ordner .ICAClient nicht vorhanden ist, weist dies auf eine Neuinstallation des Receivers hin. In diesem Fall wird die Standardeinstellung für das Feature beibehalten.

Anwendungsfälle

- Starten Sie eine Sitzung auf einem beliebigen Bildschirm im Fenstermodus und speichern Sie die Einstellung.
  Wenn Sie die Sitzung erneut starten, wird sie im selben Modus, auf demselben Bildschirm und an derselben Position angezeigt.
- Starten Sie eine Sitzung auf einem beliebigen Bildschirm im Vollbildmodus und speichern Sie die Einstellung.
  Wenn Sie die Sitzung erneut starten, wird sie im Vollbildmodus auf demselben Bildschirm angezeigt.
- Ziehen Sie eine Sitzung im Fenstermodus über mehrere Bildschirme und wechseln Sie dann in den Vollbildmodus. Die Sitzung wird dann im Vollbildmodus auf allen Bildschirmen angezeigt.
  Wenn Sie die Sitzung erneut starten, wird sie im Vollbildmodus über alle Bildschirme hinweg angezeigt.

> **Hinweis**
>
> Das Layout wird bei jeder Speicherung überschrieben und nur auf dem aktiven StoreFront gespeichert.
>
> Wenn Sie mehrere Desktopsitzungen von demselben StoreFront-Store auf unterschiedlichen Bildschirmen starten, werden beim Speichern des Layouts in einer Sitzung die Layoutinformationen aller Sitzungen gespeichert.

Konfigurieren des Features zur Layoutspeicherung

Aktivieren der Layoutspeicherung:

1. Installieren Sie StoreFront Version 3.15 oder höher (gleich oder höher als v3.15.0.12) auf einem kompatiblen Delivery Controller (DDC).
2. Laden Sie den Retailbuild von Citrix Receiver für Linux 13.10 von der Downloadseite herunter und installieren Sie ihn auf der Linux-Maschine.
3. Legen Sie die ICAROOT-Umgebungsvariable auf den Installationsort fest.
4. Überprüfen Sie, ob die Datei **All_Regions.ini** im Ordner **.ICAClient** vorhanden ist. Wenn ja, löschen Sie sie.
5. Suchen Sie in der Datei **$ICAROOT/config/All_Regions.ini** nach dem Feld **SaveMultiMonitorPref**. Der Standardwert in diesem Feld ist "True" (das Feature ist aktiviert). Ändern Sie den Wert in "False", um das Feature auszuschalten.
   Wenn Sie den Wert für **SaveMultiMonitorPref** ändern, müssen Sie die Datei **All_Regions.ini** im Ordner **.ICAClient** löschen, um Wertkonflikte und eine mögliche Profilsperrung zu verhindern. Aktivieren oder deaktivieren Sie das Flag **SaveMultiMonitorPref**, bevor Sie Sitzungen starten.
6. Starten Sie eine neue Desktopsitzung.
7. Klicken Sie in der Desktop Viewer-Symbolleiste auf **Layout speichern**, um das aktuelle Sitzungslayout zu speichern. Am rechten unteren Bildrand wird die Speicherung in einer Meldung bestätigt.
   Wenn Sie auf "Layout speichern" klicken, wird das Symbol grau angezeigt. Dies zeigt an, dass ein Speichervorgang ausgeführt wird. Nach der Speicherung des Layouts wird das Symbol wieder normal angezeigt.
   Wenn das Symbol für längere Zeit ausgegraut ist, finden Sie im Knowledge Center-Artikel CTX235895 Informationen zur Fehlerbehebung.
8. Trennen Sie die Sitzung oder melden Sie sich ab.
   Starten Sie die Sitzung erneut. Sie wird dann im selben Modus, auf demselben Bildschirm und an derselben Position angezeigt.

Einschränkungen und nicht unterstützte Szenarien

- Für Sitzungen im Fenstermodus wird das Speichern eines Layouts über mehrere Bildschirme hinweg aufgrund von Einschränkungen beim Linux-Anzeigemanager nicht unterstützt.
- Das bildschirmübergreifende Speichern von Sitzungsinformationen bei Bildschirmen mit unterschiedlicher Auflösung wird in diesem Release nicht unterstützt und kann zu unvorhersehbarem Verhalten führen.
- Kundenbereitstellungen mit mehreren Storefront-Stores

Verwenden von Citrix Virtual Desktops auf zwei Monitoren

1. Wählen Sie den Desktop Viewer aus und klicken Sie auf den Pfeil nach unten.
2. Wählen Sie **Fenster**.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die beiden Monitore. Stellen Sie sicher, dass etwa die Hälfte des Bildschirms in jedem Monitor angezeigt wird.
4. Wählen Sie auf der Symbolleiste des Citrix Virtual Desktops die Option **Vollbild** aus.

   Der Bildschirm ist nun auf beide Monitore erweitert.

Verbessern der Benutzererfahrung

March 11, 2019

Sie können die Erfahrung der Benutzer mit den folgenden unterstützten Features verbessern:

Festlegen von Einstellungen

Sie können Einstellungen festlegen, indem Sie im Citrix Workspace-App-Menü auf "Einstellungen" klicken. Sie können steuern, wie Desktops angezeigt werden, Verbindung mit verschiedenen Anwendungen und Desktops herstellen und den Datei- und Gerätezugriff verwalten.

Verwalten eines Kontos

Für den Zugriff auf Desktops und Anwendungen benötigen Sie ein XenDesktop- oder XenApp-Konto. Ihr IT-Helpdesk fordert Sie u. U. auf, zu diesem Zweck ein Konto zu Citrix Workspace hinzuzufügen. Oder Sie werden aufgefordert, einen anderen NetScaler Gateway- oder Access Gateway-Server für ein vorhandenes Konto zu verwenden. Sie können Konten auch aus Citrix Workspace entfernen.

1. Führen Sie auf der Seite Konten im Dialogfeld Einstellungen einen der folgenden Schritte aus:
   - Klicken Sie auf Hinzufügen, um ein Konto hinzuzufügen. Ihr Helpdesk stellt möglicherweise alternativ eine Provisioningdatei mit Kontoinformationen bereit, mit der Sie ein Konto erstellen können.
   - Zum Ändern der Details eines von dem Konto verwendeten Stores, z. B. des Standardgateways, klicken Sie auf Bearbeiten.
   - Zum Entfernen eines Kontos klicken Sie auf Entfernen.
2. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen. Es kann erforderlich sein, dass Sie sich bei dem Server authentifizieren.

Ändern der Anzeige Ihrer Desktops

Dieses Feature steht nicht für Citrix XenApp für UNIX-Sitzungen zur Verfügung.

Sie können Desktops über den ganzen Bildschirm hinweg auf dem Benutzergerät anzeigen (Vollbildmodus, Standardeinstellung) oder im Fenstermodus, d. h. in einem separaten Fenster.

- Wählen Sie im Dialogfeld "Einstellungen" auf der Seite "Allgemein" einen Modus mit der Option **Anzeige für Desktops**.

Die Citrix Workspace-App hat nun eine Funktion zum **Aktivieren des Desktop Viewer** über die Symbolleiste, sodass Sie die Fensterkonfiguration Ihrer Remotesitzung dynamisch anpassen können.

Desktop Viewer

Jedes Unternehmen hat andere Anforderungen. Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern. Die Benutzererfahrung beim Verbinden mit virtuellen Desktops und der Umfang der Benutzereingriffe beim Konfigurieren der Verbindungen hängen davon ab, wie Sie die Citrix Workspace-App für Linux einrichten.

Verwenden Sie Desktop Viewer für die Interaktion der Benutzer mit dem virtuellen Desktop. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario können Benutzer mit der Symbolleistenfunktionalität von Desktop Viewer in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore. Benutzer können zwischen Desktopsitzungen wechseln und auf einem Benutzergerät mit mehreren Desktops über mehrere XenDesktop-Verbindungen arbeiten. Zur bequemen Verwaltung einer Benutzersitzung gibt es Schaltflächen zum Minimieren aller Desktopsitzungen, zum Übermitteln der Tastenkombination Strg+Alt+Entf, zum Trennen der Sitzung und zum Abmelden.

Als Eingabehilfe von Desktop Viewer werden die Schaltflächen der Desktop Viewer-Symbolleiste in einem Popupfenster angezeigt, wenn Sie Strg+Alt+Untbr drücken.

Weitere Informationen zu erweiterten Konfigurationseinträgen zum Aktivieren oder Deaktivieren von Desktop Viewer oder zum Ändern der Zugriffstastenabfolge finden Sie im Linux OEM Guide.

Automatisches Wiederherstellen von Sitzungsverbindungen

Die Citrix Workspace-App kann Desktops und Anwendungen, deren Verbindung getrennt wurde (zum Beispiel bei einem Problem mit der Netzwerkinfrastruktur), wiederverbinden:

- Wählen Sie auf der Seite Allgemein im Dialogfeld Einstellungen eine Option unter Apps und Desktops wieder verbinden aus.

Steuern des Zugriffs auf lokale Dateien

Ein virtueller Desktop oder eine Anwendung benötigt ggf. Zugriff auf Dateien auf dem Gerät. Sie können diesen Zugriff steuern.

1. Wählen Sie auf der Seite Dateizugriff im Dialogfeld Einstellungen ein zugeordnetes Laufwerk und dann eine der folgenden Optionen aus:
   - Lesen/Schreiben: ermöglicht dem Desktop bzw. der Anwendung das Lesen bzw. Ändern der lokalen Dateien.
   - Leserechte: ermöglicht dem Desktop bzw. der Anwendung das Lesen, jedoch nicht das Ändern der lokalen Dateien.
   - Kein Zugriff: Der Desktop bzw. die Anwendung hat keinen Zugriff auf lokale Dateien.
   - Immer fragen: zeigt jedes Mal, wenn der Desktop oder die Anwendung Zugriff auf lokale Dateien benötigt, eine Aufforderung an.
2. Wenn Sie eine der Optionen, die Zugriff auf lokale Dateien ermöglichen, auswählen, können Sie außerdem beim Ansteuern von Speicherorten auf dem Benutzergerät Zeit einsparen. Klicken Sie auf Hinzufügen, geben Sie den Speicherort an und wählen Sie ein Laufwerk für die Zuordnung aus.

Einrichten eines Mikrofons oder einer Webcam

Sie können die Art und Weise, wie ein virtueller Desktop oder eine virtuelle Anwendung auf das lokale Mikrofon oder die Webcam zugreift, ändern:

Wählen Sie auf der Seite Mikrofon & Webcam im Dialogfeld Einstellungen eine der folgenden Optionen aus:

- Mikrofon und Webcam verwenden: ermöglicht das Verwenden von Mikrofon und Webcam durch den Desktop bzw. die Anwendung.
- Mikrofon und Webcam nicht verwenden: unterbindet das Verwenden von Mikrofon und Webcam durch den Desktop bzw. die Anwendung.

Einrichten von Flash Player

Sie können wählen, wie Flash-Inhalt angezeigt wird. Solcher Inhalt wird normalerweise in Flash Player angezeigt und enthält Animationen, Videos und Anwendungen:

Wählen Sie auf der Seite Flash im Dialogfeld Einstellungen eine der folgenden Optionen aus:

- Inhalt optimieren: steigert die Wiedergabequalität, wobei die Sicherheit vermindert werden kann.
- Inhalt nicht optimieren: liefert eine einfache Wiedergabequalität ohne Minderung der Sicherheit.

- Immer fragen: Bei jeder Anzeige von Flash-Inhalt wird eine Aufforderung angezeigt.

Konfigurieren der ClearType-Schriftartenglättung

Mit ClearType-Schriftartenglättung (auch Subpixel-Rendering von Schriftarten genannt) wird eine höhere Qualität der Schriftartenanzeige erzielt als bei traditioneller Schriftartenglättung oder Anti-Aliasing. Sie können dieses Feature ein- und ausschalten. Sie können auch die Art der Glättung über die folgende Einstellung im Abschnitt [WFClient] der jeweiligen Konfigurationsdatei angeben:

FontSmoothingType = Nummer

wobei Nummer einen der folgenden Werte haben kann:

Wert	Ergebnis
0	Die lokale Einstellung auf dem Gerät wird verwendet. Dieser Wert wird über die Einstellung “FontSmoothingTypePref” festgelegt.
1	Keine Glättung
2	Standardglättung
3	ClearType-Glättung (horizontale Subpixel-Technologie)

Sowohl Standardglättung als auch ClearType-Glättung können die Bandbreitenanforderungen der Citrix Workspace-App erhöhen.

Wichtig: Vom Server kann FontSmoothingType über die ICA-Datei konfiguriert werden. Dies hat Vorrang vor dem Wert in der [WFClient]. Wenn der Wert vom Server auf 0 festgelegt wird, wird die lokale Einstellung von einer anderen Einstellung im [WFClient] bestimmt:

FontSmoothingTypePref = Nummer

wobei Nummer einen der folgenden Werte haben kann:

Wert	Ergebnis
0	Keine Glättung
1	Keine Glättung
2	Standardglättung

Wert	Ergebnis
3	ClearType-Glättung (horizontale Subpixel-Technologie, Standard)

Konfigurieren der Umleitung spezieller Ordner

Jeder Benutzer hat zwei spezielle Ordner:

- Ordner “Desktop”
- Ordner “Dokumente” (“Eigene Dateien” unter Windows XP)

Mit der Funktion Umleitung spezieller Ordner können Sie den Speicherort der speziellen Ordner Ihrer Benutzer angeben, damit diese auch bei Verwendung verschiedener Servertypen und Serverfarmkonfigurationen bestehen bleiben. Dies ist wichtig, wenn Benutzer, die häufig den Standort wechseln, sich an Servern in unterschiedlichen Serverfarmen anmelden. Bei Benutzern, die einen festen Schreibtisch haben und sich an Servern anmelden, die sich in derselben Serverfarm befinden, ist die Umleitung spezieller Ordner selten notwendig.

Konfigurieren der Umleitung spezieller Ordner

Der Vorgang besteht aus zwei Schritten. Zuerst aktivieren Sie die Umleitung spezieller Ordner mit einem Eintrag in module.ini; anschließend geben Sie die Speicherorte der Ordner im Abschnitt [WFClient] wie im Folgenden beschrieben an:

1. Fügen Sie module.ini (z. B. $ICAROOT/config/module.ini) folgenden Text hinzu:

   [ClientDrive]

   SFRAllowed = True

2. Fügen Sie im Abschnitt [WFClient] (z. B. $HOME/.ICAClient/wfclient.ini) folgenden Text hinzu:

   DocumentsFolder = Dokumente

   DesktopFolder = Desktop

   Dabei sind Dokumente und Desktop die UNIX-Dateinamen, einschließlich vollständiger Pfade, der Verzeichnisse, die für die Benutzerordner “Dokumente” und “Desktop” verwendet werden sollen. Beispiel:

   DesktopFolder = $HOME/.ICAClient/desktop

   - Sie können alle Komponenten in dem Pfad als Umgebungsvariablen angeben, z. B. $HOME.

- Geben Sie für beide Parameter Werte an.
- Die angegebenen Verzeichnisse müssen über die Clientgerätzuordnung verfügbar sein. Das heißt, das Verzeichnis muss sich in der Struktur eines verknüpften Clientgeräts befinden.
- Verwenden Sie die Laufwerksbuchstaben C oder höher.

Einrichten der Server-zu-Client-Inhaltsumleitung

Mit der Server-zu-Client-Inhaltsumleitung können Administratoren festlegen, dass URLs in einer veröffentlichten Anwendung mit einer lokalen Anwendung geöffnet werden. Wenn Sie beispielsweise einen Link zu einer Webseite öffnen, während Sie Microsoft Outlook in einer Sitzung verwenden, wird die erforderliche Datei mit dem Browser auf dem Benutzergerät geöffnet. Diese Funktion ermöglicht Administratoren eine wesentlich effizientere Zuordnung der Citrix Ressourcen, wobei für Benutzer gleichzeitig eine Leistungsverbesserung erzielt wird.

Folgende URL-Typen können umgeleitet werden:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Ältere Real Player)

Wenn die Citrix Workspace-App für Linux keine geeignete Anwendung hat oder nicht direkt auf den Inhalt zugreifen kann, wird die URL mit der Serveranwendung geöffnet.

Die Server-zu-Client-Inhaltsumleitung ist auf dem Server konfiguriert und standardmäßig in der Citrix Workspace-App aktiviert, falls der Pfad RealPlayer und mindestens einen Browser wie Firefox, Mozilla oder Netscape enthält.

> **Hinweis**
>
> Weitere Informationen über RealPlayer für Linux finden Sie unter http://www.real.com/resources/unix/.

Aktivieren der Server-zu-Client-Inhaltsumleitung, wenn der Pfad weder einen Browser noch RealPlayer enthält

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Bearbeiten Sie im Abschnitt [Browser] die folgenden Einstellungen:

   Path=path

   Command=command

Dabei ist path das Verzeichnis, in dem sich die ausführbare Browserdatei befindet, und command ist der Name der ausführbaren Datei zur Verarbeitung umgeleiteter Browser-URLs, an die die vom Server gesendete URL angehängt wird. Beispiel:

$ICAROOT/nslaunch netscape,firefox,mozilla

Mit dieser Einstellung wird Folgendes festgelegt:

- Das Hilfsprogramm “nslaunch” wird ausgeführt, um die URL in ein vorhandenes Browserfenster zu verschieben.
- Jeder Browser in der Liste wird der Reihe nach ausprobiert, bis der Inhalt richtig angezeigt wird.

3. Bearbeiten Sie im Abschnitt [Player] die folgenden Einstellungen:

   Path=path

   Command=command

   Dabei ist path das Verzeichnis, in dem sich die ausführbare RealPlayer-Datei befindet, und command ist der Name der ausführbaren Datei zur Verarbeitung umgeleiteter Multimedia-URLs, an die die vom Server gesendete URL angehängt wird.

4. Speichern und schließen Sie die Datei.

> **Hinweis**
>
> Für beide Einstellungen für “Path” brauchen Sie nur das Verzeichnis anzugeben, in dem sich die ausführbaren Dateien für den Browser und RealPlayer befinden. Sie brauchen nicht dem vollständigen Pfad zu den ausführbaren Dateien anzugeben. Beispiel: Im Abschnitt [Browser] kann “Path” auf /usr/X11R6/bin statt auf /usr/X11R6/bin/netscape eingestellt sein. Außerdem können Sie mehrere Verzeichnisnamen in einer durch Doppelpunkte getrennten Liste angeben. Wenn diese Einstellungen nicht angegeben sind, wird die aktuelle Variable $PATH des Benutzers verwendet.

Deaktivieren der Server-zu-Client-Inhaltsumleitung in Citrix Workspace

1. Öffnen Sie die Konfigurationsdatei module.ini.
2. Ändern Sie die Einstellung CREnabled zu “Off”.
3. Speichern und schließen Sie die Datei.

Steuern des Tastaturverhaltens

Generieren der Tastenkombination Strg+Alt+Entfernen remote

1. Entscheiden Sie, welche Tastenkombination Strg+Alt+Entf auf dem remoten virtuellen Desktop generieren soll.
2. Konfigurieren Sie in der jeweiligen Konfigurationsdatei im Abschnitt WFClient UseCtrlAltEnd:
    - True bedeutet, dass mit Strg+Alt+Ende die Tastenkombination Strg+Alt+Entfernen an den Remotedesktop weitergegeben wird.
    - False bedeutet, dass mit Strg+Alt+Eingabetaste die Tastenkombination Strg+Alt+Entfernen an den Remotedesktop weitergegeben wird.

Verwenden von xcapture

Das Citrix Workspace-App-Paket enthält das Hilfsprogramm xcapture, mit dem Grafikdaten zwischen der Zwischenablage des Servers und nicht-ICCCM-kompatiblen X Windows-Anwendungen auf dem X-Desktop ausgetauscht werden können. Mit xcapture können Sie folgende Funktionen ausführen:

- Aufnehmen von Dialogfeldern und Bildschirmbereichen und Kopieren zwischen dem Benutzerdesktop (einschließlich nicht-ICCCM-kompatibler Anwendungen) und einer Anwendung, die in einem Verbindungsfenster ausgeführt wird
- Kopieren von Grafiken zwischen einem Verbindungsfenster und den X-Grafikbearbeitungsprogrammen xmag oder xv

Starten von xcapture von der Befehlszeile

Geben Sie an der Eingabeaufforderung /opt/Citrix/ICAClient/util/xcapture ein und drücken Sie die EINGABETASTE, wobei /opt/Citrix/ICAClient das Verzeichnis ist, in dem Sie die Citrix Workspace-App installiert haben.

Kopieren von Informationen vom Benutzerdesktop

1. Klicken Sie im xcapture-Dialogfeld auf Von Bildschirm. Der Cursor wird als Fadenkreuz dargestellt.
2. Wählen Sie eine der folgenden Optionen:
    - Auswählen eines Fensters: Verschieben Sie den Cursor auf das Fenster, das Sie kopieren möchten, und klicken Sie auf die mittlere Maustaste.
    - Auswählen eines Bereichs: Ziehen Sie den Cursor bei gedrückter linker Maustaste über den Bereich, den Sie kopieren möchten.
    - Aufheben der Auswahl: Klicken Sie mit der rechten Maustaste. Beim Ziehen der Maus können Sie die Auswahl aufheben, indem Sie vor dem Loslassen der mittleren oder linken Maustaste mit der rechten Maustaste klicken.
3. Klicken Sie im Dialogfeld xcapture auf Nach ICA. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.

4. Verwenden Sie nach dem Abschluss der Übertragung in einer über das Verbindungsfenster gestarteten Anwendung den entsprechenden Befehl zum Einfügen.

Kopieren von Informationen aus xv in eine Anwendung in einem Verbindungsfenster

1. Kopieren Sie die Informationen in “xv”.
2. Klicken Sie im Dialogfeld xcapture auf Von XV und dann auf Nach ICA. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.
3. Verwenden Sie nach dem Abschluss der Übertragung in einer über das Verbindungsfenster gestarteten Anwendung den entsprechenden Befehl zum Einfügen.

Kopieren von Informationen aus einer Anwendung in einem Verbindungsfenster in xv

1. Kopieren Sie die Informationen von der Anwendung im Verbindungsfenster.
2. Klicken Sie im Dialogfeld xcapture auf Von ICA und dann auf Nach XV. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.
3. Fügen Sie nach Abschluss der Übertragung die Informationen in “xv” ein.

Automatische Wiederverbindung von Benutzern

In diesem Abschnitt wird die automatische HDX Broadcast-Wiederverbindung von Clients beschrieben. Citrix empfiehlt, dass Sie dieses Feature mit der HDX Broadcast -Sitzungszuverlässigkeit verwenden.

Benutzer können von ICA-Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit dem Feature zur automatischen HDX Broadcast-Wiederverbindung von Clients kann die Citrix Workspace-App für Linux unabsichtlich getrennte Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden.

Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können. Mit einer festgelegten Anzahl von Versuchen versucht Citrix Workspace, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Wenn eine Benutzerauthentifizierung erforderlich ist, wird dem Benutzer bei der automatischen Wiederverbindung ein Dialogfeld zur Eingabe der Anmeldeinformationen angezeigt. Die automatische Wiederverbindung findet nicht statt, wenn Benutzer Anwendungen beenden, ohne sich abzumelden. Benutzer können sich nur mit getrennten Sitzungen wieder verbinden.

Standardmäßig wartet die Citrix Workspace-App für Linux 30 Sekunden, bevor versucht wird, die Verbindung zu einer getrennten Sitzung wiederherzustellen. Es werden drei Versuche gemacht, die Verbindung wiederherzustellen.

Bei einer Verbindung über Access Gateway steht ACR nicht zur Verfügung. Zum Schutz gegen Netzwerkausfälle sollten Sie sicherstellen, dass die Sitzungszuverlässigkeit auf dem Server und Client aktiviert und auf dem Access Gateway konfiguriert ist.

Weitere Informationen zur Konfiguration der automatische HDX Broadcast-Wiederverbindung von Clients finden Sie in der XenApp- und XenDesktop-Dokumentation.

Sicherstellen der Sitzungszuverlässigkeit

In diesem Abschnitt wird die HDX Broadcast-Sitzungszuverlässigkeit beschrieben, die standardmäßig aktiviert ist.

Die HDX Broadcast-Sitzungszuverlässigkeit bedeutet, dass den Benutzern das Fenster einer veröffentlichten Anwendung angezeigt wird, selbst wenn die Verbindung zur Anwendung unterbrochen ist. Beispiel: Benutzer, die eine drahtlose Verbindung verwenden und in einen Tunnel fahren, können die Verbindung im Tunnel verlieren. Die Verbindung wird bei der Ausfahrt aus dem Tunnel wiederhergestellt. Während der Ausfallzeit werden die Daten des Benutzers, die gedrückten Tasten und andere Interaktionen gespeichert und die Anwendung erscheint als fixiert. Wenn die Verbindung wiederhergestellt ist, werden diese Interaktionen in der Anwendung wiedergegeben.

Bei Konfiguration der automatischen Wiederverbindung von Clients und der Sitzungszuverlässigkeit hat die Sitzungszuverlässigkeit bei einem Verbindungsproblem Vorrang. Die Sitzungszuverlässigkeit versucht, eine Verbindung zu der vorhandenen Sitzung wieder herzustellen. Das Erkennen eines Verbindungsproblems kann bis zu 25 Sekunden dauern. Dann wird nach einem definierbaren Zeitraum (der Standard ist 180 Sekunden) eine Wiederverbindung versucht. Wenn die Sitzungszuverlässigkeit keine Wiederverbindung herstellen kann, versucht die automatische Wiederverbindung von Clients eine Wiederverbindung.

Wenn die HDX Broadcast-Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

Citrix Workspace-Benutzer können die Servereinstellungen nicht außer Kraft setzen. Weitere Informationen finden Sie in der Dokumentation von
XenApp und XenDesktop.

> **Wichtig**
>
> Für die HDX Broadcast-Sitzungszuverlässigkeit muss das Common Gateway Protocol (mit Richtlinieneinstellungen) auf dem Server aktiviert sein. Bei Deaktivierung von Common Gateway Protocol wird die HDX Broadcast-Sitzungszuverlässigkeit auch deaktiviert.

Relative Maus

Durch die Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Funktion ist für Anwendungen erforderlich, die relative Mauseingabe statt absoluter Eingabe erfordern.

> **Hinweis**
>
> Dieses Feature ist nur in Sitzungen verfügbar, die auf XenApp oder XenDesktop 7.8 (oder höher) ausgeführt werden. In der Standardeinstellung ist das Steuerelement deaktiviert.

Aktivieren des Features:

Fügen Sie der Datei $HOME/.ICAClient/wfclient.ini im Abschnitt [WFClient] folgenden Eintrag hinzu: RelativeMouse=1.

Damit wird das Feature aktiviert, zum Verwenden müssen Sie es jedoch noch einschalten.

> **Tipp**
>
> Im Abschnitt Alternative relative Mauswerte finden Sie weitere Informationen zum Aktivieren der relativen Mausfunktion.

Einschalten des Features:

Geben Sie Strg/F12 ein.

Nachdem das Feature aktiviert ist, drücken Sie erneut Strg/F12, um die Serverzeigerposition mit dem Client zu synchronisieren. Die Server- und Clientzeigerpositionen werden bei Verwendung einer relativen Maus nicht synchronisiert.

Deaktivieren des Features:

Geben Sie Strg-Umschalt/F12 ein.

Das Feature wird ebenfalls deaktiviert, wenn ein Sitzungsfenster den Fokus verliert.

Alternative relative Mauswerte

Alternativ gibt es folgende Werte für RelativeMouse:

- RelativeMouse=2 Aktiviert das Feature und schaltet es ein, wenn ein Sitzungsfenster den Fokus erhält.
- RelativeMouse=3 Aktiviert das Feature und es bleibt immer eingeschaltet.
- RelativeMouse=4 Aktiviert oder deaktiviert das Feature, wenn der clientseitige Mauszeiger angezeigt oder ausgeblendet wird. In diesem Modus kann die relative Maus automatisch aktiviert oder deaktiviert werden für Anwendungsoberflächen im Gamingstil in Ich-Perspektive.

Durch Eingeben folgender Einstellungen können Sie Tastaturbefehle ändern:

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

Die unterstützten Werte für **RelativemouseOnChar** und **RelativemouseOffChar** sind unter [Hotkey Keys] in der Datei config/module.ini in der Citrix Workspace-App-Installationsstruktur aufgeführt. Die Werte für **RelativeMouseOnShift** und **RelativeMouseOffShift** legen die zu verwendenden Zusatztasten fest und werden unter der Überschrift [Hotkey Shift States] aufgeführt.

Sicherheit

February 22, 2019

Dieser Abschnitt enthält folgende Themen:

- Herstellen von Verbindungen über Proxyserver
- Verbinden mit Secure Gateway oder dem Citrix SSL-Relay
- Verbindung über NetScaler Gateway
- Konfigurieren von veralteten Verschlüsselungssammlungen

Zum Sichern der Kommunikation zwischen der Serverfarm und Citrix Receiver können Sie Citrix Receiver-Verbindungen zur Serverfarm mit zahlreichen Sicherheitsverfahren integrieren, u. a.:

- Einen SOCKS-Proxyserver oder Secure Proxyserver (auch Security Proxyserver, HTTPS-Proxyserver oder SSL-Tunneling-Proxyserver genannt) Mit Proxyservern schränken Sie den Zugriff auf das und vom Netzwerk ein und verarbeiten Verbindungen zwischen Receiver und Servern. Receiver unterstützt die Protokolle SOCKS und Secure Proxy.
- Secure Gateway- oder SSL-Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen. Die TLS-Versionen 1.0 bis 1.2 werden unterstützt.
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie Receiver mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.

Herstellen von Verbindungen über Proxyserver

Proxyserver werden zur Beschränkung des Netzwerkzugriffs sowie beim Herstellen von Verbindungen zwischen Citrix Receiver und Citrix XenApp- oder Citrix XenDesktop-Bereitstellungen verwendet. Citrix Receiver unterstützt das SOCKS-Protokoll zusammen mit Secure Gateway und Citrix SSL-Relay, das Secure Proxy-Protokoll und Windows NT Challenge/Response (NTLM)-Authentifizierung.

Die unterstützten Proxytypen sind durch die Inhalte von Trusted_Regions.ini und Untrusted_Regions.ini auf die Typen “Auto”, “None” und “Wpad” beschränkt. Wenn Sie die Typen “SOCKS”, “Secure” oder “Script” verwenden, bearbeiten Sie die genannten Dateien und fügen Sie die zusätzlichen Typen der Liste der zulässigen Typen hinzu.

> **Hinweis**
>
> Aktivieren Sie zur Gewährleistung einer sicheren Verbindung TLS.

Verbinden über einen sicheren Proxyserver

Durch das Konfigurieren des Secure Proxy-Protokolls wird gleichzeitig auch Unterstützung für Windows NT Challenge/Response (NTLM)-Authentifizierung aktiviert. Wenn dieses Protokoll zur Verfügung steht, wird es beim Start erkannt und ohne zusätzliche Konfiguration ausgeführt.

> **Wichtig**
>
> Um NTLM verwenden zu können, muss die OpenSSL-Bibliothek libcrypto.so auf dem Benutzergerät installiert sein. Diese Bibliothek ist häufig in Linux-Distributionen enthalten, kann aber bei Bedarf auch von http://www.openssl.org/ in einem neuen Fenster heruntergeladen werden.

Verbinden mit Secure Gateway oder dem Citrix SSL-Relay

Sie können Receiver in eine Umgebung mit Secure Gateway oder dem SSL (Secure Sockets Layer)-Relay integrieren. Receiver unterstützt das TLS-Protokoll. TLS (Transport Layer Security) ist die neueste normierte Version des SSL-Protokolls. Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von SSL als offenem Standard übernahm. TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie FIPS 140 (Federal Information Processing Standard). FIPS 140 ist ein Standard für die Kryptografie.

Verbinden mit Secure Gateway

Sie können Secure Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen Citrix Receiver und dem Server bereitzustellen. Citrix Receiver muss nicht konfiguriert werden, wenn Sie Secure Gateway im Normalmodus verwenden und Benutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Secure Gateway-Servern verwendet Citrix Receiver Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Informationen zum Konfigurieren der Proxyservereinstellungen für Citrix Receiver finden Sie in der Webinterface-Dokumentation.

Wenn Secure Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Secure Gateway Proxy im Relaymodus verwenden. Weitere Informationen finden Sie in der XenApp-Dokumentation (Secure Gateway).

Wenn Sie den Relaymodus verwenden, fungiert der Secure Gateway-Server als Proxy und Sie müssen Citrix Receiver für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Secure Gateway-Servers.
- Portnummer des Secure Gateway-Servers. Der Relaymodus wird von Secure Gateway, Version 2.0 nicht unterstützt.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

Beispiel: my_computer.my_company.com ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (my_computer), einen Second-Level-Domänennamen (my_company) und einen Top-Level-Domänennamen (com) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (my_company.com) wird als Domänenname bezeichnet.

Verbinden mit dem Citrix SSL-Relay

Das Citrix SSL-Relay verwendet standardmäßig den TCP-Port 443 auf dem XenApp-Server für TLS-gesicherte Kommunikation. Wenn das SSL-Relay eine TLS-Verbindung empfängt, werden die Daten entschlüsselt und dann an den Server übergeben.

Wenn Sie SSL-Relay so konfigurieren, dass ein anderer Port als 443 abgehört wird, müssen Sie Citrix Receiver für diese geänderte Portnummer konfigurieren.

Mit dem Citrix SSL-Relay kann folgende Kommunikation gesichert werden:

- Zwischen einem TLS-fähigen Benutzergerät und einem Server
- Mit Webinterface zwischen dem XenApp-Server und dem Webserver

Weitere Informationen zum Konfigurieren und Sichern der Installation mit SSL-Relay finden Sie in der XenApp-Dokumentation. Weitere Informationen zum Konfigurieren des Webinterface für die TLS-Verschlüsselung finden Sie in der Webinterface-Dokumentation.

Konfigurieren und Aktivieren von TLS

Die Versionen des TLS-Protokolls, die ausgehandelt werden können, können Sie steuern, indem Sie die folgenden Konfigurationsoptionen im Abschnitt [WFClient] hinzufügen:

- MinimumTLS=1.0
- MaximumTLS=1.2

Diese Werte sind die Standardwerte, die als Code implementiert werden. Passen Sie sie nach Bedarf an.

Hinweis: Diese Werte werden bei jedem Programmstart gelesen. Wenn Sie sie nach dem Start von selfservice oder storebrowse ändern, geben Sie Folgendes ein: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.

Hinweis: Die Verwendung des SSLv3-Protokolls ist in Citrix Receiver für Linux nicht zulässig.

Citrix Receiver für Linux unterstützt DTLS 1.0 und TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen:

- RSA+AES256-SHA (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-1 für Digest)
- RSA+AES256-SHA256 (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-256 für Digest)
- RSA+AES128-SHA (RSA für Schlüsselaustausch, AES-128 für die Verschlüsselung, SHA-1 für Digest)
- RSA+DES-CBC3-SHA (RSA für Schlüsselaustausch, Triple DES für die Verschlüsselung, SHA-1 für Digest)
- RSA+RC4128-MD5 (RSA für Schlüsselaustausch, RC4-128 für die Verschlüsselung, MD5 für Digest)
- RSA+RC4128-SHA (RSA für Schlüsselaustausch, RC4-128 für die Verschlüsselung, SHA-1 für Digest)
- RSA+AES128_GCM-SHA256 (RSA für Schlüsselaustausch, AES-128 für die Verschlüsselung, SHA-256 für Digest)
- RSA+AES256_GCM-SHA384 (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-384 für Digest)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Elliptic Curve Diffie-Hellman für Schlüsselaustausch, RSA für Authentifizierung, AES-256 und GCM SHA-384 für Digest)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (Elliptic Curve Diffie-Hellman für Schlüsselaustausch, RSA für Authentifizierung, AES-256 und GCM SHA-384 für Digest)
- TLS_RSA_AES256_CBC_SHA256 (RSA für Authentifizierung, AES-256 und CBC SHA-256 für Digest)

Die effektive Größe der Verschlüsselungsschlüssel für die oben aufgeführten SSL/TLS-Standardverschlüsselungssa
sind wie folgt definiert:

- RC4-Algorithmus: 128 Bits (Stromverschlüsselung)
- Triple DES-Algorithmus: 3 x 64 Bits (effektive Größe: 3 x 56 = 168 Bits) (Blockgröße: 64 Bits)
- AES-Algorithmus: 128 Bits oder 256 Bits (Blockgröße: 128 Bits)
- Für RSA-Schlüsselaustausch und Authentifizierung werden Schlüssellängen (Modulus) zwischen 1024 Bits und 4096 Bits unterstützt.
- Für ECDH-Schlüsselaustausch werden die elliptischen Kurven NIST P-256 und NIST P-384 (256 Bits und 384 Bits Schlüssellänge) unterstützt.

Zum Auswählen der Verschlüsselungssammlung fügen Sie die folgende Konfigurationsoption im Abschnitt [WFClient] hinzu:

- SSLCiphers=GOV

Dieser Wert ist der Standardwert. Die Werte COM und ALL werden ebenfalls erkannt.
Hinweis: Wenn Sie dies nach dem Start von selfservice oder storebrowse ändern, müssen Sie wie bei der Konfiguration der TLS-Version Folgendes eingeben:
killall AuthManagerDaemon ServiceRecord selfservice storebrowse

Installieren von Stammzertifikaten auf Benutzergeräten

Zur Verwendung von TLS benötigen Sie ein Stammzertifikat auf dem Benutzergerät, das die Signatur der Zertifizierungsstelle auf dem Serverzertifikat überprüfen kann. Standardmäßig unterstützt Citrix Receiver die folgenden Zertifikate.

Zertifikat	Zertifizierungsstelle
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

Für die Verwendung der Zertifikate von diesen Zertifizierungsstellen ist es nicht erforderlich, Stammzertifikate zu beziehen und auf dem Benutzergerät zu installieren. Wenn Sie sich jedoch entscheiden, eine andere Zertifizierungsstelle zu verwenden, müssen Sie ein Stammzertifikat dieser Zertifizierungsstelle haben und es auf jedem Benutzergerät installieren.

Citrix Receiver für Linux unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hin-

aus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

Hinweis: Receiver für Linux 13.0 verwendet
c_rehash vom lokalen Gerät. Version 13.1 und höhere Versionen verwenden das Tool
ctx_rehash, wie in den folgenden Schritten beschrieben.

Verwenden eines Stammzertifikats

Wenn Sie ein Serverzertifikat authentifizieren, das von einer Zertifizierungsstelle ausgestellt wurde und dem von dem Benutzergerät noch nicht vertraut wird, befolgen Sie die nachfolgenden Anweisungen, bevor Sie einen StoreFront-Store hinzufügen.

1. Beziehen Sie das Stammzertifikat im PEM-Format.
   Tipp: Wenn Sie kein Zertifikat in diesem Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.
2. Als Benutzer, der das Paket installiert hat (normalerweise root):
   a) Kopieren Sie die Datei in $ICAROOT/keystore/cacerts.
   b) Führen Sie den folgenden Befehl aus:
   ```
   $ICAROOT/util/ctx_rehash
   ```

Verwenden Sie ein Zwischenzertifikat

Wenn der StoreFront-Server keine Zwischenzertifikate bereitstellen kann, die dem verwendeten Zertifikat entsprechen, oder wenn Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren, führen Sie diese Schritte aus, bevor Sie einen StoreFront-Store hinzufügen.

1. Besorgen Sie sich die einzelnen Zwischenzertifikate im PEM-Format.
   Tipp: Wenn Sie kein Zertifikat in diesem Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.
2. Als Benutzer, der das Paket installiert hat (normalerweise root):
   a) Kopieren Sie eine oder mehrere Dateien zu $ICAROOT/keystore/intcerts.
   b) Führen Sie den folgenden Befehl als Benutzer, der das Paket installiert hat, aus:
   ```
   $ICAROOT/util/ctx_rehash
   ```

Aktivieren der Smartcardunterstützung

Citrix Receiver für Linux unterstützt verschiedene Smartcardleser. Wenn Smartcardunterstützung sowohl auf dem Server als auch Receiver aktiviert ist, können Smartcards zu folgenden Zwecken eingesetzt werden:

- Smartcard-Anmeldeauthentifizierung: Verwendung von Smartcards zur Authentifizierung von Benutzern an Citrix XenApp-Servern.

- Smartcard-Anwendungsunterstützung: Zugriff auf lokale Smartcardgeräte über smartcard-fähige veröffentlichte Anwendungen.

Die sicherheitsrelevanten Smartcarddaten sollten über einen sicheren, authentifizierten Kanal, z. B. TLS, übertragen werden.

Für die Smartcardunterstützung müssen folgende Voraussetzungen erfüllt sein:

- Die Smartcardleser und die veröffentlichten Anwendungen müssen dem PC/SC-Industriestandard entsprechen.
- Installieren Sie den passenden Treiber für die Smartcard.
- Installieren Sie das PCSC Lite-Paket.
- Installieren Sie den pcscd Daemon, der Middleware für den Zugriff auf die Smartcard mit PC/SC bereitstellt, und führen Sie ihn aus.
- Auf einem 64-Bit-System muss die 64-Bit- und 32-Bit-Version des “libpscslite1”-Pakets vorhanden sein.

Wichtig: Wenn Sie das Sun Ray-Terminal mit Sun Ray-Serversoftware (Version 2.0 oder höher) verwenden, installieren Sie zunächst das PC/SC SRCOM-Bypass-Paket, das unter http://www.sun.com/ zur Verfügung steht.

Weitere Informationen zur Konfiguration der Smartcardunterstützung auf den Servern finden Sie in der Dokumentation für XenApp und XenDesktop.

Verbindung über NetScaler Gateway

Citrix NetScaler Gateway (früher Access Gateway) sichert Verbindungen mit StoreFront-Stores und ermöglicht Administratoren eine genaue Steuerung des Benutzerzugriffs auf Desktops und Anwendungen.

Herstellen einer Verbindung mit Desktops und Anwendungen über NetScaler Gateway

1. Geben Sie die vom Administrator erhaltene NetScaler Gateway-URL ein. Dafür stehen folgende Methoden zur Auswahl:

   - Bei der ersten Verwendung der Self-Service-Benutzeroberfläche werden Sie aufgefordert, die URL im Dialogfeld Konto hinzufügen einzugeben.
   - Wenn Sie die Self-Service-Benutzeroberfläche später verwenden, geben Sie die URL ein, indem Sie auf Einstellungen > Konten > Hinzufügen klicken.
   - Beim Herstellen einer Verbindung mit dem Befehl “storebrowse” geben Sie die URL in der Befehlszeile ein.

   Über die URL wird das Gateway und optional ein bestimmter Store angegeben:

- Zum Herstellen einer Verbindung mit dem ersten Store, den Receiver findet, verwenden Sie eine URL im Format https://gateway.company.com.
- Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im Format https://gateway.company.com? <storename>. Diese dynamische URL besitzt kein standardmäßiges Format, verwenden Sie kein = (Gleichheitszeichen) in der URL. Beim Herstellen einer Verbindung mit einem bestimmten Store mit storebrowse müssen Sie die URL im storebrowse-Befehl wahrscheinlich in Anführungszeichen setzen.

2. Wenn Sie dazu aufgefordert werden, stellen Sie eine Verbindung mit dem Store (über das Gateway) unter Verwendung Ihres Benutzernamens, Kennworts und Sicherheitstokens her. Weitere Informationen zu diesem Schritt finden Sie in der NetScaler Gateway-Dokumentation.

   Wenn die Authentifizierung abgeschlossen ist, werden Ihre Desktops und Anwendungen angezeigt.

Konfigurieren von veralteten Verschlüsselungssammlungen

Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten Forward Secrecy nicht. Diese Verschlüsselungssammlungen werden von der Branche mittlerweile allgemein als veraltet eingestuft. Um die Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop zu unterstützen, kann Receiver für Linux diese Verschlüsselungssammlungen aktivieren.

Flags wurden erstellt, um die Verwendung veralteter Verschlüsselungssammlungen zu ermöglichen. In Receiver für Linus Version 13.10 sind diese Flags standardmäßig aktiviert. Die Kategorisierung der Verschlüsselungssammlungen als veraltet mit den AES- oder 3DES-Algorithmen wird jedoch nicht standardmäßig erzwungen. Sie können diese Flags jedoch ändern und verwenden, um die Kategorisierung strenger durchzusetzen.

Setzen Sie das Flag Enable_TLS_RSA_ auf False, um die Sicherheit weiter zu erhöhen.

Im Folgenden finden Sie eine Liste der veralteten Verschlüsselungssammlungen:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Hinweis**
>
> Die beiden letzten Verschlüsselungssammlungen verwenden den RC4-Algorithmus und

> sind veraltet, weil sie unsicher sind. Sie könnten auch die Verschlüsselungssammlung TLS_RSA_3DES_CBC_EDE_SHA als veraltet betrachten. Mit Flags können Sie alle Kategorisierungen durchsetzen.

Informationen zum Konfigurieren von DTLS v1.2 finden Sie unter Adaptiver Transport.

Voraussetzung

Mit dem folgenden Schritt konfigurieren Sie dieses Feature auf dem Client:

Wenn .ICAClient bereits im Basisordner des aktuellen Benutzers vorhanden ist:

- Löschen Sie die Datei All_Regions.ini.

Oder

- Fügen Sie folgende Zeilen am Ende des Abschnitts [Network\SSL] hinzu, um die Datei AllRegions.ini beizubehalten:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

Wenn der Ordner .ICAClient nicht im Basisordner des aktuellen Benutzers vorhanden ist, weist dies auf eine Neuinstallation des Receivers hin. In diesem Fall wird die Standardeinstellung für die Features beibehalten.

Konfigurieren von veralteten Verschlüsselungssammlungen

1. Öffnen Sie die Datei **$ICAROOT/config/All_Regions.ini**.
2. Verwenden Sie im Abschnitt **Network\SSL** folgende drei Flags, um die veralteten Verschlüsselungssammlungen zu aktivieren oder zu deaktivieren:
   - **Enable_TLS_RSA_**: Die Standardeinstellung für das Flag Enable_TLS_RSA_ ist True.
     Legen Sie das Flag Enable_TLS_RSA_ auf True fest, um folgende Verschlüsselungssammlungen anzuzeigen:
     - TLS_RSA_AES256_GCM_SHA384
     - TLS_RSA_AES128_GCM_SHA256
     - TLS_RSA_AES256_CBC_SHA256
     - TLS_RSA_AES256_CBC_SHA
     - TLS_RSA_AES128_CBC_SHA
     - TLS_RSA_3DES_CBC_EDE_SHA

> **Wichtig**
>
> Legen Sie das Flag Enable_TLS_RSA_ auf True fest, um die anderen beiden Verschlüsselungssammlungen Enable_RC4-MD5 und Enable_RC4_128_SHA zu verwenden.

- **Enable_RC4-MD5**: Die Standardeinstellung für das Flag Enable_RC4-MD5 ist **False**.
  Legen Sie dieses Flag auf True fest, um die Verschlüsselungssammlung RC4-MD5 zu aktivieren.
- **Enable_RC4_128_SHA**: Die Standardeinstellung für das Flag Enable_RC4_128_SHA ist **False**.
  Legen Sie dieses Flag auf True fest, um die Verschlüsselungssammlung RC4_128_SHA zu aktivieren.

3. Speichern Sie die Datei.

Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

> **Wichtig**
>
> Zukünftig wird Citrix nur folgende drei Verschlüsselungssammlungen unterstützen:
>
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS 1.2/DTLS 1.2, GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS 1.2/DTLS 1.2 GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – TLS 1.0/1.1/1.2, DTLS 1.0/1.2 COM/ALL
>
> **Hinweis**
>
> Alle oben genannten Verschlüsselungssammlungen sind FIPS- und SP800-52-konform. Die ersten beiden Sammlungen sind nur für (D)TLS1.2-Verbindungen zulässig. Umfassende Informationen zur Unterstützung von Verschlüsselungssammlungen finden Sie in **Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen**.

Problembehandlung

February 22, 2019

Dieser Artikel enthält Informationen für Administratoren zur Fehlerbehebung von Problemen in Citrix Receiver für Linux.

Verbindungsprobleme

Die folgenden Verbindungsprobleme kommen vor.

Benutzer haben Probleme beim Herstellen einer Verbindung zu einer veröffentlichten Ressource oder einer Desktopsitzung

Wenn beim Herstellen einer Verbindung mit einem Windows-Server ein Dialogfeld mit der Meldung "Verbindung zu Server … wird hergestellt…" aber danach kein Verbindungsfenster angezeigt wird, müssen Sie den Server möglicherweise mit einer Clientzugriffslizenz (CAL) konfigurieren. Weitere Informationen zur Lizenzierung finden Sie unter Lizenzierung.

Wiederherstellung von Verbindungen zu Sitzungen ist manchmal nicht möglich

Manchmal sind Wiederverbindungen mit Sitzungen, die eine höhere Farbtiefe als der von Receiver angeforderten verwenden, nicht möglich. Der Grund hierfür ist ein Speichermangel auf dem Server. Wenn die Wiederverbindung fehlschlägt, versucht Receiver, die ursprüngliche Farbtiefe zu verwenden. Andernfalls versucht der Server, eine neue Sitzung mit der angeforderten Farbtiefe zu starten. Die ursprüngliche Sitzung bleibt in diesem Fall getrennt. Die zweite Sitzung kann aber auch fehlschlagen, wenn immer noch nicht genügend Speicher auf dem Server verfügbar ist.

Verbindungsherstellung zu einem Server mit dem vollständigen Internetnamen ist nicht möglich

Citrix empfiehlt, DNS auf Ihrem Netzwerk zu konfigurieren, damit die Namen der Server, zu denen Sie eine Verbindung herstellen möchten, aufgelöst werden können. Wenn Sie DNS nicht konfiguriert haben, kann der Servername eventuell nicht in eine IP-Adresse aufgelöst werden. Alternativ können Sie den Server mit der IP-Adresse statt dem Namen angeben. Für TLS-Verbindungen ist ein vollqualifizierter Domänenname und keine IP-Adresse erforderlich.

Bei der Verbindungsherstellung wird ein Proxyerkennungsfehler angezeigt

Wenn Ihre Verbindung für automatische Proxyerkennung konfiguriert ist und Sie beim Versuch, eine Verbindung herzustellen, die Fehlermeldung "Proxyerkennung fehlgeschlagen: JavaScript-Fehler" erhalten, kopieren Sie die Datei wpad.dat in das Verzeichnis $ICAROOT/util. Führen Sie den folgenden Befehl aus, wobei Hostname der Hostname des Servers ist, zu dem Sie eine Verbindung herstellen möchten:

```
1 cat wpad.dat | ./pacexec pac.js FindProxyForURL <http://hostname>
    hostname 2>&1 | grep "undeclared variable"
```

Wenn Sie keine Ausgabe erhalten, liegt ein schwerwiegendes Problem in der Datei wpad.dat auf dem Server vor, das untersucht werden muss. Wenn Sie eine Ausgabe mit ungefähr folgendem Inhalt erhalten, können Sie das Problem jedoch beheben: "assignment to undeclared variable …". Öffnen Sie

pac.js für jede in der Ausgabe aufgeführte Variable und fügen Sie am Anfang der Datei eine Zeile in folgendem Format hinzu, wobei "…" der Variablenname ist.

var …;

Sitzungsstart ist sehr langsam

Wenn eine Sitzung nicht startet, bevor Sie die Maus bewegen, liegt möglicherweise ein Problem mit der Zufallszahlengenerierung im Linux-Kernel vor. Als Workaround führen Sie einen Entropie generierenden Daemon wie rngd (hardwarebasiert) oder haveged (von Magic Software) aus.

Schwache Verschlüsselungssammlungen für SSL-Verbindungen

Für das Herstellen einer TLS-Verbindung bietet Receiver für Linux mit der Version 13.7 standardmäßig einen moderneren und eingeschränkteren Satz von Verschlüsselungssammlungen.
Wenn Sie eine Verbindung zu einem Server herstellen, der eine ältere Verschlüsselungssammlung erfordert, legen Sie im Abschnitt [WFClient] einer Konfigurationsdatei die Konfigurationsoption SSLCiphers=ALL fest.

Bei der Verwendung des UDT-Protokolls wird folgende Fehlermeldung angezeigt: Verbindung mit "…" wurde unterbrochen

Der Grund könnte sein, dass die Verbindung über einen Router erfolgt, wobei die maximale Übertragungseinheit für UDT kleiner ist als die Standardeinstellung von 1500 Bytes. Probieren Sie beides aus:

- Heben Sie die Auskommentierung des Eintrags udtMSS in $ICAROOT/config/All_Regions.ini und in $HOME/.ICAClient/All_Regions.ini auf.
- Legen Sie in einer Konfigurationsdatei folgende Einstellung fest: udtMSS=1000

Verbindungsfehler

Verbindungsfehler können eine Vielzahl unterschiedlicher Fehlermeldungen erzeugen. Beispiele:

- Fehler bei Verbindung: Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten.
- Es konnte kein Kontakt mit dem Authentifizierungsdienst hergestellt werden.
- Ihr Konto kann nicht mit dieser Serveradresse hinzugefügt werden

Verschiedene Probleme können solche Fehler verursachen, einschließlich der Folgenden:

- Der lokale Computer und der Remotecomputer können kein gemeinsames TLS-Protokoll verhandeln. Weitere Informationen finden Sie unter Konfigurieren und Aktivieren von TLS.

- Der Remotecomputer erfordert eine ältere Verschlüsselungssammlung für eine TLS-Verbindung. In diesem Fall legen Sie im Abschnitt [WFClient] einer Konfigurationsdatei die Konfigurationsoption SSLCiphers=ALL fest. Führen Sie **killall AuthManagerDaemon ServiceRecord selfservice storebrowse** aus, bevor Sie die Verbindung neu starten.
- Der Remotecomputer fordert falscherweise ein Clientzertifikat an. IIS sollte Zertifikate nur für "Citrix/Authentication/Certificate" akzeptieren oder anfordern.
- Andere Probleme:

Anzeigeprobleme

Warum tritt Tearing auf dem Bildschirm auf?

Tearing wird verursacht, wenn Teile von zwei (oder mehreren) unterschiedlichen Frames gleichzeitig auf dem Bildschirm in horizontalen Blöcken angezeigt werden. Dies ist besonders bei großen Bereichen von sich schnell änderndem Inhalt auf dem Bildschirm erkennbar. Die Daten werden am VDA auf eine Weise erfasst, die Tearing verhindert, und sie werden an den Client auf eine Weise weitergegeben, dass kein Tearing auftritt. X11 (das Linux/Unix-Grafiksubsystem) bietet jedoch keine konsistente Möglichkeit der Erstellung von Frames, die Tearing verhindert.

Zum Verhindern von Tearing empfiehlt Citrix die Standardmethode, bei der der Anwendungsaufbau mit dem Aufbau des Bilds synchronisiert wird. Dies bedeutet, dass vsvnc den Aufbau des nächsten Frames initiiert. Abhängig von der auf dem Client verwendeten Grafikhardware und dem verwendeten Fenstermanager bietet Linux verschiedene Optionen. Diese Optionen lassen sich in zwei Lösungsgruppen einteilen:

- X11 GPU-Einstellungen
- Verwenden eines Kompositionsmanagers

X11 GPU-Konfiguration

Erstellen Sie für Intel HD-Grafiken in xorg.conf.d eine
20-intel.conf genannte Datei mit folgenden Inhalten:

Section "Device"

```
1 Identifier "Intel Graphics"
2
3 Driver         "intel"
4
5 Option "AccelMethod" "sna"
6
7 Option "TearFree" "true"
```


EndSection

Navigieren Sie für Nvidia-Grafiken zu der Datei im Ordner xorg.conf.d, die die Option “MetaModes” für Ihre Konfiguration enthält. Fügen Sie für jeden durch Komma getrennten MetaMode Folgendes hinzu:

{ForceFullCompositionPipeline = On}

Zum Beispiel:

Option “MetaModes” “DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}”

Hinweis: Unterschiedliche Linux-Bereitstellungen verwenden unterschiedliche Pfade zu xorg.conf.d, z. B. /etc/X11/xorg.conf.d oder /user/share/X11/xorg.conf.d.

Kompositionsmanager

Verwenden Sie Folgendes:

- Compiz (integriert in Ubuntu Unity). Installieren Sie den “CompizConfig Settings Manager”.

  Führen Sie “CompizConfig Settings Manager” aus.

  Unter “General > Composition” deaktivieren Sie “Undirect Fullscreen Windows”.

Hinweis: Seien Sie vorsichtig bei der Verwendung von “CompizConfig Settings Manager”, da das System u. U. nicht starten kann, wenn Sie Werte fehlerhaft ändern.

- Compton (ein Add-On-Hilfsprogramm). Ausführliche Informationen finden Sie auf der Hauptseite bzw. in der Dokumentation von Compton. Führen Sie beispielsweise den folgenden Befehl aus:

  compton –vsync opengl –vsync -aggressive

Falsches Anzeigen von Tastatureingaben bei der Verwendung der Tastatur

Wenn Sie keine englische Tastatur verwenden, stimmt die Bildschirmanzeige möglicherweise nicht mit der Tastatureingabe überein. In dieser Situation müssen Sie den verwendeten Tastaturtyp und das verwendete Tastaturlayout angeben. Weitere Informationen zur Angabe der Tastaturen finden Sie unter Steuern des Tastaturverhaltens.

Beim Verschieben von Seamlessfenstern wird der Bildschirm ständig neu aufgebaut

Einige Fenstermanager übertragen beim Verschieben von Fenstern ständig die neue Fensterposition, was zu einem wiederholten Neuaufbau des Bildschirms führen kann. Sie können dieses Problem beheben, indem Sie den Fenstermanager zu einem Modus wechseln, bei dem beim Verschieben von Fenstern nur die Konturen gezeichnet werden.

Kompatibilität von Symbolen

Receiver erstellt Fenstersymbole, die mit den meisten Fenstermanagern verwendet werden können, aber nicht vollständig kompatibel mit den X Window-Kommunikationsrichtlinien für Clients (ICCCM, X Inter-Client Communication Convention Manual) sind.

Erreichen voller Kompatibilität von Symbolen

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Bearbeiten Sie die folgende Zeile im Abschnitt [WFClient]: UseIconWindow=True
3. Speichern und schließen Sie die Datei.

Der Cursor ist schlecht sichtbar

Der Cursor ist manchmal schlecht zu erkennen, wenn er dieselbe oder eine ähnliche Farbe wie der Hintergrund hat. Sie können dieses Problem lösen, indem Sie erzwingen, dass Bereiche des Cursors schwarz oder weiß sind.

Ändern der Farbe des Cursors

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Fügen Sie dem Abschnitt [WFClient] eine der folgenden Zeilen hinzu:

   CursorStipple=ffff,ffff (der Cursor wird schwarz angezeigt)

   CursorStipple=0,0 (der Cursor wird weiß angezeigt)
3. Speichern und schließen Sie die Datei.

Farbwechsel auf dem Bildschirm

Wenn Sie den Mauszeiger über ein Verbindungsfenster verschieben, können in dem Fenster, das gerade nicht den Fokus hat, Farbwechsel auftreten. Dies ist eine bekannte Einschränkung bei der Verwendung von X Window System mit PseudoColor-Anzeigen. Falls möglich sollten Sie die Farbtiefe für die betroffene Verbindung erhöhen.

Schnelle Farbwechsel bei TrueColor-Anzeigen

Benutzer haben bei der Herstellung einer Verbindung zu einem Server die Option, 256 Farben zu verwenden. Voraussetzung für diese Option ist, dass die Videohardware Paletten unterstützt, damit Anwendungen zum Erzeugen animierter Anwendungen die Farbpalette wechseln können.

TrueColor-Anzeigen können die Funktion zum Erzeugen von Animationen durch schnelles Wechseln der Palette nicht emulieren. Software-Emulationen dieser Funktion gehen zu Lasten von Schnelligkeit und Datenverkehr im Netzwerk. Um diese Einschränkungen zu reduzieren, puffert Receiver schnelle Palettenwechsel und aktualisiert die eigentliche Palette nur in Abständen von einigen Sekunden.

Japanische Zeichen werden nicht richtig angezeigt

Receiver verwendet die EUC-JP- oder UTF-8-Zeichencodierung für japanische Zeichen, während der Server SJIS verwendet. Receiver kann diese Zeichensätze nicht übersetzen. Dies kann zu Problemen führen, wenn auf dem Server gespeicherte Dateien lokal angezeigt werden oder lokal gespeicherte Dateien auf dem Server angezeigt werden. Dies Problem betrifft auch japanische Zeichen in Parametern, die bei der erweiterten Parameterübergabe verwendet werden.

Benutzer möchten eine Sitzung erstellen, die bildschirmübergreifend angezeigt wird

Sitzungen im Vollbildmodus gehen standardmäßig über alle Monitore. Es gibt außerdem für Befehlszeilen eine Steuerungsoption für die Anzeige auf mehreren Monitoren: -span. Hiermit können Vollbildschirmsitzungen über mehrere Monitore gestreckt werden.

Mit der Symbolleistenfunktionalität von Desktop Viewer können Sie in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore. Weitere Informationen finden Sie unter Verbessern der Benutzererfahrung.

Wichtig: Dies hat keinen Einfluss auf Sitzungen mit Seamless- oder normalen Fenstern (einschließlich Sitzungen mit maximierten Fenstern).

Die Option hat das folgende Format:
-span [h][o][a|mon1[,mon2[,mon3,mon4]]]

Wenn h angegeben wird, wird eine Liste von Monitoren auf stdout ausgegeben. Wenn dies der einzige Optionswert ist, wird wfica anschließend beendet.

Wenn o angegeben wird, enthält das Sitzungsfenster das Weiterleitungsattribut “override-redirect”.

Achtung: Von der Verwendung dieses Optionswerts wird abgeraten. Er ist als letzter Ausweg für problematische Fenstermanager vorgesehen. Das Sitzungsfenster ist im Fenstermanager nicht sichtbar, hat kein Symbol und kann nicht neu angeordnet werden. Es kann nur durch Beenden der Sitzung entfernt werden.

Wenn a angegeben wird, wird von Receiver versucht, eine Sitzung zu erstellen, die alle Monitore abdeckt.

Dabei wird angenommen, dass der Rest des Werts der Option “-span” eine Liste der Monitornummern ist. Ein einzelner Wert gibt einen bestimmten Monitor an, zwei Werte geben Monitore oben links und

unten rechts in dem erforderlichen Bereich an und vier Werte geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

Wenn o nicht angegeben wurde, fordert wfica mit der Meldung _NET_WM_FULLSCREEN_MONITORS ein entsprechendes Fensterlayout vom Fenstermanager an, wenn dies unterstützt wird. Sonst werden Größe- und Positionstipps verwendet, um das gewünschte Layout anzufordern.

Mit dem folgenden Befehl können Sie die Fenstermanager-Unterstützung testen:
xprop -root | grep _NET_WM_FULLSCREEN_MONITORS

Wenn es keine Ausgabe gibt, werden keine Fenstermanager unterstützt. Wenn keine Unterstützung vorhanden ist, benötigen Sie ein Fenster mit override-redirect. Sie können ein solches Fenster mit -span o einrichten.

Erstellen einer Sitzung, die sich über mehrere Monitore erstreckt, an der Befehlszeile

1. Geben Sie an der Eingabeaufforderung Folgendes ein:

   /opt/Citrix/ICAClient/wfica -span h

   Es wird eine Liste mit Nummern der zurzeit an das Benutzergerät angeschlossenen Monitore auf stdout ausgegeben und wfica wird beendet.

2. Notieren Sie diese Monitornummern.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   /opt/Citrix/ICAClient/wfica -span h

   wobei w, x, y und z Monitornummern sind, die Sie in Schritt 1 oben erhalten haben. Der einzelne Wert w gibt einen bestimmten Monitor an, zwei Werte w und x geben Monitore oben links und unten rechts in dem erforderlichen Bereich an und vier Werte w, x, y und z geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

   Wichtig: Definieren Sie die Variable WFICA_OPTS, bevor Sie selfservice starten oder über einen Browser eine Verbindung zum Webinterface herstellen. Bearbeiten Sie hierzu Ihre Profildatei, die üblicherweise unter $HOME/.bash_profile oder $HOME/.profile ist. Fügen Sie hier eine Zeile hinzu, um die Variable WFICA_OPTS zu definieren. Zum Beispiel:

   export WFICA_OPTS=”-span a”

   Diese Änderung wirkt sich auf XenApp- und XenDesktop-Sitzungen aus.

   Wenn Sie selfservice oder storebrowse gestartet haben, entfernen Sie die von ihnen gestarteten Prozesse, damit die neue Umgebungsvariable wirksam wird. Entfernen Sie die Prozesse mit folgendem Befehl:

   killall AuthManagerDaemon ServiceRecord storebrowse

Der Vollbildmodus einer Sitzung kann nicht mit der Escape-Taste beendet werden, um lokale Anwendungen oder eine andere Sitzung zu verwenden

Der Grund dafür ist, dass die clientseitige Systembenutzeroberfläche verborgen ist und das Feature “Tastaturtransparenz” den üblichen Tastaturbefehl, z. B. Alt+Tab, deaktiviert und den Befehl stattdessen an den Server sendet.

Deaktivieren Sie zur Problembehebung das Feature “Tastaturtransparenz” vorübergehend mit Strg+F2, bis der Fokus wieder zum Sitzungsfenster zurückgeht. Als alternativen Workaround können Sie TransparentKeyPassthrough in $ICAROOT/config/module.ini auf No einstellen. Das Feature “Tastaturtransparenz” wird hiermit deaktiviert. Sie müssen jedoch u. U. die ICA-Datei durch Hinzufügen dieser Einstellung in der Datei All_regions.ini überschreiben.

Browserprobleme

Beim Klicken auf einen Link in einer Windows-Sitzung wird der Inhalt in einem lokalen Browser angezeigt

Die Server-zu-Client-Inhaltsumleitung ist in der Datei wfclient.ini aktiviert. Dies führt zur Ausführung einer lokalen Anwendung. Informationen zum Deaktivieren der Server-zu-Client-Inhaltsumleitung finden Sie unter Einrichten der Server-zu-Client-Inhaltsumleitung.

Beim Zugreifen auf veröffentlichte Ressourcen fordert der Browser den Benutzer zum Speichern einer Datei auf

Andere Browser als Mozilla, Firefox und Chrome müssen möglicherweise konfiguriert werden, bevor Sie auf eine veröffentlichte Ressource zugreifen können. Wenn Sie eine Verbindung über das Webinterface herstellen, können Sie möglicherweise die Webinterface-Homepage mit der Liste der Ressourcen öffnen. Wenn Sie jedoch versuchen, eine Ressource durch Klicken auf das Symbol auf der Seite zu öffnen, fordert Sie der Browser zum Speichern der ICA-Datei auf.

Konfigurieren eines anderen Browsers für das Webinterface

Die Angaben hängen vom Browser ab, aber Sie können die MIME-Datentypen im Browser so einrichten, dass $ICAROOT/wfica als Hilfsprogramm ausgeführt wird, wenn der Browser auf Daten mit dem MIME-Typ “application/x-ica” oder eine ICA-Datei trifft.

Der Installer unterstützt einen bestimmten Browser nicht

Wenn Sie Probleme mit einem bestimmten Webbrowser haben, geben Sie für die Umgebungsvariable BROWSER den lokalen Pfad und Namen des erforderlichen Browsers ein, bevor Sie setupwfc ausführen.

Beim Start von Desktops oder Anwendungen in Firefox geschieht nichts

Versuchen Sie ein Aktivieren des ICA-Plug-Ins.

Das ICA-Plug-In ist in Firefox aktiviert, jedoch können Desktop- und Anwendungssitzungen nicht gestartet werden

Versuchen Sie ein Deaktivieren des ICA-Plug-Ins.

Andere Probleme

Folgende Probleme können ebenfalls auftreten.

Hat der Server Receiver angewiesen, eine Sitzung zu schließen?

Sie können sich mit dem Programm *wfica* anmelden, wenn Receiver vom Server den Befehl erhalten hat, die Sitzung zu beenden.

Damit diese Informationen vom Syslog aufgezeichnet werden, fügen Sie *SyslogThreshold* mit dem Wert 6 im Abschnitt [WFClient] der Konfigurationsdatei hinzu. Hierdurch wird die Protokollierung von Nachrichten mit der Priorität LOG_INFO oder höher aktiviert. Der Standardwert für *SyslogThreshold* ist 4 (=LOG_WARNING).

Damit *wfica* die Informationen als Standardfehler sendet, fügen Sie *PrintLogThreshold* mit dem Wert 6 im Abschnitt [WFClient] hinzu. Der Standardwert für *PrintLogThreshold* ist 0 (=LOG_EMERG).

Anleitungen zum Konfigurieren des syslog-Systems finden Sie in der Dokumentation zu Ihrem Betriebssystem.

Einstellungen der Konfigurationsdatei funktionieren nicht mehr

Für jeden Eintrag in wfclient.ini muss ein entsprechender Eintrag in All_Regions.ini gemacht werden, damit die Einstellung wirksam wird. Zusätzlich muss für jeden Eintrag in den Abschnitten [Thinwire3.0], [ClientDrive] und [TCP/IP] von wfclient.ini ein entsprechender Eintrag in canonicalization.ini

gemacht werden, damit die Einstellung wirksam wird. Weitere Informationen finden Sie in den Dateien All_Regions.ini und canonicalization.ini im Verzeichnis $ICAROOT/config.

Beim Ausführen veröffentlichter Anwendungen, die auf einen seriellen Port zugreifen, treten Probleme auf

Beim Zugriff einer veröffentlichten Anwendung auf einen seriellen Port kann die Anwendung fehlschlagen (je nach der Anwendung mit oder ohne Fehlermeldung), wenn der Port durch eine andere Anwendung gesperrt ist. Überprüfen Sie in solchen Fällen, dass keine Anwendungen vorhanden sind, die den seriellen Port vorübergehend gesperrt haben oder die den seriellen Port gesperrt haben und beendet wurden, ohne ihn wieder freizugeben.

Um dieses Problem zu lösen, beenden Sie die Anwendung, die den seriellen Port derzeit belegt. Bei UUCP-Sperren ist nach dem Beenden der Anwendung eventuell noch eine Sperrdatei vorhanden. Der Speicherort dieser Sperrdateien hängt vom verwendeten Betriebssystem ab.

Receiver kann nicht gestartet werden

Wenn Receiver nicht gestartet werden kann, wird die Fehlermeldung “Application default file could not be found or is out of date” angezeigt. In diesem Fall ist die Umgebungsvariable ICAROOT möglicherweise nicht richtig definiert. Die Variable muss richtig definiert werden, wenn Sie Receiver nicht im Standardverzeichnis installiert haben. Citrix empfiehlt hierfür zwei Lösungsvorschläge:

- Definieren Sie ICAROOT als Installationsverzeichnis.

  Um zu überprüfen, ob die Umgebungsvariable ICAROOT richtig definiert wurde, versuchen Sie, Receiver von einer Terminalsitzung zu starten. Wenn die Fehlermeldung weiterhin angezeigt wird, ist die Umgebungsvariable ICAROOT wahrscheinlich nicht richtig definiert.

- Installieren Sie Receiver im Standardverzeichnis neu. Weitere Informationen zur Installation von Receiver finden Sie unter Installation und Einrichtung.

  Wenn Receiver vorher im Standardverzeichnis installiert worden war, sollten Sie vor der Neuinstallation das Verzeichnis /opt/Citrix/ICAClient oder $HOME/ICAClient/Plattform entfernen.

Ermitteln der Versionsnummer für das Citrix CryptoKit (früher SSLSDK) oder OpenSSL

Führen Sie den folgenden Befehl aus, um die Versionsnummer für das ausgeführte Citrix SSLSDK oder OpenSSL zu bestätigen:
strings libctxssl.so | grep “Citrix SSLSDK”

Sie können diesen Befehl auch für AuthManagerDaemon oder PrimaryAuthManager ausführen

Tastenkombinationen funktionieren nicht richtig

Ihre Tastenkombinationen funktionieren unter Umständen nicht richtig, wenn der Fenstermanager dieselben Tastenkombinationen für systemeigene Funktionen verwendet. Im KDE-Fenstermanager werden beispielsweise die Kombinationen von STRG+UMSCHALT+F1 bis STRG+UMSCHALT+F4 verwendet, um zwischen den Desktops 13 bis 16 zu wechseln. Wenn dieses Problem auftritt, versuchen Sie Folgendes:

- Mit dem Übersetzungsmodus auf der Tastatur werden lokale Tastenkombinationen serverseitigen Tastenkombinationen zugeordnet. Beispielsweise wird im Übersetzungsmodus standardmäßig STRG+UMSCHALT+F1 serverseitig der Tastenkombination ALT+F1 zugeordnet. Um diese Zuordnung in eine andere lokale Tastenkombination zu ändern, aktualisieren Sie den folgenden Eintrag im Abschnitt [WFClient] der Datei $HOME/.ICAClient/wfclient.ini. Auf diese Weise wird die lokale Tastenkombination Alt+Ctrl+F1 der Kombination Alt+F1 zugeordnet:
  - Ändern Sie Hotkey1Shift=Ctrl+Shift in Hotkey1Shift=Alt+Ctrl.
- Im direkten Modus werden alle Tastenkombinationen direkt an den Server gesendet. Sie werden nicht lokal verarbeitet. Legen Sie zum Konfigurieren des direkten Modus im Abschnitt [WFClient] der Datei $HOME/.ICAClient/wfclient.ini TransparentKeyPassthrough auf Remote fest.
- Konfigurieren Sie den Fenstermanager so, dass Standardtastaturkombinationen unterdrückt werden.

Remote-Tastatur für Kroatisch soll aktiviert werden

Diese Vorgehensweise stellt sicher, dass ASCII-Zeichen korrekt an remote virtuelle Desktops mit kroatischen Tastaturlayouts gesendet werden.

1. Setzen Sie im Abschnitt WFClient der entsprechenden Konfigurationsdatei UseEUKSforASCII auf True.
2. Setzen Sie UseEUKS auf 2.

Verwenden einer japanischen Tastatur auf dem Client

Zum Konfigurieren einer japanischen Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Japanese (JIS)

Verwenden einer ABNT2-Tastatur auf dem Client

Zum Konfigurieren einer ABNT2-Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

Einige Tasten auf der lokalen Tastatur verhalten sich nicht wie erwartet

Wählen Sie in der Liste in der Datei $ICAROOT/config/module.ini das passendste Serverlayout aus.

Windows Media Player gibt bestimmte Dateiformate nicht wieder

Citrix Receiver hat möglicherweise nicht die nötigen GStreamer-Plug-Ins, um ein gewünschtes Format zu verarbeiten. Normalerweise fordert der Server dann ein anderes Format an. Manchmal wird bei der anfänglichen Prüfung irrtümlich ein passendes Plug-In festgestellt. Dies sollte erkannt werden und auf dem Server eine Fehlermeldung auslösen, die darauf hinweist, dass Windows Media Player beim Wiedergeben der Datei ein Problem hatte. Erneutes Wiedergeben der Datei in der Sitzung funktioniert normalerweise, weil das Format von Citrix Receiver abgelehnt wird. Der Server wird daraufhin ein anderes Format anfordern oder das Medium selbst wiedergeben.

Manchmal wird nicht erkannt, dass kein passendes Plug-In vorhanden ist, und die Datei wird nicht richtig wiedergegeben, obwohl sich die Fortschrittsanzeige in Windows Media Player wie erwartet bewegt.

Vermeiden der Fehlermeldung oder des Wiedergabefehlers in zukünftigen Sitzungen:

1. Fügen Sie beispielsweise in der Datei $Home/.ICAClient/wfclient.ini vorübergehend die Konfigurationsoption “SpeedScreenMMAVerbose=On” im Abschnitt [WFClient] hinzu.
2. Starten Sie wfica über einen selfservice, der von einem Terminal aus gestartet wurde.
3. Geben Sie ein Video wieder, das diesen Fehler auslöst.
4. Bestimmen Sie in der Ausgabe der Ablaufverfolgung den MIME-Typ des fehlenden Plug-Ins oder den MIME-Typ, der unterstützt werden sollte, aber nicht wiedergegeben wird (z. B. “video/x-h264..”).
5. Bearbeiten Sie $ICAROOT/config/MediaStreamingConfig.tbl. Fügen Sie dazu in der Zeile mit dem MIME-Typ ein “?” zwischen dem “:” und dem MIME-Typ ein. Dadurch wird das Format deaktiviert.
6. Wiederholen Sie die Schritte 2 bis 5 (oben) für andere Medienformate, die diesen Fehler verursachen.
7. Verteilen Sie die bearbeitete Datei MediaStreamingConfig.tbl auf andere Maschinen, die dieselben GStreamer-Plug-Ins haben.

Hinweis: Nachdem Sie den MIME-Typ identifiziert haben, können Sie u. U. ein GStreamer-Plug-In installieren und ihn decodieren.

Ich möchte eine Einstellung für einen seriellen Anschluss konfigurieren

Zum Konfigurieren eines seriellen Anschlusses fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=1

ComPort1=device

Zum Konfigurieren von mehreren seriellen Anschlüssen fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Fehler bei der Verbindungskonfiguration

Diese Fehler können auftreten, wenn Sie einen Verbindungseintrag nicht richtig konfiguriert haben.

E_MISSING_INI_SECTION – Überprüfen der Konfigurationsdatei: "…". In der Konfigurationsdatei fehlt der Abschnitt "…".

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_MISSING_INI_ENTRY – Überprüfen der Konfigurationsdatei: "…". Der Abschnitt "…" muss einen Eintrag "…" enthalten.

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_INI_VENDOR_RANGE – Überprüfen der Konfigurationsdatei: "…". Der X Server-Herstellerbereich "…" in der Konfigurationsdatei ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Bitte wenden Sie sich an Citrix.

Konfigurationsfehler in wfclient.ini

Diese Fehler können auftreten, wenn Sie die Datei wfclient.ini nicht richtig bearbeitet haben.

E_CANNOT_WRITE_FILE – Datei kann nicht geschrieben werden: "…"

Es liegt ein Problem beim Speichern der Verbindungsdatenbank vor, z. B. nicht genügend Festplattenspeicher.

E_CANNOT_CREATE_FILE – Datei kann nicht erstellt werden: "…"

Beim Erstellen einer Verbindungsdatenbank ist ein Problem aufgetreten.

E_PNAGENT_FILE_UNREADABLE – Citrix XenApp-Datei kann nicht gelesen werden "…": Datei oder Verzeichnis nicht gefunden.

– oder –

Citrix XenApp-Datei "…" kann nicht gelesen werden: Zugriff verweigert.

Sie versuchen, eine Ressource über einen Desktopeintrag oder ein Menü zu öffnen. Die XenApp-Datei für die Ressource steht jedoch nicht zur Verfügung. Aktualisieren Sie die Liste der veröffentlichten Ressourcen. Wählen Sie im Menü **Ansicht** die Option **Anwendungsaktualisierung** und versuchen Sie erneut, die Ressource zu öffnen. Sollte das Problem weiterhin auftreten, prüfen Sie die Eigenschaften des Desktopsymbols oder des Menüeintrags und XenApp-Datei, auf die das Symbol oder der Eintrag verweist.

PAC-Datei-Fehler

Folgende Fehler können auftreten, wenn Ihre Bereitstellung die automatische Proxykonfiguration mit PAC-Dateien verwendet:

Proxyerkennungsfehler: Falsche Autokonfigurations-URL.

Eine Adresse im Browser wurde mit einem falschen URL-Typ angegeben. Gültige Typen sind http:// und https://. Andere Typen werden nicht unterstützt. Ändern Sie die Adresse zu einem gültigen URL-Typ und versuchen Sie es erneut.

Proxyerkennung fehlgeschlagen: HTTP-Download von PAC-Skript ist fehlgeschlagen: Verbindung fehlgeschlagen.

Überprüfen Sie, ob Name oder Adresse falsch eingegeben wurden. Ist dies der Fall, berichtigen Sie die Adresse und versuchen Sie es erneut. Wenn dies nicht der Fall ist, könnte der Server ausgefallen sein. Versuchen Sie es später erneut.

Proxyerkennungsfehler: PAC-Skript-HTTP-Download fehlgeschlagen: Pfad nicht gefunden.

Die angeforderte PAC-Datei ist nicht auf dem Server. Wechseln Sie entweder den Server oder konfigurieren Sie den Browser neu.

Proxyerkennungsfehler: PAC-Skript-HTTP-Download fehlgeschlagen.

Die Verbindung wurde während des Downloads der PAC-Datei unterbrochen. Stellen Sie die Verbindung wieder her und versuchen Sie es erneut.

Proxyerkennungsfehler: Leeres Autokonfigurationsskript.

Die PAC-Datei ist leer. Wechseln Sie entweder den Server oder konfigurieren Sie den Browser neu.

Proxyerkennungsfehler: Keine JavaScript-Unterstützung.

Die ausführbare PAC-Datei oder die Textdatei pac.js fehlen. Installieren Sie Receiver neu.

Proxyerkennungsfehler: JavaScript-Fehler.

Die PAC-Datei enthält ungültiges JavaScript. Ändern Sie die PAC-Datei auf dem Server. Weitere Informationen finden Sie unter Verbindungsprobleme.

Proxyerkennungsfehler: Falsches Ergebnis vom Proxy-Autokonfigurationsskript.

Eine ungültige Antwort wurde vom Server gesendet. Beheben Sie das Problem auf dem Server oder konfigurieren Sie den Browser neu.

Andere Fehler

Dieser Abschnitt enthält weitere Fehlermeldungen, die bei der Verwendung von Receiver möglicherweise häufiger angezeigt werden.

Es ist ein Fehler aufgetreten. Fehler 11 (E_MISSING_INI_SECTION). Weitere Informationen finden Sie in der Dokumentation. Anwendung wird beendet.

Bei der Ausführung von Receiver über die Befehlszeile lässt diese Meldung in der Regel darauf schließen, dass die in der Befehlszeile angegebene Beschreibung in der Datei appsrv.ini nicht gefunden wurde.

E_BAD_OPTION – Die Option "…" ist ungültig.

Fehlendes Argument für Option "…".

E_BAD_ARG – Die Option "…" hat ein ungültiges Argument: "…".

Ungültiges Argument für Option "…".

E_INI_KEY_SYNTAX – Der Schlüssel "…" in der Konfigurationsdatei "…" ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Erstellen Sie eine Konfigurationsdatei.

E_INI_VALUE_SYNTAX – Der Wert "…" in der Konfigurationsdatei "…" ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Erstellen Sie eine Konfigurationsdatei.

E_SERVER_NAMELOOKUP_FAILURE – Verbindung zu Server "…" kann nicht hergestellt werden.

Der Name des Servers konnte nicht aufgelöst werden.

In mindestens eine Datei kann nicht geschrieben werden: "…". Beheben Sie Probleme beim Speicherplatz auf der Festplatte oder der Verbindung und versuchen Sie es erneut.

Überprüfen Sie, ob die Festplatte voll ist oder ob Probleme mit den Rechten bestehen. Wenn Sie das Problem gefunden und gelöst haben, wiederholen Sie den Vorgang, der die Fehlermeldung ausgelöst hat.

Die Verbindung zum Server wurde unterbrochen. Stellen Sie die Verbindung wieder her und versuchen Sie es erneut. In diesen Dateien fehlen u. U. Daten: "…".

Stellen Sie die Verbindung wieder her und wiederholen Sie den Vorgang, der den Fehler ausgelöst hat.

Senden von Diagnoseinformationen an den technischen Support von Citrix

Wenn Sie beim Verwenden von Receiver Probleme feststellen, werden Sie vom Technical Support möglicherweise gebeten, Diagnoseinformationen bereitzustellen. Diese Informationen unterstützen dieses Team bei der Diagnose und helfen, das Problem zu beheben.

Erhalten von Diagnoseinformationen zu Receiver

1. Geben Sie im Installationsverzeichnis util/lurdump ein. Es empfiehlt sich, diesen Vorgang auszuführen, während eine Sitzung geöffnet ist und möglichst während das Problem auftritt.

   Es wird eine Datei generiert, die detaillierte Diagnoseinformationen enthält, u. a. Version, Inhalt der Receiver-Konfigurationsdateien und die Werte der verschiedenen Systemvariablen.

2. Überprüfen Sie, ob diese Datei vertrauliche Informationen enthält, bevor Sie sie an den technischen Support senden.

SDK und API

November 15, 2018

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für zusätzliche virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalanwendungen sind auf XenApp- oder XenDesktop-Servern. Diese Version des SDK bietet Unterstützung zum Schreiben neuer virtueller Kanäle für Receiver für Linux. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.

- Funktionierender Quellcode für mehrere Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen zum SDK finden Sie unter Citrix Virtual Channel SDK for Citrix Receiver for Linux.

Befehlszeilenreferenz und -parameter

Weitere Informationen zu Befehlszeilenreferenz und Parametern finden Sie unter Citrix Receiver for Linux Command Reference.

Platform Optimization SDK

Im Rahmen der HDX SoC-Initiative für Citrix Receiver für Linux haben wir das “Platform Optimization SDK” entwickelt, um ein Ökosystem kostengünstiger Geräte mit niedrigem Energieverbrauch, hoher Leistung und innovativen Formfaktoren zu ermöglichen.

Das Platform Optimization SDK kann von Entwicklern genutzt werden, um die Leistung von Linux-basierten Geräten zu verbessern, indem sie Plug-In-Erweiterungen für die ICA-Engine-Komponente (wfica) von Citrix Receiver für Linux entwickeln. Plug-Ins werden als freigegebene Bibliotheken entwickelt, die von wfica dynamisch geladen werden. Mit diesen Plug-Ins können Sie die Leistung Ihrer Linux-Geräte optimieren, indem Sie die folgenden Funktionen aktivieren:

- Beschleunigtes Decodieren von JPEG- und H.264-Daten, mit denen das Sitzungsbild erstellt wird
- Steuern der Speicherzuordnung zum Erstellen des Sitzungsbilds
- Verbessern der Leistung durch Steuern der unteren Ebene beim Erstellen des Sitzungsbilds
- Bereitstellen von Diensten für die Grafikausgabe und Benutzereingabe für Betriebssystemumgebungen, die X11 nicht unterstützen

Weitere Informationen finden Sie unter Citrix Receiver for Linux - Platform Optimization SDK.

