Systemanforderungen

May 12, 2015

In diesem Abschnitt werden die System- und Benutzeranforderungen für die Installation von Citrix Receiver für Linux beschrieben.

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 20 MB freier Speicherplatz für die installierte Receiver-Version und mindestens 40 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.

Für das clientseitige Rendering muss die Version des Adobe Flash Plug-Ins, die auf dem Benutzergerät ausgeführt wird, die gleiche oder eine höhere Version sein, die auf dem XenApp- oder XenDesktop-Server ausgeführt wird. Sonst steht nur das serverseitige Rendering zur Verfügung.

Citrix empfiehlt, immer die aktuelle Version des Plug-Ins zu verwenden, um die neuesten Funktionen und Sicherheitskorrekturen zu erhalten.

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 Pakets mit den Good Plug-Ins der Distribution.

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; im Allgemeinen ist Version 0.10.15 oder höher für HDX MediaStream Windows Media-Umleitung ausreichend.

Hinweis: Ansonsten können Sie GStreamer auch von http://gstreamer.freedesktop.org herunterladen. Für die Verwendung bestimmter Codecs ist u. U. eine Lizenz des Herstellers der jeweiligen Technologie erforderlich. Sie sollten sich von Ihrer Rechtsabteilung beraten lassen, ob für die Codecs, die Sie verwenden möchten, zusätzliche Lizenzen notwendig sind.

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
>
> 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. Speichern Sie den Speicherort mit den folgenden Schritten in einer Konfigurationsdatei, damit Receiver für Linux den PKCS#11-Treiber findet:

1. Suchen Sie die Konfigurationsdatei: $ICAROOT/config/AuthManConfig.xml
2. Suchen Sie die Zeile PKCS11module und fügen Sie den Treiberspeicherort dem Element 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 SmartCardRemovalAction und fügen Sie dem Element "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 (eines der folgenden Produkte):
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5, Feature Pack 2 für Windows Server 2008 R2

    - Citrix XenApp 6.5 Feature Pack 1 für Windows Server 2008 R2
    - Citrix XenApp 6.5 für Windows Server 2008 R2
    - Citrix XenApp 6 für Windows Server 2008 R2
    - Citrix XenApp 5 für Windows Server 2008
    - Citrix XenApp 4, Feature Pack 2, für Unix-Betriebssysteme
- XenDesktop (eines der folgenden Produkte):
    - XenDesktop 7.6
    - XenDesktop 7.5
    - XenDesktop 7.1
    - XenDesktop 7.0
    - XenDesktop 5.6 Feature Pack 1
    - XenDesktop 5.6
    - XenDesktop 5.5
    - XenDesktop 5
- Citrix VDI-in-a-Box
    - VDI-in-a-Box 5.3
    - VDI-in-a-Box 5.2
- Sie können den browserbasierten Zugriff auf Citrix Receiver für Linux 13.3 (mit oder ohne NetScaler Gateway-Plug-In) in Kombination mit StoreFront Receiver für Web und dem Webinterface verwenden.
  StoreFront:

    - StoreFront 3.0.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 in Kombination mit StoreFront
    - Angebot der Installation von Citrix Receiver für Web-Site (mit StoreFront konfiguriert)
    - Angebot der Installation von Receiver von Citrix Webinterface 5.4
    - Bereitstellen über Active Directory-Gruppenrichtlinienobjekte
    - Bereitstellen über Microsoft System Center 2012 Configuration Manager

Browser

- Internet Explorer
  Verbindungen mit Receiver für Web oder dem Webinterface unterstützen den 32-Bit-Modus von Internet Explorer. Weitere Informationen zu den unterstützten Internet Explorer-Versionen finden Sie unter StoreFront-Systemanforderungen und Webinterface-Systemanforderungen.

- Mozilla Firefox 18.x (unterstützte Mindestversion)
- Google Chrome 21 oder 20 (erfordert StoreFront)
  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.

  Weitere Informationen zu in Domänen eingebundenen und nicht in Domänen eingebundenen Geräten finden Sie in der XenDesktop 7-Dokumentation.

- Für sichere Remote- oder lokale Verbindungen:
  - 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

  Verwaltete Windows-Geräte, die zu einer Domäne gehören (lokal und remote, mit oder ohne VPN), und Geräte, die nicht zu einer Domäne gehören (mit oder ohne VPN) werden unterstützt.

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

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 erfolgreich 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 eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Wenn der Benutzer weiterarbeitet, wird eine Liste der Apps angezeigt; die Apps können jedoch nicht gestartet werden.

Installieren von Stammzertifikaten auf Benutzergeräten

Weitere Informationen zur Installation von Stammzertifikaten auf Benutzergeräten und zur Webinterface-Konfiguration für die Verwendung von Zertifikaten finden Sie unter Sichern der Receiver-Kommunikation.

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 Konfigurieren von Zwischenzertifikaten.

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 sh hdxcheck.sh ein, um das Skript auszuführen.

Installation und Einrichtung

Jun 08, 2016

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_13.3.0.344519_amd64.deb	Self-Service-Support, 64 Bit, x86_64
icaclient_13.3.0.344519_i386.deb	Self-Service-Support, 32 Bit, x86
icaclient_13.3.0.344519_armhf.deb	Self-Service-Support, ARM HF
icaclient_13.3.0.344519_armel.deb	Self-Service-Support, ARM EL
icaclientWeb_13.3.0.344519_amd64.deb	nur Web Receiver, 64 Bit, x86_64
icaclientWeb_13.3.0.344519_i386.deb	nur Web Receiver, 32 Bit, x86
icaclientWeb_13.3.0.344519_armhf.deb	nur Web Receiver, ARM HF
icaclientWeb_13.3.0.344519_armel.deb	nur Web Receiver, ARM EL
ctxusb_2.6.344519_amd64.deb	USB-Paket, 64 Bit, x86_64
ctxusb_2.6.344519_i386.deb	USB-Paket, 32 Bit, x86
ctxusb_2.6.344519_armhf.deb	USB-Paket, ARM HF
ctxusb_2.6.344519_armel.deb	USB-Paket, ARM EL
Red Hat-Pakete (Red Hat, SUSE, Fedora, usw.)	
ICAClient-rhel-13.3.0.344519-0.x86_64.rpm	Self-Service-Support, basierend auf Red Hat (einschl. Linux-VDA), 64 Bit, x86_64

ICAClient-rhel-13.3.0.344519-0.i386.rpm	Self-Service-Support, basierend auf RedHat, 32 Bit, x86
ICAClient-suse-13.3.0.344519-0.x86_64.rpm	Self-Service-Support, basierend auf SUSE, 64 Bit, x86_64
ICAClient-suse-13.3.0.344519-0.i386.rpm	Self-Service-Support, basierend auf SUSE, 32-Bit, x86
ICAClient-suse11sp3-13.3.0.344519-0.x86_64.rpm	Self-Service-Support, basierend auf SUSE 11 sp3 (einschl. Linux-VDA), 64 Bit, x86_64
ICAClient-suse11sp3-13.3.0.344519-0.i386.rpm	Self-Service_Support, basierend auf SUSE 11 sp3, 32-Bit, x86
ICAClientWeb-rhel-13.3.0.344519-0.x86_64.rpm	nur Web Receiver, basierend auf Red Hat, 64 Bit, x86_64
ICAClientWeb-rhel-13.3.0.344519-0.i386.rpm	nur Web Receiver, basierend auf RedHat, 32 Bit, x86
ICAClientWeb-suse-13.3.0.344519-0.x86_64.rpm	nur Web Receiver, basierend auf SUSE, 64 Bit, x86_64
ICAClientWeb-suse-13.3.0.344519-0.i386.rpm	nur Web Receiver, basierend auf SUSE, 32 Bit, x86
ctxusb-2.6.344519-1.x86_64.rpm	USB-Paket, 64 Bit, x86_64
ctxusb-2.6.344519-1.i386.rpm	USB-Paket, 32 Bit, x86
Tarballs (Skriptinstallation für die Distribution)	
linuxx64-13.3.0.344519.tar.gz	64 Bit Intel
linuxx86-13.3.0.344519.tar.gz	64 Bit Intel
linuxarm-13.3.0.344519.tar.gz	ARM EL
linuxarmhf-13.3.0.344519.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 Obermenge 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, dann 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 normalerweise einfacher zu verwenden, da sie automatisch alle erforderlichen Pakete installieren. Wenn die den Installationsort steuern möchten, installieren Sie Citrix Receiver vom Tarball-Paket.

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 ***Paketname*** 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 **dpkg -i packagename.deb** eingeben. Beispiel:

- dpkg -i icaclient_13.2.1.328635 _amd64.deb
- dpkg -i icaclientWeb_13.2.1.328635_amd64.db
- dpkg -i ctxusb_2.5.328635_amd64.deb

4. Installieren Sie alle fehlenden Elemente 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 ***Paketname*** durch den Namen des Pakets, das Sie installieren.
Hinweis: Wenn in einer Fehlermeldung angezeigt wird, dass die Installation auf der Basis der Red Hat-Distributionen (RHEL, CentOS, Fedora, usw.) libwebkitgtk-1.0.so.0 erfordert, 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.3

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** an einer Befehlszeile unter OpenSUSE oder **yum localinstall** 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 3 Pakete aus, indem Sie "zypper" in packagename.rpm eingeben.

3. Öffnen Sie ein Terminal-Fenster.

    Für SUSE-Installationen:

    zypper in ICAClient-suse-13.2.1.328635-0.x86_64.rpm

    zypper in ICAClient-suse-11sp3-13.2.1.328635-0.i386.rpm

    zypper in ctxusb-2.5.328635-1.x86_64.rpm

    Für Red Hat-Installationen:

    yum localinstall ICAClient-rhel-13.2.1.328635-0.i386.rpm

    yum localinstall ICAClientWeb-rhel-13.2.1.328635-0.i386.rpm

    yum localhost ctxusb-2.5.328365.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 "j" 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.

Hinweis: Damit die Integration zuverlässig funktioniert, wenn Receiver nicht am Standardspeicherort installiert wird, legen Sie den Speicherort in $ICAROOT in $HOME/.profile oder $HOME/.bash_profile fest.

8. Wenn Sie GStreamer installiert haben, können Sie entscheiden, ob GStreamer mit Receiver integriert werden soll, und so HDX Mediastream-Multimediabeschleunigung bereitstellen.Um Receiver mit GStreamer zu integrieren, geben Sie an der Eingabeaufforderung "j" ein.

9. Wenn Sie als privilegierter Benutzer (root) angemeldet sind, können Sie entscheiden, ob Sie die USB-Unterstützung für mit XenDesktop und XenApp veröffentlichte Anwendungen aktivieren möchten.Geben Sie an der Eingabeaufforderung "j" 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

Feb 10, 2015

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

> ## Hinweis
>
> Sie können einer Beispielinstallation im folgenden Citrix Blog-Artikel folgen: Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop.

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 Receiver-Paket vor. Sie können dem Paket beispielsweise ein neues 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 neues SSL-Stammzertifikat hinzufügen, finden Sie unter
   — Installieren von Stammzertifikaten auf Benutzergeräten
   in den eDocs. Weitere Informationen über integrierte Zertifikate finden Sie unter
   — Konfigurieren und Aktivieren von SSL und TLS
   in den eDocs.
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 sollte immer cor eingestellt sein)
   - Berechtigungen
   - Besitzer
   - Gruppe
   - Größe
8. Speichern und schließen Sie die Datei.
9. Erstellen Sie die Receiver-Paketdatei mit dem Befehl tar neu, z. B.: tar czf ../newpackage.tar.gz * wobei newpackage der Name der neuen Receiver-Paketdatei ist.

Starten von Citrix Receiver für Linux

Jul 15, 2013

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 ICAROOT auf das richtige Installationsverzeichnis verweisen.

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

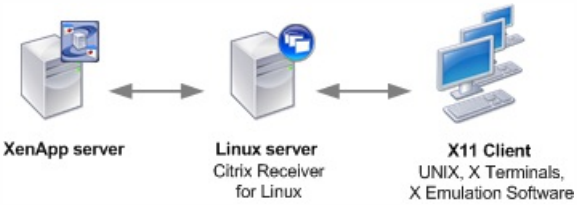
Sep 24, 2014

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. Folglich können Sie 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:

- 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.

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 <proxy server name>
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.

Deinstallieren von Citrix Receiver für Linux

Sep 18, 2014

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

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

Sep 22, 2014

Citrix Receiver 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 Receiver- Benutzeroberfläche

Die Citrix Receiver-Homepage 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 der gleiche Name für mehrere Stores auf dem StoreFront-Server verwendet wird, erscheinen die Stores auf der Seite "Konten" als identisch. Um Klarheit für die Benutzer zu schaffen, sollten Administratoren beim Konfigurieren von Stores eindeutige Namen verwenden. Für PNAgent wird die Store-URL angezeigt, die den Store eindeutig identifiziert.

Nach dem Herstellen einer Verbindung zu einem Store können Benutzer Desktops und Anwendungen suchen oder zu diesen navigieren, indem sie auf das Pluszeichen (+) auf der Citrix Receiver-Homepage klicken. Beim Klicken auf ein Desktop- oder Anwendungssymbol wird die Ressource zur Homepage kopiert, auf der Benutzer mit einem weiteren Klick die Ressource starten. Dabei wird eine Verbindung erstellt.

Konfigurieren von Verbindungseinstellungen

Sie können eine Reihe von Standardeinstellungen für Verbindungen zwischen Citrix Receiver und XenApp- und XenDesktop-Servern konfigurieren. Sie können diese Einstellungen für einzelne Verbindungen ändern, wenn dies erforderlich ist.

Die Informationen im übrigen Teil der eDocs enthalten Verfahren für typische, von Benutzern von Citrix Receiver ausgeführten Aufgaben. Obwohl sich die Aufgaben und Verantwortungsbereiche von Administratoren und Benutzern überschneiden können, wird der Ausdruck "Benutzer" in diesem eDocs-Abschnitt dort verwendet, wo Aufgaben beschrieben werden, die normalerweise von Benutzern und nicht von Administratoren ausgeführt werden.

- Verbinden mit Ressourcen per Eingabeaufforderung oder Browser
- Problembehandlung bei Verbindungen mit Ressourcen
- Anpassen von Receiver mit Konfigurationsdateien

Verbinden mit Ressourcen per Eingabeaufforderung oder Browser

Sep 18, 2014

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 auf dem Server verfügbar ist. Falls erforderlich, fügen Sie ihn mit dem folgenden Befehl hinzu:

./util/storebrowse --addstore

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

     ./util/storebrowse -S
2. Führen Sie folgenden Befehl aus, um den Desktop oder die Anwendung zu starten:
   ./util/storebrowse –L

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

Für Mozilla, Netscape und Chrome erfolgt die Verbindungskonfiguration normalerweise automatisch während der Installation.

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

1. Für MAILCAP-Dateien erstellen oder bearbeiten Sie im Verzeichnis $HOME die MAILCAP-Datei und fügen Sie die folgende Zeile hinzu:
   application/x-ica; /opt/Citrix/ICAClient/wfica.sh %s; x-mozilla-flags=plugin:Citrix ICA

2. Für MIME-Dateien erstellen oder bearbeiten Sie im Verzeichnis $HOME die Datei .mime.types und fügen Sie die folgende Zeile hinzu:
   application/x-ica ica

   Die Zeichenfolge x- vor dem Format ica gibt an, dass es sich bei ica um einen inoffiziellen MIME-Typ handelt, der nicht von IANA (Internet Assigned Numbers Authority) unterstützt wird.

Problembehandlung bei Verbindungen mit Ressourcen

Sep 18, 2014

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. Hierbei 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 Receiver-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

Aug 16, 2013

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 Änderungen auf alle Citrix Receiver-Benutzer

Wenn Ihre Änderungen für alle Citrix Receiver-Benutzer gelten sollen, 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 Standardwert festgelegt wird, wird der Wert in module.ini nicht verwendet.

Anwenden von Änderungen auf neue Citrix Receiver-Benutzer

Wenn Ihre Änderungen für alle zukünftigen Citrix Receiver-Benutzer gelten sollen, bearbeiten Sie die Konfigurationsdateien im Verzeichnis $ICAROOT/config. Damit Änderungen für alle Verbindungen gelten, müssen Sie die Datei wfclient.ini in diesem Verzeichnis aktualisieren.

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. 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. Wenn Änderungen für alle Receiver-Benutzer gelten sollen, ändern Sie die Datei module.ini.

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

Jul 15, 2013

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.

> **Important**
>
> 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.

Receiver erkennt nicht alle Dateitypen. Das System erkennt nur dann den Dateityp der veröffentlichten Inhalte und die Benutzer können die Inhalte nur dann über Recevier anzeigen, wenn eine Zuordnung zwischen einer veröffentlichten Anwendung und dem Dateityp der veröffentlichten Datei besteht. Um beispielsweise eine veröffentlichte Adobe PDF-Datei mit Receiver 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

Aug 16, 2013

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
- Steigern der Leistung über Verbindungen mit geringer Bandbreite
- Steigern der Multimedialeistung
- Optimieren der Leistung für Bildschirmkacheln

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 Clientlaufwerkszuordnung 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 Clientlaufwerkszuordnung 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 Laufwerkszuordnung:

- Die statische Clientlaufwerkszuordnung 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 Einhängepunkte von Hardwaregeräten wie CD-ROMs, DVDs oder USB-Sticks zuordnen.
- Die dynamische Clientlaufwerkszuordnung überwacht die Verzeichnisse, in denen Hardwaregeräte wie CD-ROMs, DVDs und USB-Sticks üblicherweise auf dem Benutzergerät eingehängt 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 XenApp- und XenDesktop-Dokumentation.

Benutzer können Laufwerke im Dialogfeld Einstellungen zuordnen. Weitere Informationen finden Sie unter Festlegen von Einstellungen.

Hinweis: Standardmäßig wird durch das Aktivieren der statischen Clientlaufwerkzuordnung auch die dynamische Clientlaufwerkzuordnung aktiviert. Damit beim Aktivieren der statischen Clientlaufwerkszuordnung die dynamische Clientlaufwerkszuordnung 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, 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 Benutzer von Receiver einzuschränken, die das Programm selfservice nach der vorgenommenen Änderung als erste verwenden.
2. Geben Sie im Abschnitt [WFClient] der Datei Folgendes ein:
   ClientPrinterList=printer1:printer2:printer3

   Dabei sind printer1, printer2 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 in den meisten Fällen 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. Klicken Sie im Startmenü auf Einstellungen > Drucker.
3. Klicken Sie im Menü Datei auf Drucker hinzufügen.

   Der Druckerinstallations-Assistent wird angezeigt.

4. Fügen Sie mit dem Assistenten einen Netzwerkdrucker aus dem Client-Netzwerk und der Client-Domäne hinzu. in den meisten Fällen ist dies ein Standarddruckername, ähnlich den Druckernamen, die mit den Remotedesktopdiensten erstellt werden, z. B. "HP LaserJet 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 im Abschnitt XenApp für Unix in den eDocs.

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 XenApp- und XenDesktop-Dokumentation.

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 = <device>

Die Informationen für device 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 und 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 Webkameras, Mikrofone, Lautsprecher und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz und hoher Geschwindigkeit unterstützt, in den meisten Fällen ist die standardmäßige Audio- oder Webkameraumleitung jedoch geeigneter.

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

- Tastaturen
- Mäuse
- Smartcards
- Headsets
- Webkameras

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-Geräte-Liste.

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

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 und es wird möglicherweise 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. Verwenden Sie auf Geräten mit Debian die Debian-Menüleiste, indem Sie unter System > Einstellungen > Wechseldatenträger und -medien auf der Registerkarte Speicherort unter Wechseldatenträger das Kontrollkästchen Wechselmedien beim Einlegen einbinden deaktivieren.
Hinweis: Wenn die Serverrichtlinie Client-USB-Geräteumleitung aktiviert ist, werden Massenspeichergeräte wie USB-Geräte umgeleitet, selbst wenn die Clientlaufwerkzuordnung aktiviert ist.

Webkameras

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen jedoch, müssen Benutzer Webcams mit USB-Unterstützung anschließen. Hierzu müssen Sie HDX RealTime-Webkameravideokomprimierung deaktivieren. Weitere Informationen finden Sie unter Konfigurieren von 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 und eine Kamera kann möglicherweise über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

Hinweis: Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkszuordnung 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 Clientlaufwerkszuordnung 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)

Viele Geräte verwenden herstellerspezifische Protokolle oder Protokolle, die nicht vom USB-Konsortium genormt sind; sie werden normalerweise als herstellerspezifisch (Geräteklasse ff) angezeigt.

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 werden ohne USB-Unterstützung ausreichend gehandhabt und 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. Webkameras, 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 neue Richtlinienregeln erstellen, verwenden Sie die USB-Klassencodes, die Sie auf der USB-Website unter http://www.usb.org/ finden.
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 neue 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 Verweigernregel in den USB-Richtlinien auf dem Server (Registrierungseintrag) oder dem Benutzergerät (Konfigurationsdatei der Richtlinienregeln) deaktiviert ist.
FALSE	Keine USB-Geräte starten.

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 mit einer Reihe von Änderungen in der 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 der 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 der Farbanzahl**: Reduzieren Sie die Anzahl der Farben auf 256. Legen Sie auf der XenApp Services-Site die Sitzungsoptionen fest.
- **Verringern der 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		
		Hoch	Mittel	Niedrig
Audioqualität auf dem Server	Hoch	Hoch	Mittel	Niedrig
	Mittel	Mittel	Mittel	Niedrig
	Niedrig	Niedrig	Niedrig	Niedrig

Wenn UDP-Audio aktiviert ist aber die resultierende Qualität nicht "Mittel" ist, wird TCP und nicht UDP für die Audioübertragung verwendet.

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 Clientlaufwerkszuordnung 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**: Das Wiedergeben von Multimedia-Inhalten 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

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), er behandelt aber keine Mediendaten. Dieses Feature erfordert erweiterte GStreamer-Multimediabibliotheken auf dem Gerät.

Implementieren der Windows Media-Umleitung

1. Installieren Sie GStreamer 0.10, ein Open-Source-Multimedia-Framework, auf jedem erforderlichen Benutzergerät. Normalerweise installieren Sie GStreamer vor Receiver.
   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 Receiver auf dem Gerät die GStreamer-Option.

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 sollten möglichst eine Standard-URL angeben, die nicht auf diese Dateitypen verweist. Überprüfen Sie mit gst-launch, ob eine URL gültig ist.

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 **Ask**. 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 Megabytes (MB). Die Größe kann zwischen 25 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. Damit Receiver-Sitzungen Tastatur- und Mauseingaben innerhalb und außerhalb eines Fensters handhabt, in dem Flash-Inhalte wiedergegeben werden, ändern Sie in der Datei /config/module.ini den Eintrag FlashV2=Off zu FlashV2=On.

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, Skype oder Microsoft Office Communicator 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" gesetzt 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 jedoch, 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 (standardmäßig über HDX RealTime-Webcamvideokomprimierung)

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.

Verbessern der Benutzererfahrung

Jan 31, 2011

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

- Festlegen von Einstellungen
- Konfigurieren der ClearType-Schriftartenglättung
- Konfigurieren der Umleitung spezieller Ordner
- Einrichten der Server-zu-Client-Inhaltsumleitung
- Steuern des Tastaturverhaltens
- Verwenden von xcapture
- Automatische Wiederverbindung von Benutzern
- Sicherstellen der Sitzungszuverlässigkeit

Festlegen von Einstellungen

Sie können Einstellungen festlegen, indem Sie im Citrix Receiver-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 neues Konto zu Citrix Receiver hinzuzufügen, oder aber einen anderen NetScaler Gateway- oder Access Gateway-Server für ein vorhandenes Konto zu verwenden. Sie können Konten auch aus Citrix Receiver 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 neues 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.

1. Wählen Sie auf der Seite Allgemein im Dialogfeld Einstellungen einen Modus unter Anzeige für Desktops aus.

Automatisches Wiederherstellen von Sitzungsverbindungen

Citrix Receiver kann Desktops und Anwendungen, deren Verbindung getrennt wurde (zum Beispiel bei einem Problem mit der Netzwerkinfrastruktur), wiederverbinden.

1. 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:

1. 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:

1. 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 oder die Art der Glättung über die folgende Einstellung im Abschnitt [WFClient] der jeweiligen Konfigurationsdatei angeben:

FontSmoothingType = number

wobei number einen der folgenden Werte haben kann:

Wert	Ergebnis

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

Sowohl Standardglättung als auch ClearType-Glättung erhöhen die Bandbreitenanforderungen von Receiver erheblich.

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 = Nummernumber

wobei number einen der folgenden Werte haben kann:

Wert	Ergebnis
0	Keine Glättung
1	
2	Standardglättung
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 besonders wichtig, wenn Benutzer, die häufig den Standort wechseln, sich an Servern in unterschiedlichen Serverfarmen anmelden müssen. 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.
   - Sie müssen für beide Parameter Werte angeben.
   - Die Verzeichnisse, die Sie angeben, müssen über die Clientgerätzuordnung verfügbar sein, d. h. das Verzeichnis muss sich in der Struktur eines verknüpften Clientgeräts befinden.
   - Sie müssen die Laufwerksbuchstaben C oder höher verwenden.

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 Citrix Receiver 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 Citrix Receiver aktiviert, vorausgesetzt der Pfad enthält RealPlayer und mindestens einen Browser wie Firefox, Mozilla oder Netscape.

> **Hinweis**
>
> RealPlayer für Linux steht unter http://proforma.real.com/real/player/unix/unix.html zur Verfügung.

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 Dienstprogramm "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 Receiver

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+Entfernen 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 Receiver-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 Receiver 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 dieses Feature mit der HDX Broadcast -Sitzungszuverlässigkeit verwendet wird.

Benutzer können von ICA-Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit der automatischen HDX Broadcast-Wiederverbindung von Clients kann Citrix Receiver 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 Receiver, 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 Citrix Receiver 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 Verbindungsproblem kann bis zu 25 Sekunden dauern; dann wird nach einem konfigurierbaren 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 Receiver-Benutzer können die Servereinstellungen nicht außer Kraft setzen. Weitere Informationen hierzu finden Sie in der XenApp- und XenDesktop-Dokumentation.

Important

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.

Sicherheit

Feb 16, 2016

Dieser Abschnitt enthält folgende Themen:

- Herstellen von Verbindungen über Proxyserver
- Verbinden mit Secure Gateway oder dem Citrix SSL-Relay
- Verbindungen über NetScaler Gateway

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" benötigen, 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.

> **Important**
>
> 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 auch von http://www.openssl.org/ heruntergeladen werden.

Verbinden mit Secure Gateway oder dem Citrix SSL-Relay

Sie können Receiver in eine Umgebung mit Secure Gateway oder dem SSL-Relay (Secure Sockets Layer) 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 nacheinander 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 im Allgemeinen 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 der Benutzer SSL/TLS+HTTPS-Browsing gewählt hat, werden die Daten an den Citrix XML-Dienst 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

Dies 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: Diese Version von Citrix Receiver für Linux deaktiviert die Verwendung des SSLv3-Protokolls.
Für TCP-Verbindungen zwischen Citrix Receiver und XenApp/XenDesktop unterstützt Citrix Receiver für Linux TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Für UDP-Verbindungen zwischen Citrix Receiver und XenApp/XenDesktop unterstützt Citrix Receiver für Linux DTLS 1.0 mit den folgenden Verschlüsselungssammlungen:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

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

Zertifikat	Zertifizierungsstelle
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

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.

Wichtig: Citrix Receiver unterstützt nur Schlüssel mit maximal 4096 Bits. Sie müssen sicherstellen, dass die Stamm- und Zwischenzertifikate der Zertifizierungsstellen sowie ihre Serverzertifikate maximal 4096 Bits lang sind.
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 müssen, 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):
   1. Kopieren Sie die Datei in $ICAROOT/keystore/cacerts.
   2. 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 Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren müssen, führen Sie die 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):
   1. Kopieren Sie die Datei(en) zu $ICAROOT/keystore/intcerts.
   2. Führen Sie den folgenden Befehl als der Benutzer aus, der das Paket installiert hat:
      $ICAROOT/util/ctx_rehash

Aktivieren der Smartcard-Unterstützung

Citrix Receiver für Linux unterstützt zahlreiche Smartcardleser. Wenn Smartcard-Unterstützung 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 Smartcard-Unterstützung müssen folgende Voraussetzungen erfüllt sein:

- Die Smartcardleser und die veröffentlichten Anwendungen müssen dem PC/SC-Industriestandard entsprechen.
- Für den Smartcardleser muss der geeignete Treiber installiert werden.
- Sie müssen das PC/SC Lite-Paket installieren.
- Sie müssen den pcscd Daemon installieren und ausführen, der Middleware für den Zugriff auf die Smartcard mit PC/SC bereitstellt.
- 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, müssen Sie das PC/SC SRCOM-Bypass-Paket installieren, das unter http://www.sun.com/ zum Download zur Verfügung steht.
Weitere Informationen zur Konfiguration der Smartcard-Unterstützung auf den Servern finden Sie in der Dokumentation für XenDesktop und XenApp.

Verbindungen 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 des Formats https://gateway.company.com.
   - Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im Format https://gateway.company.com? . 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.

Problembehandlung

May 28, 2013

Dieser Artikel enthält Informationen für Administratoren zur Fehlerbehebung von Problemen in Citrix Receiver für Linux.

Verbindungsprobleme

Die folgenden Verbindungsprobleme kommen vor.

Windows Media Player gibt bestimmte Dateiformate nicht wieder

Citrix Receiver hat möglicherweise nicht die 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 und der Server dann ein anderes Format anfordert oder das Medium selbst wiedergibt.

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.

Benutzer haben Probleme beim Herstellen einer Verbindung zu einer

veröffentlichten Ressource oder einer Desktopsitzung

Wenn beim Herstellen einer Verbindung 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 Lizenzieren des Produkts.

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. Beachten Sie aber, dass für TLS-Verbindungen ein vollqualifizierter Domänenname und keine IP-Adresse erforderlich ist.

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:

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.

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=
Zum Konfigurieren von mehreren seriellen Anschlüssen fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=2
ComPort1=
ComPort2=

Verbindungsfehler

Eine Fehlermeldung mit folgendem Wortlaut wird angezeigt: "Fehler bei Verbindung: Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten". Dieser Fehler kann durch verschiedene Probleme verursacht werden:

- Der lokale Computer und der Remotecomputer können kein gemeinsames TLS-Protokoll verhandeln.
- 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, was bedeutet, dass vSync 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"
        Identifier    "Intel Graphics"
        Driver        "intel"
        Option        "AccelMethod" "sna"
        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}
```

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). Sie müssen den "ComprizConfig Settings Manager" installieren.

  Führen Sie "ComprizConfig Settings Manager"
  unter "General->Composition" aus und deaktivieren Sie "Undirect Fullscreen Windows"
  Hinweis: Seien Sie vorsichtig bei der Verwendung von "ComprizConfig Settings Manager", da das System u. U. nicht starten kann, wenn Sie die falschen Werte 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 schnell 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.

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, verwendet wfica die Meldung _NET_WM_FULLSCREEN_MONITORS, um ein entsprechendes Fensterlayout vom Fenstermanager anzufordern, 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: Sie müssen die Variable WFICA_OPTS definieren, bevor Sie Self-Service 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. Beispiel:
   export WFICA_OPTS="-span a"
   Beachten Sie, dass sich diese Änderung auf XenApp- und XenDesktop-Sitzungen auswirkt.
   Wenn Sie selfservice oder storebrowse schon gestartet haben, müssen Sie die von ihnen gestarteten Prozesse entfernen, 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

Dies tritt auf, da 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

Zusätzlich kommen die folgenden Probleme vor.

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

Wenn eine veröffentlichte Anwendung Zugriff auf einen seriellen Port benötigt, 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 sperrt; 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 und die Fehlermeldung "Application default file could not be found or is out of date" angezeigt wird, 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 Herunterladen und Installieren von Receiver für Linux.

  Wenn Receiver vorher im Standardverzeichnis installiert worden war, sollten Sie vor der Neuinstallation das Verzeichnis /opt/Citrix/ICAClient oder $HOME/ICAClient/Plattform entfernen.

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.

Ermitteln der Versionsnummer für das Citrix 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

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.

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 neuen 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 neue Konfigurationsdatei.

E_INI_VALUE_SYNTAX – Der Wert "..." in der Konfigurationsdatei "..." ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Erstellen Sie eine neue 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.

Befehlszeilenparameter

Mar 03, 2015

In den Tabellen unten werden Befehlszeilenparameter für Citrix Receiver für Linux aufgeführt.

> ## Hinweis
>
> Eine Liste der Parameter erhalten Sie durch Eingabe von wfica oder storebrowse mit der Option -?, -help oder -h.

wfica

Sie können eine Verbindungsdatei verwenden, wenn Sie einfach den Dateinamen nach wfica ohne eine der folgenden Optionen eingeben.

Vorgang	Eingabe
Festlegen der in der Verbindungsdatei zu verwendenden benutzerdefinierten Verbindung **Hinweis:** Mit der neuen Self-Service-Benutzeroberfläche können Sie auf diese Weise keine benutzerdefinierte Verbindung einrichten.	-desc description -description description
Geben Sie eine Desktopdatei an, die für den Start verwendet wird.	-desktop filename
Festlegen einer Verbindungsdatei	-file connection filename
Festlegen einer alternativen Protokolldatei. Dies ermöglicht die Verwendung einer alternativen module.ini-Datei.	-protocolfile filename
Festlegen einer alternativen Client-Konfigurationsdatei. Dies ermöglicht die Verwendung einer alternativen wfclient.ini-Datei.	-clientfile filename
Anzeigen eines anderen Namens für Citrix Receiver, festgelegt durch Name, wenn der Name angezeigt wird. Der Standardname ist der Gerätename. Bei Verwendung eines Sun Ray-Gerätes wird der Standardname jedoch von der MAC-Adresse des Geräts abgeleitet. Dieser wird jedoch durch den Eintrag "ClientName" in der Datei .ICAClient/wfclient.ini überschrieben; dieser wird wiederum durch den Befehl -clientname Name überschrieben.	-clientname name
Anzeigen dieser Parameterliste.	-help
Anzeigen von Versionsinformationen.	-version

Vorgang	Eingabe
Anzeigen von Fehlernummern und -meldungen.	-error
Festlegen des Speicherorts von Receiver-Installationsdateien. Dies entspricht der Einstellung der Umgebungsvariablen ICAROOT.	-icaroot directory
Unterdrücken von Verbindungsdialogfeldern.	-quiet
Protokollieren des Anmeldevorgangs.	-log
Aktivieren der Tastaturprotokollierung	-keylog
Einrichten der Geometrie der Sitzung.	-geometry WxH+X+Y
Festlegen der Farbtiefe.	-depth <4 | 8 | 16 | 24 | auto>
Festlegen der Monitorausrichtung.	-span [h][o] [a | mon1[,mon2[,mon3,mon4]]]
Verwenden einer eigenen Farbzuordnung.	-private
Verwenden einer gemeinsam genutzten Farbzuordnung.	-shared
Festlegen einer Zeichenfolge, die einer veröffentlichten Anwendung hinzugefügt wird.	-param string
Festlegen des UNIX-Pfads, auf den eine veröffentlichte Anwendung über die Clientlaufwerkszuordnung zugreifen kann.	-fileparam unixpath
Angeben eines Benutzernamens.	-username username
Angeben eines verschlüsselten Kennworts.	-password password
Angeben eines Klartextkennworts.	-clearpassword "clear password"
Festlegen einer Domäne.	-domain domain
Festlegen eines Startprogramms.	-program program
Festlegen eines Verzeichnisses, das das erste Programm verwenden kann.	-directory directory

Vorgang	Eingabe
Aktivieren der Tonwiedergabe.	-sound
Deaktivieren der Tonwiedergabe.	-nosound
Überschreiben von Laufwerkszuordnungen. Diese sind im Format A$=Pfad, wobei Pfad eine Umgebungsvariable enthalten kann (z. B. A$=$HOME/tmp). Diese Option muss für jedes zu überschreibende Laufwerk wiederholt werden. Es muss eine Zuordnung vorhanden sein, damit die Überschreibung funktioniert, die Zuordnung muss jedoch nicht aktiviert sein.	-drivemap string

Tip: Alle wfica-Befehlszeilenoptionen können auch in der Umgebungsvariable WFICA_OPTS angegeben werden. Hierdurch können sie mit der nativen Benutzeroberfläche von Receiver oder mit Citrix StoreFront verwendet werden.

storebrowse

In der folgenden Tabelle werden die Optionen aufgeführt, die Sie mit dem Hilfsprogramm storebrowse verwenden können.

Option	Beschreibung	Hinweise
-L, --launch	Gibt den Namen der veröffentlichten Ressourcen an, mit denen Sie eine Verbindung herstellen möchten. Es wird eine Verbindung zu einer veröffentlichten Ressource gestartet. Das Hilfsprogramm wird dann beendet, die erfolgreich verbundene Sitzung bleibt zurück.	
-E, --enumerate	Enumeriert die verfügbaren Ressourcen.	Standardmäßig werden Ressourcenname, Anzeigename und Ordner der Ressource angezeigt. Weitere Informationen können mit der Option --details angezeigt werden.
-S, --subscribed	Listet die abonnierten Ressourcen auf.	Standardmäßig werden Ressourcenname, Anzeigename und Ordner der Ressource angezeigt. Weitere Informationen können mit der Option –details angezeigt werden.
-M, --details Verwendung zusammen mit der Option -E oder -S	Wählt, welche Attribute der veröffentlichten Anwendungen zurückgegeben werden. Das zugehörige Argument ist die Summe der Zahlen, die mit den erforderlichen Details korrespondieren: Publisher(0x1), Video Type(0x2), Sound Type(0x4), AppInStartMenu(0x8), AppOnDesktop(0x10), AppIsDesktop(0x20), AppIsDisabled(0x40),WindowType(0x80), WindowScale(0x100), DisplayName(0x200) und AppIsMandatory(0x10000). CreateShortcuts(0x100000) kann zusammen mit -S,	Manche dieser Details sind nicht über storebrowse verfügbar. In dem Fall ist die Ausgabe 0. Werte können auch dezimal sowie hexadezimal (z. B. 512 für 0x200) ausgedrückt werden.

Option	Beschreibung	Hinweise
	-s und -u verwendet werden, um Menüeinträge für abonnierte Anwendungen zu erstellen. RemoveShortcuts(0x200000) kann mit -S zum Löschen aller Menüeinträge verwendet werden.	
-v, --version	Schreibt die Versionsnummer von storebrowse in die Standardausgabe.	
-?, -h, --help	Listet die Syntax für storebrowse auf.	Eine verkürzte Version dieser Tabelle wird angezeigt.
-U, --username	Gibt den Benutzernamen an den Server weiter.	Diese Optionen sind veraltet und werden ggf. aus zukünftigen Releases entfernt. Sie funktionieren bei Program Neighborhood Agent-Sites, bei StoreFront-Sites werden sie jedoch ignoriert. Citrix empfiehlt, diese Optionen nicht zu verwenden, sondern zuzulassen, dass Benutzer vom System aufgefordert werden, ihre Anmeldeinformationen einzugeben.
-P, --password	Gibt das Kennwort an den Server weiter.	
-D, --domain	Gibt die Domäne an den Server weiter.	
-r, --icaroot	Gibt das Stammverzeichnis für die Receiver für Linux-Installation an.	Der Wert wird zur Laufzeit ermittelt, wenn Sie ihn nicht angeben.
-i, --icons Verwendung zusammen mit der Option -E oder -S	Ruft Desktop- oder Anwendungssymbole im PNG-Format in der mit dem Argument best bzw. size vorgegebenen Größe und Tiefe ab. Wird das Argument best verwendet, wird das Symbol auf dem Server in der besten Größe abgerufen. Sie können es in jede erforderliche Größe umwandeln. Das Argument best ist nach Speicher- und Bandbreitengesichtspunkten das effizienteste und kann die Skripterstellung vereinfachen. Wird das Argument size verwendet, wird ein Symbol der angegebenen Größe und Tiefe abgerufen. In beiden Fällen werden Symbole in einer Datei für jede Ressource, die mit der Option "-E" oder "-S" zurückgegeben wird, gespeichert.	Durch das Argument best wird ein Symbol im Format .png erstellt. Das Argument size besitzt die Form WxB, wobei W die Breite des Symbols (es ist nur ein Wert erforderlich, da alle Symbole quadratisch sind) und B die Farbtiefe (d. h. die Anzahl der Bits pro Pixel) ist. W ist erforderlich, B ist optional. Wird B nicht angegeben, werden Symbole aller verfügbaren Tiefen in der Größe abgerufen. Die erstellten Dateien erhalten den Namen _WxWxB.png.
-u, --unsubscribe	Kündigt das Abonnement der angegebenen Ressource aus dem jeweiligen Store.	
-s, --subscribe	Abonniert die angegebene Ressource aus dem jeweiligen Store.	Wenn Sie einen anderen Receiver verwenden, gehen Abonnements auf Program

Option	Beschreibung	Hinweise
-W [r|R], --reconnect [r|R]	Stellt die Verbindung getrennter und aktiver Sitzungen wieder her.	r stellt die Verbindung für alle getrennten Sitzungen des Benutzers wieder her. R stellt die Verbindung für alle aktiven und getrennten Sitzungen wieder her.
-WD, --disconnect	Trennt alle Sitzungen.	Betrifft nur Sitzungen an dem Store, der in der Befehlszeile angegebenen wurde.
-WT, --logoff	Meldet alle Sitzungen ab.	Betrifft nur Sitzungen an dem Store, der in der Befehlszeile angegebenen wurde.
-l, --liststores	Listet die bekannten StoreFront-Stores auf, d. h. solche, die storebrowse kontaktieren kann. Dies sind die beim ServiceRecord-Proxy registrierten Stores. Außerdem werden die Program Neighborhood-Sites aufgelistet.	
-a, --addstore	Registriert einen neuen Store einschließlich Gateway und Beacon beim Diensteintragsdaemon.	Gibt die vollständige URL des Stores zurück. Wenn dies fehlschlägt, wird ein Fehler gemeldet.
-g, --storegateway	Legt das Standardgateway für einen Store fest, der bereits beim Diensteintragsdaemon registriert ist.	Dieser Befehl hat das folgende Format: ./util/storebrowse --storegateway "" " Wichtig: Der eindeutige Gatewayname (unique gateway name) muss in der Liste der Gateways für den angegebenen Store enthalten sein.
-d, --deletestore	Hebt die Registrierung eines Stores beim Diensteintragsdaemon auf.	
-c, --configselfservice	Dient zum Aufrufen und Festlegen der in StoreCache.ctx gespeicherten Einstellungen der Self-Service-Benutzeroberfläche. Das zugehörige Argument hat das Format . Wenn nur ein Eintrag (entry) vorhanden ist, wird der aktuelle Wert der Einstellung aufgerufen. Ist ein Wert (value) vorhanden, wird er zum Konfigurieren der Einstellung verwendet.	Beispiel: storebrowse --configselfservice SharedUserMode=True Wichtig: Bei Eintrag und Wert wird zwischen Groß- und Kleinschreibung unterschieden. Befehle mit dieser Option schlagen fehl, wenn die Groß- und Kleinschreibung nicht der in StoreCache.ctx dokumentierten Groß- und Kleinschreibung der Einstellung selbst entspricht.
-C, --addCR	Liest die bereitgestellte Citrix Receiver-Datei (CR) und fordert den Benutzer zum Hinzufügen jedes Stores auf.	Die Ausgabe ist wie bei -a, kann aber mehrere Stores auf jeweils neuen Zeilen enthalten.
-K, --killdaemon	Beendet den storebrowse-Daemonprozess.	Alle Anmeldeinformationen und Tokens werden gelöscht.

Neighborhood Agent-Servern verloren.

Option	Beschreibung	Hinweise
pnabrowse		

Wichtig: Das Hilfsprogramm pnabrowse ist veraltet, kann aber trotzdem zur Abfrage von Program Neighborhood Agent-Sites verwendet werden, auf denen das Webinterface für Listen von Servern und veröffentlichten Ressourcen ausgeführt wird, und es ermöglicht das Herstellen einer Verbindung zu einer veröffentlichten Ressource. Citrix rät von der Verwendung von pnabrowse für StoreFront-Stores ab. Verwenden Sie stattdessen storebrowse. storebrowse kann die Eingabe von Anmeldeinformationen für Sites und Stores anfordern. Die Optionen -U, -P und -D funktionieren nur bei Program Neighborhood Agent-Sites.
Ein optionales Argument von pnabrowse gibt den Server an, mit dem eine Verbindung hergestellt werden soll. Es wird Folgendes zurückgegeben:

- Name des XenApp-Servers bei Option -A und -S
- URL des Servers, auf dem Webinterface ausgeführt wird, bei Option -E und -L

Das Hilfsprogramm "pnabrowse" gibt einen Beendigungswert mit Erfolgs- oder Fehlermeldung zurück und verwendet mit XenApp die folgenden Optionen:

Option	Beschreibung
-S	Listet Server auf (jeweils einen pro Zeile).
-A	Listet die veröffentlichten Anwendungen auf (jeweils eine pro Zeile).
-m	Wird zusammen mit -A verwendet. Dadurch werden die zu veröffentlichten Anwendungen zurückgegebenen Informationen um Herausgeber, Videotyp, Audiotyp, AppInStartMenu, AppOnDesktop, AppIsDesktop, AppIsDisabled, Fenstertyp, WindowScale und Anzeigenamen erweitert.
-M	Wird zusammen mit -A verwendet. Dadurch werden einzelne Informationsspalten über veröffentlichte Anwendungen für die Ausgabe ausgewählt. Das zugehörige Argument ist die Summe der Zahlen (1-1023), die mit den erforderlichen Details korrespondieren: Publisher(1), VideoType(2), Sound Type(4), AppInStartMenu(8), AppOnDesktop(16), AppIsDesktop(32), AppIsDisabled(64), Window Type(128), Window Scale(256) und DisplayName(512).
-c	Wird dies an Option -A angehängt, dann werden Dateien erstellt, welche die für das Clientmodul zum Herstellen einer Verbindung zu veröffentlichten Anwendungen erforderlichen Mindestinformationen enthalten (z. B. Anwendungsname, Server für die Navigation, Fensterauflösung, Farbtiefe, Audio und Verschlüsselungseinstellungen. Dateinamen erhalten folgendes Format: /tmp/xxx_1.ica, /tmp/xxx_2.ica, wobei xxx durch den dezimalen Prozessbezeichner des pnabrowse-Prozesses ersetzt wird.
-d	Gibt in Zusammenhang mit -L die XDG-Desktopdatei an.
-e	Zeigt Fehlernummern.
-i	Schließt Pfade zu Dateien mit Symbolbildern für veröffentlichte Anwendungen in die Ausgabe von Option -A ein. Es werden je nach Verwendung der Größenoption (WxB) entweder XPM- oder PNG-Dateien

Option	Beschreibung
	zurückgegeben: • -i gibt 16x16-Symbole im XPM-Format mit 4 Bit pro Pixel zurück. • -iWxB gibt WxW-Symbole im PNG-Format mit B Bit pro Pixel zurück.
-f	Schließt Citrix XenApp-Ordnernamen für veröffentlichte Anwendungen in die Ausgabe von Option -A ein.
-u	Dient zum Angeben eines Benutzernamens für die Authentifizierung auf einem Proxyserver.
-p	Dient zum Angeben eines Kennworts für die Authentifizierung auf einem Proxyserver.

Die folgenden Optionen stellen die Funktionalität von Citrix XenApp (Program Neighborhood Agent) Services bereit und können mit der XenApp- und XenDesktop-Funktionalität verwendet werden:

Option	Beschreibung
-D	Gibt eine Domäne an für die Authentifizierung des Benutzers bei dem Server, auf dem Webinterface ausgeführt wird, oder auf dem Server, auf dem der Citrix XenApp-Dienst (Program Neigborhood Agent) ausgeführt wird.
-E	Ruft Citrix XenApp auf und listet alle veröffentlichten Ressourcen auf. Wenn Sie -E und -L angeben, wird die letzte Option in der Befehlszeile verwendet. Das Hilfsprogramm wird dann beendet, wobei möglicherweise eine Verbindung geöffnet bleibt. Für jede Ressource werden die folgenden Details in einfachen Anführungszeichen und getrennt durch Tabstoppzeichen in die Standardausgabe geschrieben: Name: Anzeigename im Dialogfeld "Anwendungseigenschaften" der Access Management Console Ordner: Program Neighborhood-Ordner im Dialogfeld "Anwendungseigenschaften" der Access Management Console Typ: Anwendungen oder Inhalt Symbol: vollständiger Pfad einer Symboldatei im XPM-Format
-L	Gibt den Namen der veröffentlichten Ressourcen an, mit der eine Verbindung hergestellt werden soll. Damit wird Citrix XenApp aufgerufen und eine Verbindung zu einer veröffentlichten Ressource hergestellt. Wenn Sie -E und -L angeben, wird die letzte Option in der Befehlszeile verwendet. Das Hilfsprogramm wird dann beendet, wobei möglicherweise eine Verbindung geöffnet bleibt.
-N	Angeben eines neuen Kennworts. Diese Option muss mit vorhandenen Anmeldeinformationen verwendet werden und gilt nur, wenn das vorhandene Kennwort abgelaufen ist (gemäß Beendigungscode 238: E_PASSWORD_ABGELAUFEN).

Option	Beschreibung
-P	Gibt eine Domäne an für die Authentifizierung des Benutzers bei dem Server, auf dem Webinterface ausgeführt wird, oder auf dem Server, auf dem der XenApp (Program Neigborhood Agent) ausgeführt wird.
-U	Gibt einen Benutzernamen an für die Authentifizierung des Benutzers bei dem Server, auf dem Webinterface ausgeführt wird, oder auf dem Server, auf dem der Citrix XenApp-Dienst (Program Neigborhood Agent) ausgeführt wird.
-WD	Trennt alle aktiven Sitzungen für den Benutzer.
-WT	Beendet alle Sitzungen für den Benutzer.
-Wr	Stellt eine Verbindung mit allen getrennten Sitzungen des Benutzers wieder her.
-WR	Stellt die Verbindung mit allen Sitzungen (aktiv oder getrennt) für den Benutzer wieder her.
-k	Verwendet ein vorhandenes Kerberos-Ticket zur Authentifizierung anstelle von Benutzernamen, Kennwort und Domäne. Dies erfordert die Konfiguration von Client und Server. Weitere Informationen finden Sie unter *— Using Kerberos with Citrix Receiver for Linux Guide* . Diese Anleitung ist von Citrix unter einem Geheimhaltungsvertrag erhältlich.

Die folgenden allgemeinen Optionen werden verwendet:

Option	Beschreibung
-q	Stiller Modus: keine Fehlermeldungen ausgeben.
-r	Symbolrohdaten für veröffentlichte Anwendungen in die Ausgabe der Option -E oder -A einschließen.
-v	Zeigt Versionsdetails an.
-h	Nutzungsmeldung mit einer Liste der Optionen ausgeben.
-?	Nutzungsmeldung mit einer Liste der Optionen ausgeben.