Citrix Workspace-App für Linux

Contents

Info zu diesem Release

May 21, 2021

Neue Features in Release 2104

Unterstützung von App-Schutz auf Red Hat Package Manager (RPM) - experimentelles Feature

App-Schutz wird jetzt für die RPM-Version der Citrix Workspace-App unterstützt.

Weitere Informationen finden Sie unter App-Schutz.

Verbesserungen am HDX Enlightened Data Transport-Protokoll (EDT)

Wenn `HDXoverUDP` in älteren Releases auf `Preferred` festgelegt ist, erfolgt der Datentransport über EDT. Wenn dies nicht möglich ist, erfolgt er über TCP.

Bei aktivierter Sitzungszuverlässigkeit werden EDT und TCP bei der ersten Verbindung, bei einer Sitzungszuverlässigkeits-Wiederverbindung und einer automatischen Wiederverbindung von Clients parallel versucht. Wenn EDT bevorzugt wird, aber der erforderliche zugrunde liegende UDP-Transport nicht verfügbar ist und TCP verwendet werden muss, wird durch diese Verbesserung die Verbindungszeit verkürzt.

Nach dem Fallback auf TCP sucht der adaptive Transport standardmäßig alle fünf Minuten nach EDT.

Optimierung für Microsoft Teams

Ab dieser Version ist die Funktion zur Echounterdrückung standardmäßig deaktiviert. Wir empfehlen, dass Sie nicht die integrierten Lautsprecher und das Mikrofon für Anrufe verwenden. Verwenden Sie stattdessen Kopfhörer.

Dieser Fix soll die Audiowiedergabeprobleme lösen, die bei Thin Clients festgestellt wurden.

Servicekontinuität (Technical Preview)

> **Hinweis:**
>
> Dieses Feature ist als Technical Preview verfügbar. Citrix empfiehlt, das Feature nur in Nicht-Produktionsumgebungen zu verwenden. Verwenden Sie das folgende Podio-Formular, um sich anzumelden: Sign up: Service continuity Tech Preview for Citrix Workspace.

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Benutzer können so ihre virtuellen Apps und Desktops unabhängig vom Integritätsstatus der Cloud-Dienste starten.

Weitere Informationen finden Sie unter Servicekontinuität in der Dokumentation zu Citrix Workspace.

Neue Features in Release 2103

Pinnen des Bildschirmlayouts im Multimonitormodus

Ab diesem Release können Sie die Auswahl für das Bildschirmlayout im Multimonitormodus speichern. Das Layout bestimmt, wie eine Desktopsitzung angezeigt wird. Durch Pinnen wird das ausgewählte Layout beim Neustarten einer Sitzung beibehalten, was die Benutzererfahrung optimiert.

Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu, um das Feature zum Pinnen des Bildschirmlayouts zu aktivieren:

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

Erst nachdem Sie den oben angegebenen Schlüssel hinzugefügt haben, können Sie die Option **Bildschirmlayout** im **App-Indikator** sehen.

> **Hinweis:**
>
> Dieses Feature ist beim Webstart der Citrix Workspace-App nicht verfügbar.

Weitere Informationen finden Sie unter Pinnen des Bildschirmlayouts im Multimonitormodus.

Erhöhung der Anzahl der unterstützten virtuellen Kanäle

In früheren Versionen des Clients wurden bis zu 32 virtuelle Kanäle in einer Sitzung unterstützt.

Ab dieser Version können Sie bis zu 64 virtuelle Kanäle in einer Sitzung nutzen.

Verbesserungen bei Microsoft Teams

Der VP9-Videocodec ist jetzt standardmäßig deaktiviert.

Neue Features in Release 2101

Verbesserung der Clientlaufwerkzuordnung (CDM)

Ab diesem Release gibt es für den Zugriff auf zugeordnete Laufwerke ein zusätzliches Sicherheitsfeature.

Sie können jetzt die Zugriffsebene für das zugeordnete Laufwerk für jeden Store in einer Sitzung auswählen.

Um zu verhindern, dass das Dialogfeld für die Zugriffsebene jedes Mal angezeigt wird, wählen Sie die Option **Nicht wieder fragen** aus. Die Einstellung wird auf diesen bestimmten Store angewendet.

Andernfalls können Sie die Zugriffsebenen bei jedem Sitzungsstart festlegen.

Unterstützung von App-Schutz für Debian-Paket - experimentelles Feature

App-Schutz wird jetzt für die Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie für die unbeaufsichtigte Installation der App-Schutzkomponente den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

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

Verbesserungen bei Microsoft Teams

- Im Paket des Installationsprogramms der Citrix Workspace-App befinden sich jetzt die Klingeltöne von Microsoft Teams.
- Die Audioausgabe wechselt automatisch zu neu angeschlossenen Audiogeräten und eine geeignete Lautstärke wird eingestellt.
- HTTP-Proxyunterstützung für anonyme Authentifizierung.

Neue Features in Release 2012

Verbesserung der Clientlaufwerkzuordnung (CDM)

Bisher wurde Ihre Einstellung für den Dateizugriff über CDM auf alle konfigurierten Stores angewendet.

Ab diesem Release ermöglicht die Citrix Workspace-App die Konfiguration des CDM-Dateizugriffs pro Store.

> **Hinweis:**
>
> Die Einstellung für den Dateizugriff ist nicht in allen Sitzungen persistent, wenn Workspace für

> Web verwendet wird. Es wird standardmäßig die Option **Jedes Mal fragen** verwendet.

Weitere Informationen finden Sie unter Clientlaufwerkzuordnung.

App-Schutz - experimentelles Feature

> **Hinweis:**
>
> - Diese Funktion wird nur unterstützt, wenn die Citrix Workspace-App mithilfe des Tarball-Pakets installiert wird. x64 und armhf sind zudem die einzigen unterstützten Pakete.
> - Dieses Feature wird nur für On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops unterstützt.

Der App-Schutz ist eine Zusatzfunktion, die erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops bietet. Die Funktion beschränkt die Möglichkeit, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. Der App-Schutz verhindert das Exfiltrieren vertraulicher Informationen wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

Informationen zum Konfigurieren des App-Schutzes in Citrix Virtual Apps and Desktops finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation unter App-Schutz.

Weitere Informationen zum App-Schutz in der Citrix Workspace-App finden Sie unter App-Schutz.

Verbesserung der Authentifizierung - experimentelles Feature

Das Authentifizierungsdialogfeld befindet sich jetzt in der Citrix Workspace-App und die Storedetails werden im Anmeldebildschirm angezeigt. Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht erneut eingeben müssen.

> **Hinweis:**
>
> - Diese Verbesserung der Authentifizierung ist nur in Cloud-Bereitstellungen verfügbar.
> - Diese Verbesserung der Authentifizierung ist nicht auf der armhf-Plattform verfügbar.

Voraussetzung:

Sie müssen die Bibliothek libsecret installieren.

Diese Funktion ist in der Standardeinstellung deaktiviert.

Weitere Informationen finden Sie unter Authentifizierung.

Verbesserung der Audiokonfiguration

Ab dieser Version ist der Standardwert des Attributs `VdcamVersion4Support` in der Datei `module.ini` auf `True`festgelegt.

Weitere Informationen finden Sie unter Audio.

Neue Features in Release 2010

Verbesserte Audioumleitung

Bisher wurde nur das Standard-Audiogerät in einer Sitzung zugeordnet, selbst wenn viele Geräte auf der Maschine verfügbar waren. Das zugeordnete Gerät war üblicherweise als **Citrix HDX Audio** zu sehen.

Ab dieser Version zeigt die Citrix Workspace-App für Linux alle lokalen Audiogeräte an, die in einer Sitzung verfügbar sind. Anstelle von **Citrix HDX Audio** werden sie nun mit den entsprechenden Gerätenamen aufgeführt. In einer Sitzung können Sie dynamisch zu jedem der verfügbaren Geräte wechseln. Anders als in früheren Versionen müssen Sie nicht mehr das Standard-Audiogerät auswählen, bevor Sie die Sitzung starten. Sitzungen werden dynamisch aktualisiert, wenn Sie Audiogeräte anschließen oder entfernen.

Weitere Informationen finden Sie unter Audio.

Darüber hinaus werden in diesem Release Probleme behoben, um das Multistream-ICA-Feature zu verbessern.

Neue Features in Release 2009

Verbesserte Protokollierung

Bislang wurden die Dateien `debug.ini` und `module.ini` zum Konfigurieren der Protokollierung verwendet.

Ab Version 2009 können Sie die Protokollierung über eines der folgenden Verfahren konfigurieren:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

Ab Version 2009 wird die Konfigurationsdatei `debug.ini` aus dem Installationspaket der Citrix Workspace-App entfernt.

Die Protokollierung erfasst Bereitstellungsdetails, Konfigurationsänderungen und Administratoraktivitäten der Citrix Workspace-App in einer Protokollierungsdatenbank. Drittanbieterentwickler können das Protokollierungs-SDK nutzen, das im Platform Optimization SDK der Citrix Workspace-App enthalten ist.

Verwenden Sie die Protokollinformationen für Folgendes:

- Diagnostizieren und Beheben von Problemen, die nach Änderungen auftreten. Das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen.
- Bericht über Administratoraktivitäten.

> **Hinweis:**
>
> Dieser Protokollierungsmechanismus ist nur im Retailbuild anwendbar.

Weitere Informationen zur Protokollierung finden Sie unter Protokollierung.

Neue Features in Release 2006

Optimierung für Microsoft Teams

Citrix bietet eine Optimierung für die Verwendung der Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops und der Citrix Workspace-App. Die Optimierung für Microsoft Teams ähnelt der Komponente HDX RealTime Optimization für Microsoft Skype for Business. Der Unterschied besteht darin, dass wir alle notwendigen Komponenten für die Optimierung von Microsoft Teams im VDA und in der Workspace-App bündeln.

Die Citrix Workspace-App für Linux unterstützt Audio-, Video- und Bildschirmfreigabefunktionen mit der Optimierung für Microsoft Teams.

> **Hinweis:**
>
> Die Optimierung für Microsoft Teams wird nur auf der x64-Linux-Distributionen unterstützt.

Weitere Informationen zum Aktivieren der Protokollierung erhalten Sie, wenn Sie die Schritte unter Protokollierung für Microsoft Teams ausführen.

Informationen zu Systemanforderungen finden Sie unter Optimierung für Microsoft Teams.

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams und Microsoft Teams-Umleitung.

Unterstützung für den virtuellen NSAP-Kanal (NetScaler App Experience)

Der virtuelle NSAP-Kanal (NetScaler App Experience) wurde bisher als experimentelles Feature zur Verfügung gestellt und ist nun vollständig funktionsfähig. Der virtuelle NSAP-Kanal hilft bei der Erfassung von HDX Insight-Daten und verbessert dadurch Leistung und Skalierbarkeit. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert. Um das Feature zu deaktivieren, legen Sie das NSAP-Flag `NSAP=Off` in der Datei `module.ini` fest.

Weitere Informationen finden Sie unter HDX Insight in der Dokumentation zu Linux Virtual Delivery Agent und unter HDX Insight in der Dokumentation zum Citrix Application Delivery Management Service.

Aktualisieren auf den Citrix Analytics-Dienst

Die Citrix Workspace-App überträgt Daten von ICA-Sitzungen, die Sie über einen Browser starten, an den Citrix Analytics-Dienst.

Weitere Informationen dazu, wie die Citrix Analytics diese Informationen verwendet, finden Sie unter Self-Service für Leistung und Self-Service-Suche für Virtual Apps and Desktops.

TLS-Versionsupdate

Bislang war die unterstützte TLS-Mindestversion 1.0 und die unterstützte TLS-Höchstversion 1.2.

Ab diesem Release wird als Mindest- und Höchstversion TLS 1.2 unterstützt. Informationen zum Konfigurieren eines anderen Werts für `MinimumTLS` finden Sie unter TLS.

CryptoKit-Update

CryptoKit-Version 14.2 ist in OpenSSL 1.1.1d integriert.

Neue Features in Release 2004

Sprachunterstützung

Die Citrix Workspace-App für Linux ist jetzt auf Italienisch verfügbar.

Verbesserte Anmelde- und Enumerationsleistung

Dieses Release beschleunigt die Anmeldung und App-Enumeration für Cloud-Benutzerkonten.

Audiooptimierung für Microsoft Teams - experimentelles Feature

Die Citrix Workspace-App bietet als experimentelles Feature eine Audiooptimierung für Microsoft Teams, die in einer Citrix Virtual Desktops-Sitzung ausgeführt wird.

> **Hinweis:**
>
> Die Audiooptimierung für Microsoft Teams wird nur auf x64-Linux-Distributionen unterstützt.

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams und Microsoft Teams-Umleitung in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung für den virtuellen NSAP-Kanal (NetScaler App Experience) - experimentelles Feature

Für dieses experimentelle Feature werden HDX Insight-Daten im virtuellen NSAP-Kanal erfasst und unkomprimiert gesendet. Dies verbessert die Skalierbarkeit und Leistung. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert. Um das Feature zu deaktivieren, legen Sie das NSAP-Flag `NSAP=Off` in der Datei `module.ini` fest.

Weitere Informationen finden Sie unter HDX Insight in der Dokumentation zu Linux Virtual Delivery Agent und unter HDX Insight in der Dokumentation zum Citrix Application Delivery Management Service.

Neue Features in Release 1912

Verbesserung der transparenten Benutzeroberfläche

In Version 1910 wurde das TUI-Feature (transparente Benutzeroberfläche) einschließlich **VDTUI**-Flag eingeführt. Durch das Feature kann das Clientsystem die vom Server gesendeten TUI-Pakete empfangen und der Client kann auf UI-Komponenten zugreifen. Wenn das Flag jedoch auf **Off** gesetzt war, wurde die Anmeldeaufforderung vom Dialogfeld "<Anwendung> wird gestartet" verdeckt.

Jetzt ist das **VDTUI**-Flag (in der Datei `module.ini`) standardmäßig auf **On** gesetzt. Das Dialogfeld "<Anwendung> wird gestartet" wird daher beim Start einer App nicht mehr angezeigt. Stattdessen ist das Dialogfeld "Verbinden mit <Anwendung>" mit einer Fortschrittsanzeige zu sehen. Das Dialogfeld zeigt auch den Fortschritt des App-Starts an.

Unterstützung für GStreamer 1.x - experimentelles Feature

In älteren Releases war GStreamer 0.10 die für die Multimediaumleitung unterstützte Standardversion. Ab dieser Version können Sie GStreamer 1.x als Standardversion konfigurieren.

Einschränkungen:

- Bei der Videowiedergabe funktioniert die Option zum Vor- und Zurückspulen möglicherweise nicht wie erwartet.
- Wenn Sie die Citrix Workspace-App auf ARMHF-Geräten starten, funktioniert GStreamer 1.x möglicherweise nicht wie erwartet.

Weitere Informationen finden Sie unter Aktivieren von GStreamer 1.x.

Chromium Embedded Framework (CEF) für die Umleitung des Browserinhalts - experimentelles Feature

Das BCR-Feature leitet Inhalte eines Webbrowsers an ein Clientgerät um. Das Feature erstellt einen entsprechenden Browser, der in die Citrix Workspace-App eingebettet wird.

Bislang verwendete BCR ein Overlay auf der Basis von `WebkitGTK+`, um den Inhalt wiederzugeben. Ab diesem Release verwendet BCR ein CEF-basiertes Overlay, um eine bessere Benutzererfahrung zu erzielen. Sie trägt dazu bei, dass Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen werden.

Weitere Informationen finden Sie unter Aktivieren der CEF-basierten Umleitung des Browserinhalts.

Informationen zur Umleitung des Browserinhalts finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation unter Umleitung des Browserinhalts.

> **Hinweise:**
>
> - Die Binärdatei **pacexec** wurde aus der x86-Version der Citrix Workspace-App entfernt.
> - Citrix Files ist möglicherweise nicht kompatibel mit dem intelligenten Workspace.

Neue Features in Release 1910

Sprachunterstützung

Die Citrix Workspace-App für Linux ist jetzt auf Portugiesisch (Brasilien) verfügbar.

App-Indikatorsymbol

Der App-Indikator wird beim Start der Citrix Workspace-App gestartet und ist ein Symbol im Infobereich. Die Einführung des App-Indikators verbessert die Anmeldeleistung der Citrix Workspace-App für Linux.

Sie können Leistungsverbesserungen in folgenden Situationen bemerken:

- Erster Start der Citrix Workspace-App
- Schließen und Neustarten der App
- Beenden und Neustarten der App

> **Hinweis:**
>
> Das Paket `libappindicator` ist erforderlich, damit der App-Indikator angezeigt wird. Installieren Sie das für Ihre Linux-Distribution geeignete Paket `libappindicator` aus dem Internet.

Transparente Benutzeroberfläche

Das Citrix ICA-Protokoll verwendet das Protokoll “Transparent User Interface Virtual Channel” [TUI VC], um Daten zwischen Citrix Virtual Apps and Desktops und Hostservern zu übertragen. Das TUI-Protokoll überträgt Komponentenmeldungen der Benutzeroberfläche [Benutzeroberfläche] für Remoteverbindungen.

Bisher wurde das TUI VC-Feature von der Citrix Workspace-App für Linux nicht unterstützt. Daher konnte das Clientsystem UI-Komponentendaten vom Server nicht effizient verarbeiten. Beim Start einer App wurde das Dialogfeld "<Anwendung> wird gestartet" daher über andere Anwendungen gelegt.

Jetzt unterstützt die Citrix Workspace-App für Linux das TUI VC-Feature. Durch das Feature kann der Client die vom Server gesendeten TUI-Pakete empfangen und auf UI-Komponenten zugreifen. Durch diese Funktion können Sie die Anzeige des überlagernden Standardbildschirms steuern. Sie können das `VDTUI`-Flag in der Datei `module.ini` ein- und ausschalten: `VDTUI - On/Off`

Weitere Informationen zu virtuellen Kanälen finden Sie unter Virtuelle ICA-Kanäle von Citrix in der Dokumentation zu Citrix Virtual Apps and Desktops.

Behobene Probleme

Behobene Probleme in Release 2104

- Wenn Sie die Browserinhaltsumleitung verwenden, wechselt der Tastaturfokus auch nach der Suche in der YouTube-Suchleiste nicht zum übergeordneten Fenster zurück. [RFLNX-5349]
- Wenn Sie einen Bildschirm in Microsoft Teams während eines Peer-zu-Peer-Anrufs freigeben, kann das Audio verzerrt sein. Das Problem tritt bei Dell Wyse Thin Clients 5070 und 5470 auf. [RFLNX-6537]
- Wenn Sie Microsoft Teams in der Citrix Workspace-App für Linux verwenden, werden Anrufe u. U. unerwartet getrennt. [RFLNX-6719]
- In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern. [RFLNX-7006]
- Bei Verwendung eines Chromium Embedded Framework kann die Umleitung von Browserinhalten zu einer hohen CPU-Auslastung führen. [RFLNX-7217]
- Beim Wechsel zwischen den veröffentlichten und lokalen Anwendungen wird die veröffentlichte Anwendung im Vollbildmodus möglicherweise nicht richtig skaliert. [CVADHELP-14812]
- Wenn Sie Microsoft Excel über die Citrix Workspace-App für Linux öffnen und zu **Daten** > **Neue Abfrage** navigieren, wird das Kontextmenü **Datenquelleneinstellung** möglicherweise nicht wie erwartet geöffnet. [CVADHELP-16509]
- Die Versionen 2101 und 2102 der Citrix Workspace-App für Linux enthalten möglicherweise eine ungültige Client-IP-Adresse in Citrix Director [CVADHELP-16923]
- Der Name des Audiogeräts wird möglicherweise fehlerhaft angezeigt. Das Problem tritt bei chinesischen Betriebssystemen auf. [CVADHELP-17290]

Behobene Probleme in früheren Releases

Behobene Probleme in Release 2103

- Versuche, einen nicht optimierten Videoanruf zu tätigen, können zum Verlust von Audio führen.

Das Audio kann erst wiederhergestellt werden, wenn Sie die Verbindung trennen und die Sitzung erneut verbinden. [CVADHELP-16846]

- Mit diesem Fix wird der Standardwert für AudioLatencyControlEnabled auf True festgelegt, wodurch die Audiolatenz reduziert wird. [RFLNX-6620]
- Die Bildschirmfreigabefunktion in Microsoft Teams schlägt möglicherweise im Seamlessmodus fehl. [RFLNX-6659]

Behobene Probleme in Release 2101

- Wenn Sie einen benutzerdefinierten Proxy verwenden, wird möglicherweise eine zusätzliche Authentifizierungsaufforderung angezeigt. Das Problem wird durch das Chromium Embedded Framework (CEF) verursacht, das bei der Browserinhaltsumleitung verwendet wird. Konfigurieren Sie als Workaround Ihren Agent so, dass er die zusätzliche Aufforderung umgeht. [CVADHELP-14804]
- Wenn Sie versuchen, eine Verbindung zu einer Sitzung wiederherzustellen, reagiert die Sitzung möglicherweise nicht mehr. Das Problem tritt bei Sitzungen auf, die per Smartcard aktiviert wurden. Als Workaround setzen Sie die Smartcard erneut ein. [CVADHELP-15028]
- Wenn Microsoft Teams im **optimierten** Modus ist, reagiert die Videowiedergabe bei Konferenzgesprächen möglicherweise nicht mehr. Das Problem tritt auf, wenn ein Teilnehmer zwischen einer integrierten Kamera und einer USB-Kamera wechselt. [CVADHELP-16400]
- Wenn Microsoft Teams im **optimierten** Modus ist, wird der Prozess `HdxRtcEngine.exe` möglicherweise unerwartet beendet. [CVADHELP-16504]

Behobene Probleme in Release 2012

- Der Start einer per Browserinhaltsumleitung umgeleiteten Webseite kann dazu führen, dass die Webseite nicht mehr reagiert. Das Problem tritt auf, wenn Sie auf einen Link klicken, der in einem neuen Fenster oder in einer neuen Registerkarte geöffnet wird. [RFLNX-5306]
- Bei der CEF-basierten Umleitung des Browserinhalts werden Mikrofone und Kameras nicht umgeleitet. Legen Sie das Attribut `CefEnableMediaDevices` in `All_Regions.ini` auf `True` fest, um die Umleitung zu aktivieren.[RFLNX-5337]
- Wenn Sie Tasten **ALT+Strg** drücken, bleiben die Tasten möglicherweise hängen. Das Problem tritt auf, wenn die Option "Tastaturlayout" auf "Standardserver" festgelegt ist. [RFLNX-5444]
- Das Auswählen der USB-Optionen PTP (Picture Transfer Protocol) bzw. MTP (Media Transfer Protocol) auf einem Android-Telefon schlägt möglicherweise fehl. Um dieses Problem bei Windows- und Linux-VDAs zu beheben, fügen Sie in der Datei usb.conf folgende Zulassungsregel hinzu:

  ALLOW: VID = (VID des Geräts) disableselectconfig=1

  [CVADHELP-15304]

- Citrix Director gibt die Versionsnummer der Citrix Workspace-App möglicherweise falsch als 2009 statt 2010 an. [RFLNX-5743]
- Sie können die Citrix Workspace-App für Linux beim ersten Versuch erfolgreich starten, spätere Versuche schlagen jedoch möglicherweise fehl. [RFLNX-5971]
- Beim Versuch, einen nicht authentifizierten (anonymen) Store hinzuzufügen, werden möglicherweise zwei Fehlermeldungen angezeigt. Das Problem tritt bei der Citrix Workspace-App 2010 für Linux auf. [RFLNX-5980]

Behobene Probleme in Release 2010

- Wenn Sie einen Videoanruf ausführen oder den Bildschirm in Microsoft Teams freigeben, flackert der Bildschirm möglicherweise. [RFLNX-4778]
- Das Anpassen der Dateien webrpc.log und webrtc.log schlägt fehl. [RFLNX-5221]
- Ressourcen werden für den Store aufgelistet, auch nachdem der Store mit dem Dienstprogramm storebrowse gelöscht wurde. [RFLNX-5499]
- Wenn das deutsche oder französische Gebietsschema auf der Maschine installiert ist, funktioniert die Optimierung für Microsoft Teams möglicherweise nicht. [RFLNX-5599]
- Beim Start einer Sitzung über die Citrix Workspace-App für Linux flackert die Sitzung möglicherweise. Das Problem tritt auf, da die Sitzung getrennt und erneut verbunden wird. Das Problem tritt hauptsächlich bei Microsoft-Anwendungen auf. [CVADHELP-14194]
- Wenn Sie Zwischenablagevorgänge wie das Kopieren und Einfügen von Inhalten zwischen verschiedenen Sitzungen ausführen, schlagen die Vorgänge möglicherweise zeitweise fehl. [CVADHELP-15228]
- Wenn Sie eine Diashow-Präsentation starten und Microsoft PowerPoint über die Citrix Workspace-App für Linux ab Version 1906 gestartet wurde, wird die Präsentation möglicherweise nicht im Vollbildmodus geöffnet. [CVADHELP-15648]
- Die Citrix Workspace-App für Linux zeigt möglicherweise kein Dialogfeld zur Authentifizierung für Stores an, die lokalen HTML5-Speicher verwenden. Das Problem tritt auf, wenn Sie die Self-Service-Benutzeroberfläche verwenden. [CVADHELP-15720]

Behobene Probleme in Release 2009

- Gelegentlich wird die Besprechungsansicht beim Multitasking in Microsoft Teams nicht wiederhergestellt. Das Problem tritt auf, wenn ein lokales Fenster das Remotefenster überlagert. Das Remotefenster empfängt dann die Mausereignisse nicht. Als Workaround bewegen Sie auf dem minimierten Bildschirm den Mauszeiger über die digitale Uhr und doppelklicken auf den Namen des Anrufers. [RFLNX-4937]
- In einer Sitzung, die auf UDP-Verbindungen ausgeführt wird, kann die Leistung beeinträchtigt sein. [RFLNX-5135]

- Wenn Sie das Fenster einer veröffentlichten Seamless-Drittanbieteranwendung über den Bildschirm ziehen, wird das Fenster möglicherweise automatisch minimiert. [CVADHELP-13677]
- Ein einzelnes USB-Gerät, das zu einer Sitzung auf einem Gerät umgeleitet wird, wird möglicherweise unerwartet zu einer eingehenden Sitzung weitergeleitet, die auf demselben Gerät ausgeführt wird. [CVADHELP-13684]
- Wenn Sie in einer Multimonitorumgebung versuchen, eine Sitzung im Vollbildmodus auf einem Monitor neu zu starten, verbleibt die Verbindungsleiste auf einem anderen Monitor. Das Problem tritt auch dann auf, wenn der Mauszeiger auf demselben Monitor bleibt. [CVADHELP-14642]
- Beim Versuch, die Verbindung zu einer Sitzung wiederherzustellen, wird die Sitzung möglicherweise sofort getrennt, nachdem der Desktop angezeigt wird. Das Problem tritt bei Sitzungen mit erforderlicher Smartcard-Authentifizierung auf. [CVADHELP-15036]

Behobene Probleme in Release 2006

- Bei Verwendung von Microsoft Teams wird die Option "Testanruf" nicht angezeigt. [RFLNX-4234]
- Der Sitzungsstart schlägt möglicherweise auf Red Hat 8.2-, CentOS 8.x-, Fedora 29-, 30- und 31-Distributionen fehl. [RFLNX-3114] [RFLNX-4438] [RFLNX-4296]
- Eine unnötige Abhängigkeit, die von LIBS_GTK eingeführt wurde, wurde durch das Hinzufügen der `wfica_for_plugins`-Binärdateien zum Platform Optimization SDK wieder entfernt. [RFLNX-4604]
- Serverabruf- und Clientrendervorgänge für die CEF-basierte Umleitung des Browserinhalts (BCR) schlagen fehl. Infolgedessen schlägt die Browserinhaltsumleitung fehl. [RFLNX-4459]
- Nachdem Sie in Citrix StoreFront auf eine veröffentlichte Anwendung geklickt haben, wird ein Verbindungsdialogfeld angezeigt und bleibt offen. Das Problem tritt im Nicht-Seamlessmodus auf. [CVADHELP-13896]
- Nachdem Sie die Option **Aktivieren** zum Aktivieren der Citrix Workspace-App auf dem Desktop ausgewählt haben, wird die Datei **receiverconfig.cr** heruntergeladen. Versuche, den Store der Citrix Workspace-App durch Starten dieser Datei hinzuzufügen, schlagen möglicherweise fehl. [CVADHELP-14389]
- Versuche, die Citrix Workspace-App für Linux einem seriellen COM-Port zuzuordnen, schlagen möglicherweise fehl, was darauf hinweist, dass der Port nicht erreicht werden kann. Das Problem tritt auf, wenn die vorherigen COM-Einträge nicht ausgefüllt werden. [CVADHELP-14391]
- Die Citrix Workspace-App für Linux erkennt möglicherweise bestimmte Smartcards nicht. Daher schlagen Versuche, eine Sitzung mit diesen Karten zu starten, fehl. [CVADHELP-14878]

Behobene Probleme in Release 2004

- Wenn Sie den Abschnitt **Preferences** aus der Datei **All_Regions.ini** entfernen, schlägt der wfica-Prozess fehl. Sitzungen können dann keine Verbindung herstellen. [RFLNX-3965]

- Das Untermenü **Einstellungen** > **Konten** wird nicht im Self-Service-Fenster angezeigt, wenn Sie zum ersten Mal einen Cloudstore hinzugefügt haben. [RFLNX-3605]
- Das Linux Platform Optimization SDK funktioniert nicht für die Citrix Workspace-App-Versionen 1908, 1910 und 1912. Das Problem tritt auf, wenn die `wfica_for_plugins`-Binärdateien aus dem Installationspaket der Citrix Workspace-App entfernt werden. [RFLNX-4298]
- Wenn Sie einen Store mit dem Befehl **storebrowse** hinzufügen, wird der Store nicht auf der Registerkarte **Einstellungen** > **Konten** angezeigt. Das Problem tritt auf, wenn die Self-Service-Benutzeroberfläche auf dem Back-End ausgeführt wird. [RFLNX-3683]
- In einer Sitzung wird wfica u. U. unerwartet auf einer Website beendet, wenn die Browserinhaltsumleitung aktiviert ist. Das Problem tritt auf, wenn Sie den Wert von **AllowMultiStream** auf **True** festlegen. [CVADHELP-13168]
- Bei einem Setup mit zwei Monitoren schlägt der Versuch, die Anzeige des veröffentlichten Desktops in den Vollbildmodus zu ändern, möglicherweise fehl, wenn die Monitore unterschiedliche Auflösungen haben. [CVADHELP-13990]
- In Seamlesssitzungen können Anzeigeprobleme auftreten. Das Problem tritt auf, wenn Sie die Größe eines Seamlessfensters ändern oder zwischen Seamlessfenstern wechseln. [CVADHELP-13458]
- Nachdem Sie eine Desktopsitzung von einem PNA-Store aus gestartet haben, bleibt das Statusfenster möglicherweise offen, wenn Sie es nicht manuell schließen. [CVADHELP-14405]

Behobene Probleme in Release 1912

- Unter Ubuntu16.04x64 wird das Citrix Workspace-App-Symbol möglicherweise falsch auf der Taskleiste angezeigt. [RFLNX-3582]
- Wenn Sie die symbolische Verknüpfung [symlink] von gst-play in gst-play1.0 ändern, werden MP4-Videodateien möglicherweise mit einem schwarzen Bildschirm im Hintergrund und ohne Audio wiedergegeben. [RFLNX-2429]
- Wenn Sie vom Bildschirmschonermodus in den Vollbild-ICA-Sitzungsmodus wechseln, verliert die Tastatur möglicherweise den Fokus. Das Problem tritt auf ArmhardFloat-Geräten mit Raspberry Pi-OS auf. [RFLNX-3553]
- Wenn Sie die Self-Service-Benutzeroberfläche verwenden, funktionieren die Optionen im Fenster **Voreinstellungen** möglicherweise nicht wie erwartet. Das Problem tritt auf, wenn das Paket “libwebkit1” nicht verfügbar ist, wie es bei Debian 10 Buster-Clients der Fall ist. [RFLNX-3596]
- Wenn ein anderer Systembenutzer (nicht der erste Benutzer) versucht, die Citrix Workspace-App zu starten, wird die Self-Service-Benutzeroberfläche möglicherweise nicht geöffnet und die folgende Fehlermeldung angezeigt:

  Bind Error - address already in use.

[RFLNX-3601]

- Wenn Sie unter Ubuntu ab 18.04 die Self-Service-Benutzeroberfläche zum Starten von Anwendungen verwenden, lautet der Name der gestarteten Anwendung fälschlicherweise "wfica_seamless". Das Problem tritt auf, weil die Standarddesktopumgebung GNOME ist. [RFLNX-3650]
- Wenn Sie sich ab- und dann mit einem anderen Benutzerkonto wieder anmelden, wird auf der Seite "Home > Favoriten" eine falsche Liste bevorzugter Apps angezeigt. [RFLNX-3458]
- Nachdem Sie die Self-Service-Benutzeroberfläche geschlossen haben, wird die folgende Fehlermeldung angezeigt:

  "free(): double free detected in tcache 2 Aborted."

  Das Problem tritt auf ArmhardFloat-Geräten mit Raspbian Buster-OS auf. [RFLNX-3578]
- Wenn die Richtlinie "Einheitliche Benutzeroberfläche" deaktiviert ist, werden deaktivierte Anwendungen in der Citrix Workspace-App für Linux möglicherweise weiterhin angezeigt. [CVADHELP-13742]
- Ein USB-Wechseldatenträger kann auf CentOS 7.7-Clients keinem VDA zugeordnet werden. [CVADHELP-13422]

Behobene Probleme in Release 1910

- Die Installation der Citrix Workspace-App für Linux war von libcurl3 abhängig. Durch diesen Fix wurde die Abhängigkeit zur einfacheren Installation entfernt. [RFLNX-3487]
- Das Rendern von H.264-codierten Daten mit dem Optimization Pack für Video Decode and Presentation API for Unix (VDPAU) funktioniert möglicherweise nicht wie erwartet. [RFLNX-2892]
- Wenn Sie die Citrix Workspace-App für Linux Version 1906 oder 1908 verwenden, wird die Anmeldeseite möglicherweise nicht angezeigt, wenn sich gemeinsame Benutzer von ihrem Workspace abmelden. Stattdessen wird die folgende Anmeldeaufforderung angezeigt: Melden Sie sich an, um auf Ihren Workspace zuzugreifen. [RFLNX-3519]
- Wenn eine Desktopsitzung mehrere Monitore umfasst, wird die Symbolleiste möglicherweise nicht mehr angezeigt. [RFLNX-3248]

Bekannte Probleme

Bekannte Probleme in Release 2104

- In VDA-Version 1912 LTSR CU2 werden Sitzungen möglicherweise getrennt. Das Problem tritt auf, wenn Sie auf dem Delivery Controller die Richtlinie **Multistream** aktivieren. Aktualisieren Sie als Workaround den VDA auf Version 2012 oder höher. [RFLNX-6960]

Bekannte Probleme in früheren Versionen

Bekannte Probleme in Release 2103

- Während eines Videoanrufs oder der Bildschirmfreigabe reagiert Microsoft Teams möglicherweise nicht mehr und der Anruf kann abrupt enden. [CVADHELP-16918]

Bekannte Probleme in Release 2101

- Wenn Sie lange Videos abspielen, stoppt die Audioausgabe, aber das Video wird weiterhin nahtlos wiedergegeben. Das Problem tritt auf, wenn Sie `VdcamVersion4Support` auf `True` festlegen. Deaktivieren Sie als Workaround die Option für Multiaudio, indem Sie `VdcamVersion4Support` auf `False` festlegen. [RFLNX-6472]
- Während einer Microsoft Teams-Besprechung ist die Audioausgabe bei Stummschaltung möglicherweise abgehackt. Das Problem tritt bei Thin Clients auf. [RFLNX-6537]
- Manchmal kann die Citrix Workspace-App die eingehenden Videos in Microsoft Teams nicht rendern. [RFLNX-6662]
- Wenn Sie das Flag `cefenablemediadevices` mit Microsoft Teams verwenden, funktioniert das Mikrofon nicht wie vorgesehen. Das Problem tritt auf, wenn eine CEF-basierte Browserinhaltsumleitung mit Microsoft Teams verwendet wird. [RFLNX-6689]

Bekannte Probleme in Release 2012

- Beim abrupten Beenden oder Trennen einer Sitzung wird der Prozess `HdxRtcEngine.exe` möglicherweise unerwartet beendet. [RFLNX-5885]
- Wenn Sie versuchen, Text einzugeben, erscheint der Cursor weiß. Das Problem tritt in einem Double-Hop-Szenario auf, wenn die Verbindung von einer Linux-Endpunktmaschine erfolgt. Einen Workaround finden Sie in den Knowledge Center-Artikeln CTX272423 und CTX131504. [CVADHELP-16170]
- Das Einrichten der HDX-Optimierung für einen Microsoft Teams-Videoanruf kann dazu führen, dass Bild und Ton nicht mehr übertragen werden. Das Problem tritt auf, wenn Sie während des Anrufs ein Headset trennen oder erneut anschließen. [CVADHELP-16186]

Bekannte Probleme in Release 2010

- Dateien können auf der Registerkarte **Dateien** nicht angezeigt werden. Das Problem tritt bei Cloud-Bereitstellungen auf. [RFLNX-5596]
- In Microsoft Teams müssen Sie das Audiogerät manuell auswählen. Das Audiogerät wird nicht automatisch als Standard festgelegt. [RFLNX-5652]
- Der Versuch, das Dropdownmenü in einer Sitzung im Vollbildmodus zu verwenden, schlägt möglicherweise fehl. Das Problem tritt auf, wenn die Browser-Inhaltsumleitung aktiviert ist. [CVADHELP-13884]

- Die TCP-Fallbackoption funktioniert möglicherweise nicht, selbst wenn `HDXoverUDP` auf `Preferred` festgelegt ist. Das Problem tritt auf, wenn Sie eine Verbindung mit Citrix Gateway herstellen. [CVADHELP-15526]

Bekannte Probleme in Release 2009

- Das Multistream-ICA-Feature funktioniert möglicherweise nicht ordnungsgemäß. [RFLNX-4286]
- Wenn Sie einen Videoanruf ausführen oder den Bildschirm in Microsoft Teams freigeben, flackert der Bildschirm möglicherweise. [RFLNX-4778]
- Versuche, zwischen Desktopsitzungen zu wechseln, schlagen möglicherweise fehl. [CVADHELP-15229]

Bekannte Probleme in Release 2006

- Gelegentlich wird die **Besprechungsansicht** beim Multitasking in Microsoft Teams nicht wiederhergestellt. Das Problem tritt auf, wenn ein lokales Fenster das Remotefenster überlagert. Das Remotefenster empfängt dann die Mausereignisse nicht. Als Workaround bewegen Sie auf dem minimierten Bildschirm den Mauszeiger über die digitale Uhr und doppelklicken auf den Namen des Anrufers. [RFLNX-4937]
- Die Sitzungswiederverbindung schlägt gelegentlich fehl. Das Problem tritt auf, wenn Sie das Multi-Stream ICA-Protokoll (MSI) mit einem einzigen Port über TCP mit SD-WAN konfigurieren. [RFLNX-4782]

Bekannte Probleme in Release 2004

- Die Citrix Workspace-App für Linux erkennt möglicherweise bestimmte Smartcards nicht. Daher schlagen Versuche, eine Sitzung mit der Karte zu starten, fehl.
- Wenn Sie das MSI-Protokoll (Multi-Stream ICA) in der Workspace-App und auf SD-WAN aktiviert haben, wird eine Sitzung beim Starten möglicherweise unerwartet beendet. Die folgende Fehlermeldung wird angezeigt:

  "Die Verbindung zum VDA wurde unterbrochen…"

  Das Problem tritt auf, weil Single-Port-MSI nicht unterstützt wird. [RFLNX-4219]
- Der Sitzungsstart schlägt möglicherweise auf CentOS 8.x-, Fedora 29-, 30- und 31-Distributionen fehl. Einen Workaround enthält der Knowledge Center-Artikel CTX270926. [RFLNX-3114]

Bekannte Probleme in Release 1912

- Bei der Verwendung der CEF-basierten Umleitung des Browserinhalts liegt der Tastaturfokus nicht wieder auf dem Hauptfenster, wenn eine URL umgeleitet wird. Erstellen Sie als Workaround eine Browserregisterkarte und wechseln Sie, um auf die Hauptregisterkarte zuzugreifen. [RFLNX-3871]
- Bei Verwendung der CEF-basierten Umleitung des Browserinhalts wird möglicherweise gemeldet, dass der Webcontainer-Prozess beendet wurde. Das Problem tritt auf, wenn Sie die Browserinstanz schließen. [RFLNX-3872]
- Bei Verwendung der Self-Service-Benutzeroberfläche funktionieren die Optionen des Fensters **Einstellungen** möglicherweise nicht wie erwartet und die Workspace-Anwendung reagiert vorübergehend nicht. Das Problem tritt bei der Ubuntu 19.10-Distribution auf. [RFLNX-3720]
- Feeds des intelligenten Workspace werden in Version 1912 der Citrix Workspace-App nicht unterstützt.
- Die Webcamumleitung funktioniert nicht mit Microsoft Teams. Dies ist eine Einschränkung, da Microsoft Teams Optimization [MTOP] in der Citrix Workspace-App für Linux nicht unterstützt wird. [RFLNX-3674]

Bekannte Probleme in Release 1910

- Wenn Sie die Self-Service-Benutzeroberfläche verwenden, funktionieren die Optionen im Fenster **Voreinstellungen** möglicherweise nicht wie erwartet. Das Problem tritt auf, wenn das Paket “libwebkit1” nicht verfügbar ist, wie es bei Debian 10 Buster-Clients der Fall ist. Entfernen Sie als Workaround die Bibliothek **UIdialogLibWebKit.so**, die sich im Verzeichnis `install/path/lib` befindet. [RFLNX-3596]
- Aufgrund architektonischer Änderungen können Sie keine Verbindung mehr mit dem Cloudstore [Cloudsetup] herstellen. Citrix empfiehlt, dass Sie die neueste Version der Citrix Workspace-App verwenden.

Hinweise zu Drittanbietern

Die Citrix Workspace-App enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

Citrix Workspace-App für Linux – Hinweise zu Drittanbietern

Experimentelle Features

Gelegentlich veröffentlicht Citrix experimentelle Features als Möglichkeit, Feedback von Kunden zur potenziellen Erwünschtheit neuer Technologien oder Features zu erhalten. Citrix akzeptiert keine Supportanfragen für experimentelle Features, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf

das Feedback vor. Citrix unterliegt keiner Verpflichtung, experimentelle Features in ein Produktrelease zu übernehmen und behält sich das Recht vor, diese Features jederzeit aus beliebigem Grund zurückziehen.

Voraussetzungen für die Installation der Citrix Workspace-App

June 10, 2021

Systemanforderungen und Kompatibilität

Systemanforderungen finden Sie in der folgenden Liste:

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

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

Network	Requirements
Network protocol	- TCP/IP

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

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

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

* Nach Veröffentlichung von Release 1910 funktioniert die Citrix Workspace-App für Linux möglicherweise nicht wie erwartet, wenn das Betriebssystem die folgenden GCC-Versionskriterien nicht erfüllt:

- GCC-Version für x64-Architektur: 4.8 oder höher
- GCC-Version für ARMHF-Architektur: 4.9 oder höher

> **Hinweis**
>
> Ab Release 2101 funktioniert die Citrix Workspace-App für Linux möglicherweise nicht wie erwartet, wenn das Betriebssystem nicht die folgenden Anforderungen erfüllt:
>
> - GCC Version 4.9 oder höher
> - glibcxx 3.4.20 oder höher

Kompatibilitätsmatrix

Die Citrix Workspace-App für Linux ist mit allen derzeit unterstützten Versionen der folgenden Citrix-Produkte kompatibel. Weitere Informationen zum Citrix Produktlebenszyklus und wann Citrix die Unterstützung bestimmter Produktversionen beendet, finden Sie unter Citrix Product Lifecycle Matrix.

Serveranforderungen

StoreFront

- Sie können alle derzeit unterstützten Versionen der Citrix Workspace-App für den Zugriff auf StoreFront-Stores über interne Netzwerkverbindungen und über Citrix Gateway verwenden:
  - StoreFront 1811 und höher.
  - StoreFront 3.12.
- Sie können StoreFront verwenden, das mit Workspace für Web konfiguriert wurde. Workspace für Web ermöglicht den Zugriff auf StoreFront-Stores über einen Webbrowser. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie unter Wichtige Überlegungen in der StoreFront-Dokumentation.

Verbindungen und Zertifikate

Verbindungen

Die Citrix Workspace-App für Linux unterstützt HTTPS- und ICA-über-TLS-Verbindungen über folgende Konfigurationen.

- LAN-Verbindungen:
  - StoreFront mit StoreFront Services oder Workspace für Web
- Für sichere Remote- oder lokale Verbindungen:
  - Citrix Gateway 12.0
  - NetScaler Gateway 10.1 und höher
  - NetScaler Access Gateway Enterprise Edition 10
  - NetScaler Access Gateway Enterprise Edition 9.x
  - NetScaler Access Gateway VPX

  Weitere Informationen zu den von StoreFront unterstützten Citrix Gateway-Versionen finden Sie unter den Systemanforderungen von StoreFront.

Zertifikate

Verwenden Sie die folgenden Zertifikate, um sichere Transaktionen zwischen Server und Client sicherzustellen:

Private (selbstsignierte) Zertifikate

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

> **Hinweis:**
>
> Wenn das Zertifikat des Remotegateways 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, werden die Apps angezeigt, können jedoch nicht gestartet werden. Das Stammzertifikat muss im Zertifikatspeicher des Clients installiert werden.

Stammzertifikate

Für in Domänen eingebundene Maschinen können Sie ZS-Zertifikate mit der administrativen Gruppenrichtlinienobjektvorlage verteilen und als vertrauenswürdig einstufen.

Für nicht domänengebundene Maschinen können Unternehmen ein benutzerdefiniertes Installationspaket erstellen und damit das Zertifikat der Zertifizierungsstelle verteilen und installieren. Wenden Sie sich bei Fragen an den Systemadministrator.

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 die Citrix Workspace-App die folgenden Zertifikate.

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

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App 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 Server-

namen in der Subject Alternative Name-Erweiterung, in Betracht gezogen werden. Solche Zertifikate können von privaten und öffentlichen Zertifizierungsstellen ausgestellt werden.

Zwischenzertifikate und Citrix Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter Konfigurieren von Zwischenzertifikaten in der Dokumentation zu Citrix Gateway.

Wenn der StoreFront-Server keine Zwischenzertifikate bereitstellen kann, die dem verwendeten Zertifikat entsprechen, oder wenn Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren, führen Sie diese Schritte aus, bevor Sie einen StoreFront-Store hinzufügen.

1. Besorgen Sie sich die einzelnen Zwischenzertifikate im PEM-Format.

   > **Tipp:**
   >
   > Wenn Sie kein Zertifikat im PEM-Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.

2. Installieren Sie als Benutzer das Paket (normalerweise root):

   a) Kopieren Sie eine oder mehrere Dateien zu $ICAROOT/keystore/intcerts.

   b) Führen Sie den folgenden Befehl als Benutzer, der das Paket installiert hat, aus:

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

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

Die Citrix Workspace-App für Linux hat eine strenge Validierungsrichtlinie für Serverzertifikate.

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

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

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

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"
- "Beispielstammzertifikat"

Die Citrix Workspace-App für Linux überprüft dann, ob alle Zertifikate gültig sind. Die Citrix Workspace-App für Linux überprüft ebenfalls, ob dem "Beispielstammzertifikat" bereits vertraut wird. Wenn die Citrix Workspace-App für Linux dem "Beispielstammzertifikat" nicht vertraut, schlägt die Verbindung fehl.

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

Die Citrix Workspace-App für Linux verwendet dann diese beiden Zertifikate. Dann sucht die App nach einem Stammzertifikat auf dem Benutzergerät. Wird ein gültiges Zertifikat gefunden, das auch vertrauenswürdig ist (z. B. "Beispielstammzertifikat"), ist die Verbindung erfolgreich. Andernfalls schlägt

die Verbindung fehl. Diese Konfiguration stellt der Citrix Workspace-App für Linux das benötigte Zwischenzertifikat zur Verfügung und ermöglicht auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"
- "Falsches Stammzertifikat"

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Die Citrix Workspace-App für Linux ignoriert das falsche Stammzertifikat jedoch nicht und die Verbindung schlägt fehl.

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat 1"
- "Beispielzwischenzertifikat 2"

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"
- "Übergreifendes Beispielzwischenzertifikat" [nicht empfohlen]

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

- "Beispielserverzertifikat"

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

Hdxcheck

Citrix stellt das Skript hdxcheck.sh als Teil des Citrix Workspace-App-Installationspakets bereit. Das Skript überprüft, ob das Gerät alle Systemanforderungen erfüllt, um die gesamte Funktionalität der Workspace-App für Linux zu unterstützen. Das Skript befindet sich im Verzeichnis `Utilities` des Installationspakets.

Ausführen des Skripts hdxcheck.sh

1. Öffnen Sie das Terminal auf Ihrer Linux-Maschine.
2. Geben Sie `cd $ICAROOT/util` ein und drücken Sie die **EINGABETASTE**, um zum Verzeichnis `Utilities` des Installationspakets zu navigieren.
3. Geben Sie `./hdxcheck.sh` ein, um das Skript auszuführen.

Installieren, Deinstallieren und Aktualisieren

May 4, 2021

Sie können die Citrix Workspace-App mit einer der folgenden Methoden installieren:

- Laden Sie die Citrix Workspace-App von Citrix Downloads herunter.
- Bereitstellen der Citrix Workspace-App mit Workspace für Web (mit StoreFront konfiguriert).

Manuelle Installation

Laden Sie die folgenden Pakete von Citrix Downloads herunter.

Debian-Pakete

Installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `Icaclient`-Pakete oder eines der `IcaclientWeb`-Pakete.

Um die generische USB-Umleitung zu verwenden, installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `ctxusb`-Pakete.

Paketname	Inhalt
Debian-Pakete (Ubuntu, Debian, Linux Mint usw.)	
icaclient_20.06.0.15_amd64.deb	Self-Service-Support, 64 Bit, x86_64
icaclient_20.06.0.15_i386.deb	Self-Service-Support, 32 Bit, x86
icaclient_20.06.0.15_armhf.deb	Self-Service-Support, ARM HF
icaclientWeb_20.06.0.15_amd64.deb	nur Web Receiver, 64 Bit, x86_64
icaclientWeb_20.06.0.15_i386.deb	nur Web Receiver, 32 Bit, x86
icaclientWeb_20.06.0.15_armhf.deb	nur Web Receiver, ARM HF
ctxusb_20.06.0.15_amd64.deb	USB-Paket, 64 Bit, x86_64
ctxusb_20.06.0.15_i386.deb	USB-Paket, 32 Bit, x86
ctxusb_20.06.0.15_armhf.deb	USB-Paket, ARM HF

Installation mit einem Debian-Paket

Wenn Sie die Citrix Workspace-App mit dem Debian-Paket unter Ubuntu installieren, öffnen Sie die Pakete im Ubuntu Software Center.

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

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. Falls kein Paketmanager verfügbar ist, empfiehlt Citrix das Befehlszeilentool **gdebi**.

> **Voraussetzungen:**
>
> Sie müssen das Paket `icaclient` oder das Paket `icaclientWeb` installieren.

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 drei Pakete aus, indem Sie `gdebi packagename.deb` eingeben. Beispiel:
   - `gdebi icaclient\\_19.0.6.6\\_amd64.deb`
   - `gdebi icaclientWeb\\_19.0.6.6\\_i386.deb`
   - `gdebi ctxusb\\_2.7.6\\_amd64.deb`

   Um in den obigen Beispielen `dpkg` zu verwenden, ersetzen Sie `gdebi` mit `dpkg -i`.

   Wenn Sie `dpkg` verwenden, installieren Sie fehlende Abhängigkeiten durch Eingabe von `sudo apt-get -f install`.

   > **Hinweis:**
   >
   > - Das `ctxusb`-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.
   > - Ab Version 2101 werden Sie über eine interaktive Meldung aufgefordert, den App-Schutz zu installieren.
4. Akzeptieren Sie die Lizenzvereinbarung.

Installieren der App-Schutzkomponente auf Debian-Paketen:

Ab Version 2102 wird der App-Schutz von der Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie für die unbeaufsichtigte Installation der App-Schutzkomponente den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

```
1 `export DEBIAN_FRONTEND=”noninteractive”`
2
3 `sudo debconf-set-selections <<< ”icaclient app_protection/
    install_app_protection select no”`
4
5 `sudo debconf-show icaclient`
6
7 `sudo apt install -f ./icaclient_<version>._amd64.deb`
```

Red Hat-Pakete

Installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `ICAClient`-Pakete oder eines der `ICAClientWeb`-Pakete.

Um die generische USB-Umleitung zu verwenden, installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `ctxusb`-Pakete.

Paketname	Inhalt
Redhat-Pakete (Redhat, SUSE, Fedora usw.)	
ICAClient-rhel-20.06.0.15-0.x86_64.rpm	Self-Service-Support, basierend auf Red Hat (einschl. Linux VDA), 64 Bit, x86_64
ICAClient-rhel-20.06.0.15-0.i386.rpm	Self-Service-Support, basierend auf Red Hat, 32 Bit, x86
ICAClientWeb-rhel-20.06.0.15-0.x86_64.rpm	nur Web Receiver, basierend auf Red Hat, 64 Bit, x86_64
ICAClientWeb-rhel-20.06.0.15-0.i386.rpm	nur Web Receiver, basierend auf Red Hat, 32 Bit, x86
ICAClient-suse-20.06.0.15-0.x86_64.rpm	Self-Service-Support, basierend auf SUSE, 64 Bit, x86_64
ICAClient-suse-20.06.0.15-0.i386.rpm	Self-Service-Support, basierend auf SUSE, 32-Bit, x86
ICAClientWeb-suse-20.06.0.15-0.x86_64.rpm	nur Web Receiver, basierend auf SUSE, 64 Bit, x86_64
ICAClientWeb-suse-20.06.0.15-0.i386.rpm	nur Web Receiver, basierend auf SUSE, 32 Bit, x86
ctxusb-20.06.0.15-1.x86_64.rpm	USB-Paket, 64 Bit, x86_64
ctxusb-20.06.0.15-1.i386.rpm	USB-Paket, 32 Bit, x86

> **Hinweis:**
>
> Das RPM-Paket *SuSE 11 SP3 Full Package (Self-Service Support)* ist veraltet.

Installation mit einem RPM-Paket

Wenn Sie die Citrix Workspace-App vom RPM-Paket auf SUSE installieren, verwenden Sie das Hilfsprogramm YaST oder Zypper. Das RPM-Dienstprogramm installiert das RPM-Paket. Ein Fehler tritt auf, wenn die erforderlichen Abhängigkeiten fehlen.

Einrichten des EPEL-Repositorys auf Red Hat

Laden Sie das entsprechende RPM-Quellpaket hier herunter: https://fedoraproject.org/wiki/EPEL#Extra_Packages_for_Enterprise_Linux_.28EPEL.29.

Informationen zur Verwendung finden Sie unter https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F.

Beispielsweise können Sie unter Red Hat Enterprise 7.x das EPEL-Repository mit folgendem Befehl installieren:

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

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

Installation von einem RPM-Paket

> **Voraussetzungen:**
>
> Sie müssen das Paket `icaclient` oder das Paket `icaclientWeb` installieren.

1. Richten Sie das EPEL-Repository ein.
2. Melden Sie sich als privilegierter Benutzer (root) an.
3. Führen Sie die Installation der folgenden drei Pakete aus, indem Sie “zypper” in \ eingeben.

   > **Hinweis:**
   >
   > - `ctxusb` ist ein optionales Paket. Installieren Sie das Paket zur Unterstützung der generischen USB-Umleitung.
   > - `ctxappprotection` ist ein optionales Paket. Installieren Sie das Paket nur, wenn Sie die App-Schutzkomponente installieren möchten.

4. Öffnen Sie ein Terminal-Fenster.

   Für SUSE-Installationen:

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

   Für Red Hat-Installationen:

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

5. Akzeptieren Sie die Lizenzvereinbarung.

Installieren eines fehlenden Pakets

Wenn bei einer auf Red Hat basierenden Distribution (RHEL, CentOS, Fedora usw.) die folgende Fehlermeldung angezeigt wird:

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

Fügen Sie ein EPEL-Repository hinzu (Details finden Sie unter https://fedoraproject.org/wiki/EPEL).

Tarball-Pakete

Installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der folgenden Pakete.

Paketname	Inhalt
Tarballs (Skriptinstallation für jede Distribution)	
linuxx64-20.06.0.15.tar.gz	64 Bit Intel
linuxx86-20.06.0.15.tar.gz	32 Bit Intel
linuxarmhf-20.06.0.15.tar.gz	ARM HF

Der Unterschied zwischen den Paketen für die Web Workspace-App und für Self-Service ist, dass die Pakete mit Unterstützung für Self-Service die dafür erforderlichen Abhängigkeiten enthalten (zusätzlich zu den für die Web Workspace-App erforderlichen Abhängigkeiten). Die Abhängigkeiten für Self-Service sind eine Obermenge der für die Web Workspace-App erforderlichen Abhängigkeiten. Die installierten Dateien sind jedoch identisch.

- Wenn Sie nur die Workspace-App für Web benötigen oder Ihre Distribution nicht die erforderlichen Pakete für Self-Service umfasst, installieren Sie nur das Paket für die Workspace-App für Web.
- Andernfalls installieren Sie die Citrix Workspace App mit dem Debian-Paket oder RPM-Paket.

Diese Dateien sind einfacher zu verwenden, da sie automatisch alle erforderlichen Pakete installieren.

- Wenn Sie den Installationsort anpassen möchten, installieren Sie die Citrix Workspace-App vom Tarball-Paket.

> **Hinweis:**
>
> - Verwenden Sie nicht zwei unterschiedliche Installationsmethoden auf derselben Maschine. Andernfalls kann es zu Fehlermeldungen und unerwünschtem Verhalten kommen.

Installation mit 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. Extrahieren Sie den Inhalt der `.tar.gz`-Datei 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` (Citrix Workspace-App 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 ohne eine Eingabe vorzunehmen, um die Citrix Workspace-App 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 `$HOME/ICAClient/platform`. "platform" ist ein systemgenerierter Bezeichner des installierten Betriebssystems, z. B. `$HOME/ICAClient/linuxx86` für die Linux/x86-Plattform.

   > **Hinweis:**
   >
   > Wenn Sie einen anderen Speicherort als den Standardspeicherort verwenden, legen Sie ihn in $ICAROOT in `$HOME/.profile` oder `$HOME/.bash\\_profile` fest.

6. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie `y` ein und drücken Sie die Eingabetaste.
7. Wählen Sie, ob die Citrix Workspace-App in die Desktopumgebung integriert werden soll. Die Installation erstellt eine Menüoption, über die Benutzer die Citrix Workspace-App starten können.

Geben Sie an der Eingabeaufforderung `y` ein, um die Integration zu aktivieren.

8. Wenn Sie GStreamer installiert haben, können Sie entscheiden, ob Sie GStreamer in die Citrix Workspace-App integrieren und damit die HDX MediaStream-Multimediabeschleunigung bereitstellen. Um die Citrix Workspace-App mit GStreamer zu integrieren, geben Sie an der Eingabeaufforderung `y` ein.

   > **Hinweis:**
   >
   > Auf einigen Plattformen kann die Installation des Clients mit einem Tarball-Paket dazu führen, dass das System nicht mehr reagiert, nachdem Sie zur Integration mit KDE und GNOME aufgefordert wurden. Das Problem tritt bei der ersten Initialisierung von gstreamer-0.10 auf. Wenn dieses Problem auftritt, brechen Sie den Installationsvorgang mit Strg+C ab und führen Sie den folgenden Befehl aus: `gst-inspect-0.10 -- gst-disable-registry-fork --version`. Nach dem Ausführen des Befehls können Sie das Tarball-Paket erneut ausführen, ohne dass das Problem auftritt.

9. Wenn Sie sich als privilegierter Benutzer (root) anmelden, können Sie entscheiden, ob Sie die USB-Unterstützung für mit Citrix Virtual Apps and Desktops veröffentlichte VDI-Anwendungen aktivieren möchten. Geben Sie an der Eingabeaufforderung `y` ein, um die USB-Unterstützung zu installieren.

   > **Hinweis:**
   >
   > Wenn Sie nicht als privilegierter Benutzer (root) angemeldet sind, wird die folgende Warnung angezeigt:
   >
   > "USB-Unterstützung kann nur von Root-Benutzern installiert werden. Führen Sie den Installer als root aus, um diese Option installieren zu können."

10. Nach Abschluss der Installation wird das Hauptinstallationsmenü wieder angezeigt. Geben Sie zum Beenden des Setups `3` ein und drücken Sie die Eingabetaste.

Deinstallieren

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

Die Umgebungsvariable ICAROOT muss für das Installationsverzeichnis des Clients festgelegt sein. Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist `$HOME/ICAClient/platform`. Die Variable "platform" ist ein systemgenerierter Bezeichner des installierten Betriebssystems, z. B. `$HOME/ICAClient/linuxx86` für die Linux/x86-Plattform. Das Standardverzeichnis für Installationen durch privilegierte Benutzer ist `/opt/Citrix/ICAClient`.

> **Hinweis:**
>
> Um die Citrix Workspace-App zu deinstallieren, müssen Sie als der Benutzer angemeldet sein, der die Installation durchgeführt hat.

Deinstallieren des Tarball-Pakets

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**.

Upgrade

Für das Upgrade von Citrix Receiver auf die Citrix Workspace-App laden Sie die aktuelle Version der Citrix Workspace-App von Citrix Downloads herunter und installieren Sie sie.

Die **Citrix Workspace**-Bildschirmüberlagerung wird beim ersten Start der App, beim Upgrade und bei der Deinstallation und Neuinstallation der App angezeigt. Klicken Sie auf **Verstanden**, um die Citrix Workspace-App weiter zu verwenden, oder klicken Sie auf **Weitere Informationen**, um weitere Informationen zu erhalten.

Erste Schritte

May 4, 2021

Einrichten

Sie können das Installationspaket herunterladen, die Konfiguration anpassen und dann die Citrix Workspace App-installieren. Sie können den Inhalt des Citrix Workspace-App-Pakets ändern und die Dateien anschließend neu verpacken.

Anpassen der Installation

1. Entpacken Sie das Citrix Workspace-App-Paket in einem leeren Verzeichnis. Die Paketdatei heißt platform.major.minor.release.build.tar.gz (z. B. linuxx86.13.2.0.nnnnnn.tar.gz für die Plattform Linux/x86).
2. Nehmen Sie die erforderlichen Änderungen am Citrix Workspace-App-Paket vor. Sie können dem Paket beispielsweise ein TLS-Stammzertifikat hinzufügen, um ein Zertifikat einer Zerti-

fizierungsstelle zu verwenden, die nicht Teil der Standardinstallation der Citrix Workspace-App ist.

3. Öffnen Sie die Datei `PkgID`.
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.
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. Ohne Aktualisierung kann bei der Installation des neuen Pakets en 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 (immer auf `cor` einzustellen)
   - Berechtigungen
   - Besitzer
   - Gruppe
   - Größe
8. Speichern und schließen Sie die Datei.
9. Verwenden Sie den Befehl tar, um die Paketdatei der Citrix Workspace-App neu zu erstellen. Zum Beispiel `tar czf ../newpackage.tar.gz *`, wobei `newpackagez` der Name der neuen Paketdatei der Citrix Workspace-App ist.

Aktuelle Webkitunterstützung

Die Citrix Workspace-App für Linux erfordert libwebkit2gtk (2.16.6+).

libwebkit2gtk hat folgende Vorteile:

- Verbesserte Benutzeroberfläche. webkit2gtk ist mit der Funktion für die Browserinhaltsumleitung kompatibel. Verwenden Sie webkit2gtk Version 2.24 und höher für ein besseres YouTube-Erlebnis.
- webkit2gtk Version 2.16.6 und höher verbessert und beschleunigt die Anmeldeerfahrung.

- Die App funktioniert besser mit den neueren Linux-Distributionen und umfasst die neuesten Webkit-Sicherheitsupdates.

> **Hinweis:**
>
> Auf einigen Linux-Distributionen ist webkit2gtk nicht verfügbar. Als Workaround gibt es die folgenden Optionen:
>
> - Erstellen Sie das webkit2gtk aus der Quelle, bevor Sie die Citrix Workspace-App Version 1906 installieren.
> - Laden Sie das Webpaket von der Downloadseite herunter. Nur Webstarts werden von diesem Paket unterstützt.
> - Wechseln Sie zu einer neueren Linux-Distribution, die webkit2gtk 2.16.6 oder höher unterstützt.

Starten

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

Die Umgebungsvariable `ICAROOT` muss auf das richtige Installationsverzeichnis verweisen.

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

Terminal-Eingabeaufforderung

Geben Sie Folgendes ein, um die Citrix Workspace-App an der Terminal-Eingabeaufforderung zu starten:
`/opt/Citrix/ICAClient/selfservice`

Hierbei ist /opt/Citrix/ICAClient das Verzeichnis, in dem Sie die Citrix Workspace-App installiert haben. Drücken Sie dann die Eingabetaste.

Linux-Desktop

Mithilfe eines Dateimanagers können Sie die Citrix Workspace-App von einer Desktopumgebung für Linux aus starten.

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

Einstellungen

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

Verwalten eines Kontos

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

1. Führen Sie auf der Seite **Konten** im Dialogfeld **Einstellungen** einen der folgenden Schritte aus:
   - Klicken Sie auf **Hinzufügen**, um ein Konto hinzuzufügen. Wenden Sie sich an Ihren Systemadministrator, um weitere Informationen zu erhalten.
   - 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. Authentifizieren Sie sich beim Server, wenn Sie dazu aufgefordert werden.

Desktopanzeige

> **Hinweis:**
>
> Dieses Feature steht nicht für Citrix Virtual Apps für UNIX-Sitzungen zur Verfügung.

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

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

Verwenden Sie die Symbolleistenfunktion zum **Aktivieren des Desktop Viewer**, um die Fensterkonfiguration Ihrer Remotesitzung dynamisch zu ändern.

Desktop Viewer

Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern.

Verwenden Sie Desktop Viewer für die Interaktion der Benutzer mit dem virtuellen Desktop. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen

Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario können Benutzer mit der Symbolleistenfunktionalität von Desktop Viewer in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore. Benutzer können zwischen Desktopsitzungen wechseln und auf einem Benutzergerät mit mehreren Desktops über mehrere Citrix Virtual Apps and Desktops-Verbindungen arbeiten. Zur bequemen Verwaltung einer Benutzersitzung gibt es Schaltflächen zum Minimieren aller Desktopsitzungen, zum Übermitteln der Tastenkombination Strg+Alt+Entf, zum Trennen der Sitzung und zum Abmelden.

Durch Drücken von **Strg+Alt+Untbr** werden die Schaltflächen der Desktop Viewer-Symbolleiste in einem Popup-Fenster angezeigt.

Automatische Sitzungswiederverbindung

Die Citrix Workspace-App kann Desktops und Anwendungen, deren Verbindung getrennt wurde, wiederverbinden. Dies kann beispielsweise bei einem Problem mit der Netzwerkinfrastruktur erforderlich sein.

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

Zugriff auf lokale Dateien

Virtuelle Desktops bzw. Anwendungen benötigen 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:
    - **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 eine Aufforderung an, wenn der Desktop oder die Anwendung Zugriff auf lokale Dateien benötigt.
2. Klicken Sie auf **Hinzufügen**, geben Sie den Speicherort an und wählen Sie ein Laufwerk für die Zuordnung.

Mikrofon und Webcam

Zum Ein richten eines Mikrofons oder einer Webcam können Sie die Art und Weise ändern, wie ein virtueller Desktop oder eine Anwendung auf Ihr lokales Mikrofon oder Ihre Webcam zugreift:

Wählen Sie im Dialogfeld **Einstellungen** auf der Seite **Mikrofon & Webcam** 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.

Flash Player

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

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

- **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.

Verbinden

Die Citrix Workspace-App 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 Legacy-webseiten verwaltet.

Herstellen einer Verbindung zu Ressourcen mit der Citrix Workspace-Benutzeroberfläche

Die Homepage der Citrix Workspace-App zeigt virtuelle Desktops und Anwendungen an, die Benutzern basierend auf deren Kontoeinstellungen (d. h. dem Server, mit dem sie eine Verbindung herstellen) und basierend auf den von Citrix Virtual Apps and Desktops-Administratoren konfigurierten Einstellungen zur Verfügung stehen. Mit der Seite **Einstellungen** > **Konten** können Sie die URL eines StoreFront-Servers konfigurieren oder bei konfigurierter E-Mail-basierter Kontenermittlung die E-Mail-Adresse eingeben.

> **Tipp:**
>
> Wenn Sie denselben Namen für mehrere Stores auf dem StoreFront-Server verwenden, vermeiden Sie Duplikationen, indem Sie Nummern hinzufügen. Die Namen dieser Stores hängen von

> der Reihenfolge ab, in der sie hinzugefügt werden. Für die Citrix Workspace-App wird die Store-URL angezeigt und identifiziert den Store eindeutig.

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

Konfigurieren von Verbindungseinstellungen

Sie können einige Standardeinstellungen für Verbindungen zwischen der Citrix Workspace-App und Citrix Virtual Apps and Desktops-Servern konfigurieren. Sie können diese Einstellungen ggf. für einzelne Verbindungen ändern.

Obwohl sich die Aufgaben und Verantwortungsbereiche von Administratoren und Benutzern überschneiden können, wird der Ausdruck “Benutzer” verwendet, um zwischen den typischen von Benutzern ausgeführten Aufgaben im Gegensatz zu von Administratoren ausgeführten Aufgaben zu unterscheiden.

Verbinden mit Ressourcen per Eingabeaufforderung oder Browser

Verbindungen mit Servern werden hergestellt, wenn Sie auf der Citrix Workspace-App-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

Voraussetzung:

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

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

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

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

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

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


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

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

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

Herstellen einer Verbindung mit einem Webbrowser

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

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

1. Führen Sie die folgenden Befehle aus, wenn die Citrix Workspace-App von einem Benutzer ohne Administratorrechte installiert wird. Die Einstellungen von ICAROOT werden möglicherweise geändert, wenn sie nicht in einem Standardspeicherort installiert werden. Sie können das Ergebnis mit dem Befehl

   `xdg-mime query default application/x-ica` testen, der “wfica.desktop” zurückgeben muss.

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

   ```
   xdg-icon-resource install --size 64
   ```

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

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

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

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

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

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

   Möglicherweise müssen Sie in Firefox unter “Einstellungen > Anwendungen” Konfigurationen vornehmen.

Wählen Sie für “Citrix ICA settings file content” Folgendes aus:

- “Citrix Workspace app Engine (default)” im Dropdownmenü

  oder

- “Use other …” und dann die Datei /usr/share/applications/wfica.desktop (für die Administratorinstallation der Citrix Workspace-App)

  oder

- $HOME/.local/share/applications/wfica.desktop (für eine Installation ohne Administratorrechte).

Connection Center

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

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

Verwalten einer Verbindung

Verwalten einer Verbindung mit dem **Connection Center**:

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

   Die verwendeten Server und die jeweils aktiven Sitzungen werden aufgelistet.

2. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie einen Server, trennen Sie die Verbindung oder melden Sie sich ab, oder zeigen Sie seine Eigenschaften an.
   - Wählen Sie eine Anwendung aus und schließen Sie das Fenster.

Konfigurieren

June 10, 2021

Wenn Sie die Citrix Workspace-App für Linux verwenden, führen Sie die folgenden Konfigurationsschritte aus, damit die Benutzer auf ihre gehosteten Anwendungen und Desktops zugreifen können.

Einstellungen

Konfigurationsdateien

Zum Ändern erweiterter oder selten verwendeter Einstellungen können Sie die Konfigurationsdateien der Citrix Workspace-App 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. Diese Einstellung kann dazu führen, dass in einer Konfigurationsdatei vorgenommene Änderungen ignoriert werden.

Standardeinstellungen

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

> **Hinweis:**
>
> Wenn ein Eintrag in `All\\_Regions.ini` auf einen bestimmten Wert festlegt ist, wird der Wert in `module.ini` für diesen Eintrag nicht verwendet. Die Werte in `All\\_Regions.ini` haben Vorrang vor dem Wert in `module.ini`.

Vorlagendatei

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

Benutzereinstellungen

Um Konfigurationsänderungen für einen Benutzer anzuwenden, ändern Sie die Datei `wfclient.ini` im Benutzerverzeichnis `$HOME/.ICAClient`. Die Einstellungen in dieser Datei gelten für zukünftige Verbindungen für diesen Benutzer.

Überprüfen von Einträgen in Konfigurationsdateien

Um die Werte für Einträge in `wfclient.ini` zu beschränken, müssen Sie die zulässigen Optionen oder Optionsbereiche in der Datei `All\\_Regions.ini` festlegen.

Wenn Sie nur einen Wert angeben, wird dieser Wert verwendet. `$HOME/.ICAClient/All\\_Regsions.ini` kann nur mit den in `$ICAROOT/config/All\\_Regions.ini` angegebenen Werten übereinstimmen oder sie reduzieren. Beschränkungen können nicht aufgehoben werden.

> **Hinweis:**
>
> Der in `wfclient.ini` festgelegte Wert hat Vorrang vor dem Wert in `module.ini`.

Parameter

Die Parameter in jeder Datei sind in Abschnitte zusammengefasst. Jeder Abschnitt beginnt mit einem Namen in 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

`All\\_Regions.ini` definiert Parameter, die durch andere Dateien festgelegt werden können. In dieser Datei können Werte für Parameter eingeschränkt oder genau festgelegt werden.

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

1. `All\\_Regions.ini` - Die 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 Citrix Workspace-App-Code verwendet.

> **Hinweis:**
>
> Es gibt Ausnahmen bei dieser Rangfolge. Beispielsweise werden vom Code aus Sicherheitsgründen gezielt einige Werte aus `wfclient.ini` gelesen.

Pinnen des Bildschirmlayouts im Multimonitormodus

Ab Version 2103 können Sie die Auswahl für das Bildschirmlayout im Multimonitormodus speichern. Das Layout bestimmt, wie eine Desktopsitzung angezeigt wird. Durch Pinnen wird das ausgewählte Layout beim Neustarten einer Sitzung beibehalten, was die Benutzererfahrung optimiert.

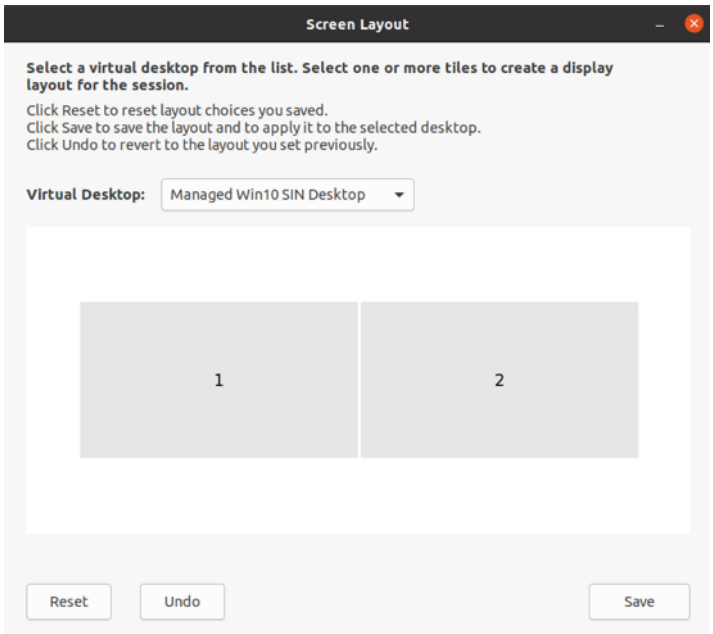
Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu:

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

Erst nachdem Sie den oben angegebenen Schlüssel hinzugefügt haben, können Sie die Option **Bildschirmlayout** im App-Indikator sehen. Weitere Informationen zum App-Indikator finden Sie unter App-Indikatorsymbol.

Um das Bildschirmlayout auszuwählen, klicken Sie auf das App-Indikatorsymbol in der Taskleiste und wählen Sie **Bildschirmlayout**. Das Dialogfeld **Bildschirmlayout** wird angezeigt.

Alternativ können Sie das Dialogfeld **Bildschirmlayout** im Self-Service-Fenster durch Drücken der Tastenkombination **Ctrl+M** öffnen.



Wählen Sie einen virtuellen Desktop aus dem Dropdownmenü aus. Die Layoutauswahl wird nur auf den ausgewählten Desktop angewendet.

Wählen Sie eine oder mehrere Kacheln aus, um eine rechteckige Auswahl für das Layout zu bilden. Die Sitzung wird dann gemäß der Layoutauswahl angezeigt.

Einschränkungen:

- Durch Aktivieren des Pinnens wird die Funktion zum Speichern des Bildschirmlayouts in einer Sitzung deaktiviert.
- Dieses Feature gilt nur für Desktops, die als Favorit gekennzeichnet sind.

App-Schutz - experimentelles Feature

> **Hinweis:**
>
> - Diese Funktion wird nur unterstützt, wenn die Citrix Workspace-App mithilfe des Tarball-Pakets installiert wird. x64 und armhf sind zudem die einzigen unterstützten Pakete.
> - Dieses Feature wird nur für On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops unterstützt.

Der App-Schutz ist eine Zusatzfunktion, die erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops bietet. Die Funktion beschränkt die Möglichkeit, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. Der App-Schutz verhindert das Exfiltrieren vertraulicher Informationen wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

Voraussetzung:

Ubuntu 18.04 oder höher.

Installieren der App-Schutzkomponente:

Wenn Sie die Citrix Workspace-App mit dem Tarball-Paket installieren, wird die folgende Meldung angezeigt.

“Möchten Sie die App-Schutzkomponente installieren? Warnung: Sie können dieses Feature nicht deaktivieren. Zum Deaktivieren müssen Sie die Citrix Workspace-App deinstallieren. Weitere Informationen erhalten Sie von Ihrem Systemadministrator. [Standard $INSTALLER_N]:”

Geben Sie **Y** ein, um die App-Schutzkomponente zu installieren.

Die App-Schutzkomponente ist standardmäßig nicht installiert.

Starten Sie die Maschine neu, damit die Änderungen wirksam werden. Sie müssen eventuell die Maschine neu starten, damit der App-Schutz wie erwartet funktioniert.

Installieren der App-Schutzkomponente auf RPM-Paketen:

Ab Version 2104 wird der App-Schutz von der RPM-Version der Citrix Workspace-App unterstützt.

Mit den folgenden Schritten installieren Sie den App-Schutz:

1. Installieren Sie die Citrix Workspace-App.

2. Installieren Sie das App-Schutzpaket `ctxappprotection<version>.rpm` aus dem Installer der Citrix Workspace-App.
3. Starten Sie das System neu, damit die Änderungen wirksam werden.

Installieren der App-Schutzkomponente auf Debian-Paketen:

Ab Version 2101 wird der App-Schutz von der Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie für die unbeaufsichtigte Installation der App-Schutzkomponente den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

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

sudo debconf-show icaclient
* app_protection/install_app_protection: no

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

Bekannte Probleme:

- Wenn Sie einen geschützten Bildschirm minimieren, läuft der App-Schutz weiterhin im Hintergrund.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Citrix Workspace-App für Linux und sendet die Daten automatisch an Google Analytics.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Citrix Workspace-App zu verbessern.

Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix und schützt sie gemäß der Anlage zur Sicherheit von Citrix Diensten, die unter Citrix Trust Center verfügbar ist.

Citrix verwendet Google Analytics, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu sammeln. Bitte lesen Sie, wie Google die für Google Analytics gesammelten Daten handhabt.

Auf folgende Weise können Sie das Senden von CEIP-Daten an Citrix und Google Analytics deaktivieren (mit Ausnahme der beiden für Google Analytics erfassten Datenelemente, die durch ein * in der zweiten Tabelle unten gekennzeichnet sind):

1. Navigieren Sie zum Ordner `\<ICAROOT\>/config/module.ini` und dann zum Abschnitt `CEIP`.
2. Wählen Sie den Eintrag `EnableCeip` aus und legen Sie ihn auf `Disable` fest.

> **Hinweis:**
>
> Wenn Sie den Schlüssel `EnableCeip` auf `Disable` festgelegt haben und dann das Senden der letzten beiden CEIP-Datenelemente an Google Analytics deaktivieren möchten (Betriebssystemversion und Version der Workspace-App), navigieren Sie zum folgenden Registrierungseintrag und legen Sie den Wert wie vorgeschlagen fest:

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

Abschnitt: `GoogleAnalytics`

Eintrag: `DisableHeartBeat`

Wert: `True`

Folgende CEIP-Datenelemente werden von Google Analytics erfasst:

Betriebssystemversion*	Version der Workspace-App*	App-Name	Client-ID
Sitzungsstartmethode	Compiler-Version	Hardwareplattform	

App-Indikatorsymbol

Der App-Indikator wird beim Start der Citrix Workspace-App gestartet und ist ein Symbol im Infobereich. Die Einführung des App-Indikators verbessert die Anmeldeleistung der Citrix Workspace-App für Linux.

Sie können Leistungsverbesserungen in folgenden Situationen bemerken:

- Erster Start der Citrix Workspace-App
- Schließen und Neustarten der App
- Beenden und Neustarten der App

> **Hinweis:**
>
> Das Paket `libappindicator` ist erforderlich, damit der App-Indikator angezeigt wird. Installieren Sie das für Ihre Linux-Distribution geeignete Paket `libappindicator` aus dem Internet.

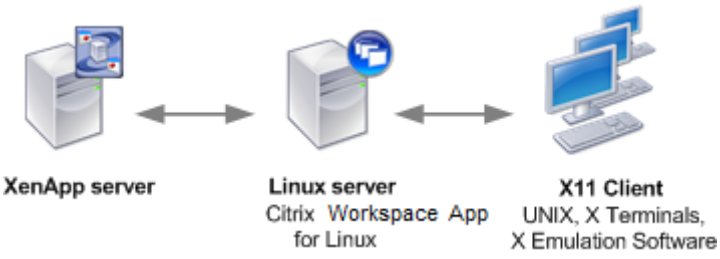
ICA-zu-X-Proxy

Sie können eine Workstation, auf der die Citrix Workspace-App 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 die Citrix Workspace-App nicht gibt.

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

Die Citrix Workspace-App kann als ICA-X11-Konverter angesehen werden, der die X11-Ausgabe auf den lokalen Linux-Desktop leitet. Natürlich können Sie die Ausgabe auch auf ein anderes X11-Display umleiten. Sie können mehrere Kopien der Citrix Workspace-App 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 die Citrix Workspace-App 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 die Citrix Workspace-App auf dem Linux-Server ausführen, der normalerweise die X-Anwendungen für die X-Terminals bereitstellt.
- Wenn Sie UNIX-Workstations einsetzen möchten, für die es die Citrix Workspace-App nicht gibt, benötigen Sie einen eigenen Server, der als Proxy dient. Hier wäre ein PC, auf dem Linux ausgeführt wird, denkbar.

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:

- Bereitstellen der lokalen UNIX-Workstation über NFS auf der als Proxy dienenden Workstation und Zuordnen eines Clientlaufwerks am NFS-Bereitstellungspunkt auf dem Proxy.
- Verwenden eines NFS-SMB-Proxys (z. B. SAMBA) oder eines NFS-Clients auf dem Server (z. B. Microsoft Services for UNIX).

Einige Leistungsmerkmale werden nicht an das Endgerät weitergeleitet:

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

Starten der Citrix Workspace-App mit serverseitigem ICA von einem X-Terminal oder einer UNIX-Workstation:

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

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

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

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

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
- HTTPS
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Ältere Real Player)

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

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

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

```
1 Mit dieser Einstellung wird Folgendes festgelegt:
2
3 - Das Hilfsprogramm ”nslaunch” wird ausgeführt, um die URL mit Push in
    ein vorhandenes Browserfenster zu übertragen.
4 - Jeder Browser in der Liste wird der Reihe nach ausprobiert, bis der
    Inhalt richtig angezeigt wird.
```

1. 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.

2. Speichern und schließen Sie die Datei.

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

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

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

Verbindung

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 der Citrix Workspace-App bei Verbindungen mit hoher Latenz für die Tastatur deaktiviert und nur für die Maus aktiviert. Weitere Informationen finden Sie in der Dokumentation "Citrix Workspace app for Linux OEM's Reference Guide".
- **Aktivieren Sie die Datenkomprimierung**: Mit der Datenkomprimierung wird die in der Verbindung übertragene Datenmenge reduziert. Für das Komprimieren und Dekomprimieren werden zusätzliche Prozessorressourcen benötigt. Dies kann jedoch die Leistung

bei Verbindungen mit eingeschränkter Bandbreite erhöhen. Verwenden Sie die Citrix-Richtlinieneinstellungen **Audioqualität und Bildkomprimierung**, um dieses Feature zu aktivieren.

- **Reduzieren Sie die Fenstergröße**: Ändern Sie die Fenstergröße auf die kleinste Größe, mit der Sie noch gut arbeiten können. Legen Sie in der Farm die Sitzungsoptionen fest.
- **Reduzieren Sie die Farbanzahl**: Reduzieren Sie die Anzahl der Farben auf 256. Legen Sie auf der Citrix Virtual Apps and Desktops-Site die Sitzungsoptionen fest.
- **Verringern Sie die Audioqualität**: Wenn die Audiozuordnung aktiviert ist, verringern Sie die Audioqualität mit der Citrix Richtlinieneinstellung “Audioqualität” auf die niedrigste Einstellung.

Schriftart

ClearType-Schriftartenglättung

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

FontSmoothingType = Zahl

“Zahl” kann einer der folgenden Werte sein:

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

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

> **Wichtig:**
>
> FontSmoothingType kann vom Server 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 = Zahl

“Zahl” kann einer der folgenden Werte sein:

Wert	Ergebnis
0	Keine Glättung
1	Keine Glättung
2	Standardglättung
3	ClearType-Glättung (horizontale Subpixel-Technologie, Standard)

Ordner

Konfigurieren der Umleitung spezieller Ordner

Jeder Benutzer hat zwei spezielle Ordner:

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

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

Konfigurieren der Umleitung spezieller Ordner:

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

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

   [ClientDrive]

   SFRAllowed = True

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

   DocumentsFolder = Dokumente

DesktopFolder = Desktop

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

DesktopFolder = $HOME/.ICAClient/desktop

- Sie können alle Komponenten in dem Pfad als Umgebungsvariablen angeben, z. B. $HOME.
- Geben Sie für beide Parameter Werte an.
- Die angegebenen Verzeichnisse müssen über die Clientgerätzuordnung verfügbar sein. Das heißt, das Verzeichnis muss sich in der Struktur eines verknüpften Clientgeräts befinden.
- Verwenden Sie die Laufwerksbuchstaben C oder höher.

Clientlaufwerkzuordnung

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf dem Citrix Virtual Apps- oder Citrix Virtual Desktops-Server auf Verzeichnisse, die auf dem lokalen Benutzergerät vorhanden sind. In einer Citrix-Benutzersitzung kann beispielsweise das Laufwerk H einem Verzeichnis auf dem lokalen Computer, auf dem die Workspace-App ausgeführt wird, zugeordnet werden.

Mit der Clientlaufwerkzuordnung werden alle auf dem lokalen Benutzergerät bereitgestellten Verzeichnisse, einschließlich CDs, DVDs oder USB-Sticks, in Sitzungen für den Benutzer verfügbar, wenn der lokale Benutzer Zugriffsrechte hat. Wenn ein Server für die Clientlaufwerkzuordnung konfiguriert ist, können Benutzer auf lokal gespeicherte Dateien zugreifen, diese in ihren Sitzungen bearbeiten und dann entweder auf einem lokalen Laufwerk oder einem Laufwerk auf dem Server speichern.

Die Citrix Workspace-App unterstützt Clientgerätzuordnung für Verbindungen zu Citrix Virtual Apps and Desktops-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 Citrix Virtual Apps and Desktops) auswirken. Wenn Sie eines dieser Features (oder beide) benötigen, deaktivieren Sie SELinux, bevor Sie es auf dem Server konfigurieren.

Es gibt zwei Arten von Laufwerkzuordnung:

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

Wenn eine Verbindung zwischen der Citrix Workspace-App und Citrix Virtual Apps oder Citrix Virtual Desktops hergestellt wird, werden die Clientlaufwerkzuordnungen wiederhergestellt, es sei denn, die Clientgerätzuordnung ist deaktiviert. Sie können mit Richtlinien genauer steuern, wie die Clientgerätzuordnung angewendet wird. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

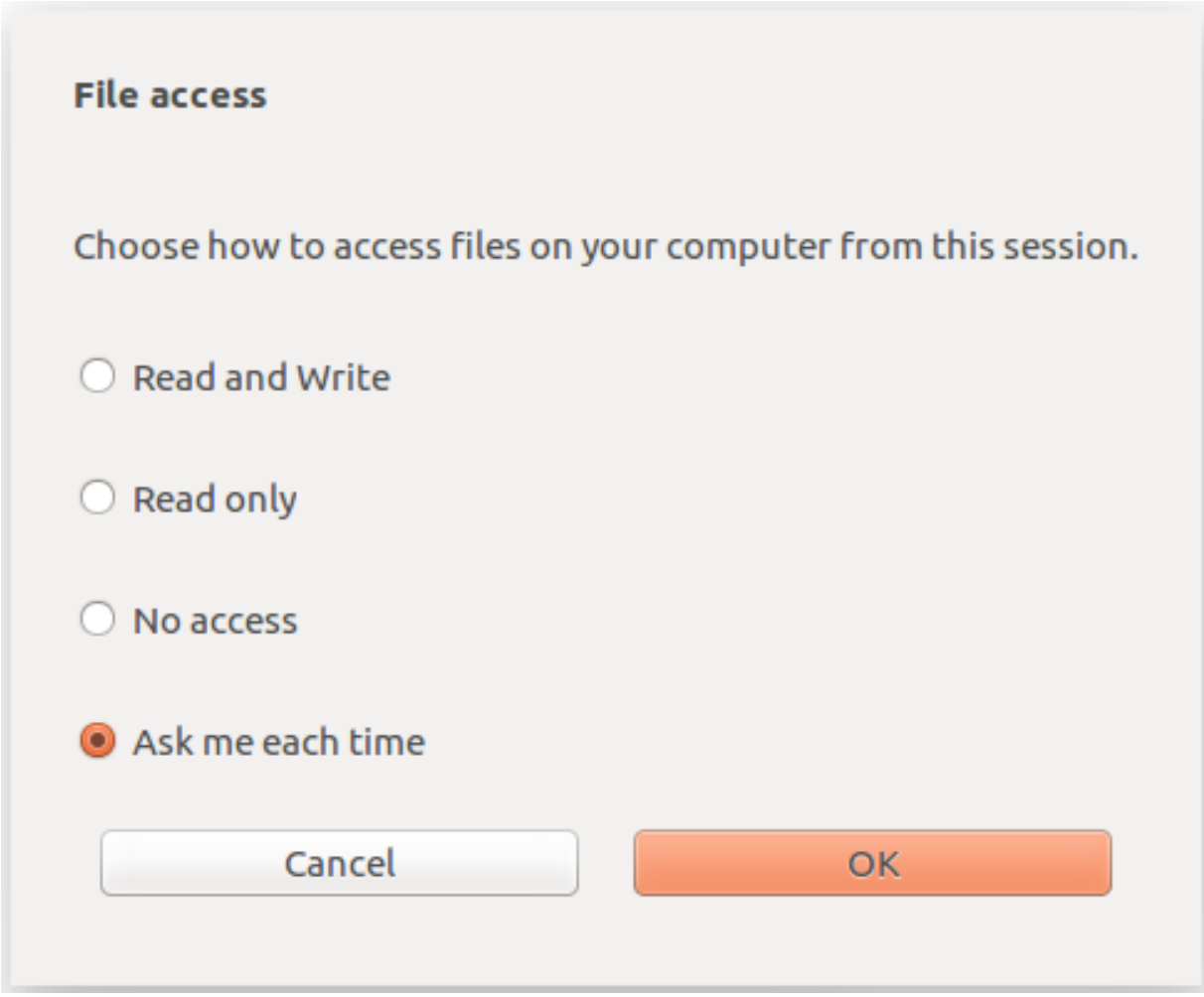
Benutzer können Laufwerke im Dialogfeld Einstellungen zuordnen.

> **Hinweis:**
>
> Standardmäßig wird durch das Aktivieren der statischen Clientlaufwerkszuordnung auch die dynamische Clientlaufwerkszuordnung aktiviert. Um letztere zu deaktivieren und erstere zu aktivieren, setzen Sie `DynamicCDM` in `wfclient.ini` auf `False`.

Bisher wurde Ihre Einstellung für den Dateizugriff über CDM auf alle konfigurierten Stores angewendet.

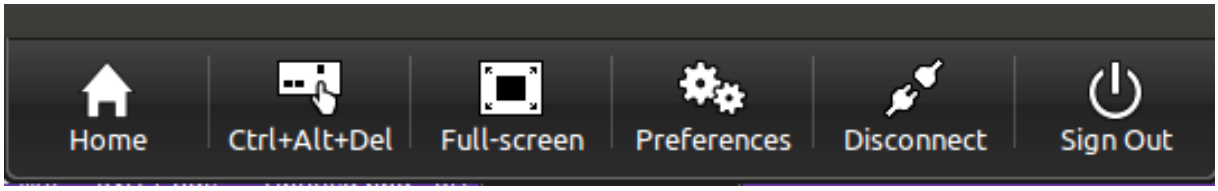
Ab Version 2012 ermöglicht die Citrix Workspace-App die Konfiguration des CDM-Dateizugriffs pro Store.

> **Hinweis:**
>
> Die Einstellung für den Dateizugriff ist nicht in allen Sitzungen persistent, wenn Workspace für Web verwendet wird. Es wird standardmäßig die Option **Jedes Mal fragen** verwendet.

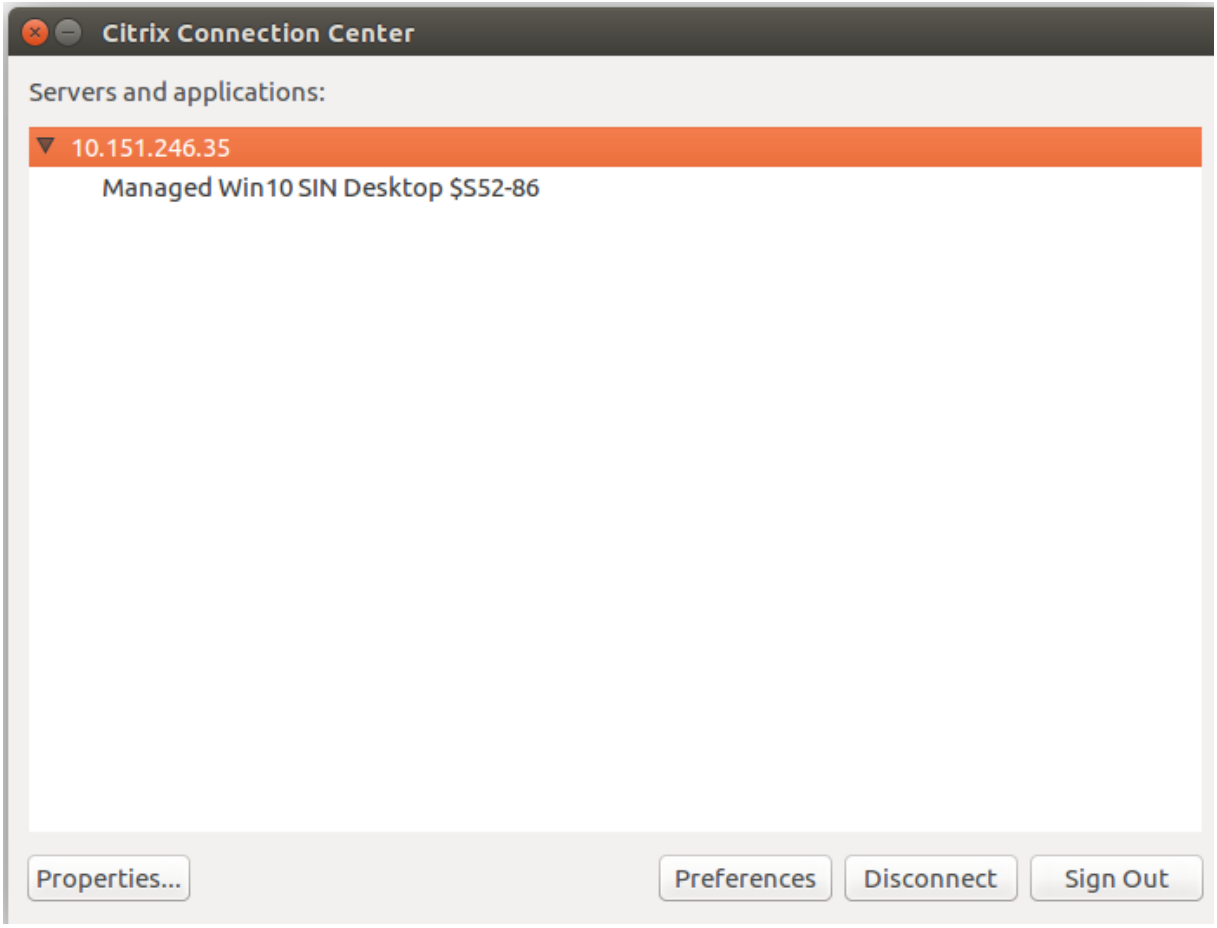


Mit der Datei `wfclient.ini` können Sie den zugeordneten Pfad und die Dateinamenattribute konfigurieren. Verwenden Sie die GUI, um eine Dateizugriffsebene festzulegen, wie im obigen Screenshot angezeigt.

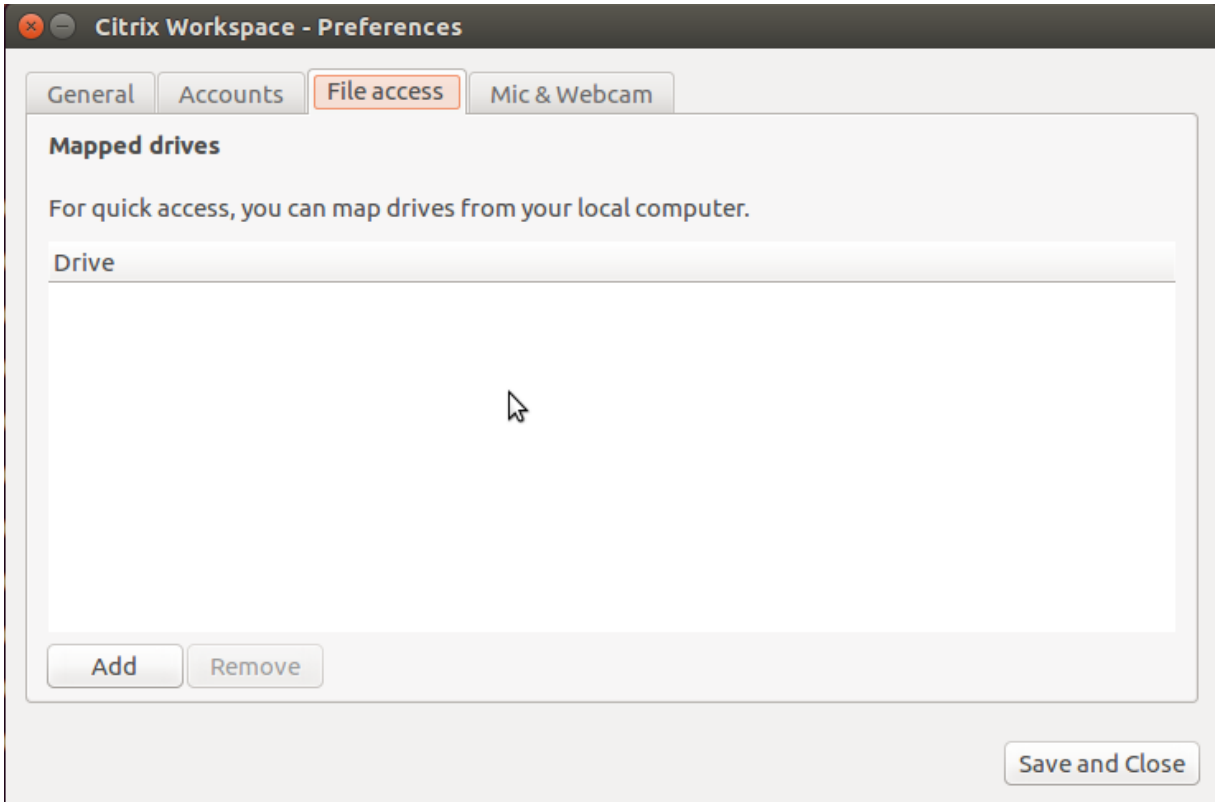
In einer Desktopsitzung können Sie eine Dateizugriffsebene festlegen, indem Sie im Desktop Viewer zum Dialogfeld **Einstellungen** > **Dateizugriff** navigieren.



In einer App-Sitzung können Sie eine Dateizugriffsebene festlegen, indem Sie im **Citrix Connection Center** das Dialogfeld **Dateizugriff** öffnen.



Das Dialogfeld **Dateizugriff** enthält Namen und Pfad des zugeordneten Ordners.



Das Flag für die Zugriffsebene wird in der Datei `wfclient.ini` nicht mehr unterstützt.

Zuordnen von Clientdruckern

Die Citrix Workspace-App unterstützt das Drucken auf Netzwerkdruckern und auf lokal an Benutzergeräte angeschlossenen Druckern. Citrix Virtual Apps ermöglicht Benutzern Folgendes, außer wenn Sie dies durch Richtlinien verhindern:

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

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

Die Sicherheitsrichtlinien des Unternehmens könnten es außerdem erforderlich machen, dass Sie das benutzerseitige Zuordnen lokaler Druckerports nicht zulassen. Hierfür stellen Sie auf dem Server die ICA-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 Workspace-App-Benutzer einzuschränken. In diesem Fall sind "alle Benutzer" diejenigen, die das Self-Service-Programm nach der Änderung zuerst verwenden.

2. Geben Sie im Abschnitt [WFClient] der Datei Folgendes ein:

   ClientPrinterList=Drucker1:Drucker2:Drucker3

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

3. Speichern und schließen Sie die Datei.

Zuordnen von Clientdruckern für UNIX

In UNIX-Umgebungen werden von der Citrix Workspace-App 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 Virtual Apps für UNIX auf einem Clientdrucker drucken können, muss der Systemadministrator diese Funktion aktivieren. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation im Abschnitt über Citrix Virtual Apps für UNIX.

Zuordnen eines lokalen Druckers

Die Citrix Workspace-App für Linux unterstützt den universellen Citrix PS Druckertreiber. Daher ist normalerweise keine lokale Konfiguration erforderlich, damit Benutzer mit Netzwerkdruckern oder Druckern, die an die lokalen Benutzergeräte angeschlossen sind, drucken können. Sie müssen Clientdrucker unter Citrix Virtual Apps 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 der Citrix Workspace-App und melden Sie sich an einem Server an, auf dem Citrix Virtual Apps ausgeführt wird.
2. Wählen Sie im Startmenü **Einstellungen > Drucker**.
3. Wählen Sie im Menü "Datei" die Option **Drucker hinzufügen**.

   Der Druckerinstallationsassistent wird angezeigt.

4. Fügen Sie mit dem Assistenten einen Netzwerkdrucker aus dem Clientnetzwerk und der Clientdomäne hinzu. Hierbei handelt es sich normalerweise um einen Standarddruckernamen, ver-

gleichbar mit denen, die durch native Remotedesktopdienste erstellt werden, z. B. “HPLaserJet 4 von Clientname in Sitzung 3”.

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

Audio

Bisher wurde nur das Standard-Audiogerät in einer Sitzung zugeordnet, selbst wenn viele Geräte auf der Maschine verfügbar waren. Das zugeordnete Gerät war üblicherweise als **Citrix HDX Audio** zu sehen.

Ab Version 2010 zeigt die Citrix Workspace-App für Linux alle lokalen Audiogeräte an, die in einer Sitzung verfügbar sind. Anstelle von **Citrix HDX Audio** werden sie nun mit den entsprechenden Gerätenamen aufgeführt. In einer Sitzung können Sie dynamisch zu jedem der verfügbaren Geräte wechseln. Anders als in früheren Versionen müssen Sie nicht mehr den Standard-Audioeingang oder -ausgang auswählen, bevor Sie die Sitzung starten. Sitzungen werden dynamisch aktualisiert, wenn Sie Audiogeräte anschließen oder entfernen.

Ab Version 2012 ist die erweiterte Audioumleitung standardmäßig aktiviert.

Um das Feature zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zum Ordner `\<ICAROOT\>/config/` und öffnen Sie die Datei module.ini.
2. Gehen Sie zum Abschnitt `clientaudio` und fügen Sie folgenden Eintrag hinzu:

   VdcamVersion4Support=False

> **Hinweis:**
>
> - Wenn die erweiterte Audioverleitung deaktiviert ist, wird nur das Standard-Audiogerät mit dem Namen **Citrix HDX Audio** in der Sitzung angezeigt.
> - Die Option **Mikrofon und Webcam** im Dialogfeld **Einstellungen** bleibt standardmäßig deaktiviert. Informationen zum Aktivieren von Mikrofon und Webcam finden Sie unter Einstellungen.

Bekannte Einschränkungen:

- Auf VDAs mit Windows Server 2016 können Sie die Audiogerätauswahl in einer Sitzung nicht ändern. Die Auswahl ist auf den Standard-Audioeingang und -ausgang beschränkt.
- Die Audiogerätumleitung wird für Bluetooth-Audiogeräte nicht unterstützt.
- Sie können das Standard-Audiogerät nur unter Windows 10, Windows 7 und Windows 8 ändern. Unter Windows-Serverbetriebssystemen wie Windows Server 2012, 2016 und 2019 können Sie das Standardaudiogerät aufgrund einer Einschränkung in der Microsoft-Remotedesktop-Sitzung nicht ändern.

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 Standardeinstellungen.
2. Fügen Sie die folgende Option hinzu. Wenn dieser Abschnitt nicht vorhanden ist, erstellen Sie ihn.

```
[ClientAudio]

AudioDevice = <device>
```

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

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

Zuordnen von Clientaudio

Die Clientaudiozuordnung ermöglicht es, dass auf Citrix Virtual Apps-Servern oder Citrix Virtual Desktops 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 Server-CPU in Anspruch genommen.

Sie können die Clientaudiozuordnung mit Richtlinien konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

> **Hinweis:**
>
> Clientaudiozuordnung steht nicht bei einer Verbindung zu Citrix Virtual Apps für UNIX zur Verfügung.

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.

Einschränkungen:

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

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

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

UDP auf dem Client

Fügen Sie in der Datei `$ICAROOT/config/module.ini` Folgendes hinzu:

Unter dem Abschnitt [ClientAudio]:

EnableUDPAudio=True
UDPAudioPortLow=int
UDPAudioPortHigh=int

Fügen Sie Folgendes in der Datei $HOME/.ICAClient/wfclient.ini hinzu:

Unter dem Abschnitt [WFClient]:

AllowAudioInput=True
EnableAudioInput=true
AudioBandWidthLimit=1

> **Hinweis:**
>
> Wenn der Ordner .ICAClient nicht vorhanden ist (nur beim Starten nach Erstinstallation), starten Sie die Citrix Workspace-App und schließen Sie die App. Dadurch wird der Ordner .ICAClient erstellt.

Fügen Sie Folgendes in wfclient.ini hinzu. Richtlinieneinstellung auf dem DDC:

Legen Sie “Windows Media-Umleitung” auf “Nicht zugelassen” fest
Legen Sie “Audio über UDP” auf “Zugelassen” fest
Legen Sie “Audio über UDP mit Real-Time Transport” auf “Aktiviert” fest
Legen Sie “Audioqualität” auf “Mittel” fest

Ändern der Verwendungsweise der Citrix Workspace-App

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

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

USB

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 entweder Citrix Virtual Apps 7.6 (oder höher) oder Citrix Virtual Desktops. Citrix Virtual Apps unterstützt nicht die USB-Umleitung von Massenspeichergeräten. Für die Unter-

stützung von Audiogeräten ist eine besondere Konfiguration erforderlich. Details hierzu finden Sie unter Citrix Virtual Apps 7.6-Dokumentation.

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

Die folgenden Gerätetypen werden direkt in einer Citrix Virtual Apps and Desktops-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards
- Headsets
- Webcams

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

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops-Sitzung verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs

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

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

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 Workspace-App-Software nicht akzeptiert. Möglicherweise wird ein separater Linux-Dateibrowser geöffnet. Aus diesem Grund empfiehlt Citrix, dass Sie die Benutzergeräte so konfigurieren, dass die Einstellung **Wechselmedien beim Einlegen einbinden** standardmäßig deaktiviert ist. Wählen Sie dazu auf Geräten mit Debian auf der Debian-Menüleiste, Folgendes: **System > Einstellungen > Wechseldatenträger und -medien**. Deaktivieren Sie auf der Registerkarte **Speichermedien** unter **Wechseldatenträger** das Kontrollkästchen **Wechselmedien beim Einlegen einbinden**.

Beachten Sie für die Client-USB-Geräteumleitung Folgendes.

> **Hinweis:**
>
> - Wenn die Serverrichtlinie Client-USB-Geräteumleitung aktiviert ist, werden Massenspeichergeräte wie USB-Geräte umgeleitet, selbst wenn die Clientlaufwerkzuordnung aktiviert ist.
> - Die App unterstützt keine Umleitung von Verbundgeräten für USB-Geräte.

USB-Klassen

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

- Audio (Geräteklasse 01)

  Umfasst Mikrofone, Lautsprecher, Kopfhörer und MIDI-Controller.

- Physikalische Schnittstelle (Geräteklasse 05)

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

- Bilder (Geräteklasse 06)

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

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

- Drucker (Geräteklasse 07)

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

  Drucker funktionieren normalerweise ohne USB-Unterstützung.

- Massenspeicher (Geräteklasse 08)

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

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

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

  Wichtig: Einige Viren werden aktiv mit allen Typen des Massenspeichers übertragen. Überlegen Sie genau, ob die Verwendung von Massenspeichergeräten entweder über die Clientlaufwerkzuordnung oder die USB-Unterstützung im Unternehmen wirklich erforderlich ist. Zur

Verringerung dieses Risikos kann auf dem Server konfiguriert werden, dass Dateien über die Clientlaufwerkzuordnung ausgeführt werden.

- Content Security (Geräteklasse 0d)

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

- Personal Healthcare (Geräteklasse 0f)

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

- Anwendung und herstellerspezifisch (Geräteklasse fe und ff)

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

USB-Geräteklassen

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

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

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

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

- HID (Human Interface Devices) (Geräteklasse 03)

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

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

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

- USB-Hub (Geräteklasse 09)

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

- Chipkarte (Smartcard) (Geräteklasse 0b)

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

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

- Video (Geräteklasse 0e)

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

  Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung.

- Kabelloser Controller (Geräteklasse e0)

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

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

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

Liste der USB-Geräte

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

USB-Richtlinienregeln

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

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

Wenn Sie eine Richtlinienregel erstellen, beachten Sie Folgendes:

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

Beispiel

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

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

DENY: Class=08 SubClass=05 # Massenspeichergeräte

DENY: Class=0D # Alle Sicherheitsgeräte

Startmodi

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

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

Webcams

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

Webcamumleitung

Im Folgenden ein paar Hinweise zur Webcamumleitung:

- Die Webcamumleitung funktioniert mit und ohne RTME.
- Die Webcamumleitung funktioniert für 32-Bit-Anwendungen. Zum Beispiel für Skype und GoToMeeting. Verwenden Sie einen 32-Bit-Browser, um die Webcamumleitung online zu verifizieren. Beispielsweise www.webcamtests.com
- Die Verwendung der Webcam ist pro Anwendung exklusiv. Wenn in Skype beispielsweise eine Webcam ausgeführt wird und Sie GoToMeeting starten, müssen Sie Skype beenden, um die Webcam in GoToMeeting zu verwenden.

Xcapture

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

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

Starten von xcapture von der Befehlszeile:

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

Kopieren von Informationen vom Benutzerdesktop:

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

Maus

Relative Maus

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

> **Hinweis:**
>
> Dieses Feature ist nur in Sitzungen verfügbar, die unter Citrix Virtual Apps oder Citrix Virtual Desktops 7.8 (oder höher) ausgeführt werden. In der Standardeinstellung ist das Steuerelement deaktiviert.

Aktivieren des Features:

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

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

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

Einschalten des Features:

Geben Sie Strg/F12 ein.

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

Deaktivieren des Features:

Geben Sie Strg-Umschalt/F12 ein.

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

Alternative relative Mauswerte

Alternativ gibt es folgende Werte für RelativeMouse:

- RelativeMouse=2 Aktiviert das Feature und schaltet es ein, wenn ein Sitzungsfenster den Fokus erhält.

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

Durch Eingeben folgender Einstellungen können Sie Tastaturbefehle ändern:

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

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

Tastatur

Tastaturverhalten

Generieren der Tastenkombination Strg+Alt+Entfernen remote

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

Generische Umleitung

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

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

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

    ```
    lsusb
    ```

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

ALLOW: vid=1188 pid=9545

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

   ```
   systemctl restart ctxusbd
   ```

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

Selektive Umleitung

Dieses Feature ermöglicht den Einsatz der Bloomberg v4-Tastaturschnittstelle über mehrere Sitzungen hinweg. Damit kann die Tastatur flexibel in allen Remotesitzungen verwendet werden, außer bei Fingerabdruck- und Audioschnittstellen. Fingerabdruck- und Audioschnittstellen werden wie bisher zu einzelnen Sitzungen umgeleitet.

Sie können die Bloomberg-Tastaturumleitung wie folgt durchführen:

- über die generische USB-Umleitung
- über die generische USB-Umleitung bei Unterstützung der selektiven Umleitung

> **Hinweis:**
>
> Dieses Feature ist standardmäßig für x86- und x64-Plattformen aktiviert und für ARMHF-Plattformen deaktiviert.

Aktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei config/All_Regions.ini wie folgt.

   ```
   BloombergRedirection=true
   ```

2. Führen Sie alle unter Generische Umleitung aufgeführten Schritte aus.

Deaktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei config/All_Regions.ini.
2. Setzen Sie den Wert BloombergRedirection auf false.

   ```
   BloombergRedirection=false
   ```

3. Führen Sie alle unter Generische Umleitung aufgeführten Schritte aus.

> **Hinweis:**
>
> Wenn Sie den Wert auf false festlegen, wird die Funktionalität auf das Verhalten in den

> Vorgängerversionen des Clients zurückgesetzt und alle Schnittstellen werden zu einer einzigen Sitzung umgeleitet.

Umleitung des Browserinhalts

Chromium Embedded Framework (CEF) für die Umleitung des Browserinhalts [experimentell]

In Versionen vor Version 1912 wurde bei der Umleitung des Browserinhalts ein WebKitGTK+-basiertes Overlay verwendet, um den Inhalt wiederzugeben. Bei Thin Clients gab es jedoch Leistungsprobleme. Ab Version 1912 wird für die Umleitung des Browserinhalts ein CEF-basiertes Overlay verwendet. Diese Funktionalität bereichert die Benutzererfahrung bei der Umleitung des Browserinhalts. Sie trägt dazu bei, dass Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen werden.

Aktivieren der CEF-basierten Umleitung des Browserinhalts

Aktivieren der CEF-basierten Umleitung des Browserinhalts:

1. Bearbeiten Sie folgende Datei:
   `$ICAROOT/config/All_Regions.ini`
   , wobei $ICAROOT hier für das Standardinstallationsverzeichnis der Citrix Workspace-App steht.
2. Fügen Sie den folgenden Eintrag im Abschnitt [Client Engine\WebPageRedirection] hinzu:

```
UseCefBrowser=true
```

Bekanntes Problem:

- Wenn Sie in `~/.ICAClient/All_Regions.ini` die Option `UseCefBrowser` auf **`true`** festlegen, funktioniert der japanische, chinesische und koreanische IME in Eingabefeldern möglicherweise nicht. Die Citrix Workspace-App für Linux unterstützt den japanischen, chinesischen und koreanischen IME nicht, wenn sichere SaaS mit dem eingebetteten Citrix-Browser verwendet wird.

Informationen zur Umleitung des Browserinhalts finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation unter Umleitung des Browserinhalts.

Automatische Wiederverbindung

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

Benutzer können von ICA-Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit dem

Feature zur automatischen HDX Broadcast-Wiederverbindung von Clients kann die Citrix Workspace-App für Linux unabsichtlich getrennte Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden.

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

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

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

Weitere Informationen zur Konfiguration der automatische HDX Broadcast-Wiederverbindung von Clients finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

Sitzungszuverlässigkeit

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

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

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

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

Citrix Workspace-Benutzer können die Servereinstellungen nicht außer Kraft setzen.

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

Multimedialeistung

Die Citrix Workspace-App 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

> **Hinweis:**
>
> Citrix unterstützt die Koexistenz von RealTime Optimization Pack mit der Citrix Workspace-App für Linux Version 1901 und höher und mit GStreamer 0.1.

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 von Windows Media Player und anderen kompatiblen Playern, 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

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

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

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

Einrichten von HDX MediaStream Windows Media-Umleitung:

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

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

2. Um den clientseitigen Inhaltsabruf zu aktivieren, installieren Sie die erforderlichen GStreamer 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 der Citrix Workspace-App auf dem Gerät die Option “GStreamer”, wenn Sie das Tarball-Skript verwenden. Für DEB- und RPM-Pakete erfolgt die Auswahl automatisch.

Beachten Sie Folgendes beim clientseitigen Inhaltsabruf:

- Standardmäßig ist dieses Feature aktiviert. Sie können es in All-Regions.ini im Abschnitt “Multimedia” mit der Option SpeedScreenMMACSFEnabled deaktivieren. Wenn Sie für diese Option “False” einstellen, wird die Windows Media-Umleitung für die Medienverarbeitung verwendet.

- Standardmäßig verwenden alle MediaStream-Features das GStreamer-Protokoll “playbin2”. Sie können auf ein früheres playbin-Protokoll für alle MediaStream-Features außer dem clientseitigen Inhaltsabruf zurückgehen, der weiter playbin2 verwendet. Stellen Sie dazu in All-Regions.ini im Abschnitt “Multimedia” die Option SpeedScreenMMAEnablePlaybin2 ein.
- Die Citrix Workspace-App erkennt nicht Playlistdateien oder Streamkonfigurationsdateien wie ASX- oder NSC-Dateien. Benutzer müssen eine Standard-URL angeben, die nicht auf diese Dateitypen verweist. Überprüfen Sie mit gst-launch, ob eine URL gültig ist.

Beachten Sie bei GStreamer 1.0:

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

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

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

Aktivieren von GStreamer 1.x

In Releases vor 1912 war GStreamer 0.10 die für die Multimediaumleitung unterstützte Standardversion. Ab Version 1912 können Sie GStreamer 1.x als Standardversion konfigurieren.

Einschränkungen:

- Bei der Videowiedergabe funktioniert die Vorwärts- und Rückwärtssuche möglicherweise nicht wie erwartet.
- Wenn Sie die Citrix Workspace-App auf ARMHF-Geräten starten, funktioniert GStreamer 1.x möglicherweise nicht wie erwartet.

Installieren von GStreamer 1.x

Installieren Sie das GStreamer 1.x-Framework und die folgenden Plug-Ins von https://gstreamer.freedesktop.org/documentation/installing/on-linux.html:

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

Lokales Erstellen von Binärdateien

Bei einigen Linux-Betriebssystemdistributionen, z. B. SUSE und openSUSE, findet das System die GStreamer-Pakete möglicherweise nicht in der Standardquellliste. Laden Sie in diesem Fall den Quellcode herunter und erstellen Sie alle Binärdateien lokal:

1. Laden Sie den Quellcode von https://gstreamer.freedesktop.org/src/ herunter.
2. Extrahieren Sie den Inhalt.
3. Navigieren Sie zu dem Verzeichnis mit dem extrahierten Paket.
4. Führen Sie die folgenden Befehle aus:

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

Standardmäßig sind die generierten Binärdateien unter */usr/local/lib/gstreamer-1.0/*.

Weitere Informationen zur Behandlung von Problemen finden Sie im Knowledge Center-Artikel CTX224988.

Konfigurieren von GStreamer 1.x

Zum Konfigurieren von GStreamer 1.x für die Verwendung mit der Citrix Workspace-App wenden Sie die folgende Konfiguration über die Shell-Eingabeaufforderung an:

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

Hierbei gilt:

- ICACLIENT_DIR ist der Installationspfad der Citrix Workspace-App für Linux.

- GST_PLUGINS_PATH ist der Plug-In-Pfad von GStreamer. Auf einer 64-Bit-Debian-Maschine ist dies beispielsweise */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

Einschränkungen:

- Wenn Sie GStreamer Version 1.15.1 oder höher verwenden, schlägt die Webcamumleitung möglicherweise fehl und die Sitzung wird u. U. getrennt.

HDX MediaStream Flash-Umleitung

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

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt. Weitere Informationen finden Sie unter Systemanforderungen.
2. Fügen Sie in der Datei wfclient.ini im Abschnitt [WFClient] (für alle Verbindungen eines bestimmten Benutzers) oder in der Datei All_Regions.ini im Abschnitt [Client Engine\Application Launching] (für alle Benutzer in Ihrer Umgebung) folgende Parameter hinzu:

   - **HDXFlashUseFlashRemoting=Ask**: **Never**; **Always**

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

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

     Aktiviert oder deaktiviert den serverseitigen Inhaltsabruf für die Citrix Workspace-App. Die Standardeinstellung ist **Disabled**.

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

     Aktiviert oder deaktiviert HTTP-Cookie-Umleitung. Die Standardeinstellung ist **Disabled**.

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

     Aktiviert oder deaktiviert die clientseitige Zwischenspeicherung für von der Citrix Workspace-App abgerufene Inhalte. Die Standardeinstellung ist **Enabled**.

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

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

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

Definiert den Zwischenspeicherungstyp, den die Citrix Workspace-App für mit serverseitigem Inhaltsabruf abgerufene Inhalte verwendet. Die Standardeinstellung ist **Persistent**.

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

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

HDX RealTime-Webcamvideokomprimierung

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

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

Deaktivieren Sie die HDX RealTime-Webcamvideokomprimierung

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

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

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

   HDXWebCamEnabled=Off

   Weitere Informationen finden Sie unter Standardeinstellungen.

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.

Sicheres SaaS mit integriertem Citrix Browser - experimentelles Feature

Der sichere Zugriff auf SaaS-Anwendungen bietet eine einheitliche Benutzererfahrung bei der Bereitstellung veröffentlichter SaaS-Anwendungen. SaaS-Anwendungen sind mit Single Sign-On verfügbar. Administratoren können jetzt Netzwerk und Endbenutzergeräte vor Malware und Datenlecks schützen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.

Die Citrix Workspace-App für Linux unterstützt die Verwendung von SaaS-Anwendungen unter Einsatz des Access Control Service. Über diesen Dienst können Administratoren eine geschlossene Erfahrung mit Single Sign-On und Inhaltsinspektion bereitstellen.

Voraussetzung:

Stellen Sie sicher, dass das Paket `libgtkglext1` verfügbar ist.

Die Bereitstellung von SaaS-Anwendungen über die Cloud hat folgende Vorteile:

- Einfache Konfiguration: einfach zu bedienen, zu aktualisieren und zu nutzen.
- Single Sign-On: mühelose Anmeldung.
- Standardvorlage für verschiedene Anwendungen: vorlagenbasierte Konfiguration beliebter Anwendungen.

> **Hinweis:**
>
> SaaS mit Citrix Browser Engine wird nur auf x64- und x86-Plattformen und nicht auf armhardFloatPort-Hardware (armhf) unterstützt.

Weitere Informationen zum Konfigurieren von SaaS-Anwendungen mit Zugriffssteuerung finden Sie unter Zugriffssteuerung.

Weitere Informationen zu SaaS-Apps mit der Citrix Workspace-App finden Sie unter Workspacekonfiguration in der Dokumentation zur Citrix Workspace-App für Windows.

H.264

Die Citrix Workspace-App unterstützt die H.264-Grafikanzeige einschließlich der von Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops-Richtlinie "Bildqualität". Wenn Sie eine verlustfreie Einstellung wählen, ist die H.264-Codierung auf dem Server deaktiviert und funktioniert für die Citrix Workspace-App 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.

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.

Protokollierung

In früheren Versionen wurden die Dateien `debug.ini` und `module.ini` zum Konfigurieren der Protokollierung verwendet.

Ab Version 2009 können Sie die Protokollierung über eines der folgenden Verfahren konfigurieren:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

Ab Version 2009 wird die Konfigurationsdatei `debug.ini` auch aus dem Installationspaket der Citrix Workspace-App entfernt.

Die Protokollierung erfasst Bereitstellungsdetails, Konfigurationsänderungen und Administratoraktivitäten für die Citrix Workspace-App in einer Protokollierungsdatenbank. Drittanbieterentwickler können diesen Protokollierungsmechanismus über das Protokollierungs-SDK nutzen, das im Platform Optimization SDK der Citrix Workspace-App enthalten ist.

Verwenden Sie die Protokollinformationen für Folgendes:

- Diagnostizieren und Beheben von Problemen, die nach Änderungen auftreten. Das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen.
- Bericht über Administratoraktivitäten.

Bei Installation der Citrix Workspace-App mit Root-Benutzerrechten werden die Protokolle in `/var/log/ICAClient.log` gespeichert. Andernfalls werden die Protokolle in `${ HOME } /.ICAClient/logs/ICAClient.log` gespeichert.

Befehlszeilenoberfläche

1. Navigieren Sie an der Eingabeaufforderung zum Pfad `/opt/Citrix/ICAClient/util`.
2. Führen Sie den folgenden Befehl aus, um die Protokolleinstellungen festzulegen.

   ```
   ./setlog help
   ```

Alle verfügbaren Befehle werden angezeigt.

Die folgende Tabelle listet verschiedene Module und die entsprechenden Traceklassenwerte auf: Verwenden Sie die folgende Tabelle, um einen bestimmten Befehlszeilenprotokollwert festzulegen:

Modul	Protokollklasse
Assertions	LOG_ASSERT
Audio Monitor	TC_CM
BCR with CEF	TC_CEFBCR
Clientaudiozuordnung	TC_CAM
Connection Center	TC_CONNCENTER
Client Communication Port	TC_CCM
Client Drive Mapping	TC_CDM
Clip	TC_CLIP
Clientdruckerzuordnung	TC_CPM
Clientdruckerzuordnung	TC_CPM
Schriftart	TC_FONT
Frame	TC_FRAME
Graphics Abstraction	TC_GA
Eingabemethoden-Editor	TC_IME

Modul	Protokollklasse
IPC	TC_IPC
Tastaturzuordnung	TC_KEY
Lizenzierungstreiber	TC_VDLIC
Multimedia	TC_MMVD
Mauszuordnung	TC_MOU
MS Teams	TC_MTOP
Andere Bibliotheken	TC_LIB
Protokolltreiber	TC_PD
PNA Store	TC_PN
Standardereignisprotokolle	LOG_CLASS
SRCC	TC_SRCC
SSPI Login	TC_CSM
Smartcard	TC_SCARDVD
Selfservice	TC_SS
Selfservice Extension	TC_SSEXT
StorefrontLib	TC_STF
Transport Driver	TC_TD
Thinwire	TC_TW
Transparent Window Interface	TC_TUI
Virtueller Kanal	TC_VD
PAL	TC_VP
Benutzeroberfläche	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
USB Daemon	TC_CTXUSB
Video Frame Driver	TC_VFM
Webkit	TC_WEBKIT
WinStation Driver	TC_WD
WfICA	TC_NCS

Modul	Protokollklasse
Wfica Engine	TC_WENG
Wfica Shell	TC_WFSHELL
Web helper	TC_WH
Zero Latency	TC_ZLC

Grafische Benutzeroberfläche (GUI)

Gehen Sie zu **Menü** > **Einstellungen**. Das Dialogfeld **Citrix Workspace - Einstellungen** wird angezeigt.

Mit zunehmender Detailtiefe sind folgende Werte verfügbar:

- Deaktiviert
- Nur Fehler
- Normal
- Ausführlich

Standardmäßig ist für die **Protokollierung** die Option **Normal** festgelegt.

Da bei der Ablaufverfolgung große Datenmengen generiert werden können, kann sie sich erheblich auf die Leistung der Citrix Workspace-App auswirken. Die Option **Ausführlich** sollte daher nur für die Problembehandlung verwendet werden.

Klicken Sie nach Auswahl der gewünschten Protokollierungsstufe auf **Speichern und Schließen**. Die Änderungen werden in der Sitzung dynamisch angewendet.

Klicken Sie auf das Symbol “Einstellungen” neben dem Dropdownmenü für die **Protokollierung**. Das Dialogfeld **Citrix-Protokolleinstellungen** wird angezeigt.

> **Hinweis:**
>
> Wenn Sie die Datei `ICAClient.log` löschen, müssen Sie den Protokollierungsdienst `ctxlogd` neu starten.
>
> Wenn Sie beispielsweise ein systemd-fähiges Setup verwenden, führen Sie folgenden Befehl aus:

`systemctl restart ctxlogd`.

Aktivieren der Protokollierung für Version 2006 und früher:

Wenn Sie Version 2006 und früher verwenden, aktivieren Sie die Protokollierung wie folgt:

1. Laden Sie die Citrix Workspace-App auf Ihre Linux-Maschine herunter und installieren Sie sie.

2. Legen Sie die Umgebungsvariable `ICAROOT` auf das Installationsverzeichnis fest.

   Beispiel: `/opt/Citrix/ICAClient`.

   Standardmäßig ist die Traceklasse `TC_ALL` aktiviert, um alle Tracingberichte bereitzustellen.

3. Um Protokolle für ein bestimmtes Modul zu sammeln, öffnen Sie die Datei `debug.ini` unter `$ICAROOT` und fügen Sie die erforderlichen
   Ablaufverfolgungsparameter zum Abschnitt [wfica] hinzu.

   Fügen Sie die Traceklassen mit einem "+"-Symbol hinzu. Beispiel: `+TC_LIB`.

   Sie können mehrere Klassen hinzufügen, indem Sie sie durch einen senkrechten Strich trennen. Beispiel: `+TC_LIB|+TC_MMVD`.

Die folgende Tabelle listet verschiedene Module und die entsprechenden Traceklassenwerte auf:

Problembehandlung:

Wenn `ctxlogd` nicht mehr reagiert, werden die Protokolle in syslog erfasst.

Weitere Informationen zum Abrufen neuer und aktualisierter Protokolle bei nachfolgenden Starts finden Sie unter Syslog-Konfiguration.

Syslog-Konfiguration

Standardmäßig werden alle syslog-Protokolle unter /var/log/syslog gespeichert. Sie können Pfad und Namen der Protokolldatei konfigurieren, indem Sie die folgende Zeile im Abschnitt [RULES] in der Datei `/etc/rsyslog.conf` bearbeiten. Zum Beispiel:

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

Speichern Sie Ihre Änderungen und starten Sie den syslog-Dienst mit dem folgenden Befehl neu:

```
sudo service rsyslog restart
```

Wichtige Punkte:

- Um sicherzustellen, dass ein neuer syslog-Dienst verfügbar ist, löschen Sie syslog und führen Sie folgenden Befehl aus: `sudo service rsyslog restart`.
- Um doppelte Benachrichtigungen zu vermeiden, fügen Sie **$RepeatedMsgReduction on** am Anfang der Datei `rsyslog.conf` hinzu.
- Stellen Sie sicher, dass die Zeile **$ModLoad imuxsock.so** am Anfang der Datei `rsyslog.conf` nicht auskommentiert ist.

Remoteprotokollierung

So aktivieren Sie die Remoteprotokollierung:

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

  ```
  $ModLoad imtcp

  $InputTCPServerRun 10514
  ```

- **Clientseitige Konfiguration:** Fügen Sie die folgende Zeile in der Datei rsyslog.conf hinzu, indem Sie localhost durch die IP-Adresse des Remoteservers ersetzen:

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

Optimierung für Microsoft Teams

Citrix bietet eine Optimierung für die Verwendung der Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops und der Citrix Workspace-App. Die Optimierung für Microsoft Teams ähnelt der Komponente HDX RealTime Optimization für Microsoft Skype for Business. Der Unterschied besteht darin, dass wir alle notwendigen Komponenten für die Optimierung von Microsoft Teams im VDA und in der Workspace-App für Linux bündeln.

Die Citrix Workspace-App für Linux unterstützt Audio-, Video- und Bildschirmfreigabefunktionen mit der Optimierung für Microsoft Teams.

> **Hinweis:**
>
> - Die Optimierung für Microsoft Teams wird nur auf der x64-Linux-Distributionen unterstützt.

Weitere Informationen zum Aktivieren der Protokollierung erhalten Sie, wenn Sie die Schritte unter Protokollierung für Microsoft Teams ausführen.

Informationen zu Systemanforderungen finden Sie unter Optimierung für Microsoft Teams.

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams und Microsoft Teams-Umleitung.

Protokollierung für Microsoft Teams

Aktivieren der Protokollierung für Microsoft Teams:

1. Navigieren Sie zur Datei `/opt/Citrix/ICAClient/debug.ini`.
2. Ändern Sie den Abschnitt [HDXTeams] wie folgt:


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

Unterstützung für den virtuellen NSAP-Kanal (NetScaler App Experience)

Der virtuelle NSAP-Kanal (NetScaler App Experience) wurde bisher als experimentelles Feature zur Verfügung gestellt und wird nun vollständig unterstützt. Alle HDX Insight-Daten entstammen dem virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Dieser Ansatz verbessert die Skalierbarkeit und Leistung von Sitzungen. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert. Um das Feature zu deaktivieren, legen Sie das VDNSAP-Flag in der Datei module.ini auf `VDNSAP=Off` fest.

Weitere Informationen finden Sie unter HDX Insight in der Dokumentation zu Linux Virtual Delivery Agent und unter HDX Insight in der Dokumentation zum Citrix Application Delivery Management Service.

Layoutspeicherung im Multimonitormodus

Mit diesem Feature werden die Angaben zum Bildschirmlayout einer Sitzung über Endpunkte hinweg beibehalten. Die Sitzung wird dann gemäß Konfiguration stets auf denselben Monitoren angezeigt.

Voraussetzung:

Dieses Feature erfordert Folgendes:

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

  Löschen Sie die Datei All_Regions.ini.

  oder

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

  SubscriptionUrl =

  PreferredWindowsBounds =

  PreferredMonitors=

PreferredWindowState=

SaveMultiMonitorPref=

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

Anwendungsfälle

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

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

Layout speichern

Aktivieren der Layoutspeicherung:

1. Installieren Sie StoreFront Version 3.15 oder höher (gleich oder höher als v3.15.0.12) auf einem kompatiblen Delivery Controller (DDC).
2. Laden Sie den Build der Citrix Workspace-App 1808 oder höher für Linux von der Seite Downloads herunter und installieren Sie ihn auf der Linux-Maschine.
3. Legen Sie die ICAROOT-Umgebungsvariable auf den Installationsort fest.
4. Überprüfen Sie, ob die Datei **All_Regions.ini** im Ordner **.ICAClient** vorhanden ist. Wenn ja, löschen Sie sie.
5. Suchen Sie in der Datei **$ICAROOT/config/All_Regions.ini** nach dem Feld **SaveMultiMonitorPref**. Der Standardwert in diesem Feld ist “True” (das Feature ist aktiviert). Ändern Sie den Wert

in “False”, um das Feature auszuschalten.
Wenn Sie den Wert für **SaveMultiMonitorPref** ändern, müssen Sie die Datei **All_Regions.ini** im Ordner **.ICAClient** löschen, um Wertkonflikte und eine mögliche Profilsperrung zu verhindern. Aktivieren oder deaktivieren Sie das Flag **SaveMultiMonitorPref**, bevor Sie Sitzungen starten.

6. Starten Sie eine neue Desktopsitzung.
7. Klicken Sie in der Desktop Viewer-Symbolleiste auf **Layout speichern**, um das aktuelle Sitzungslayout zu speichern. Am rechten unteren Bildrand wird die Speicherung in einer Meldung bestätigt.
   Wenn Sie auf “Layout speichern” klicken, wird das Symbol grau angezeigt. Dies zeigt an, dass ein Speichervorgang ausgeführt wird. Nach der Speicherung des Layouts wird das Symbol wieder normal angezeigt.
   Wenn das Symbol für längere Zeit ausgegraut ist, finden Sie im Knowledge Center-Artikel CTX235895 Informationen zur Fehlerbehebung.
8. Trennen Sie die Sitzung oder melden Sie sich ab.
   Starten Sie die Sitzung erneut. Sie wird dann im selben Modus, auf demselben Bildschirm und an derselben Position angezeigt.

Einschränkungen und nicht unterstützte Szenarien:

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

Verwenden von Citrix Virtual Desktops auf zwei Monitoren

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

   Der Bildschirm ist nun auf beide Monitore erweitert.

Workspace Launcher

Citrix führt Workspace Launcher (WebHelper) ein, um veröffentlichte Desktops und Anwendungen zu starten.

Bisher ermöglichte das zusammen mit der Citrix Workspace-App für Linux bereitgestellte Browser-Plug-In, das auf der NPAPI basiert, Benutzern das Starten veröffentlichter Desktops und Anwendungen.

Als Lösung führt Citrix daher den Workspace Launcher (WebHelper) ein. Um dieses Feature zu aktivieren, konfigurieren Sie StoreFront so, dass Anforderungen an den Workspace Launcher gesendet werden, um die installierte Citrix Workspace-App zu erkennen.

Ab Version 1901 funktioniert Citrix Workspace Launcher über direkte Verbindungen zu StoreFront und Citrix Gateway. Mit diesem Feature wird die ICA-Datei automatisch gestartet und die Citrix Workspace-App erkannt.

Als Lösung führt Citrix daher den Workspace Launcher (WebHelper) ein. Um dieses Feature zu aktivieren, konfigurieren Sie StoreFront so, dass Anforderungen an den Workspace Launcher gesendet werden, um die installierte Citrix Workspace-App zu erkennen.

Informationen zum Konfigurieren von StoreFront finden Sie unter **Solution – 2** > **a) Administrator configuration** im Knowledge Center-Artikel CTX237727.

> **Hinweis:**
>
> Citrix Workspace Launcher funktioniert derzeit nur bei einer direkten Verbindung zu StoreFront. Es wird nicht in anderen Situationen, z. B. bei Verbindungen über Citrix Gateway, unterstützt.

Deaktivieren des neuen Workspace-Weboberflächenmodus

Wenn Sie die Citrix Workspace-App für Linux mit der ausführbaren Self-Service-Datei des Thin Client eines Drittanbieters starten, reagiert die Anwendung möglicherweise aufgrund 100%iger CPU-Auslastung nicht mehr.

Sie umgehen das Problem, indem Sie zurück zum alten Benutzeroberflächenmodus wechseln:

1. Entfernen Sie zwischengespeicherte Dateien mit dem folgenden Befehl:
   `rm -r ~/.ICAClient`
2. Navigieren Sie zur Datei `$ICAROOT/config/AuthManconfig.xml`.
3. Ändern Sie den Schlüsselwert `CWACapableEnabled` in “false”.
4. Starten Sie die Citrix Workspace-App für Linux. Die ausführbare Self-Service-Datei lädt die alte Benutzeroberfläche.

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung zwischen Client und VDA ermöglicht es Ihnen, bei der Verwendung eines Windows VDA oder Linux VDA zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist in der Standardeinstellung deaktiviert.

Voraussetzung:

- Aktivieren Sie die Unicode-Tastaturlayoutzuordnung auf dem Windows VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX226335.
- Aktivieren Sie die dynamische Tastaturlayoutsynchronisierung auf dem Linux VDA. Weitere Informationen finden Sie unter Dynamische Tastaturlayoutsynchronisierung
- Die Tastaturlayoutsynchronisierung hängt von der XKB lib ab, die die automatische Synchronisierung des Tastaturlayouts zwischen dem VDA und dem Client ermöglicht.
- Wenn Sie einen Windows Server 2016 oder Windows Server 2019 verwenden, navigieren Sie im Registrierungs-Editor zum folgenden Pfad: `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`. Fügen Sie einen neuen DWORD-Wert mit dem Schlüsselnamen `DisableKeyboardSync` hinzu und legen Sie den Wert auf `0` fest.

Um dieses Feature zu aktivieren, fügen Sie der Datei module.ini die folgenden Zeilen hinzu:

```
[ICA 3.0]

KeyboardSync=On

[KeyboardSync]

DriverName = VDIME.DLL
```

Wenn Sie **KeyboardSync=On** in der Datei module.ini festlegen und **KeyboardLayout=(Benutzerprofil)** in der Datei **wfclient.ini** festlegen, erkennt der virtuelle Treiber vdime das aktive Tastaturlayout auf dem Client und sendet die Informationen an den VDA. Wenn sich das Tastaturlayout in einer Clientsitzung ändert, erkennt der vdime-Treiber dies und sendet das neue Layout sofort an den VDA.

Um diese Funktion zu deaktivieren, legen Sie **KeyboardSync=Off** in der Datei module.ini fest, damit das ursprüngliche Verhalten wiederhergestellt wird. Beim ursprünglichen Verhalten wird das Tastaturlayout aus der Datei **$HOME/.ICAClient/wfclient.ini** gelesen und zusammen mit anderen Clientinformationen beim Start der Sitzung an den VDA gesendet.

Verwendung

Wenn das Feature aktiviert ist, ändert sich das Tastaturlayout auf dem VDA automatisch zusammen mit dem auf dem Clientgerät.

Tastaturlayoutunterstützung für Windows VDA und Linux VDA

> **Hinweis:**
>
> In der folgenden Tabelle ist das Gebietsschema der Linux-Tastatur für alle Referenzen ein Bindestrich.

Linux-Tastaturlayout	Linux-Tastatur / Linux VDA-Layout	Windows-Gebietsschema	Windows-Tastatur-ID	Linux VDA-Layout
ara	-	ar-SA	00000401	ara
ara	azerty	ar-DZ	00020401	ara
at	-	de-AT	00000407	at
be	iso-alternativ	fr-BE	0000080c	be
be	-	nl-BE	00000813	be
bg	-	bg-BG	00030402	bg
bg	phonetic	bg-BG	00040402	bg
bg	bas_phonetic	bg-BG	00020402	bg
br	-	pt-BR	00000416	br
by	-	be-BY	00000423	by
ca	eng	en-CA	00000409	ca
ca	multix	fr-CA	00011009	ca
ca	fr-legacy	fr-CA	00000c0c	ca
ca	-	fr-CA	00001009	ca
ch	fr	fr-CH	0000100c	ch
ch	-	de-CH	00000807	ch
cn	-	en-US	00000409	us
cz	-	cs-CZ	00000405	cz
cz	qwerty	cs-CZ	00010405	cz
de	-	de-DE	00000407	de
de	mac	de-DE	00000407	de
dk	-	da-DK	00000406	dk
ee	-	et-EE	00000425	ee
es	-	es-ES	0000040a	es
es	mac	es-ES	0000040a	es
fi	-	fi-FI	0000040b	fi
fr	-	fr-FR	0000040c	fr
fr	mac	fr-FR	0000040c	fr

Linux-Tastaturlayout	Linux-Tastatur / Linux VDA-Layout	Windows-Gebietsschema	Windows-Tastatur-ID	Linux VDA-Layout
gb	-	en-GB	00000809	gb
gb	mac	en-GB	00000809	gb
gb	extd	en-GB	00000452	gb
gr	-	el-GR	00000408	gr
hr	-	hr-HR	0000041a	hr
hu	-	hu-HU	0000040e	hu
ie	-	en-IE	00001809	ie
il	-	he-IL	0002040d	il
eingehend	eng	en-IN	00004009	eingehend
iq	-	ar-IQ	00000401	iq
is	-	is-IS	0000040f	is
it	-	it-IT	00000410	it
jp	-	en-US	00000409	us
jp	mac	en-US	00000409	us
kr	-	en-US	00000409	us
latam	-	es-MX	0000080a	latam
lt	-	lt-LT	00010427	lt
lt	ibm	lt-LT	00000427	lt
lt	std	lt-LT	00020427	lt
lv	-	lv-LV	00020426	lv
no	-	nb-NO	00000414	no
pl	-	pl-PL	00000415	pl
pl	qwertz	pl-PL	00010415	pl
pt	-	pt-PT	00000816	pt
pt	mac	pt-PT	00000816	pt
ro	std	ro-RO	00010418	ro
rs	-	sr-Cyrl-RS	00000c1a	rs
rs	latin	sr-Latn-RS	0000081a	rs

Linux-Tastaturlayout	Linux-Tastatur / Linux VDA-Layout	Windows-Gebietsschema	Windows-Tastatur-ID	Linux VDA-Layout
ru	-	ru-RU	00000419	ru
ru	typewriter	ru-RU	00010419	ru
ru	mac	ru-RU	00000419	ru
se	-	sv-SE	0000041d	se
se	mac	sv-SE	0000041d	se
si	-	sl-SI	00000424	si
sk	-	sk-SK	0000041b	sk
sk	qwerty	sk-SK	0001041b	sk
th	-	th-TH	0000041e	th
th	pat	th-TH	0001041e	th
tj	-	tg-Cyrl-TJ	00000428	tj
tr	-	tr-TR	0000041f	tr
tr	f	tr-TR	0001041f	tr
tw	-	en-US	00000409	us
ua	-	uk-UA	00000422	ua
us	-	en-US	00000409	us
us	mac	en-US	00000409	us
us	dvorak	en-US	00010409	us
us	dvorak-l	en-US	00030409	us
us	dvorak-r	en-US	00040409	us
us	intl	nl-NL	00020409	us
vn	-	vi-VN	0000042a	vn

VDA-Tastaturlayout

Mit dem VDA-Tastaturlayout-Feature können Sie das Tastaturlayout des VDA unabhängig von den Tastaturlayouteinstellungen des Clients verwenden. Die folgenden Tastaturtypen werden unterstützt: PC/XT 101, 102, 104, 105, 106.

Verwenden des serverseitigen Tastaturlayouts:

1. Starten Sie die Datei wfclient.ini.
2. Ändern Sie den Wert des Attributs `KeyboardLayout` wie folgt:

   `KeyboardLayout=(Server Default)`

   Der Standardwert für das Attribut `KeyboardLayout` ist (Benutzerprofil).
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Dateitypzuordnungen

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

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

Aktivieren von Dateitypzuordnung auf dem Client:

1. Stellen Sie sicher, dass die App, die Sie zuordnen möchten, ein Favorit oder eine abonnierte Anwendung ist.
2. Um die Liste der veröffentlichten Anwendungen und die Server-URL abzurufen, führen Sie die folgenden Befehle aus:

```
./util/storebrowse  -l

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

3. Führen Sie den Befehl ./util/ctx_app_bind mit der folgenden Syntax aus:

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

   Beispiel:
   `./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.bvt.local/citrix/store/discovery`
4. Stellen Sie sicher, dass für die Datei, die Sie öffnen möchten, die Clientlaufwerkzuordnung (CDM) aktiviert ist.

5. Doppelklicken Sie auf die Datei, um sie mit der zugeordneten Anwendung zu öffnen.

Zuordnen einer veröffentlichten Anwendung zu Dateitypen

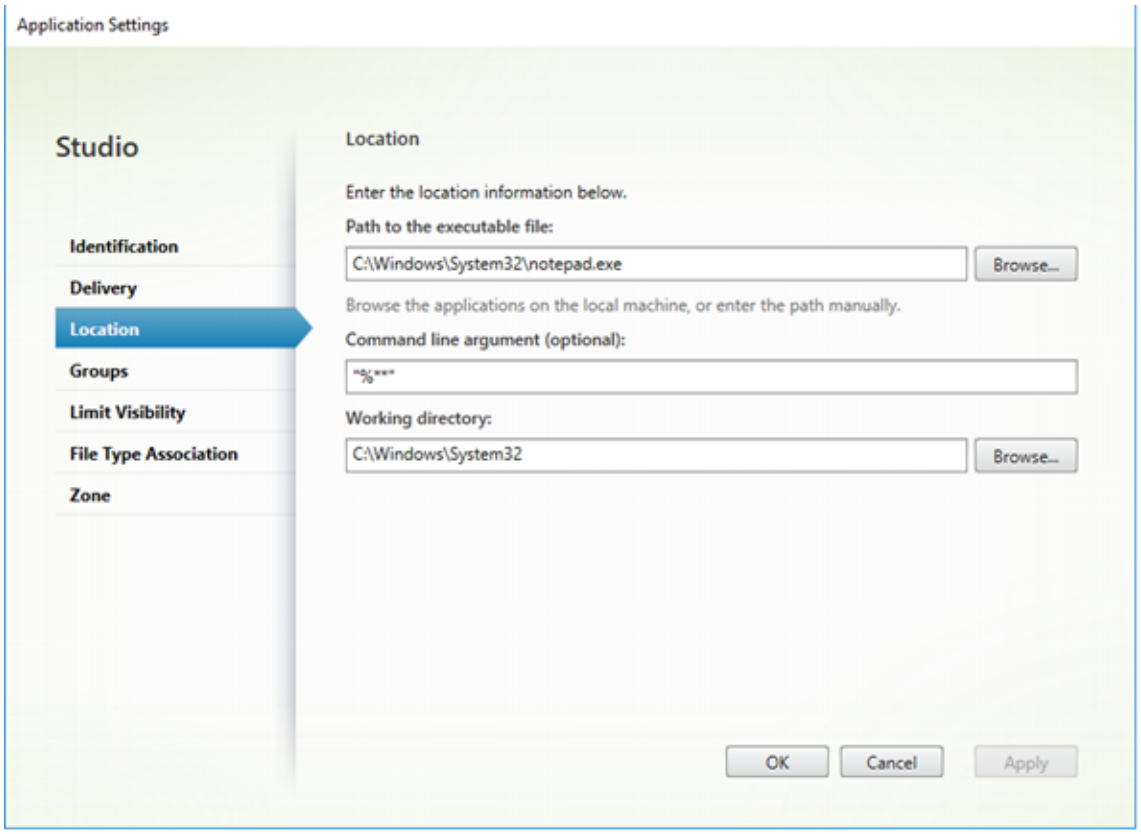
Die Citrix Workspace-App liest die von Administratoren in Citrix Studio konfigurierten Einstellungen und wendet sie an.

Voraussetzung:

Stellen Sie sicher, dass Sie eine Verbindung mit dem Store-Server herstellen, auf dem die Dateitypzuordnung konfiguriert ist.

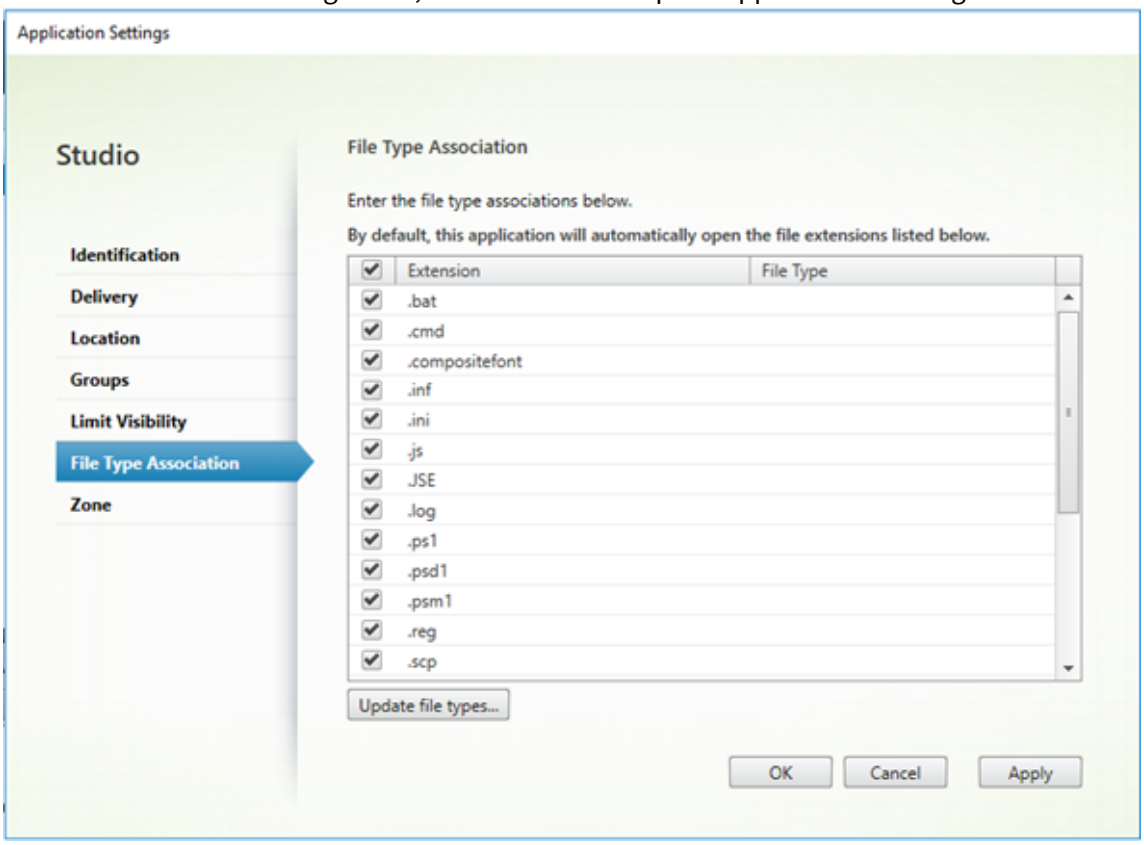
Verknüpfen einer Dateinamenerweiterung mit einer Citrix Workspace-App für Linux:

1. VeröffentlichenSie die Anwendung.
2. Melden Sie sich bei Citrix Studio an.
3. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften**.
4. Wählen Sie **Speicherort**.
5. Fügen Sie “%**” im Feld “Befehlszeilenargument (optional)” hinzu, um die Befehlszeilenprüfung zu umgehen, und klicken Sie dann auf “OK”.



6. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften**.

7. Wählen Sie **Dateitypzuordnung**.
8. Wählen Sie alle Erweiterungen aus, die die Citrix Workspace-App der Anwendung zuordnen soll.



9. Klicken Sie auf **Anwenden** und dann auf **Dateitypen aktualisieren**.
10. Führen Sie die unter Dateitypzuordnungen beschriebenen Schritte aus, um die Dateitypzuordnung auf dem Client zu aktivieren.

> **Hinweis:**
>
> Stellen Sie sicher, dass die StoreFront-Dateitypzuordnung auf “EIN” festgelegt ist. In der Standardeinstellung ist die Dateitypzuordnung aktiviert.

Unterstützung für Citrix Analytics

Die Citrix Workspace-App für Linux ist so instrumentiert, dass Protokolle sicher an Citrix Analytics übertragen werden, wenn bestimmte Ereignisse von der App ausgelöst werden. Die Protokolle werden analysiert und auf Citrix Analytics-Servern gespeichert, wenn diese aktiviert sind. Weitere Informationen zu Citrix Analytics finden Sie unter Citrix Analytics.

Transparente Benutzeroberfläche

Das Citrix ICA-Protokoll verwendet das Protokoll "Transparent User Interface Virtual Channel" [TUI VC], um Daten zwischen Citrix Virtual Apps and Desktops und Hostservern zu übertragen. Das TUI-Protokoll überträgt Komponentenmeldungen der Benutzeroberfläche [Benutzeroberfläche] für Remoteverbindungen.

Die Citrix Workspace-App für Linux unterstützt das TUI VC-Feature. Durch das Feature kann der Client die vom Server gesendeten TUI-Pakete empfangen und auf UI-Komponenten zugreifen. Durch diese Funktion können Sie die Anzeige des überlagernden Standardbildschirms steuern. Sie können das `VDTUI`-Flag in der Datei `module.ini` ein- und ausschalten: `VDTUI - On/Off`

Weitere Informationen zu virtuellen Kanälen finden Sie unter Virtuelle ICA-Kanäle von Citrix in der Dokumentation zu Citrix Virtual Apps and Desktops.

Authentifizierung

March 23, 2021

Im Interesse einer verbesserten Benutzererfahrung werden ab Citrix Workspace-App 2012 das Authentifizierungsdialogfeld in der Citrix Workspace-App und die Storedetails im Anmeldebildschirm angezeigt. Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht erneut eingeben müssen.

> **Hinweis:**
>
> Diese Verbesserung der Authentifizierung ist nur in Cloud-Bereitstellungen verfügbar.

Voraussetzung:

Sie müssen die Bibliothek libsecret installieren.

Diese Funktion ist in der Standardeinstellung deaktiviert.

Aktivieren der Verbesserung:

1. Suchen Sie die Konfigurationsdatei: `$ICAROOT/config/AuthManConfig.xml`.
2. Legen Sie den Wert `AuthManLiteEnabled` auf **`true`** fest.

Smartcard

Um die Smartcard-Unterstützung in der Citrix Workspace-App für Linux zu konfigurieren, müssen Sie den StoreFront-Server über die StoreFront-Konsole konfigurieren.

Die Citrix Workspace-App unterstützt Smartcardleser, die mit PCSC-Lite- und PKCS#11-Treibern kompatibel sind. Standardmäßig sucht die Citrix Workspace-App nach `opensc-pkcs11.so` in einem der Standardspeicherorte.

Die Citrix Workspace-App kann `opensc-pkcs11.so` in einem nicht standardmäßigen Speicherort suchen oder sie kann einen anderen `PKCS\##11`-Treiber suchen. Sie können den jeweiligen Speicherort mit den folgenden Schritten speichern:

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

> **Hinweis:**
>
> Wenn Sie einen Dateinamen für den Treiberspeicherort eingeben, navigiert die Citrix Workspace-App im Verzeichnis `$ICAROOT/PKCS\ ##11` zu der Datei. Sie können auch einen absoluten Pfad verwenden, der mit "/" beginnt.

Nach dem Entfernen einer Smartcard konfigurieren Sie das Verhalten der Citrix Workspace-App, indem Sie `SmartCardRemovalAction` in der Konfigurationsdatei mit den folgenden Schritten aktualisieren:

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

Das Standardverhalten ist `noaction`. Es werden keine Maßnahmen ausgeführt, um gespeicherte Anmeldeinformationen und generierte Token beim Entfernen der Smartcard zu löschen.

Mit der Aktion `forcelogoff` werden alle Anmeldeinformationen und Token in StoreFront beim Entfernen der Smartcard entfernt.

Aktivieren der Smartcardunterstützung

Die Citrix Workspace-App unterstützt verschiedene Smartcardleser, wenn die Verwendung von Smartcards sowohl auf dem Server als auch auf der Citrix Workspace-App aktiviert ist.

Sie können Smartcards zu folgenden Zwecken verwenden:

- Smartcard-Anmeldeauthentifizierung: Authentifiziert Sie bei Citrix Virtual Apps-Servern.
- Smartcard-Anwendungsunterstützung: Ermöglicht smartcardfähigen veröffentlichten Anwendungen den Zugriff auf lokale Smartcardgeräte.

Die sicherheitsrelevanten Smartcarddaten müssen über einen sicheren, authentifizierten Kanal, z. B. TLS, übertragen werden.

Für die Smartcardunterstützung müssen folgende Voraussetzungen erfüllt sein:

- Die Smartcardleser und die veröffentlichten Anwendungen müssen dem PC/SC-Industriestandard entsprechen.
- Installieren Sie den passenden Treiber für die Smartcard.
- Installieren Sie das PCSC Lite-Paket.
- Installieren Sie den `pcscd`-Daemon, der Middleware für den Zugriff auf die Smartcard mit PC/SC bereitstellt, und führen Sie ihn aus.
- Auf einem 64-Bit-System muss die 64-Bit- und 32-Bit-Version des “libpscslite1”-Pakets vorhanden sein.

> **Wichtig:**
>
> Wenn Sie das Sun Ray-Terminal mit Sun Ray-Serversoftware (Version 2.0 oder höher) verwenden, installieren Sie zunächst das PC/SC SRCOM-Bypass-Paket, das unter http://www.sun.com/ zur Verfügung steht.

Weitere Informationen zur Konfiguration der Smartcardunterstützung auf Servern finden Sie unter Smartcards in der Dokumentation für Citrix Virtual Apps and Desktops.

Unterstützung für mehrstufige Authentifizierung (nFactor)

Die mehrstufige Authentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Mit der mehrstufigen Authentifizierung können Authentifizierungsschritte und die zugehörigen Anmeldeinformationsformulare vollständig vom Administrator konfiguriert werden.

Die native Citrix Workspace-App unterstützt dieses Protokoll über die Anmeldeformulare, die bereits für StoreFront implementiert sind. Die webbasierten Anmeldeseiten für virtuelle Citrix Gateway- und Traffic Manager-Server verwenden ebenfalls dieses Protokoll.

Weitere Informationen finden Sie in der Dokumentation zu Citrix ADC unter SAML-Authentifizierung und Mehrstufige Authentifizierung (nFactor).

Sicherheit

April 16, 2021

Zum Sichern der Kommunikation zwischen Ihrer Site und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen mit Sicherheitstechnologien wie Citrix Gateway integrieren.

> **Hinweis:**

> Citrix empfiehlt die Verwendung von Citrix Gateway zwischen StoreFront-Servern und Benutzergeräten.

- Eine Firewall: Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie die Citrix Workspace-App 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.
- Vertrauenswürdige Server.
- Nur für Citrix Virtual Apps-Bereitstellungen (gilt nicht für XenDesktop 7): Ein SOCKS-Proxyserver oder ein sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver oder TLS-Tunneling-Proxyserver). Mit Proxyservern schränken Sie den eingehenden und ausgehenden Zugriff auf das Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.
- Nur für Citrix Virtual Apps-Bereitstellungen: Citrix Secure Web Gateway- oder SSL-Relay-Lösungen mit TLS-Protokollen (Transport Layer Security). Die TLS-Versionen 1.0 bis 1.2 werden unterstützt.

Citrix Gateway

Citrix 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 Citrix Gateway:

1. Geben Sie die vom Administrator erhaltene Citrix 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 die Citrix Workspace-App findet, verwenden Sie eine URL im Format wie beispielsweise https://gateway.company.com.
   - Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im Format wie beispielsweise https://gateway.company.com? <storename>. Diese dynamische URL besitzt kein standardmäßiges Format, verwenden Sie kein = (Gleichheitsze-

ichen) 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 Citrix Gateway-Dokumentation.

   Wenn die Authentifizierung abgeschlossen ist, werden Ihre Desktops und Anwendungen angezeigt.

Proxyserver

Proxyserver werden zur Beschränkung des Netzwerkzugriffs und für Verbindungen zwischen der Citrix Workspace-App und Citrix Virtual Apps and Desktops-Bereitstellungen verwendet. Die Citrix Workspace-App unterstützt das SOCKS-Protokoll zusammen mit Citrix Secure Web Gateway und Citrix SSL-Relay, das Secure Proxy-Protokoll und Windows NT Challenge/Response (NTLM)-Authentifizierung.

Die unterstützten Proxytypen sind durch die Inhalte von Trusted_Regions.ini und Untrusted_Regions.ini auf die Typen “Auto”, “None” und “Wpad” beschränkt. Wenn Sie die Typen “SOCKS”, “Secure” oder “Script” verwenden, bearbeiten Sie die genannten Dateien und fügen Sie die zusätzlichen Typen der Liste der zulässigen Typen hinzu.

> **Hinweis:**
>
> Aktivieren Sie zur Gewährleistung einer sicheren Verbindung TLS.

Sicherer Proxyserver

Durch das Konfigurieren des Secure Proxy-Protokolls wird gleichzeitig auch Unterstützung für Windows NT Challenge/Response (NTLM)-Authentifizierung aktiviert. Wenn dieses Protokoll zur Verfügung steht, wird es beim Start erkannt und ohne zusätzliche Konfiguration ausgeführt.

> **Wichtig:**
>
> NTLM-Unterstützung erfordert die Bibliotheken OpenSSL 1.1.1d und libcrypto.so. Installieren Sie die Bibliotheken auf dem Benutzergerät. Diese Bibliotheken sind oft in Linux-Distributionen enthalten. Sie können sie auch von http://www.openssl.org/ herunterladen.

Secure Web Gateway und SSL

Sie können die Citrix Workspace-App in eine Umgebung mit Citrix Secure Web Gateway oder dem SSL (Secure Sockets Layer)-Relay integrieren. Die Citrix Workspace-App 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.

Secure Web Gateway

Sie können Citrix Secure Web Gateway im Normal- oder Relaymodus verwenden, um einen sicheren Kommunikationskanal zwischen der Citrix Workspace-App und dem Server bereitzustellen. Die Citrix Workspace-App muss nicht konfiguriert werden, wenn Sie Citrix Secure Web Gateway im Normalmodus verwenden.

Wenn Citrix Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Citrix Secure Web Gateway Proxy im Relaymodus verwenden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps (Citrix Secure Web Gateway).

Wenn Sie den Relaymodus verwenden, fungiert der Citrix Secure Web Gateway-Server als Proxy und Sie müssen die Citrix Workspace-App für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Citrix Secure Web Gateway-Servers.
- Portnummer des Citrix Secure Web Gateway-Servers. Der Relaymodus wird von Citrix Secure Web Gateway, Version 2.0 nicht unterstützt.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

Beispiel: my_computer.my_company.com ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (my_computer), einen Second-Level-Domänennamen (my_company) und einen Top-Level-Domänennamen (com) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (my_company.com) wird als Domänenname bezeichnet.

SSL-Relay

Das Citrix SSL-Relay verwendet standardmäßig den TCP-Port 443 auf dem Citrix Virtual Apps-Server für TLS-gesicherte Kommunikation. Wenn das SSL-Relay eine TLS-Verbindung empfängt, werden die Daten entschlüsselt und dann an den Server übergeben.

Wenn Sie SSL-Relay so konfigurieren, dass ein anderer Port als 443 abgehört wird, müssen Sie die Citrix Workspace-App für diese geänderte Portnummer konfigurieren.

Mit dem Citrix SSL-Relay kann folgende Kommunikation gesichert werden:

- Zwischen einem TLS-fähigen Benutzergerät und einem Server

Weitere Informationen zum Konfigurieren und Sichern der Installation mit SSL-Relay finden Sie in der Citrix Virtual Apps-Dokumentation.

TLS

Die Versionen des TLS-Protokolls, die ausgehandelt werden können, können Sie steuern, indem Sie die folgenden Konfigurationsoptionen im Abschnitt [WFClient] hinzufügen:

- MinimumTLS=1.2
- MaximumTLS=1.2

Diese Werte sind die Standardwerte, die als Code implementiert werden. Passen Sie sie nach Bedarf an.

> **Hinweis:**
>
> - Diese Werte werden bei jedem Programmstart gelesen. Wenn Sie sie nach dem Start von self-service oder storebrowse ändern, geben Sie Folgendes ein: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
> - Die Verwendung des SSLv3-Protokolls ist in der Citrix Workspace-App für Linux nicht zulässig.

Zum Auswählen der Verschlüsselungssammlung fügen Sie die folgende Konfigurationsoption im Abschnitt [WFClient] hinzu:

- SSLCiphers=GOV

Dieser Wert ist der Standardwert. Die Werte COM und ALL werden ebenfalls erkannt.

> **Hinweis:**
>
> Wenn Sie dies nach dem Start von self-service oder storebrowse ändern, müssen Sie wie bei der Konfiguration der TLS-Version Folgendes eingeben:
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

Kryptographische Aktualisierung

Mit diesem Feature ändert sich das Protokoll zur sicheren Kommunikation grundlegend. Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten kein Forward Secrecy und werden als unsicher eingestuft.

Die TLS_RSA_-Verschlüsselungssammlungen wurden vollständig entfernt. Stattdessen werden die erweiterten TLS_ECDHE_RSA_-Verschlüsselungssammlungen unterstützt. Wenn Ihre Umgebung nicht mit den TLS_ECDHE_RSA_-Verschlüsselungssammlungen konfiguriert ist, werden die Starts von Clients aufgrund schwacher Verschlüsselung nicht unterstützt. Für die Clientauthentifizierung werden 1536-Bit-RSA-Schlüssel unterstützt.

Die folgenden erweiterten Verschlüsselungssammlungen werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

DTLS v1.0 unterstützt die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS v1.2 unterstützt die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

> **Hinweis:**
>
> Ab Version 1903 und höher wird DTLS von Citrix Gateway 12.1 und höher unterstützt. Informationen zu mit DTLS unterstützten Verschlüsselungssammlungen für Citrix Gateway finden Sie unterUnterstützung des DTLS-Protokolls.

Verschlüsselungssammlungen

Um verschiedene Verschlüsselungssammlungen zu aktivieren, ändern Sie den Wert für den Parameter `SSLCiphers` in `ALL`, `COM` oder `GOV`. Standardmäßig ist die Option in der Datei `All_Regions.ini` im Verzeichnis `$ICAROOT/config` auf `ALL` festgelegt.

Die folgenden Sätze von Verschlüsselungssammlungen werden von ALL, GOV und COM bereitgestellt:

- ALL
  - Alle 3 Verschlüsselungssammlungen werden unterstützt.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Informationen zur Problembehandlung finden Sie unter Verschlüsselungssammlungen.

Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten Forward Secrecy nicht. Diese Verschlüsselungssammlungen werden von der Branche mittlerweile allgemein als veraltet eingestuft. Um die Abwärtskompatibilität mit älteren Versionen von Citrix Virtual Apps and Desktops zu unterstützen, kann die Citrix Workspace-App für Linux diese Verschlüsselungssammlungen aktivieren.

Setzen Sie das Flag `Enable\\_TLS\\_RSA\\_` auf `False`, um die Sicherheit weiter zu erhöhen.

Im Folgenden finden Sie eine Liste der veralteten Verschlüsselungssammlungen:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Hinweis:**
>
> Die beiden letzten Verschlüsselungssammlungen verwenden den RC4-Algorithmus und sind veraltet, weil sie unsicher sind. Sie könnten auch die Verschlüsselungssammlung TLS_RSA_3DES_CBC_EDE_SHA als veraltet betrachten. Mit Flags können Sie alle Kategorisierungen durchsetzen.

Weitere Informationen zum Konfigurieren von DTLS v1.2 finden Sie unter Adaptiver Transport in der Dokumentation zu Citrix Virtual Apps and Desktops.

Voraussetzung:

Wenn Sie Version 1901 oder früher verwenden, führen Sie die folgenden Schritte aus:

Wenn .ICAClient bereits im Home-Verzeichnis des aktuellen Benutzers vorhanden ist:

- Löschen Sie die Datei `All\\_Regions.ini`

oder

- Fügen Sie folgende Zeilen am Ende des Abschnitts [Network\SSL] hinzu, um die Datei `AllRegions.ini` beizubehalten:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

Wenn der Ordner .ICAClient nicht im Basisordner des aktuellen Benutzers vorhanden ist, weist dies auf eine Neuinstallation der Citrix Workspace-App hin. In diesem Fall wird die Standardeinstellung für die Features beibehalten.

Die folgende Tabelle enthält die Verschlüsselungssammlungen jeder Gruppe:
Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

> **Hinweis:**
>
> Alle oben genannten Verschlüsselungssammlungen sind FIPS- und SP800-52-konform. Die ersten beiden Sammlungen sind nur für (D)TLS1.2-Verbindungen zulässig. Umfassende Informationen zur Unterstützung von Verschlüsselungssammlungen finden Sie in **Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen**.

Storebrowse

July 6, 2020

Storebrowse ist ein einfaches Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Mit Storebrowse können Administratoren folgende Routinevorgänge automatisieren:

- Hinzufügen von Stores
- Auflisten der veröffentlichten Apps und Desktops eines konfigurierten Stores
- Abonnieren der Apps und Desktops eines konfigurierten Stores und Stornieren der Abos
- Aktivieren und Deaktivieren von Verknüpfungen für veröffentlichte Apps und Desktops
- Starten von veröffentlichten Anwendungen
- Wiederherstellen der Verbindung zu getrennten Sitzungen

Im Allgemeinen ist das Storebrowse-Hilfsprogramm im Ordner `/util` verfügbar. Dieser ist im Installationsverzeichnis. Beispiel: `/opt/Citrix/ICAClient/util`.

Voraussetzungen

Für das Storebrowse-Hilfsprogramm ist das Bibliothekspaket **libxml2** erforderlich.

Starten von veröffentlichten Desktops und Anwendungen

Es gibt zwei Möglichkeiten, eine Ressource zu starten:

- Sie können die Befehlszeilen- und Storebrowse-Befehle verwenden
- Sie können die Benutzeroberfläche verwenden, um eine Ressource zu starten.

Dieser Artikel beschreibt die Storebrowse-Befehle.

Verwendung von Befehlen

Im folgenden Abschnitt werden die Storebrowse-Befehle beschrieben, die Sie im Storebrowse-Hilfsprogramm verwenden können.

-a, –addstore

Beschreibung:

Fügt einen neuen Store mit Gateway- und Beacondetails zusammen mit dem ServiceRecord-Daemonprozess hinzu. Dieser Befehl gibt die vollständige URL des Stores zurück. Wenn das Hinzufügen eines Stores fehlschlägt, wird ein Fehler angezeigt.

Befehlsbeispiel in StoreFront:

Befehl:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Beispiel:

```
./storebrowse -a https://my.firstexamplestore.net
```

> **Hinweis:**
>
> Sie können mit dem Storebrowse-Hilfsprogramm mehrere Stores hinzufügen.

-?, -h, –help

Beschreibung:

Bietet Details zur Verwendung des Storebrowse-Hilfsprogramms.

-l –liststore

Beschreibung:

Listet die Stores auf, die Sie hinzugefügt haben.

Befehlsbeispiel in StoreFront:

```
./storebrowse -l
```

-E –enumerate

Beschreibung:

Listet die verfügbaren Ressourcen auf. Standardmäßig werden die folgenden Werte angezeigt:

- Ressourcenname
- Anzeigename
- Ordner der Ressource

Wenn Sie weitere Informationen anzeigen möchten, fügen Sie den Befehl **-M** (–details) an den Befehl **-E** an.

> **Hinweis:**
>
> Wenn Sie den Befehl **-E** ausführen, wird ein Authentifizierungsfenster angezeigt, wenn Sie Ihre Anmeldeinformationen nicht zuvor angegeben haben.

Geben Sie die gesamte Store-URL ein, die Sie mit dem Befehl **-liststore** erhalten.

Befehlsbeispiel in StoreFront:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-S –subscribed

Beschreibung:

Listet die abonnierten Ressourcen auf. Standardmäßig werden die folgenden Werte angezeigt:

- Ressourcenname
- Anzeigename
- Ordner der Ressource

Wenn Sie weitere Informationen anzeigen möchten, fügen Sie den Befehl **-M** (–details) an den Befehl **-E** an.

Befehlsbeispiel in StoreFront:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

-M –details

Beschreibung:

Dieser Befehl gibt mehrere Attribute der veröffentlichten Anwendungen zurück. Im Allgemeinen wird dieser Befehl mit den Befehlen **-E** und **-S** verwendet. Dieser Befehl umfasst ein Argument, das die Summe der Zahlen ist, die den erforderlichen Details entsprechen:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

> **Hinweise:**
>
> - Zum Erstellen von Menüeinträgen für abonnierte Anwendungen verwenden Sie das Argument CreateShortcuts(0x100000) mit den Befehlen **-S**, **-s** und **-u**.
> - Um alle Menüeinträge zu löschen, verwenden Sie RemoveShortcuts(0x200000) mit dem Befehl **-S**.

Befehlsbeispiel in StoreFront:

`./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery`

wobei 0x264 die Kombination von DisplayName(0x200), AppIsDisabled(0x40), AppIsDesktop(0x20) und SoundType(0x4) ist. Es wird eine Liste der abonnierten Ressourcen zusammen mit den Details ausgegeben.

Sie können den Befehl **-M** verwenden, um die Ressourcen mit den erforderlichen Details aufzulisten:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/
discovery
```

> **Hinweise:**
>
> - Sie können die Werte entweder im Dezimalformat oder im Hexadezimalformat darstellen. Beispiel: 512 für 0x200.
> - Wenn einige der Details nicht über Storebrowse verfügbar sind, ist der Ausgabewert Null.

-s –subscribe

Beschreibung:

Abonniert die angegebene Ressource aus dem jeweiligen Store.

Befehlsbeispiel in StoreFront:

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

-u –unsubscribe

Beschreibung:

Kündigt das Abonnement der angegebenen Ressource aus dem jeweiligen Store.

Befehlsbeispiel in StoreFront:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

-L –launch

Beschreibung:

Startet eine Verbindung zu einer veröffentlichten Ressource. Das Hilfsprogramm wird dann automatisch beendet, während die erfolgreich verbundene Sitzung bestehen bleibt.

Befehlsbeispiel in StoreFront:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```


-i –icons

Beschreibung:

Mit diesem Befehl werden Desktop- und Anwendungssymbole im PNG-Format abgerufen. Dieser Befehl wird mit dem Befehl **-E** oder **-S** verwendet.

Verwenden Sie zum Abrufen von Symbolen mit bestimmten Größen und Tiefen das Argument “best” oder das Größenargument.

Argument “best”

Mit dem Argument “best” können Sie die auf dem Server verfügbaren Symbole mit der besten Größe abrufen. Sie können die Symbole später in die erforderlichen Größen konvertieren. Das Argument “best” ist nach Speicher- und Bandbreitengesichtspunkten die effizienteste Methode und vereinfacht die Skripterstellung. Die Dateien werden im Format <Ressourcenname>.png gespeichert.

Größenargument

Verwenden Sie zum Abrufen von Symbolen mit bestimmten Größen und Tiefen das Größenargument. Wenn der Server Symbole einer bestimmten Größe oder Tiefe nicht abrufen kann, wird ein Fehler angezeigt.

Das Größenargument wird als WxB angegeben, wobei Folgendes gilt:

- **W** ist die Breite (width) der Symbole. Alle Symbole sind quadratisch, daher wird nur ein Wert benötigt, um die Größe anzugeben.
- **B** ist die Farbtiefe. Sie wird als Anzahl der Bits pro Pixel angegeben.

> **Hinweis:**
>
> Der Wert **W** ist obligatorisch. Der Wert **B** ist optional.

Wenn Sie die Werte nicht angeben, werden Symbole aller verfügbaren Bildtiefen angezeigt. Die Dateien werden im Format <Ressourcenname>_WxWxB.png gespeichert.

Bei beiden Methoden werden die Symbole für jede Ressource, die mit dem Befehl **-E** oder **-S** zurückgegeben werden, im **PNG-Format** gespeichert.

Symbole werden im Ordner **.icaClient/cache/icons** gespeichert.

Befehlsbeispiel in StoreFront:

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

-W [r|R] –reconnect [r|R]

Beschreibung:

Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [r] werden alle getrennten Sitzungen wieder verbunden. Mit der Option [r] werden alle aktiven getrennten Sitzungen wieder verbunden.

Befehlsbeispiel in StoreFront:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`

- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

-WD –disconnect

Beschreibung:

Trennt alle Sitzungen des angegebenen Stores.

Befehlsbeispiel in StoreFront:

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

-WT –logoff

Beschreibung:

Beendet alle Sitzungen des angegebenen Stores.

Befehlsbeispiel in StoreFront:

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

-v –version

Beschreibung:

Zeigt die Version des Storebrowse-Hilfsprogramms an.

Befehlsbeispiel in StoreFront:

```
./storebrowse -v
```


-r –icaroot

Beschreibung:

Gibt das Stammverzeichnis an, in dem die Citrix Workspace-App für Linux installiert ist. Wenn Sie nichts angegeben, wird das Stammverzeichnis zur Laufzeit ermittelt.

Befehlsbeispiel in StoreFront:

```
./storebrowse -r /opt/Citrix/ICAClient
```

-U –username, -P –password, -D domain

Beschreibung:

Übergibt den Benutzernamen, das Kennwort und die Domänendetails an den Server. Diese Methode funktioniert nur mit einem PNA-Store. StoreFront-Stores ignorieren diesen Befehl. Die Details werden nicht zwischengespeichert. Sie müssen die Details bei jedem Befehl eingeben.

Befehlsbeispiel in StoreFront:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
user1 -P password -D domain-name
```

-d –deletestore

Beschreibung:

Hebt die Registrierung eines Stores beim ServiceRecord-Daemon auf.

Befehlsbeispiel in StoreFront:

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

-c –configselfservice

Beschreibung:

Dient zum Aufrufen und Konfigurieren der in StoreCache.ctx gespeicherten Einstellungen der Self-Service-Benutzeroberfläche. Das zugehörige Argument hat das Format <Eintrag[=Wert]>. Wenn nur ein Eintrag vorhanden ist, wird der aktuelle Wert der Einstellung aufgerufen. Wenn jedoch ein Wert vorhanden ist, wird der Wert verwendet, um die Einstellung zu konfigurieren.

Befehlsbeispiel in StoreFront:

```
./storebrowse -c SharedUserMode=True
```


-C –addCR

Beschreibung:

Liest die bereitgestellte Citrix Receiver-Datei (CR) und fordert Sie zum Hinzufügen jedes Stores auf. Die Ausgabe ist wie beim Befehl **-a**, enthält aber mehrere Stores auf jeweils neuen Zeilen.

Befehlsbeispiel in StoreFront:

```
./storebrowse -C <path to CR file>
```

-K –killdaemon

Beschreibung:

Beendet den Storebrowse-Daemon. Alle Anmeldeinformationen und Tokens werden gelöscht.

Befehlsbeispiel in StoreFront:

```
./storebrowse -K
```

-e –listerrorcodes

Beschreibung:

Listet die registrierten Fehlercodes auf.

Befehlsbeispiel in StoreFront:

```
./storebrowse -e
```

-g –storegateway

Beschreibung:

Legt das Standardgateway für einen Store fest, der bereits beim ServiceRecord-Daemon registriert ist.

Befehlsbeispiel in StoreFront:

```
./storebrowse -g “<unique gateway name>” https://my.firstexamplestore.net/
Citrix/Store/discovery
```

> **Hinweis:**
>
> Der eindeutige Gatewayname (unique gateway name) muss in der Liste der Gateways für den angegebenen Store enthalten sein.

-q, –quicklaunch

Beschreibung:

Startet eine Anwendung über die direkte URL. Dieser Befehl funktioniert nur bei StoreFront-Stores.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```

-n –nosingleshot

Beschreibung:

Daemonisiert immer den Storebrowse-Prozess.

Befehlsbeispiel in StoreFront:

```
./storebrowse -n
```

-F –fileparam

Beschreibung:

Startet eine Datei mit dem Dateipfad und der angegebenen Ressource.

Befehlsbeispiel in StoreFront:

```
./storebrowse -F  “<path to file>”  -L <Resource Name> <https://my.firstexamplestore
.net/Citrix/Store/discovery>
```

Workflow

Dieser Artikel beschreibt einen einfachen Workflow zum Starten einer App mit den Storebrowse-Befehlen:

1. `./storebrowse -a https://my.firstexamplestore.net`

   Fügt einen Store hinzu und stellt die vollständige URL des Stores bereit. Notieren Sie sich die vollständige URL, da sie in den folgenden Befehlen verwendet wird.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

   Listet alle veröffentlichten Apps und Desktops auf. Geben Sie Ihre Anmeldeinformationen mit dem Popupfenster ein, das für den registrierten Store angezeigt wird.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

   Startet die Ressource. Verwenden Sie “Resource_Name” aus der Ausgabe des vorherigen Befehls.

4. `./storebrowse -K`

   Dieser Befehl löscht die zuvor eingegebenen Anmeldeinformationen und beendet den Storebrowse-Daemon. Wenn Sie diesen Befehl nicht explizit eingeben, wird der Storebrowse-Prozess nach einer Stunde beendet.

Problembehandlung

March 23, 2021

Dieser Artikel enthält Informationen für Administratoren zur Fehlerbehebung von Problemen in der Citrix Workspace-App für Linux.

Verbindung

Die folgenden Verbindungsprobleme kommen vor.

ICA-Start auf Fedora 29/30

Ein ICA-Start kann auf Fedora 29/30 fehlschlagen. Führen Sie als Workaround die folgenden Schritte aus:

1. Installieren Sie openssl10 mit dem Befehl

```
sudo yum install compat-openssl10.x86_64
```

1. Legen Sie fest, dass die Umgebungsvariable in ~/.bashrc in jeder Sitzung geladen werden soll. Diese Aktion verweist auf die ältere libcrypto-Bibliothek.

```
export ld_preload=/lib64/libcrypto.so.1.0.20

> **Hinweis:**
>
```



```
5  > Die App funktioniert gut in X.Org-Server im Vergleich zum Wayland
       Compositor. Für Distributionen, die Wayland als
       Standardgrafikprotokoll verwenden, heben Sie die Auskommentierung fü
       r einen der folgenden Einträge auf:
6   >
7  > `WylandEnable=false in /etc/gdm/custom.conf` oder
8   > `/et/gdm3/custome.conf`. Melden Sie sich ab und melden Sie sich
        wieder an, um auf den X.Org-Server zu verweisen.
```

Veröffentlichte Ressourcen- oder Desktopsitzung

Wenn beim Herstellen einer Verbindung mit einem Windows-Server ein Dialogfeld mit der Meldung "Verbindung zu Server … wird hergestellt…" aber danach kein Verbindungsfenster angezeigt wird, müssen Sie den Server möglicherweise mit einer Clientzugriffslizenz (CAL) konfigurieren. Weitere Informationen zur Lizenzierung finden Sie unter Lizenzierung.

Sitzungswiederverbindung

Manchmal sind Wiederverbindungen mit Sitzungen, die eine höhere Farbtiefe als der von der Citrix Workspace-App angeforderten verwenden, nicht möglich. Der Grund hierfür ist ein Speichermangel auf dem Server. Wenn die Wiederverbindung fehlschlägt, versucht die Citrix Workspace-App, 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.

Vollständiger Internetname

Citrix empfiehlt, DNS auf Ihrem Netzwerk zu konfigurieren, damit die Namen der Server, zu denen Sie eine Verbindung herstellen möchten, aufgelöst werden können. Wenn Sie DNS nicht konfiguriert haben, kann der Servername eventuell nicht in eine IP-Adresse aufgelöst werden. Alternativ können Sie den Server mit der IP-Adresse statt dem Namen angeben. Für TLS-Verbindungen ist ein vollqualifizierter Domänenname und keine IP-Adresse erforderlich.

Proxyerkennungsfehler

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 ...;
```

Langsame Sitzungen

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.

Verschlüsselungssammlungen

Wenn Ihre Verbindung mit der neuen kryptografischen Unterstützung fehlschlägt:

1. Es gibt verschiedene Tools, um zu überprüfen, welche Verschlüsselungssammlungen Ihr Server unterstützt, einschließlich der Folgenden:
   - `Ssllabs.com` (der Server muss Internetzugang haben)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. Suchen Sie in Linux Client WireShark nach dem Paket (Client Hello, Server Hello) mit dem Filter (ip.addr == VDAIPAddress), um den SSL-Abschnitt zu finden. Das Ergebnis enthält die Verschlüsselungssammlungen, die vom Client gesendet und vom Server akzeptiert werden.

Falsches Citrix Optimization SDK

Das Citrix Optimization SDK-Paket enthält eine falschen Version von UIDialogLibWebKit.so. Führen Sie als Workaround die folgenden Schritte aus:

1. Laden Sie das Citrix Optimization SDK-Paket Version 18.10 von der Seite Downloads herunter.
   a) Gehen Sie zum Pfad CitrixPluginSDK/UIDialogLib/GTK:

      ```
      cd CitrixPluginSDK/UIDialogLib/GTK
      ```

   b) Löschen Sie alle Objektdateien:

      ```
      rm -rf *.o
      ```


c) Gehen Sie zum WebKit-Ordner:

```
cd ../WebKit
```

d) Entfernen Sie die vorhandene Datei UIDialogLibWebKit.so:

```
rm -rf UIDialogLibWebKit.so
```

e) Verwenden Sie den folgenden Befehl im WebKit-Verzeichnis:

```
make all
```

Die neue UIDialogLibWebKit.so wird generiert.

f) Kopieren Sie die neue Bibliothek in das Verzeichnis **$ICAROOT/lib**.

Schwache Verschlüsselungssammlungen für SSL-Verbindungen

Für das Herstellen einer TLS-Verbindung bietet die Citrix Workspace-App für Linux standardmäßig einen moderneren und eingeschränkteren Satz von Verschlüsselungssammlungen. Wenn Sie eine Verbindung zu einem Server herstellen, der eine ältere Verschlüsselungssammlung erfordert, legen Sie im Abschnitt [WFClient] einer Konfigurationsdatei die Konfigurationsoption SSLCiphers=ALL fest.

Die folgenden erweiterten Verschlüsselungssammlungen werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

Verbindungsverlust

Bei der Verwendung des UDT-Protokolls wird u. U. folgende Fehlermeldung angezeigt: Verbindung mit "…" wurde unterbrochen Das Problem kann auftreten, wenn die Verbindung über einen Router erfolgt, wobei die maximale Übertragungseinheit für UDT kleiner ist als die Standardeinstellung von 1500 Bytes. Führen Sie folgende Schritte aus:

- Legen Sie `edtMSS=1000` in einer Konfigurationsdatei fest.

Verbindungsfehler

Verbindungsfehler können eine Vielzahl unterschiedlicher Fehlermeldungen erzeugen. Beispiele:

- Fehler bei Verbindung: Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten.
- Es konnte kein Kontakt mit dem Authentifizierungsdienst hergestellt werden.
- Ihr Konto kann nicht mit dieser Serveradresse hinzugefügt werden

Verschiedene Probleme können solche Fehler verursachen, einschließlich der Folgenden:

- Der lokale Computer und der Remotecomputer können kein gemeinsames TLS-Protokoll verhandeln. Weitere Informationen finden Sie unter TLS.
- Der Remotecomputer erfordert eine ältere Verschlüsselungssammlung für eine TLS-Verbindung. In diesem Fall legen Sie im Abschnitt `\[WFClient\]` einer Konfigurationsdatei die Konfigurationsoption `SSLCiphers=ALL` fest. Führen Sie `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` aus, bevor Sie die Verbindung neu starten.
- Der Remotecomputer fordert falscherweise ein Clientzertifikat an. IIS sollte Zertifikate nur für "Citrix", "Authentication" und "Certificate" **akzeptieren** oder **anfordern**.
- Andere Probleme:

Verbindungen mit geringer Bandbreite

Citrix empfiehlt die Verwendung der aktuellen Citrix Virtual Apps and Desktops-Version auf dem Server und der aktuellen Citrix Workspace-App-Version auf dem Benutzergerät.

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

- **Konfigurieren Sie die Citrix Workspace-App-Verbindung**: Konfigurieren der Citrix Workspace-App-Verbindungen kann die Bandbreite reduzieren, die für ICA erforderlich ist, und verbessert die Leistung
- **Ändern Sie die Verwendung der Citrix Workspace-App**: Durch Ändern der Verwendung der Citrix Workspace-App 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 Citrix Virtual Apps und der Citrix Workspace-App für Linux**: Citrix erweitert und verbessert die Leistung mit jedem Release und für viele Leistungsfeatures ist die neueste Receiver- und Serversoftware erforderlich.

Anzeigen

Tearing

Tearing wird verursacht, wenn Teile von zwei (oder mehreren) unterschiedlichen Frames gleichzeitig auf dem Bildschirm in horizontalen Blöcken angezeigt werden. Dieses Problem ist besonders bei großen Bereichen von sich schnell änderndem Inhalt auf dem Bildschirm erkennbar. Die Daten werden am VDA auf eine Weise erfasst, die Tearing verhindert, und sie werden an den Client auf eine Weise weitergegeben, dass kein Tearing auftritt. X11 (das Linux/Unix-Grafiksubsystem) bietet jedoch keine konsistente Möglichkeit der Erstellung von Frames, die Tearing verhindert.

Zum Verhindern von Tearing empfiehlt Citrix die Standardmethode, bei der der Anwendungsaufbau

mit dem Aufbau des Bilds synchronisiert wird. Dies bedeutet, dass `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”

```
1  Identifier    ”Intel Graphics”
2  Driver        ”intel”
3  Option        ”AccelMethod” ”sna”
4  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). Installieren Sie den “CompizConfig Settings Manager”.

  Führen Sie “CompizConfig Settings Manager” aus.

  Unter “General > Composition” deaktivieren Sie “Undirect Fullscreen Windows”.

> **Hinweis:**
>
> Seien Sie vorsichtig bei der Verwendung von “CompizConfig Settings Manager”, da das System u. U. nicht starten kann, wenn Sie Werte fehlerhaft ändern.

- Compton (ein Add-On-Hilfsprogramm). Ausführliche Informationen finden Sie auf der Hauptseite bzw. in der Dokumentation von Compton. Führen Sie beispielsweise den folgenden Befehl aus:

  ```
  compton --vsync opengl --vsync -aggressive
  ```

Falsche Tastatureingaben

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.

Übermäßiges Aktualisieren der Darstellung

Einige Fenstermanager übertragen beim Verschieben von Seamlessfenstern ständig die neue Fensterposition, was zu einem wiederholten Neuaufbau der Darstellung 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

Die Citrix Workspace-App für Linux 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.

Volle Kompatibilität von Symbolen

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.

Cursorfarbe

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.

Farbblitz

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.

Farbwechsel bei TrueColor-Anzeige

Benutzer haben bei der Herstellung einer Verbindung zu einem Server die Option, 256 Farben zu verwenden. Voraussetzung für diese Option ist, dass die Videohardware Paletten unterstützt, damit Anwendungen zum Erzeugen animierter Anwendungen die Farbpalette wechseln können.

TrueColor-Anzeigen können die Funktion zum Erzeugen von Animationen durch schnelles Wechseln der Palette nicht emulieren. Software-Emulationen dieser Funktion gehen zu Lasten von Schnelligkeit und Datenverkehr im Netzwerk. Um diese Einschränkungen zu reduzieren, puffert die Citrix Workspace-App schnelle Palettenwechsel und aktualisiert die eigentliche Palette nur in Abständen von einigen Sekunden.

Falsche Anzeige

Die Citrix Workspace-App verwendet die EUC-JP- oder UTF-8-Zeichencodierung für japanische Zeichen, während der Server SJIS verwendet. Die Citrix Workspace-App 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.

Spannen der Sitzung

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 gespannt werden.

Mit der Symbolleistenfunktionalität von Desktop Viewer können Sie in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore.

> **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 der gesamte Optionswert `h` ist, wird wfica 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 der Citrix Workspace-App versucht, eine Sitzung zu erstellen, die alle Monitore abdeckt.

Dabei wird von der Citrix Workspace-App angenommen, dass der Rest des Werts der Option “-span” eine Liste der Monitornummern ist. Ein einzelner Wert gibt einen bestimmten Monitor an, zwei Werte geben Monitore oben links und unten rechts in dem erforderlichen Bereich an und vier Werte geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

Wenn `o` nicht angegeben wurde, fordert wfica mit der Meldung _NET_WM_FULLSCREEN_MONITORS ein entsprechendes Fensterlayout vom Fenstermanager an, wenn dies unterstützt wird. Sonst werden Größe- und Positionstipps verwendet, um das gewünschte Layout anzufordern.

Mit dem folgenden Befehl können Sie die Fenstermanager-Unterstützung testen:

```
xprop -root | grep \\_NET\\_WM\\_FULLSCREEN\\_MONITORS
```

Wenn es keine Ausgabe gibt, werden keine Fenstermanager unterstützt. Wenn keine Unterstützung vorhanden ist, benötigen Sie ein Fenster mit override-redirect. Sie können ein solches Fenster mit `-span o` einrichten.

Erstellen einer Sitzung, die sich über mehrere Monitore erstreckt, an der Befehlszeile

1. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   /opt/Citrix/ICAClient/wfica -span h
   ```

   Es wird eine Liste mit Nummern der zurzeit an das Benutzergerät angeschlossenen Monitore auf stdout ausgegeben und wfica wird beendet.

2. Notieren Sie diese Monitornummern.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   /opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
   ```

   wobei w, x, y und z Monitornummern sind, die Sie in Schritt 1 oben erhalten haben. Der einzelne Wert w gibt einen bestimmten Monitor an, zwei Werte w und x geben Monitore oben links und unten rechts in dem erforderlichen Bereich an und vier Werte w, x, y und z geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

   > **Wichtig:**
   >
   > Definieren Sie die Variable WFICA_OPTS, bevor Sie Self-Service über einen Browser starten. 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”
   ```

   Diese Änderung betrifft sowohl Citrix Virtual Apps and Desktops-Sitzungen.

   Wenn Sie self-service oder storebrowse gestartet haben, entfernen Sie die von ihnen gestarteten Prozesse, damit die neue Umgebungsvariable wirksam wird. Entfernen Sie die Prozesse mit folgendem Befehl:

   killall AuthManagerDaemon ServiceRecord storebrowse

Lokale Anwendungen

Möglicherweise können Sie eine Vollbildsitzung nicht beenden, um lokale Anwendungen oder eine andere Sitzung zu verwenden, da die clientseitige Benutzeroberfläche des Systems ausgeblendet ist und das Feature “Tastaturtransparenz” den üblichen Tastaturbefehl deaktiviert. Zum Beispiel wird der Befehl Alt+Tab stattdessen an den Server gesendet.

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.

Browser

Lokaler Browser

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 Server-zu-Client-Inhaltsumleitung.

Zugriff auf veröffentlichte Ressourcen

Beim Zugreifen auf veröffentlichte Ressourcen werden Sie vom Browser aufgefordert, eine Datei zu speichern. Andere Browser als Mozilla, Firefox und Chrome müssen möglicherweise konfiguriert werden, bevor Sie auf eine veröffentlichte Ressource zugreifen können. 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.

Spezifische Browser

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.

Firefox-Browser

Wenn Sie Desktops oder Anwendungen in Firefox starten und die Seite nicht reagiert, aktivieren Sie das ICA-Plug-In.

ICA-Plug-In Firefox

Wenn das ICA-Plug-In in Firefox aktiviert ist, werden Desktop- und Anwendungssitzungen möglicherweise nicht gestartet. Versuchen Sie in diesem Fall, das ICA-Plug-In zu deaktivieren.

Konfigurationsfehler

Diese Fehler können auftreten, wenn Sie einen Verbindungseintrag nicht richtig konfiguriert haben.

E_MISSING_INI_SECTION – Überprüfen der Konfigurationsdatei: "…". In der Konfigurationsdatei fehlt der Abschnitt "…".

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_MISSING_INI_ENTRY – Überprüfen der Konfigurationsdatei: "…". Der Abschnitt "…" muss einen Eintrag "…" enthalten.

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_INI_VENDOR_RANGE – Überprüfen der Konfigurationsdatei: "…". Der X Server-Herstellerbereich "…" in der Konfigurationsdatei ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Bitte wenden Sie sich an Citrix.

Konfigurationsfehler in wfclient.ini

Diese Fehler können auftreten, wenn Sie die Datei wfclient.ini nicht richtig bearbeitet haben.

E_CANNOT_WRITE_FILE – Datei kann nicht geschrieben werden: "…"

Es liegt ein Problem beim Speichern der Verbindungsdatenbank vor, z. B. nicht genügend Festplattenspeicher.

E_CANNOT_CREATE_FILE – Datei kann nicht erstellt werden: "…"

Beim Erstellen einer Verbindungsdatenbank ist ein Problem aufgetreten.

E_PNAGENT_FILE_UNREADABLE – Citrix Virtual Apps-Datei kann nicht gelesen werden "…": Datei oder Verzeichnis nicht gefunden.

– oder –

Citrix Virtual Apps-Datei "…" kann nicht gelesen werden: Zugriff verweigert.

Sie versuchen, eine Ressource über einen Desktopeintrag oder ein Menü zu öffnen. Die Citrix Virtual Apps-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 Citrix Virtual Apps-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 die Citrix Workspace-App erneut.

Proxyerkennungsfehler: JavaScript-Fehler.

Die PAC-Datei enthält ungültiges JavaScript. Ändern Sie die PAC-Datei auf dem Server. Siehe auch Verbindung.

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.

Zertifikate

Wenn Sie einen Store mit SAML-Authentifizierung (mit AuthV3-Protokoll) verwenden, wird die folgende Fehlermeldung angezeigt: “Unacceptable TLS Certificate.”

Dieses Problem tritt auf, wenn Sie die Citrix Workspace-App für Linux 1906 und höher verwenden. Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel CTX260336.

Wenn der StoreFront-Server keine Zwischenzertifikate bereitstellen kann, die dem verwendeten Zertifikat entsprechen, oder wenn Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren, führen Sie diese Schritte aus, bevor Sie einen StoreFront-Store hinzufügen:

1. Besorgen Sie sich die einzelnen Zwischenzertifikate im PEM-Format.

> **Tipp:**
>
> Wenn Sie kein Zertifikat im PEM-Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.

2. Installieren Sie als Benutzer das Paket (normalerweise root):
   a) Kopieren Sie eine oder mehrere Dateien zu $ICAROOT/keystore/intcerts.
   b) Führen Sie den folgenden Befehl als Benutzer, der das Paket installiert hat, aus:

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

Wenn Sie ein Serverzertifikat authentifizieren, das von einer Zertifizierungsstelle ausgestellt wurde und dem vom Benutzergerät noch nicht vertraut wird, befolgen Sie die nachfolgenden Anweisungen, bevor Sie einen StoreFront-Store hinzufügen.

1. Beziehen Sie das Stammzertifikat im PEM-Format.
   Tipp: Wenn Sie kein Zertifikat in diesem Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.
2. Als Benutzer, der das Paket installiert hat (normalerweise root):
   a) Kopieren Sie die Datei in $ICAROOT/keystore/cacerts.
   b) Führen Sie den folgenden Befehl aus:
      ```
      $ICAROOT/util/ctx_rehash
      ```

Andere Probleme

Verbindungsprobleme

Folgende Probleme können ebenfalls auftreten.

Schließen einer Sitzung

Wenn Sie wissen möchten, ob der Server Citrix Workspace-App angewiesen hat, eine Sitzung zu schließen, können Sie mit dem *wfica*-Programm protokollieren, wann ein Befehl zum Beenden der Sitzung vom Server empfangen wurde.

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).

Weitere Informationen zur Protokollierung finden Sie unter Protokollierung. Weitere Informationen zur Konfiguration von syslog finden Sie unter Syslog-Konfiguration.

Konfigurationsdateieinstellungen

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.

Veröffentlichte Anwendungen

Beim Zugriff einer veröffentlichten Anwendung auf einen seriellen Port kann die Anwendung fehlschlagen (je nach der Anwendung mit oder ohne Fehlermeldung), wenn der Port durch eine andere Anwendung gesperrt ist. Überprüfen Sie in solchen Fällen, dass keine Anwendungen vorhanden sind, die den seriellen Port vorübergehend gesperrt haben oder die den seriellen Port gesperrt haben und beendet wurden, ohne ihn wieder freizugeben.

Um dieses Problem zu lösen, beenden Sie die Anwendung, die den seriellen Port derzeit belegt. Bei UUCP-Sperren ist nach dem Beenden der Anwendung eventuell noch eine Sperrdatei vorhanden. Der Speicherort dieser Sperrdateien hängt vom verwendeten Betriebssystem ab.

Starten der Citrix Workspace-App

Wenn die Citrix Workspace-App nicht gestartet werden kann, wird die Fehlermeldung “Application default file could not be found or is out of date” angezeigt. In diesem Fall ist die Umgebungsvariable ICAROOT möglicherweise nicht richtig definiert. Die Variable muss richtig definiert werden, wenn Sie die Citrix Workspace-App 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, die Citrix Workspace-App von einer Terminalsitzung zu starten. Wenn die Fehlermeldung weiterhin angezeigt wird, ist die Umgebungsvariable ICAROOT wahrscheinlich nicht richtig definiert.

- Installieren Sie die Citrix Workspace-App im Standardverzeichnis neu. Weitere Informationen zum Installieren der Citrix Workspace-App finden Sie unter Installation und Einrichtung.

  Wenn die Citrix Workspace-App vorher im Standardverzeichnis installiert worden war, sollten Sie vor der Neuinstallation das Verzeichnis `/opt/Citrix/ICAClient` oder `$HOME/ICAClient/` entfernen.

Citrix CrypToKit (ehemals SSL SDK)

Um die Versionsnummer für das ausgeführte Citrix CryptoKit (ehemals SSLSDK) oder OpenSSL festzustellen, führen Sie den folgenden Befehl aus:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

Sie können diesen Befehl auch für AuthManagerDaemon oder PrimaryAuthManager ausführen

Tastenkombinationen

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.

Kroatische Remotetastatur

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.

Japanische Tastatur

Zum Konfigurieren einer japanischen Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Japanese (JIS)

ABNT2-Tastatur

Zum Konfigurieren einer ABNT2-Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

Lokale Tastatur

Wenn sich einige Tasten auf der lokalen Tastatur nicht wie erwartet verhalten, wählen Sie das passendste Serverlayout aus der Liste in $ICAROOT/config/module.ini aus.

Windows Media Player

Die Citrix Workspace-App hat möglicherweise nicht die nötigen GStreamer-Plug-Ins, um ein gewünschtes Format zu verarbeiten. Normalerweise fordert der Server dann ein anderes Format an. Manchmal wird bei der anfänglichen Prüfung irrtümlich ein passendes Plug-In festgestellt. Dies sollte erkannt werden und auf dem Server eine Fehlermeldung auslösen, die darauf hinweist, dass Windows Media Player beim Wiedergeben der Datei ein Problem hatte. Erneutes Wiedergeben der Datei in der Sitzung funktioniert normalerweise, weil das Format von der Citrix Workspace-App 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.

Einstellung für seriellen Anschluss

Zum Konfigurieren eines seriellen Anschlusses fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=1

ComPort1=device

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

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Fehler

Dieser Abschnitt enthält weitere Fehlermeldungen, die bei der Verwendung der Citrix Workspace-App 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 der Citrix Workspace-App über die Befehlszeile lässt diese Meldung in der Regel darauf schließen, dass die in der Befehlszeile angegebene Beschreibung in der Datei appsrv.ini nicht gefunden wurde.

E_BAD_OPTION – Die Option "…" ist ungültig.

Fehlendes Argument für Option "…".

E_BAD_ARG – Die Option "…" hat ein ungültiges Argument: "…".

Ungültiges Argument für Option "…".

E_INI_KEY_SYNTAX – Der Schlüssel "…" in der Konfigurationsdatei "…" ist ungültig.

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

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

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

E_SERVER_NAMELOOKUP_FAILURE – Verbindung zu Server "…" kann nicht hergestellt werden.

Der Name des Servers konnte nicht aufgelöst werden.

In mindestens eine Datei kann nicht geschrieben werden: "…". Beheben Sie Probleme beim Speicherplatz auf der Festplatte oder der Verbindung und versuchen Sie es erneut.

Überprüfen Sie, ob die Festplatte voll ist oder ob Probleme mit den Rechten bestehen. Wenn Sie das Problem gefunden und gelöst haben, wiederholen Sie den Vorgang, der die Fehlermeldung ausgelöst hat.

Die Verbindung zum Server wurde unterbrochen. Stellen Sie die Verbindung wieder her und versuchen Sie es erneut. In diesen Dateien fehlen u. U. Daten: "…".

Stellen Sie die Verbindung wieder her und wiederholen Sie den Vorgang, der den Fehler ausgelöst hat.

Diagnoseinformationen

Wenn Sie beim Verwenden der Citrix Workspace-App Probleme feststellen, werden Sie vom Technischen Support möglicherweise gebeten, Diagnoseinformationen bereitzustellen. Diese Informationen unterstützen dieses Team bei der Diagnose und helfen, das Problem zu beheben.

Abfrage von Diagnoseinformationen zur Citrix Workspace-App

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 Citrix Workspace-App-Konfigurationsdateien und die Werte der verschiedenen Systemvariablen.

2. Überprüfen Sie, ob diese Datei vertrauliche Informationen enthält, bevor Sie sie an den technischen Support senden.

Problembehandlung bei Verbindungen mit Ressourcen

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

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

SDK und API

July 6, 2020

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für zusätzliche virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalanwendungen sind auf Citrix Virtual Apps and Desktops-Servern. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an den technischen Support von Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Funktionierender Quellcode für mehrere Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen finden Sie unter Citrix Virtual Channel SDK für die Citrix Workspace-App für Linux.

Befehlszeilenreferenz

Weitere Informationen zu Befehlszeilenreferenz und Parametern finden Sie unter Citrix Workspace app for Linux Command Reference.

Platform Optimization SDK

Im Rahmen der HDX SoC-Initiative für die Citrix Workspace-App für Linux haben wir das “Platform Optimization SDK” entwickelt, um ein Ökosystem kostengünstiger Geräte mit niedrigem Energieverbrauch, hoher Leistung und innovativen Formfaktoren zu ermöglichen.

Das Platform Optimization SDK kann von Entwicklern genutzt werden, um die Leistung von Linux-basierten Geräten zu verbessern, indem sie Plug-In-Erweiterungen für die ICA-Engine-Komponente (wfica) der Citrix Workspace-App für Linux entwickeln. Plug-Ins werden als freigegebene Bibliotheken entwickelt, die von wfica dynamisch geladen werden. Mit diesen Plug-Ins können Sie die Leistung Ihrer Linux-Geräte optimieren, indem Sie die folgenden Funktionen aktivieren:

- Beschleunigtes Decodieren von JPEG- und H.264-Daten, mit denen das Sitzungsbild erstellt wird
- Steuern der Speicherzuordnung zum Erstellen des Sitzungsbilds
- Verbessern der Leistung durch Steuern der unteren Ebene beim Erstellen des Sitzungsbilds
- Bereitstellen von Diensten für die Grafikausgabe und Benutzereingabe für Betriebssystemumgebungen, die X11 nicht unterstützen

Weitere Informationen finden Sie unter Citrix Workspace app for Linux - Platform Optimization SDK.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States