このリリースについて

Nov 19, 2015

Citrix Receiver for Linuxを使用すると、さまざまな種類のLinuxデバイスからデスクトップ、アプリケーション、およびデータにすばやく安全にアクセスできます。Citrix製品によるITインフラストラクチャ環境でReceiverを使用すると、作業を行うユーザーの機動性、便宜性、および柔軟性が向上します。

このトピックでは、Receiver for Linux Version 13.1の新機能、このバージョンの既知の問題、および以前のバージョンで解決された問題について説明します。

バージョン13.1の新機能

Receiver for Linux Version 13.1の新しい機能は次の通りです。

- SSLv3の使用の無効化。SSLv3プロトコルに対するPOODLEなどの新たな攻撃を防ぐため、このリリースのReceiver for LinuxはSSLv3プロトコルの使用を無効にしています。http://support.citrix.com/article/ctx200238を参照してください。
  重要：TLS 1.0、1.1、または1.2を有効にする必要があります。

Version 13.1で解決された問題

Version 13.1の既知の問題

デフォルトでは、selfserviceおよびstorebrowseコマンドのプロキシサポートは提供されません。StoreFrontサーバーでプロキシサーバーを使用するには、環境変数
— http_proxy
を設定してからこれらのコマンドを使用してください。環境変数は、次の形式で設定します：

<サーバー名>.<ドメイン>[:<ポート>]
[#403729]

スマートカードにアクセスする場合にReceiver for Linuxでセグメント化の問題が起きる場合、PKCS#11ライブラリに問題があることがあります。pkcs11-toolユーティリティでライブラリをチェックできます。pkcs11-toolユーティリティはopenscパッケージの一部です。テスト例：
pkcs11-tool --module /usr/lib/libgtop11dotnet.so -l
これによってもセグメント障害が起こる場合は、ドライバーの供給元に連絡する必要があります。また、同じ種類のカードのほかのソースのドライバーを試すこともできます。この問題は、Fedora 19およびFedora 20に含まれるGemalto .NETドライバーで見られます。[#493172]
Receiver for Linuxは複数のカードリーダーをサポートします。ただし、同時に使用できるのは1台のみです。[#494524]

接続を実行するには、Linuxマシンのホスト名を20文字以下にする必要があります。この設定は、次のコマンドを使って調査および設定することができます。hostnameコマンドを実行します。いずれのユーザーもホスト名を調査できますが、hostnameを設定できるのはルートユーザーまたは管理者権限があるユーザーだけです。[#494740]

Receiver for Linux 13.xで全画面モードのXenDesktopにアクセスする場合、ローカルのスクリーンセーバーがアクティブにならないことがあります。これはサードパーティの問題で、クライアントのオペレーティングシステムにより動作は異なります。[#496398]

Receiver for Linuxは保護されていないStoreFrontストアへの接続（http://）は許可しません。ストアの構成によっては、ユーザーが"エラー：探索ドキュメントを取得できません" []形式のエラーメッセージを受け取ったり、初期接続がhttpで実行されたあとで通信がhttpsに切り替えられたりします。または、ホスト名にIPアドレスを使用している場合は、Citrix XenAppサービス（以前のProgram Neighborhood エージェント）に関連するエラーが発生することがあります。URLを入力する場合、

https://を明示的に使用するか、あるいはサーバー名にhttp://を付けないようにしてください。[#473027、#478667、および#492402]

Receiver for Linuxは、複数の認証証明書を含むスマートカードによるログオンをサポートしません。[#488614]

全画面セッションを実行している低性能のデバイスでは、スマートカード認証によるログオンに予想よりも時間がかかり、タイムアウトすることがあります。H264の使用を無効にすることで、この問題を防ぐことができます。H624の使用を無効にするには、次のことを実行します。
1. wfclient.iniを開きます。
2. "Thinwire3.0"セクションに移動します。
3. エントリ"H264Enabled=False"を追加します。

この問題は、ハードウェアアクセラレータH264のない、armhf（ARM hard float）をベースとするマシンで見られます。[#497720]
Program Neighborhoodエージェントサーバーによりユーザーがドメインコントローラーに直接アクセスして有効期限が切れたパスワードを変更できる場合は、ライブラリのMIT互換バージョンであるlibkcpm.soでのみこれを実行できます。これは、Heimdal互換バージョンの問題によるものです。これ制限は、x86、armel、およびx64（x86 pnabrowseを使用）に適用されます。armhfには適用されません。[#498037]

ユーザーがセルフサービスUIを開いてStoreFrontストアに接続するとエラーが発生し、その後でAuthentication Managerダイアログボックスが開かれるとReceiver for Linuxウィンドウが閉じます。[#430193]

StoreFrontストアに接続しようとして間違ったスマートカードを挿入すると、「プロトコルエラー」や「指定したストアが見つかりません」といった問題について説明しないエラーメッセージが表示されることがあります。[#496904]

Receiver for Linuxはlibpng12.soを必要としますが、Fedoraベースのシステムの標準のレポジトリではこれは通常使用できません。この場合、システムに適切なRPMをインターネットで見つけてください。openSUSEの場合はlibpng12.soを使用できますが、別途インストールする必要があります。[#501937]

コネクションセンターで仮想デスクトップから切断したりログオフしたりすることはできません。[切断] ボタンは使用できず、［ログオフ］ボタンは機能しません。仮想デスクトップから切断したりログオフしたりするには、コネクションセンターではなくデスクトップセッションを使用してください。仮想アプリケーションでは、この問題は発生しません。[#423651、#424847]

12.1のHotofixは、pnabrowse終了コードE_SSLSDK_PASSWORD_LOCKED（値220）を追加しました。これにより、終了コードE_PASSWORD_EXPIREDの値は238から239に変更されました。13.0では、E_SSLSDK_PASSWORD_LOCKEDの値は240に変更され、E_PASSWORD_EXPIREDの正しい値を復元します。ただし、pnabrowse -errnoにより一覧表示された値は、220～240の正しくない値を示しています。[#502550]

システム要件

Nov 19, 2015

このトピックでは、Receiver for Linuxのインストールに必要なシステムとユーザーの要件について説明します。

Devices

- glibcxx 3.4.15以降、glibc 2.11.3以降、gtk 2.20.1以降、libcap1またはlibcap2、およびudevをサポートするLinuxカーネルのVersion 2.6.29以降。
- セルフサービスユーザーインターフェイス用
  - libwebkitまたはlibwebkitgtk 1.0
  - libxml2 2.7.8
  - libxerces-c 3.1
- ALSA（libasound2）、Speex、およびVorbisコーデックライブラリ。
- Receiverのインストールには20MBのディスク空き容量が必要です。インストールパッケージの内容を抽出するには、40MBのディスク空き容量が必要です。ディスクの空き容量を確認するには、ターミナルウィンドウで次のコマンドを実行します。
  df -k
- HDX MediaStream MediaStream Flashリダイレクトを使用するSoC（system-on-a-chip）デバイスでは、1GB以上のRAMが必要です。
- 256色以上のビデオディスプレイ。
- TCP/IPネットワークシステム。

H.264

x86デバイスの場合、1.6GHz以上のプロセッサで一般的な解像度（1280×1024ピクセルなど）の単一モニターセッションが良好に表示されます。HDX 3D Pro機能を使用する場合は、ネイティブのハードウェアアクセラレーションをサポートするクラフィックドライバと2GHz以上のプロセッサが必要です。

ARMデバイスで通常のH.264サポート機能およびHDX 3D Pro機能を使用する場合は、ハードウェアH.264デコーダーが必要です。より高速なプロセッサを使用することでパフォーマンスが向上します。

HDX MediaStream Flashリダイレクト

HDX MediaStream Flashリダイレクトの要件については、CTX134786を参照してください。

クライアント側でのレンダリングをサポートするには、ユーザーデバイス上で動作するAdobe Flashプラグインのバージョンが、XenAppサーバーやXenDesktopサーバーのものと同等またはそれ以上である必要があります。この条件が満たされない場合、サーバー側でレンダリングされます。

最新の機能およびセキュリティ上の修正を適用するために、プラグインを常に最新バージョンにアップグレードすることをお勧めします。

HDX RealTime Webカメラビデオ圧縮

HDX RealTime Webカメラビデオ圧縮の要件は以下のとおりです。
- Video4Linux互換Webカメラ
- GStreamer 0.10.25以降

HDX MediaStream Windows Mediaリダイレクト

HDX MediaStream Windows Mediaリダイレクトの要件は以下のとおりです。

- GStreamer 0.10.15以降

注：http://gstreamer.freedesktop.orgからGStreamerをダウンロードできます。特定のコーデックの使用には、その製造元からのライセンスが必要な場合があります。使用するコーデックのライセンス要件については、社内の法務部門に確認してください。

Philips SpeechMike

Philips SpeechMikeデバイスをReceiverで使用する場合には、ユーザーデバイスに関連のドライバーをインストールする必要があります。必要な情報とソフトウェアのダウンロードについては、Philips社のWebサイトにアクセスしてください。

スマートカードのサポート

Receiver for Linuxでスマートカードのサポートを構成するには、スマートカード認証を許可するよう構成されたStoreFrontサービスサイトが必要です。

注：Web Interface構成（以前のProgram Neighborhood エージェント）用のXenApp Servicesサイト、またはStoreFrontサーバーにより提供できる「従来のProgram Neighborhood エージェント」サイトでは、スマートカードはサポートされません。

Receiver for Linuxは、PCSC-Liteと互換性があるスマートカードリーダーおよび適切なLinuxプラットフォーム用のPKCS#11ドライバーがあるスマートカードをサポートします。Receiver for LinuxにPKCS#11ドライバーの位置を確実に認識させるには、次の手順に従って構成ファイル内に場所を保存します。

1. 次の構成ファイルにアクセスします：$ICAROOT/config/AuthManConfig.xml
2. 行PKCS11moduleを検索して、ドライバーの場所を=エレメントに続く行に追加します。
   注：ドライバーの場所のファイル名を入力すると、ReceiverはICAROOT/PKCS#11ディレクトリ内のそのファイルに移動します。または、"/"から始まる絶対パスを使用できます。

Receiver for Linuxのスマートカード認証を削除するには、SmartCardRemovalActionを構成ファイルで次の手順によって更新します。

1. 次の構成ファイルにアクセスします：$ICAROOT/config/AuthManConfig.xml
2. 行SmartCardRemovalActionを検索し、'noaction'または'forcelogoff'を=エレメントに続く行に追加します。

デフォルトの設定は'noaction'です。この場合、スマートカード上で削除を実行する時に、保存されている資格情報やスマートカードに関して生成されるトークンはクリアされません。'forcelogoff'を追加すると、スマートカードの削除時にすべての資格情報およびStoreFront内のトークンがクリアされます。

一部のCitrix Receiver for Linux 13.x機能での制限

Receiverの一部の機能は、新しいバージョンのXenAppおよびXenDesktopに接続した場合にのみ実行できるものがあり、またこれらの製品の最新のHotfixが必要な場合もあります。

ユーザー側の要件

Citrix Receiver for Linuxをインストールするためにスーパーユーザー（root）としてログオンする必要はありません。ただし、USBサポートを有効にするには、スーパーユーザーとしてReceiverをインストールおよび構成してください。スーパーユーザー以外のユーザーとしてReceiverをインストールした場合でも、サポートされているWebブラウザーでStoreFrontを使用したりReceiverのネイティブインターフェイスを使用したりして公開リソースにアクセスできます。

システム要件を満たしているかどうかのチェック

Citrixは、Receiverインストールパッケージの一部としてhdxcheck.shスクリプトを提供します。このスクリプトはReceiver for Linuxのすべての機能を実行できるようにするため、デバイスがすべてのシステム要件を満たしているかどうかをチェックします。このスクリプトは、インストールパッケージのUtilitiesディレクトリにあります。

hdxcheck.shスクリプトを実行するには

1. ターミナルウィンドウを開きます。
2. 「cd $ICAROOT/util」と入力してEnterキーを押し、インストールパッケージのUtilitiesディレクトリに移動します。
3. 「sh hdxcheck.sh」と入力してスクリプトを実行します。

インストールとセットアップ

Nov 19, 2015

Receiver for Linuxのインストールは、以下のパッケージを使用して行います。

- **Debian（.debファイル）：**
  - x86 - 32ビットおよび64ビットのパッケージ（32ビットバイナリを含む）
  - ARM - armelおよびarmhfプラットフォーム用32ビットパッケージ
- **RPM Package Manager（.rpmファイル）：**
  - x86 - 32ビットパッケージ
- **Tarball（.tar.gzファイル）：**
  - x86およびARM - x86、armel、およびarmhfプラットフォーム用32ビットバイナリのTarballパッケージ
  - x86 64ビット - 64ビットシステム用64ビットバイナリのTarballパッケージ

可能な場合は、RPMまたはDebianパッケージを使用してReceiverをインストールしてください。これらのファイルは、必要なすべてのパッケージが自動的にインストールされるため、一般的には取り扱いがより簡単です。特定のディレクトリにReceiverをインストールする場合は、Tarballパッケージを使用します。

これらのパッケージは、CitrixのWebサイト（http://www.citrix.com/downloads/）の「Downloads」ページからダウンロードできます。

ヒント：Ubuntu上にReceiverをDebianパッケージでインストールする場合は、Ubuntuソフトウェアセンターでパッケージを開くと便利です。

DebianパッケージからReceiver for Linuxをインストールするには

Debian 7以前の64ビットシステムに64ビットReceiver Debianパッケージをインストールしている場合、最初にi386パッケージを有効にする必要があります。i386パッケージが有効になっているかどうかをチェックするには、コマンドラインにdpkg print-foreign-architecturesと入力します。次に、入力結果に従って次のことを実行します。

- 結果としてi386と表示されたら、パッケージのインストールを実行できます。
- 結果としてi386と表示されない場合は、次のコマンドを入力してパッケージを有効にします。

1. sudo dpkg --add-architecture i386
2. sudo apt-get update

以下の手順で、packagenameに実際のインストールパッケージの名前を指定します。

ヒントこの手順ではコマンドラインを使用します。または、ファイルブラウザー上で.debパッケージをダブルクリックしてインストールできます。通常、これによりパッケージマネージャーが起動して、必要なソフトウェアが自動的にダウンロードされます。パッケージマネージャーを使用できない場合は、同様の機能を持つコマンドラインツール、gdebiを使用することをお勧めします。

1. スーパーユーザー（root）としてログオンします。
2. ターミナルウィンドウを開きます。
3. インストールを実行するには、dpkg -i packagename.debと入力します。
4. 必要な依存ソフトウェアをインストールするには、sudo apt-get -f installと入力します。
5. 同様のコマンドを実行して、USBサポートパッケージをインストールします。

RPMパッケージからReceiver for Linuxをインストールするには

以下の手順で、<packagename>に実際のインストールパッケージの名前を指定します。

ヒント：RPM Package Managerでは、必要なソフトウェアが自動的にはダウンロードされません。ソフトウェアをダウンロードしてインストールするには、zypper install <ファイル名>をOpenSUSEのコマンドライン、またはyumをFedoraで使用します。

1. スーパーユーザー（root）としてログオンします。
2. ターミナルウィンドウを開きます。
3. インストールを実行するには、「zypper install packagename.rpm」と入力します。例：zypper install ./ICAClient-suse11sp3-13.2.1.328635-0.x86_64.rpm
4. 同様のコマンドを実行して、USBサポートパッケージをインストールします。

TarballパッケージからReceiver for Linuxをインストールするには

1. ターミナルウィンドウを開きます。
2. .tar.gzファイルを展開して、その内容を一時ディレクトリに保存します。たとえば、Linuxプラットフォームでは、tar xvfz packagename.tar.gzと入力します。
3. プログラムをセットアップするには、./setupwfcと入力してEnterキーを押します。
4. デフォルトの1をそのままにして（Receiverをインストール）、Enterを押します。
5. 必要なインストールディレクトリのパスおよび名前を入力してEnterキーを押します。インストールディレクトリを指定せずにEnterキーを押すと、デフォルトの場所にReceiverがインストールされます。
   スーパーユーザー（root）のデフォルトのインストールディレクトリは、/opt/Citrix/ICAClientです。

   非スーパーユーザーのデフォルトのインストールディレクトリは、$HOME/ICAClient/platformです。platformは、システムにより生成されるオペレーティングシステムIDです。例：$HOME/ICAClient/linuxx86 for the Linux/x86 platform

   注：デフォルトのインストール先以外のディレクトリにインストールする場合は、$HOME/.profileまたは$HOME/.bash_profileの$ICAROOTにそのディレクトリを設定します。
6. インストールを続行するには、「y」と入力して、Enterキーを押します。
7. Receiverをデスクトップ環境に統合するかどうかを選択できます。これにより、Citrix Receiverを起動するためのメニューオプションがデスクトップ環境に作成されます。「y」と入力すると、デスクトップ統合が有効になります。
   注：Receiverをデフォルトのインストール先以外のディレクトリにインストールする場合は、デスクトップ統合が正しく機能するように、$HOME/.profileまたは$HOME/.bash_profileの$ICAROOTにインストール先ディレクトリを設定してください。
8. GStreamerがインストール済みの場合は、GStreamerをReceiverに統合してHDX Mediastreamマルチメディアアクセラレーションをサポートするかどうかを選択できます。 ReceiverをGStreamerと統合するには、「y」と入力します。
9. スーパーユーザー（root）としてログオンしている場合、XenDesktopおよびXenApp公開VDIアプリケーションのUSBサポートのインストールを選択できます。 「y」と入力すると、USBサポートがインストールされます。
   注：スーパーユーザー（root）としてログオンしていない場合、「USB support cannot be installed by non-root users.（root以外のユーザーはUSBサポートをインストールできません）」という警告が表示されます。この機能を使用する場合は、スーパーユーザーとしてインストーラーを実行してください。
10. インストールが完了すると、メインのインストールメニューに戻ります。 セットアッププログラムを終了するには、「3」と入力して、Enterキーを押します。

Citrix Receiver for Linuxをアンインストールするには

以下の手順は、Tarballパッケージでテストされています。RPMおよびDebianパッケージの場合は、オペレーティングシステム側の標準的なツールを使用してアンインストールしてください。

1. セットアッププログラムを実行するには、「$ICAROOT/setupwfc」と入力して、Enterキーを押します。
2. Citrix Receiver for Linuxをアンインストールするには、「2」と入力してEnterキーを押します。
   注：Citrix Receiver for Linuxをアンインストールするには、インストール時と同じユーザーアカウントでシステムにログオンする必要があります。

Receiver for Linuxのインストールのカスタマイズ

Nov 19, 2015

Receiverパッケージのコンテンツを変更しファイルを再パッケージして、インストール前にReceiver構成をカスタマイズでき ます。この変更パッケージを使用してインストールするすべてのReceiverにこの変更が含まれます。

Citrix Receiver for Linuxのインストールをカスタマイズするには

1. Receiverパッケージファイルを空のディレクトリに展開します。 パッケージファイルの名前は、<platform.major.minor.release.build>.tar.gz（Linux/x86プラットフォームならlinuxx86.13.1.0.nnnnnn.tar.gzなど）です。
2. Receiverパッケージに必要な変更を加えます。 たとえば、標準のReceiverのインストールには含まれていない発行機関からの証明書を使用する場合は、新しいTLSルート証明書をパッケージに追加します。 新しいTLSルート証明書をパッケージに追加する方法については、「ユーザーデバイスへのルート証明書のインストール」を参照してください。 Receiverに付属の証明書については、「
   — *SSLおよびTLSの構成と有効化*
   」を参照してください。
3. PkgIDファイルを開きます。
4. パッケージを変更したことを示すために次の行を追加します :MODIFIED=traceinfoここでtraceinfoは、パッケージの変更者と変更日時を示します。この情報の形式は、任意のものにできます。
5. ファイルを保存して閉じます。
6. パッケージファイルの一覧platform/platform.psf（たとえばLinux/x86プラットフォームの場合なら linuxx86/linuxx86.psf）を開きます。
7. パッケージファイルの一覧を更新して、パッケージに対する変更を適用します。 このファイルを更新しない場合、新しいパッケージのインストール時にエラーが起こることがあります。 変更には、修正したファイルのサイズの更新、またはパッケージに追加したファイルに対する新しい行の追加などを含めることができます。 パッケージファイルの一覧に含まれている列には次のようなものがあります。
   - ファイルの種類
   - 相対パス
   - サブパッケージ（corから編集不可）
   - 権限
   - 所有者
   - グループ
   - サイズ
8. ファイルを保存して閉じます。
9. vm-create-from-templateコマンドを使用します。tar を使ってReceiverパッケージファイルを再生成します。例 :tar czf ../newpackage.tar.gz *ここで<newpackage>は、新しいReceiverパッケージファイルの名前です。

Receiver for Linuxの起動

Nov 19, 2015

Receiverは、ターミナルプロンプト、またはサポートされているデスクトップ環境を使って起動できます。

Receiverをデフォルトのインストールディレクトリにインストールしなかった場合は、環境変数ICAROOTに実際のインストール先ディレクトリを指定しておく必要があります。

コマンドウインドウでReceiverを起動するには

コマンドウィンドウで、/opt/Citrix/ICAClient/selfserviceと入力して、Enterを押します（ここで、/opt/Citrix/ICAClientはReceiverをインストールしたディレクトリです）。

LinuxデスクトップからReceiverを起動するには

ファイルマネージャーを使ってLinuxデスクトップ環境からReceiverを起動できます。

一部のデスクトップでは、メニューからReceiverを起動することもできます。Linuxのディストリビューションにより、Receiverを起動するためのメニューの位置が異なる場合があります。

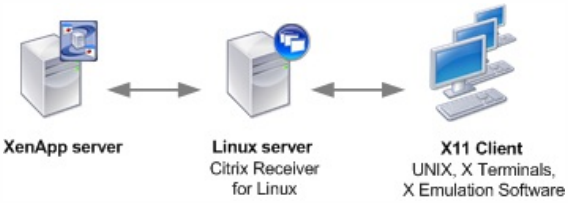
Receiver for LinuxをICA-to-Xプロキシとして使用する

Nov 19, 2015

Receiverを実行しているワークステーションをサーバーとして使用し、出力を別のX11対応デバイスに転送できます。Receive
を使用できないX端末またはUNIXワークステーションにMicrosoft Windows用アプリケーションを配信する場合などに、この
方法を使います。ただし、Receiverソフトウェアは多くのXデバイスをサポートしているため、これらのデバイスにもReceive
をインストールすることをお勧めします。ReceiverをICA-to-Xプロキシとして実行することを、サーバー側ICAとも呼びます。

この方法では、実行するReceiverをICAからX11へのコンバーターとして使うことで、X11の出力をローカルのLinuxデスクトッ
プ画面に転送します。また、その出力をさらに別のX11コンピューターの画面に転送できます。つまり、1つのシステムで複数
のReceiverのコピーを同時に実行し、それぞれの出力を別の異なるデバイスに送信できます。

この図は、Receiver for LinuxがICA-to-Xプロキシとして動作するシステムを示しています。



この方法を使うようにシステムを設定するには、LinuxサーバーをICAからX11へのプロキシサーバーとして機能させる必要が
あります。

- X端末が既にある場合は、XアプリケーションをX端末に供給するLinuxサーバーでReceiverを実行できます。
- Receiverを使用できないUNIXワークステーションにアプリケーションを配布する場合は、プロキシサーバーとして機能す
  るサーバーが1台必要です。たとえば、Linuxを実行しているPCをプロキシサーバーとして使用できます。

サポートされる機能

アプリケーションは、ICAプロトコルの機能を使用して、X11の最終デバイスに提供されます。デフォルトで、プロキシサー
バー上のドライブにアクセスするには、ドライブマッピング機能を使う方法しかありません。（通常はローカルドライブがな
い）X端末を使用している場合は、これは問題ありません。ほかのUNIXワークステーションにアプリケーションを配布する場
合は、次のいずれか実行できます。

- ローカルのUNIXワークステーションをNFSを使ってプロキシサーバーにマウントし、プロキシサーバー上のNFSマウントポ
  イントをクライアントドライブとしてマップしてアクセスする。
- SAMBAなどのNFSからSMBへのプロキシサーバー、またはMicrosoft Services for UNIXなどのサーバー上のNFSクライアン
  トを使用する。

次の機能は、最終デバイスに提供されません。

- プロキシとして機能するサーバーがオーディオをサポートしている場合でも、X11デバイスではオーディオを使用できませ
  ん。
- クライアントプリンターは、X11デバイスでは使用できません。LPD印刷機能を使ってサーバーからUNIXプリンターに手動
  でアクセスするか、ネットワークプリンターを使用する必要があります。

X端末またはUNIXワークステーションからReceiverをサーバー側ICAとして起動するには

1. sshまたはtelnetを使って、プロキシとして動作しているデバイスに接続します。
2. プロキシデバイスのシェルで、**DISPLAY**環境変数をローカルデバイスに設定します。たとえば、Cシェルでは、次のように
   入力します。
   setenv DISPLAY <local:0>

注：コマンドssh -Xを使ってプロキシとして動作するデバイスに接続する場合は、**DISPLAY**環境変数を設定する必要はありません。

3. ローカルデバイスのコマンドプロンプトで、次のように入力します。xhost <proxy server name>
4. Receiverをデフォルトのインストールディレクトリにインストールしない場合は、環境変数ICAROOTに実際のインストール先ディレクトリを指定しておく必要があります。
5. Receiverがインストールされているディレクトリを探します。コマンドプロンプトで、次のように入力します。selfservice &

Receiver for Linuxの構成

Nov 19, 2015

Receiverにより、仮想デスクトップやアプリケーションへの安全なセルフサービスアクセスと、Windows、Web、およびSaaS（Software as a Service）アプリケーションへのオンデマンドアクセスが提供されます。ユーザーのアクセスは、Citrix StoreFrontや従来のWeb InterfaceのWebページにより管理されます。

Receiverのユーザーインターフェイスを使用してリソースに接続するには

Receiverのホームページには、ユーザーのアカウント設定（つまり接続先のサーバー）とCitrix XenDesktopまたはCitrix XenAppの管理者による構成に基づいて、そのユーザーに提供されている仮想デスクトップやアプリケーションが表示されます。ユーザーは、［環境設定］ダイアログボックスの［アカウント］ページにStoreFrontサーバーのURLや自分のメールアドレス（メールアドレスによるアカウント検出が有効な場合）を入力してアカウントの構成を行います。

ヒント：StoreFrontサーバーの複数のストアに同じ名前が使用されている場合、［アカウント］ページはそれらのストアを同一のものとして表示します。このような混乱を避けるため、管理者はストアを構成するときに一意のストア名を使用する必要があります。Program Neighborhoodエージェントの場合、ストアURLが表示され、ストアを確実に識別します。
ユーザーがストアに接続すると、Receiverのホームページで特定のデスクトップやアプリケーションを検索したり、「+」（プラス記号）をクリックしてそれらの一覧を参照したりできます。デスクトップやアプリケーションのアイコンをクリックすると、その項目がホームページにコピーされます。コピーされた項目をクリックすると、その項目が起動します。このときに、コネクションが作成されます。

コネクション設定の構成

Citrix Receiverと、XenAppおよびXenDesktopサーバー間の接続に対する数々のデフォルトの設定を構成できます。また必要に応じて、個々のコネクションに対する設定を変更することもできます。

コマンドラインまたはWebブラウザーからリソースに接続する

Receiverのホームページでデスクトップやアプリケーションのアイコンをクリックすると、サーバーへのコネクションが作成されます。また、コマンドラインやWebブラウザーからコネクションを開くこともできます。

コマンドラインでProgram NeighborhoodまたはStoreFrontサーバーへのコネクションを作成するには

まず、サーバー上でストアが使用可能であることを確認します。必要に応じて、次のコマンドを実行してストアを追加します。

./util/storebrowse --addstore <ストアのURL>

1. 接続するデスクトップまたはアプリケーションの固有のIDを取得します。このIDは、以下のコマンドによる出力の最初の引用文字列です。
   - サーバー上のすべてのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。
     ./util/storebrowse -E <ストアのURL>
   - サブスクライブ済みのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。
     ./util/storebrowse -S <ストアのURL>
2. 次のコマンドを実行して、デスクトップまたはアプリケーションを起動します。
   ./util/storebrowse –L <デスクトップまたはアプリケーションのID> <ストアのURL>

サーバーに接続できない場合は、管理者がサーバーの場所またはSOCKSプロキシの詳細を変更する必要がある場合があります。詳しくは、「プロキシサーバー経由の接続」を参照してください。

Webブラウザーでコネクションを作成するには

通常、Mozilla、Netscape、またはChromeを構成する場合、インストール時に自動的にコネクションが構成されます。

Firefox、Mozilla、またはChrome用に.mailcapおよびMIMEファイルを手動で設定する必要がある場合は、次の手順に従ってファイルを変更して、ICAファイル（拡張子.ica）によりReceiverの実行可能ファイル（wfica）が起動するようにしますほかのブラウザーを使用するには、必要に合わせてブラウザー構成を変更する必要があります。

1. .mailcapファイルを変更する場合は、$HOME内で、.mailcapファイルを作成または変更して次の行を追加します。
   application/x-ica; /opt/Citrix/ICAClient/wfica.sh %s; x-mozilla-flags=plugin:Citrix ICA

2. MIMEファイルを変更する場合は、$HOME内で、.mime.typesファイルを作成または変更して次の行を追加します。
   application/x-ica ica

   ここで、icaの前にあるx- は、そのicaがInternet Assigned Numbers Authority（IANA）公認のMIMEタイプでないことを意味します。

リソース接続のトラブルシューティング

ユーザーがアクティブなコネクションを管理するには、コネクションセンターを使用します。セッションの動作が遅い、またはコネクションに問題がある場合、ユーザーや管理者はコネクションセンターを使用してトラブルシューティングを行えます。ユーザーは、コネクションセンターで以下の操作を行えます。

- アプリケーションを終了する。
- セッションからログオフする。これによりセッションが終了し、実行中のアプリケーションが終了します。
- セッションから切断する。これにより、アプリケーションを実行したまま（切断時にアプリケーションを閉じるようにサーバーを構成していない場合）、選択したコネクションのサーバー接続が切断されます。
- コネクションの転送統計値を参照する。

コネクションを管理するには

1. Receiverメニューで［コネクションセンター］を選択します。
   接続先のサーバーと、各サーバー上でアクティブなセッションが表示されます。

2. 次のいずれかを行います。
   - サーバーを選択して、切断またはログオフしたり、プロパティを表示したりします。
   - 個々のデスクトップまたはアプリケーションを選択して、ウィンドウを閉じます。

構成ファイルを使ったReceiverのカスタマイズ

Receiverの構成ファイルを編集すると、高度な設定や一般的ではない設定を変更できます。これらの構成ファイルは、wficaの起動時に毎回読み取られます。変更する内容により、異なる構成ファイルを編集できます。

セッション共有が有効な場合は、更新した構成ファイルに基づくセッションが作成される代わりに既存のセッションが使用されることがあります。この場合、更新した構成ファイルの設定はセッションに反映されません。

すべてのReceiverユーザーに変更を適用する

Receiverのすべてのユーザーに変更を適用する場合は、$ICAROOT/configディレクトリ内のmodule.ini構成ファイルを編集します。
注：module.iniの値をほかの構成ファイルで上書きする場合を除き、module.iniの構成値のエントリをAll_Regions.iniに追加する必要はありません。All_Regions.iniのエントリでデフォルト値を設定すると、その設定に対するmodule.iniの値は使用されません。

新しいReceiverユーザーに変更を適用する

Receiverのすべての新しいユーザーに変更を適用する場合は、$ICAROOT/configディレクトリ内の構成ファイルを編集します。すべてのコネクションに変更を適用する場合は、このディレクトリ内のwfclient.iniを更新します。

特定のユーザーのすべてのコネクションに変更を適用する

特定のユーザーのすべてのコネクションに変更を適用する場合は、そのユーザーの$HOME/.ICAClientディレクトリ内のwfclient.iniファイルを編集します。この構成ファイルによる設定は、そのユーザーの新しいコネクションに適用されます。

構成ファイルエントリを検証する

wfclient.iniのエントリの値を制限するには、設定可能な値またはその範囲をAll_Regions.iniで指定できます。詳しくは、$ICAROOT/configディレクトリ内のAll_Regions.iniファイルを参照してください。

注：module.iniとwfclient.iniで同一エントリに対する値を設定すると、wfclient.iniの値が優先されます。

構成ファイルのパラメーターについて

各構成ファイルのパラメーターは、セクションでグループ化されています。各セクションの冒頭には、角かっこで囲まれたセクション名（クライアント側ドライブのマッピングに関するパラメーターの[ClientDrive]など）が記述されています。

特に注記がある場合を除き、記述されていないパラメーターには自動的にデフォルト値が適用されます。パラメーターに値が設定されていない場合も、自動的にデフォルト値が適用されます。たとえば、「InitialProgram=」の後に値が記述されていない場合、デフォルトの設定である「ログオン後にプログラムを実行しない」が適用されます。

優先順位

All_Regions.iniにより、ほかの構成ファイルに設定可能なパラメーターが指定されます。設定可能な値の範囲を指定したり、特定の値を指定したりできます。すべてのReceiverユーザーに適用される設定を変更するには、module.iniを編集します。

通常、構成ファイルは以下の順序でチェックされます。

1. All_Regions.ini。この構成ファイルの値は、以下のファイルの値よりも優先されます。
   - コネクションのICAファイル
   - wfclient.ini
2. module.ini。この構成ファイルの値は、All_Regions.ini、コネクションのICAファイル、またはwfclient.iniで設定されておらず、All_Regions.iniで制限されていない場合に適用されます。

いずれの構成ファイルでも設定されていない場合は、Receiverのデフォルト設定が適用されます。

注：上記の優先順位には例外があります。たとえば、セキュリティ上の理由から、サーバーの設定が適用されないように、一部の値がwfclient.iniから読み取られる場合があります。

Web Interfaceを使用したCitrix XenApp接続の構成

このトピックの内容は、Web Interface環境にのみ適用されます。

Citrix XenAppを使用すると、ユーザーがXenApp Servicesサイト経由で公開リソース（公開アプリケーション、公開デスクトップ、および公開コンテンツ）に接続できるようになります。また、Citrix XenAppによって、公開リソースにアクセスするためのメニューおよびデスクトップアイテムが自動的に作成されます。

ネットワーク上でCitrix XenAppを実行しているすべてのユーザーに対してカスタマイズ可能なオプションは、構成ファイルのconfig.xmlで定義されます。このファイルは、Web Interfaceサーバー上に格納されています。ユーザーがCitrix XenAppを起動すると、このサーバーから構成データが読み取られます。その後、Citrix XenAppは設定およびユーザーインターフェイスをconfig.xmlファイルで指定された間隔で定期的に更新します。

重要：config.xmlの設定は、Web Interfaceサーバーで定義されたすべてのコネクションに適用されます。

コンテンツの公開

通常、Receiverではアプリケーションやデスクトップに接続します。さらに、アプリケーションに関連付けられている特定のファイルを開くこともできます。この場合、管理者はアプリケーションではなくてファイルを公開します。この処理はコンテンツの公開と呼ばれ、ネットワークユーザーと電子情報を共有する場合に便利です。

Receiverにより認識されるファイルのタイプには制限があります。システム上で公開コンテンツのファイルタイプが認識され、ユーザーがReceiverを使用してそのコンテンツを表示するためには、そのファイルタイプに関連付けられたアプリケーションが公開されている必要があります。たとえば、公開されたAdobe PDFファイルをReceiverで表示するには、Adobe PDFビューアーなどのアプリケーションが公開されている必要があります。適切なアプリケーションが公開されていない場合、ユーザーは公開コンテンツを表示できません。

Receiver環境の最適化

Nov 19, 2015

環境を最適化することで、Receiverのパフォーマンスおよびユーザーエクスペリエンスを向上させることができます。次のことを実行することで、パフォーマンスを向上させて最適化できます。

- クライアント側デバイスのマッピング
- USBサポートの構成
- 狭帯域幅接続でのパフォーマンスの向上
- マルチメディアパフォーマンスの向上
- 画面タイルのパフォーマンスの最適化

クライアント側デバイスのマッピング

Nov 19, 2015

Receiverは、XenAppおよびXenDesktopサーバーへの接続に対してクライアントデバイスのマッピングをサポートします。クライアントデバイスのマッピングによって、サーバー上で実行しているリモートアプリケーションから、ローカルのユーザーデバイスに接続しているデバイスにアクセスできるようになります。ユーザーデバイスのユーザーには、アプリケーションやシステムなどのリソースがローカルで実行されているように表示されます。クライアントデバイスのマッピングを実行する前に、サーバーでこの機能をサポートしていることを確認してください。

注：
SELinux（Security-Enhanced Linux）のセキュリティモジュールにより、XenAppおよびXenDesktopのクライアント側ドライブのマッピング機能とUSBリダイレクト機能が正しく動作しなくなることがあります。これらの機能を使用する場合は、サーバー上でこれらの機能を構成する前にSELinuxを無効にしてください。

クライアント側ドライブのマッピング

クライアント側ドライブのマッピング機能により、XenAppまたはXenDesktopサーバーのドライブ文字をローカルユーザーデバイスにあるディレクトリにリダイレクトできます。たとえば、Citrixユーザーセッション内で表示されるHドライブにアクセスしたときに、ローカルユーザーデバイスの特定のディレクトリにリダイレクトされるように設定できます。

クライアントドライブマッピングにより、CD-ROM、DVD、またはUSBメモリスティックなど、セッションにおいてユーザーが使用できるローカルユーザーデバイスにマウントされた任意のディレクトリに、ローカルユーザーがアクセスする権限を提供できます。サーバーでクライアント側ドライブのマッピングが許可されている場合、ユーザーはセッション内で各自のローカルファイルを読み込んで、再びローカルドライブに保存したり、サーバーのドライブに保存したりできます。

2種類のドライブマッピングを実行できます。

- 静的なクライアントドライブマッピングでは、ログオン時にユーザーデバイスの任意のファイルシステムがサーバー上の特定のドライブ文字にマップされるように設定できます。たとえば、CD-ROM、DVD、またはUSBメモリスティックなどのハードウェアデバイスのマウントポイントだけでなく、ユーザーのホームディレクトリや/tmpディレクトリのすべてまたは一部分をマップできます。
- 動的なクライアントドライブマッピングでは、CD-ROMドライブ、DVDドライブ、USBメモリスティックなどのハードウェアデバイスがマウントされるユーザーデバイス上のディレクトリが監視され、セッション内で追加した新しいデバイスが、サーバーで使用可能な最初のドライブ文字に自動的にマップされます。

クライアント側デバイスのマッピングを無効にしない限り、ReceiverがXenAppやXenDesktopに再接続したときに、マッピングが再確立されます。ポリシーを使用すると、クライアント側デバイスのマッピングを詳細に制御できます。詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

ユーザーがドライブマッピングを設定するときは、［環境設定］ダイアログボックスを使用します。詳しくは、「環境設定」を参照してください。

注：デフォルトでは、静的なクライアントドライブマッピングを有効にすると自動的に動的なクライアントドライブマッピングも有効になります。静的なクライアントドライブマッピングを有効にして動的なクライアントドライブマッピングを無効にするには、wfclient.iniでDynamicCDMにFalseを設定します。

クライアントプリンターのマッピング

Receiverは、ネットワークプリンターおよびユーザーデバイスにローカルで接続されているプリンターへの出力をサポートします。デフォルトでは、ポリシーを作成して変更しない限り、XenAppにより次のことを実行できます。

- ユーザーデバイスからアクセス可能なすべてのプリントデバイスに出力する
- プリンターを追加する

ただし、これらの設定はすべての環境に対して最適な設定とはならない可能性があります。たとえば、ユーザーデバイスからアクセスできるすべてのプリンターへの出力が可能なデフォルトの設定は、最も管理しやすい設定ですが、一部の環境ではログオン時間に時間がかかる要因となる可能性があります。このような状況では、ユーザーデバイス上で構成されたプリンターの一覧に制限するようにします。

また、組織のセキュリティポリシーによっては、ローカルプリンターポートのマッピングを禁止しなければならない場合があります。これを行うには、サーバーのICAポリシーで［クライアントCOMポートを自動接続する］設定で［無効］を選択します。

ユーザーデバイス上で構成されたプリンターの一覧を制限するには

1. 次のいずれかの場所にある構成ファイル（wfclient.ini）を開きます。
   - $HOME/.ICAClient（1人のユーザーに対するプリンターを制限する場合）
   - $ICAROOT/configディレクトリ（すべてのユーザーのプリンターを制限する場合。すべてのユーザーとは、構成ファイルの変更後にselfserviceプログラムを初めて使用するすべてのReceiverユーザーを指します）
2. ［WFClient］セクションに、次のパラメーターを入力します。
   ClientPrinterList=<printer1>:<printer2>:<printer3>

   ここで<printer1>、<printer2>などは、選択したプリンターの名前です。各プリンターをコロン（:）で区切って指定します。

3. ファイルを保存して閉じます。

XenApp for Windowsでのクライアントプリンターマッピング

Receiver for LinuxはCitrix PSユニバーサルプリンタードライバーをサポートします。そのためほとんどの場合、ネットワークプリンターまたはユーザーデバイスにローカルで接続されているプリンターへの出力をユーザーがローカルで構成する必要はありません。ただし、ユーザーデバイスのプリントソフトウェアがユニバーサルプリンタードライバーをサポートしていない場合などは、XenApp for Windows上でクライアントプリンターを手動でマップする必要があります。

サーバーにローカルプリンターをマップするには

1. Receiverでサーバーへのセッションを開始して起動し、XenAppサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［設定］>［プリンター］の順に選択します。
3. ［ファイル］メニューから［プリンターの追加］を選択します。
4. ウィザードを使って、クライアントネットワークやクライアントドメインからネットワークプリンターを追加します。ほんどの場合、ネイティブのリモートデスクトップサービスで作成される「セッション3の<クライアント名>からのHP LaserJet 4」などの標準のプリンター名となります。

XenApp for UNIXでのクライアントプリンターマッピング

UNIX環境では、Receiverにより定義されたプリンタードライバーは無視されます。ユーザーデバイスのプリントシステムは、アプリケーションにより生成された出力形式を制御できる必要があります。

ユーザーがCitrix XenApp for UNIX（日本語版はリリースされていません）からクライアントプリンターに出力できるようにするには、事前に管理者が印刷機能を有効にしておく必要があります。詳しくは、eDocsの「XenApp for UNIX」を参照してください。

クライアントオーディオマッピング

クライアントオーディオマッピングにより、XenAppサーバー上で実行しているアプリケーションのサウンドを、ユーザーデバイスにインストールされているサウンドデバイスで再生できます。管理者はXenAppサーバーで接続ごとに音質レベルを設

定できますが、ユーザーもユーザーデバイスで音質レベルを設定できます。ユーザーデバイスとサーバーの音質レベルの設定が異なる場合は、低い方の音質レベルが使用されます。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。音質を高くすると、オーディオデータの伝送により多くの帯域幅が必要になります。また高音質にするとサーバーのCPUもより多く使用します。

クライアントオーディオマッピングは、ポリシーを使用して構成します。詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

注：クライアントオーディオマッピングは、Citrix XenApp for UNIX（日本語版未発表）に接続する場合はサポートされません。

非デフォルトのオーディオデバイスを設定するには

デフォルトのオーディオデバイスは、一般的にはシステムに対して構成されているデフォルトのALSAデバイスです。次の方法を使って、別のデバイスを指定します。

1. 変更を適用するユーザーの構成ファイルを選択して開きます。ほかのユーザーに適用される特定の設定ファイルを更新する方法については、「設定ファイルを使ったReceiverのカスタマイズ」を参照してください。
2. 次のオプションを追加して、必要に応じてセクションを作成します。

[ClientAudio]

AudioDevice = <device>

ここで<device>情報は、オペレーティングシステム上のALSA構成ファイルにあります。
注：この情報の場所は、すべてのLinuxオペレーティングシステムでの標準ではありません。この情報の場所について詳しくは、オペレーティングシステムドキュメントを参照してください。

USBサポートの構成

Nov 19, 2015

USBサポート機能により、ユーザーが仮想デスクトップ上で作業しているときにさまざまな種類のUSBデバイスを使用できるようになります。ユーザーがコンピューターにUSBデバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。この機能では、フラッシュドライブ、スマートフォン、PDA、プリンター、スキャナー、MP3プレーヤー、セキュリティデバイス、およびタブレットなどのUSBデバイスがサポートされます。

Webカメラ、マイク、スピーカー、およびヘッドセットなどのUSBデバイスのアイソクロナス機能は、一般的な高速LAN環境でサポートされます。これにより、Microsoft Office CommunicatorやSkypeなどのパッケージでこれらのデバイスを使用できるようになります。

XenDesktopセッションでは次の種類のデバイスは直接サポートされるため、USBサポート機能は使用されません。

- キーボード
- マウス
- スマートカード
- ヘッドセット
- Webカメラ

注：特殊用途のUSBデバイス（Bloombergキーボードや3Dマウスなど）では、USBサポート機能が使用されるように構成できます。そのほかの特殊用途のUSBデバイスのポリシー規則の構成について詳しくは、CTX120292を参照してください。
デフォルトでは、特定の種類のUSBデバイスがXenDesktopセッションで動作しないように設定されています。たとえば、内部USBでシステムボードに装着されたネットワークインターフェイスカードは、リモートで動作する仮想デスクトップでの使用には適しません。次の種類のUSBデバイスは、XenDesktopセッションでの使用をデフォルトでサポートしていません。

- Bluetoothドングル
- 統合ネットワークインターフェイスカード
- USBハブ

リモート操作可能なUSBデバイスのデフォルトの一覧を更新するには、$ICAROOT/にあるusb.confファイルを変更します。詳しくは、「リモートで実行できるUSBデバイスの一覧の更新」を参照してください。

エンドポイント側のUSBデバイスを仮想デスクトップ内で使用できるようにするには、USBポリシー規則を有効にする必要があります。詳しくは、XenDesktopのドキュメントを参照してください。

USBサポートのしくみ

ユーザーがエンドポイントにUSBデバイスを接続すると、USBポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。USBポリシーで拒否されるデバイスは、ローカルのデスクトップ上でのみ使用可能になります。

デスクトップアプライアンスモードを介してアクセスするデスクトップでは、ユーザーがUSBデバイスを接続すると自動的に仮想デスクトップで使用可能になります。USBドライブの制御と表示は、仮想デスクトップにより処理されます。

マスストレージデバイス

USBマスストレージデバイスがローカルデスクトップに接続されたままユーザーが仮想デスクトップを切断した場合、その仮想デスクトップに再接続してもマスストレージデバイスは接続されません。マスストレージデバイスが仮想デスクトップに接続されるようにするには、仮想デスクトップへの再接続後にマスストレージデバイスをいったん取り外してから再度接続す

必要があります。

注：USBマスストレージデバイスのリモートサポートを拒否するように構成されているLinuxワークステーションにマスストレージデバイスを接続する場合、Receiverソフトウェアによりデバイスが受け入れられず、別のLinuxファイルブラウザーが開きます。そのためユーザーデバイス上では、事前にリムーバブルストレージの［メディアが挿入されたら参照する］設定を無効にしておくことをお勧めします。たとえばDebianベースのデバイスでは、Debianメニューバーで［システム］>［設定］>［リムーバブルデバイスとメディア］の順に選択し、［ストレージ］タブの［リムーバブルストレージ］で［メディアが挿入されたら参照する］チェックボックスをオフにします。
注：［クライアントUSBデバイスリダイレクト］サーバーポリシーを有効にすると、クライアントドライブマッピングが有効な場合でもマスストレージデバイスは常にUSBデバイスとして送信されます。

Webカメラ

デフォルトでは、HDX RealTime Webカメラビデオ圧縮機能によりWebカメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーがUSBサポート機能を使ってWebカメラを接続しなければならない場合があります。この場合、管理者がHDX RealTime Webカメラビデオ圧縮を無効にする必要があります。詳しくは、「HDX RealTime Webカメラビデオ圧縮の構成」を参照してください。

スタートアップモードの構成

デスクトップアプライアンスモードを使って、仮想デスクトップを開始したときに既に接続されているクライアント側のUSBデバイスを有効にしたり無効にしたりできます。これを行うには、各ユーザーデバイスで$ICAROOT/config/module.iniファイルを開き、DesktopApplianceMode = Booleanを以下のように設定します。

TRUE	開始時に接続されているすべてのUSBデバイスが使用可能になります（サーバー（レジストリ）またはユーザーデバイス（構成ファイル）のUSBポリシーで許可されている場合）。
FALSE	USBデバイスは使用可能になりません。

デフォルトで許可されるUSBクラス

次のUSBデバイスのクラスは、デフォルトのUSBポリシー規則により許可されます。

オーディオ（クラス01）

マイク、スピーカー、ヘッドセット、およびMIDIコントローラーがあります。

物理的インターフェイス（クラス05）

このデバイスはHIDに似ていますが、一般的にはリアルタイムの入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。

静止画（クラス06）

このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。ほとんどのデジタルカメラは、画像転送プロトコル（PTP）またはメディア転送プロトコル（MTP）を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。また、デジタルカメラはマスストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

カメラがマスストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USBサポートは必要ありません。

プリンター（クラス07）

一部のプリンターではベンダー固有のプロトコル（クラスff）が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USBハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーやFAX機能では静止画などの別のクラスが使用されます。

プリンターは通常、USBサポートなしで適切に動作します。

マスストレージデバイス（クラス08）

最も一般的なマスストレージデバイス（大容量記憶装置）として、USBフラッシュドライブがあります。そのほかには、USB接続のハードドライブ、CD/DVDドライブ、およびSD/MMCカードリーダーがあります。マスストレージインターフェイスを示す、メディアプレーヤー、デジタルカメラ、および携帯電話など、内部ストレージを持つさまざまな種類のデバイスがあります。既知のサブクラスには次のものが含まれます。

- 01 制限付きフラッシュデバイス
- 02 一般的なCD/DVDデバイス（ATAPI/MMC-2）
- 03 一般的なテープデバイス（QIC-157）
- 04 一般的なフロッピーディスクドライブ（UFI）
- 05 一般的なフロッピーディスクドライブ（SFF-8070i）
- 06 ほとんどのマスストレージデバイスはこのSCSIのバリエーションを使用します

マスストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USBサポートは必要ありません。

重要：ウィルスプログラムの中には、あらゆる種類のマスストレージデバイスを媒体にして活発に増殖するものがあります。クライアントドライブマッピングまたはUSBサポートのいずれかを介してマスストレージデバイスの使用を許可する必要があるかどうか、注意深く考慮してください。このリスクを減らすため、クライアントドライブマッピングによりファイルが実行されるのを防ぐようにサーバーが構成されている可能性があります。

コンテンツセキュリティ（クラス0d）

通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。

ビデオ（クラス0e）

このクラスのデバイスとして、ビデオ、Webカメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。

パーソナルヘルスケア（クラス0f）

このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。

アプリケーションおよびベンダー固有（クラスfeおよびff）

多くのデバイスがベンダー独自のプロトコルまたはUSBコンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有（クラスff）として分類されます。

デフォルトで拒否されるUSBデバイスのクラス

次のUSBデバイスのクラスは、デフォルトのUSBポリシー規則により拒否されます。

通信およびCDCコントロール（クラス02および0a）

モデム、ISDNアダプター、ネットワークアダプター、一部の電話およびFAX機器があります。

仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトのUSBポリシーでは
これらのデバイスのリモートでの実行は許可されていません。

ヒューマンインターフェイスデバイス（クラス03）

さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス（HID）として、キーボード、
マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、および
ントロール機能などがあります。

Subclass 01は起動インターフェイスクラスと呼ばれ、キーボードおよびマウスで使用されます。

デフォルトのUSBポリシーはUSBキーボード（クラス03、サブクラス01、プロトコル1）またはUSBマウス（クラス03、サブ
ラス01、プロトコル2）を許可しません。これは、ほとんどのキーボードおよびマウスはUSBサポートなしでも適切に処理さ
れ、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。

USBハブ（クラス09）

USBハブにより、追加のデバイスをローカルコンピューターに接続できます。これらのデバイスにリモートでアクセスする必
要はありません。

スマートカード（クラス0b）

スマートカードリーダーには、非接触式および接触式のスマートカードリーダーがあり、また埋め込みスマートカード同等
チップがあるUSBトークンもあります。

スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USBサポートは必要ありません。

ワイヤレスコントローラー（クラスe0）

このクラスのデバイスとして、ウルトラワイドバンドコントローラーやBluetoothなど、さまざまなワイヤレスコントロー
ラーがあります。

これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetoothキーボードやマウスなどの基幹周辺
装置を接続していたりするものがある場合があります。

デフォルトのUSBポリシーはこれらのデバイスを許可していません。ただし、USBサポートを使ったアクセスに適したデバイ
スもあります。

仮想デスクトップで使用できるUSBデバイスの一覧の変更

ユーザーデバイスの$ICAROOT/にあるusb.confファイルに含まれるデフォルト規則の一覧を変更して、デスクトップへリモー
トで実行できるUSBデバイスの範囲を更新できます。

新しいポリシー規則を追加して一覧を更新し、デフォルト範囲に含まれないUSBデバイスを許可または拒否します。管理者が
作成する規則は、仮想デスクトップの開始時にデフォルトの規則よりも先に適用されます。これにより、XenDesktopのデ
フォルトの規則を上書きできます。

デバイスのリモートでの実行を許可しないためのデフォルトポリシー構成は次のとおりです。

DENY: class=09 # Hub devices

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

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless Controllers

DENY: class=02 # Communications and CDC Control

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC Data

ALLOW: # Ultimate fallback: allow everything else

USBポリシー規則の作成

ヒント：新しいポリシー規則を作成する場合、USB Webサイト（http://www.usb.org/）でUSBクラスコードを参照してください。
ユーザーデバイス上のusb.confファイルで指定するポリシー規則は、{ALLOW:|DENY:}に次のタグの値をベースとした式セットが付いた形式にします。

タグ	説明
VID	デバイス記述子のベンダーID
REL	デバイス記述子のリリースID
PID	デバイス記述子の製品ID
Class	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイル記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

新しいポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の最後に、"#"で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切りとして使用されるスペースは無視されますが、番号または識別子の間にスペースを入れることはできません。たとえば、Deny: Class=08 SubClass=05は有効な規則ですが、Deny: Class=0 8 Sub Class=05は無効です。
- タグは合致を意味する演算子の"="を使用する必要があります。例えば、VID=1230です。

例

次の例は、ユーザーデバイス上のusb.confファイルのセクションを示しています。これらの規則を実装するには、サーバー上に同じ規則のセットがある必要があります。

ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive

```
DENY: Class=08 SubClass=05 # Mass Storage Devices

Class=0D # All Security Devices
```

狭帯域幅接続でのパフォーマンスの向上

Nov 19, 2015

サーバー上ではXenAppまたはXenDesktop、ユーザーデバイスではReceiverのそれぞれ最新バージョンを使用することを推奨します。

帯域幅の狭い接続を使用する場合は、Receiverの構成や使い方を変えてパフォーマンスを向上させることができます。

- **Receiverの接続構成** - Receiverの接続構成を変更することで、ICAで消費される帯域幅を減らしてパフォーマンスを改善できます。
- **Receiverの使用方法** - Receiverの使用方法を変更することで、高いパフォーマンスが求められる接続での消費帯域幅を抑えることができます。
- **UDPオーディオの有効化** - この機能を有効にすると、ネットワークトラフィック負荷の高いVoIP（Voice over IP）接続での遅延レベルが安定します。
- **最新バージョンのXenAppおよびReceiver for Linuxの使用** - Citrix製品では、パフォーマンスを向上して機能を拡張するためのバージョンアップが常に行われています。また、多くのパフォーマンス機能を使用するには、最新のReceiverおよびサーバーソフトウェアが必要である場合もあります。

コネクションの構成

デバイスのプロセッサの処理能力や接続に使用する帯域幅が限られている場合は、使用する機能とパフォーマンスのバランスを考慮する必要があります。ユーザーおよび管理者は、パフォーマンスを低下させずに多くの機能を利用できるように、構成を変更することができます。サーバーまたはユーザーデバイスで次の変更を行うと、接続に必要な帯域幅を減らしてパフォーマンスを向上させることができます。

- **SpeedScreenの有効化** - SpeedScreenを有効にすると、遅延時間の長いネットワーク接続でも、ユーザーの入力やマウスのクリックに対する反応時間が短くなります。この構成は、サーバー上でSpeedScreen管理ツールを使用して行います。Receiverにおいてデフォルトでは、これはキーボード操作に対しては無効になっており、遅延時間の長いネットワーク接続のおけるマウス操作に対してのみ有効です。詳しくは、『*— Citrix Receiver for Linux OEM's Reference Guide*』を参照してください。
- **データ圧縮の有効化** - データを圧縮すると、接続を介して転送されるデータ量が減少します。これにはデータの圧縮と展開を行うためのプロセッサリソースが必要になりますが、低帯域幅接続でのパフォーマンスを向上させることができます。この機能を有効にするには、Citrixポリシーの［音質］および［イメージ圧縮］設定を使用します。
- **ウィンドウサイズの縮小** - ウィンドウサイズを必要最小限に抑えます。XenApp Servicesサイトで、［セッションオプション］を設定します。
- **表示色数の変更** - 表示色数を256色に変更します。XenApp Servicesサイトで、［セッションオプション］を設定します。
- **音質の変更** - サウンドのサポート機能を使用する場合は、Citrixポリシーの［音質］設定で音質を下げます。

UDPオーディオの有効化

UDPオーディオ機能を有効にすると、インターネット接続を介した通話品質が向上します。この機能では、TCP（Transmission Control Protocol）の代わりにUDP（User Datagram Protocol）が使用されます。

以下の点に注意してください。

- 暗号化されたセッション（TLSまたはSecureICAを使用するセッション）では、UDPオーディオを使用できません。このようなセッションでは、TCP上でオーディオデータが転送されます。
- ICAチャネルの優先度により、UDPオーディオの動作が異なります。

1. module.iniファイルのClientAudioセクションで、以下のオプションを設定します。

- EnableUDPAudioにTrueを指定します。デフォルトではFalseが設定されており、UDPオーディオが無効になります。
- UDPAudioPortLowおよびUDPAudioPortHighに、UDPオーディオで使用されるポート番号の最小値および最大値を指定します。デフォルトでは、ポート16500～16509が使用されます。

2. 中レベルの音質が適用されるように、クライアント側およびサーバー側のオーディオ設定を以下のように構成します。

		クライアント側の音質レベル		
		高	中	低
サーバー側の音質レベル	高	高	中	低
	中	中	中	低
	低	低	低	低

UDPオーディオを有効にしても、中レベルの音質が適用されない場合はTCPが使用されます。

Receiverの使用方法

ICA技術は高度に最適化されているため、通常、処理能力の高いCPUを搭載したクライアントデバイスや広い帯域幅を必要としません。ただし、接続の帯域幅が非常に狭い接続では、適切なパフォーマンスを得るために、次のことを考慮してください。

- **クライアント側ドライブ上のサイズの大きいファイルにはアクセスしない。**クライアントドライブマッピングを使ってファイルにアクセスすると、サーバーとの接続でそのファイルのデータが転送されることになります。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。
- **クライアント側のローカルプリンターで大きな文書を印刷しない。**クライアント側のローカルプリンターで文書を印刷すると、サーバーとの接続でそのファイルのデータが転送されることになります。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。
- **マルチメディアコンテンツを再生しない。**マルチメディアファイルを再生するには、広い帯域幅が必要です。そのため、パフォーマンスが低下する可能性があります。

マルチメディアパフォーマンスの向上

Nov 19, 2015

Receiverには、メディアリッチな今日のユーザー環境に高品位なユーザーエクスペリエンスを提供する幅広い技術セットが含まれています。ホストされるアプリケーションやデスクトップに接続すると、ユーザーエクスペリエンスが向上します。

HDX MediaStream Windows Mediaリダイレクトを実行すると、Linuxユーザーデバイスでアクセスする仮想Windowsデスクトップでマルチメディア再生時の帯域幅が軽減されます。HDX MediaStream Windows Mediaリダイレクトは、サーバーではなくユーザーデバイスでメディアランタイムファイルを再生し、マルチメディアファイルの再生に必要な帯域幅を減少させるメカニズムです。

HDX MediaStream Windows Mediaリダイレクトは、仮想Windowsデスクトップで実行中のWindows Media Playerおよび互換プレーヤーのパフォーマンスを向上させます。次の形式を含む、さまざまなファイル形式をサポートしています。

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAVサウンドファイル

Receiverには、Windows用のメディア形式であるGUIDをGStreamer用のMIMEタイプに変換するためのテキストベースの変換テーブルであるMediaStreamingConfig.tblが含まれています。この変換テーブルは、以下の目的で編集できます。

- 不明またはサポートされないメディアフィルター/ファイル形式を変換テーブルに追加する。
- 問題が生じるGUIDをブラックリストに追加して、強制的にサーバー側でレンダリングされるようにする。
- GStreamerパラメーターの変更により問題のある形式をトラブルシューティングできるようにするため、追加のパラメーターを既存のMIME文字列に追加する。
- ユーザーデバイス上のGStreamerによりサポートされているメディアファイルの種類に応じて、カスタムの構成を管理および展開する。

クライアント側でのコンテンツ取得機能を使用すると、http://、mms://、およびrtsp://形式のURLからのストリーム配信メディアを、Citrixサーバーを介さずにユーザーデバイスで直接取得できます。サーバーは、ユーザーデバイスをメディアに接続して、再生、一時停止、停止、音量、シークなどの制御コマンドを送信するだけで、メディアデータの処理は行いません。この機能を使用するには、ユーザーデバイス上に高度なマルチメディアGStreamerライブラリをインストールする必要があります。

Windows Mediaリダイレクトを実装するには

1. オープンソースのマルチメディアフレームワークであるGStreamerを各ユーザーデバイス上にインストールします。通常、Receiverよりも前にGStreamerをインストールします。
   ほとんどのLinuxディストリビューションにはGStreamerが含まれています。または、http://gstreamer.freedesktop.orgからGStreamerをダウンロードできます。

2. クライアント側でのコンテンツ取得機能を有効にするには、再生するメディアのファイルタイプに対応するGStreamerのプロトコルソースプラグインをインストールします。このプラグインのインストールおよび動作を確認するには、gst-launchユーティリティを使用します。このプラグインが正しくインストールされている場合、gst-launchでURLのマルチメディアを再生できます。たとえば、次のコマンドを実行します。gst-launch-0.10 playbin2 uri=http://example-source/file.wmvビデオが正しく再生されるかチェックします。
3. Receiverをインストールするときに、GStreamerオプションを選択します。

クライアント側でのコンテンツ取得機能を使用する場合は、次のことに注意してください。

- この機能は、デフォルトで有効になります。無効にするには、All-Regions.iniファイルのMultimediaセクションにあるSpeedScreenMMACSFEnabledオプションを使用します。ここでFalseを指定すると、Windows Mediaリダイレクト機能が使用されます。
- デフォルトでは、すべてのMediaStream機能でGStreamerのplaybin2プロトコルが使用されます。従来のplaybinプロトコルが使用されるようにするには、All-Regions.iniファイルのMultimediaセクションにあるSpeedScreenMMAEnablePlaybinオプションを使用します。ただし、クライアント側でのコンテンツ取得機能では常にplaybin2プロトコルが使用されます。
- Receiverでは、.asxや.nscなどのストリーム構成情報ファイルや再生リストファイルを認識できません。可能な場合は、これらのファイルを参照しない標準的なURLをユーザーが指定する必要があります。URLが有効かどうかは、gst-launchを使用して確認できます。

HDX MediaStream Flashリダイレクトを構成するには

HDX MediaStream Flashリダイレクトにより、Adobe Flashコンテンツがユーザーデバイス上でローカルに再生され、帯域幅要件を増やすことなく高品位な音声やビデオの再生機能が提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。詳しくは、 必要なシステム」を参照してください。
2. wfclient.iniの[WFClient]セクション（特定ユーザーのすべてのコネクションに適用する場合）またはAll_Regions.iniの[Client Engine\Application Launching]セクション（環境内のすべてのユーザーに適用する場合）に、以下のパラメーターを追加します。
   - **HDXFlashUseFlashRemoting=Ask | Never | Always**
     ユーザーデバイス上でHDX MediaStream for Flashを有効にします。デフォルトでは、**Ask**に設定されています。これにより、FlashコンテンツのWebページに接続したときに、そのコンテンツを最適化するかどうかを確認するダイアログボックスが開きます。
   - **HDXFlashEnableServerSideContentFetching=Disabled | Enabled**
     サーバー側でのコンテンツ取得機能を有効または無効にします。デフォルトでは、**Disabled**に設定されています。
   - **HDXFlashUseServerHttpCookie=Disabled | Enabled**
     HTTP Cookieのリダイレクトを有効または無効にします。デフォルトでは、**Disabled**に設定されています。
   - **HDXFlashEnableClientSideCaching=Disabled | Enabled**
     Receiverにより取得されたWebコンテンツのクライアント側キャッシュを有効または無効にします。デフォルトでは、**Enabled**に設定されています。
   - **HDXFlashClientCacheSize= [25-250]**
     クライアント側でのキャッシュのサイズを、MB単位で定義します。この値は、25～250MBの間で定義できます。サイズが制限値に到達すると、キャッシュ内の既存のコンテンツが削除され、新しいコンテンツが保存されます。デフォルトでは、**100**に設定されています。
   - **HDXFlashServerSideContentCacheType=Persistent | Temporary | NoCaching**
     サーバー側でのコンテンツ取得機能により取得されたコンテンツのキャッシュの種類を定義します。デフォルトでは、**Persistent**に設定されています。
     注：このパラメーターは、**HDXFlashEnableServerSideContentFetching**を**Enabled**に設定した場合にのみ必要です。
3. Flashコンテンツの再生ウィンドウの内側および外側でキーボードやマウスを使用できるようにするには、/config/module.iniのFlashV2=OffをFlashV2=Onに変更します。

HDX RealTime Webカメラビデオ圧縮の構成

HDX RealTime機能のWebカメラビデオ圧縮オプションを使用すると、ビデオ会議で消費される帯域幅を効率化できます。これにより、GoToMeeting HD Faces、Skype、またはMicrosoft Office Communicatorなどのアプリケーションを使用するとき

に最適なパフォーマンスが提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。
2. マルチメディア仮想チャネルを有効にする必要があります。これを実行するには、$ICAROOT/configディレクトリにあるmodule.ini構成ファイルを開き、[ICA3.0]セクションのMultiMediaを"On"に設定します。
3. オーディオ入力を有効にするには、［環境設定］ダイアログボックスの［マイクとWebカメラ］ページで、［マイクとWebカメラを使用する］をクリックします。

HDX RealTime Webカメラビデオ圧縮の無効化

デフォルトでは、HDX RealTime Webカメラビデオ圧縮機能によりWebカメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーがUSBサポート機能を使ってWebカメラを接続しなければならない場合があります。これを実行するには、次の手順を実行する必要があります：

- HDX RealTime Webカメラビデオ圧縮を無効にする
- WebカメラのUSBサポートを有効にする

1. 次のパラメーターを適切なINIファイルの[WFClient]セクションに追加する :HDXWebCamEnabled=Off
   詳しくは、「構成ファイルを使ったReceiverのカスタマイズ」を参照してください。

2. usb.confファイルを開きます。通常このファイルは、$ICAROOT/usb.confにあります。
3. 次の行を削除するか、コメントアウトします。
   DENY: class=0e # UVC (default via HDX RealTime Webcam Video Compression)
4. ファイルを保存して閉じます。

H.264サポートの構成

Receiverでは、XenDesktop 7で配信されるHDX 3D Proグラフィックを含むH.264グラフィックがサポートされます。この機能では、デフォルトで有効になっている深圧縮コーデックが使用されます。これにより、専門的なグラフィック処理アプリケーションをWANネットワークを介して使用する場合でも、既存のJPEGフォーマットよりも高いパフォーマンスが提供されます。

この機能を無効にする（つまりグラフィックをJPEGコーデックで処理する）には、このトピックの手順に従ってください。深圧縮コーデックを有効にしたまま、テキストトラッキングを無効にすることもできます。グラフィックに含まれるテキストが多くないまたは重要でない場合は、テキストトラッキングを無効にすることにより、複雑なグラフィック処理時のCPU負荷を軽減できます。

重要：この機能を構成する場合は、XenDesktopのポリシーの［表示品質］設定で無損失品質を指定しないでください。無損失品質を指定するとサーバー側のH.264エンコーディングが無効になり、Receiverでこの機能が動作しなくなります。

深圧縮コーデックのサポートを無効にするには

- wfclient.iniで、H264EnabledにFalseを設定します。これにより、テキストトラッキングも無効になります。

テキストトラッキングのみを無効にするには

- 深圧縮コーデックのサポートを有効にしたまま、wfclient.iniでTextTrackingEnabledにFalseを設定します。

画面タイルのパフォーマンスの最適化

Nov 19, 2015

Direct-to-Screenビットマップデコード、バッチタイルデコード、およびXSyncの待機機能を使用すると、JPEGエンコードの画面タイルの処理パフォーマンスを最適化できます。

1. JPEGライブラリがこれらの機能をサポートすることを確認します。
2. wfclient.iniの[Thinwire3.0]セクションで、DirectDecodeおよびBatchDecodeにTrueを指定します。
   注：バッチタイルデコード機能を有効にすると、XSyncの待機機能が自動的に有効になります。

ユーザーエクスペリエンスの向上

Nov 19, 2015

Receiverには、ユーザーエクスペリエンスを向上させるための以下の機能が用意されています。

- 基本設定
- ClearTypeフォントスムージング
- ユーザーフォルダーのリダイレクト
- サーバーからクライアントへのコンテンツリダイレクト
- キーボードの動作
- xcapture

環境設定

Nov 19, 2015

各種設定を行うには、Receiverメニューの［環境設定］を選択します。ここでは、デスクトップの表示モード、セッションの自動再接続、およびローカルのファイルやデバイスへのアクセスについて設定します。

アカウントを管理するには

デスクトップやアプリケーションにアクセスするには、XenDesktopまたはXenAppのアカウントが必要です。ヘルプデスク担当者により、Receiver上でアカウントを追加したり、既存のアカウントのNetScaler GatewayまたはAccess Gatewayサーバーの指定を変更したりすることが指示される場合があります。また、Receiverからアカウントを削除することもできます。

1. ［環境設定］ダイアログボックスの［アカウント］ページで、次のいずれかを実行します。
   - アカウントを追加するには、［追加］をクリックします。ヘルプデスク担当者により、新しいアカウントを作成するためのプロビジョニングファイルが提供される場合もあります。
   - アカウントで接続するストアの詳細（デフォルトのゲートウェイなど）を変更するには、［編集］をクリックします。
   - アカウントを一覧から削除するには、［削除］をクリックします。
2. 画面の指示に従って操作します。 サーバーへの認証情報が必要な場合があります。

デスクトップの表示モードを変更するには

この機能は、Citrix XenApp for UNIXのセッションでは使用できません。

デスクトップを全画面で表示（全画面モード。デフォルト）したり、ウィンドウ内に表示（ウィンドウモード）したりできます。

1. ［環境設定］ダイアログボックスの［全般］ページを開き、［デスクトップの表示］で表示モードを選択します。

セッションへの自動再接続を有効にするには

Receiverには、ネットワークインフラストラクチャの問題があるなどの理由で切断されたデスクトップやアプリケーションのセッションに、自動的に再接続するための機能が用意されています。

1. ［環境設定］ダイアログボックスの［全般］ページを開き、［アプリやデスクトップへの再接続］でオプションを選択します。

ローカルファイルへのアクセスを制御するには

仮想デスクトップやアプリケーションからローカルコンピューター上のファイルにアクセスする場合は、そのアクセス方法を制御することができます。

1. ［環境設定］ダイアログボックスの［ファイルアクセス］ページを開き、マップするドライブを選択してから適切なオプションを選択します。
   - 読み取り/書き込み：デスクトップやアプリケーションでのローカルファイルの読み取りおよび書き込を許可します。
   - 読み取りのみ：デスクトップやアプリケーションでのローカルファイルの読み取りのみを許可し、書き込を禁止します。
   - アクセスなし：デスクトップやアプリケーションでのローカルファイルへのアクセスを禁止します。
   - 毎回確認する：デスクトップやアプリケーションでのローカルファイルにアクセスするときに、毎回確認メッセージを表示します。
2. ローカルファイルへのアクセスを許可するオプションを選択すると、ユーザーデバイス上の場所を参照するときの時間を節約できます。 ［追加］をクリックして場所を指定し、それに割り当てるドライブ文字を選択します。

マイクまたはWebカメラをセットアップするには

仮想デスクトップやアプリケーションからローカルコンピューター上のマイクやWebカメラにアクセスする場合は、そのアクセス方法を制御することができます。

1. ［環境設定］ダイアログボックスの［マイクとWebカメラ］ページでは、次のオプションを選択できます。
   - マイクとWebカメラを使用する：デスクトップやアプリケーションでのマイクやWebカメラの使用を許可します。
   - マイクとWebカメラを使用しない：デスクトップやアプリケーションでのマイクやWebカメラの使用を禁止します。

Flash Playerをセットアップするには

Flashコンテンツの表示方法を選択できます。通常、これらのコンテンツにはビデオ、アニメーション、およびアプリケーションが含まれ、Flash Playerを使って表示します。

1. ［環境設定］ダイアログボックスの［Flash］ページでは、次のオプションを選択できます。
   - コンテンツを最適化する：コンテンツの再生品質を向上させます。ただし、セキュリティが低下する可能性があります。
   - 最適化しない：セキュリティを犠牲にすることなく、標準的な再生品質が提供されます。
   - 毎回確認する：Flashコンテンツを表示するときに、毎回確認メッセージを表示します。

ClearTypeフォントスムージングの構成

Nov 19, 2015

ClearTypeフォントスムージング（サブピクセルのフォントレンダリング）は、従来のフォントスムージングやアンチエイリアスに比べて表示フォントの質を向上させます。この機能を有効/無効にしたりスムージングの種類を指定したりするには、wfclient.iniで次の設定を編集します。

FontSmoothingType = <number>

<number>に以下のいずれかの値を設定します。

値	動作
0	デバイス側の設定が適用されます。デバイス側の設定は、FontSmoothingTypePrefで定義します。
1	スムージング処理なし
2	標準のスムージング
3	ClearType（水平サブピクセル）スムージング

標準スムージングまたはClearTypeスムージングを使用すると、Receiverで消費される帯域幅が著しく増加します。

重要：サーバー側の設定は、ICAファイルのFontSmoothingTypeで定義できます。この設定は、wfclient.iniの設定よりも優先されます。FontSmoothingTypeが0の場合、wfclient.ini内の次の設定によりローカルの動作が決定されます。
FontSmoothingTypePref = <number>

<number>に以下のいずれかの値を設定します。

値	動作
0	スムージング処理なし
1	
2	標準のスムージング
3	ClearType（水平サブピクセル）スムージング（デフォルト）

ユーザーフォルダーのリダイレクトの構成

Nov 19, 2015

この機能では、ユーザーごとに個別に設定される以下の2つのユーザーフォルダー（特殊フォルダー）が対象になります。

- ユーザーのデスクトップフォルダー
- ユーザーのドキュメントフォルダー（Windows XPではマイドキュメント）

ユーザーフォルダーのリダイレクト機能では、ユーザーデバイス上の特定の場所をユーザーフォルダーとして指定できます。これにより、サーバーの種類やファーム構成が異なってもこれらのフォルダーに一貫してアクセスできるようになります。たとえば、異なるサーバーファームのサーバーにログオンする必要があるモバイルユーザーには便利な機能です。常に同じサーバーファーム内のサーバーにログオンする静的な社内ワークステーションの場合、この機能はあまり必要ではありません。

ユーザーフォルダーのリダイレクトを構成するには

2つの処理が必要です。まず、module.iniにエントリを作成してユーザーフォルダーのリダイレクトを設定します。次に、以下のようにwfclient.iniにフォルダーの場所を指定します。

1. 次の文字列をmodule.ini（$ICAROOT/config/module.iniなど）に追加します。
   [ClientDrive]

   SFRAllowed = True

2. 次の文字列をwfclient.ini（$HOME/.ICAClient/wfclient.iniなど）に追加します。
   DocumentsFolder =

   DesktopFolder =

   ここで、documentsおよびdesktopは、それぞれユーザーのDocumentsフォルダーおよびDesktopフォルダーとして使用するディレクトリのUNIXファイル名（フルパス）です。次に例を示します。

   DesktopFolder = $HOME/.ICAClient/desktop

   - $HOMEなどの環境変数として、パスで任意のコンポーネントを指定できます。
   - 両方のパラメーターの値を指定する必要があります。
   - 指定するディレクトリは、クライアントデバイスマッピングを介して使用できる必要があります。このため、このディレクトリはマップされたクライアントデバイスのサブツリーにある必要があります。
   - ドライブ文字として、Cまたはそれ以降を使用する必要があります。

サーバーからクライアントへのコンテンツリダイレクトのセットアップ

Nov 19, 2015

公開アプリケーションで使用しているファイル内に埋め込まれている特定のURLを、ローカルのアプリケーションで開くように指定できます。たとえば、セッションで実行するMicrosoft OutlookでWebページへのリンクをクリックすると、そのWebページがユーザーデバイス上のWebブラウザーで開きます。管理者は、この機能を使ってサーバーのリソースをより効率よく配分し、ユーザー側のパフォーマンスを向上させることができます。

次の種類のURLをクライアントにリダイレクトできます。

- HTTP（Hypertext Transfer Protocol）
- HTTPS（Secure Hypertext Transfer Protocol）
- RTSP（Real Player）
- RTSPU（Real Player）
- PNM（従来のReal Players）

ユーザーデバイスに適切なアプリケーションがインストールされていない場合、またはコンテンツに直接アクセスできない場合は、URLがサーバー上のアプリケーションで開きます。

サーバーからクライアントへのコンテンツリダイレクト機能は、サーバー側で構成します。Receiverでは、RealPlayerとWebブラウザー（Firefox、Mozilla、またはNetscapeの内の最低1つ）がUNIXパスに指定されている場合は、この機能がデフォルトで有効になります。

注：Linux用のRealPlayerは、次のWebサイトからダウンロードできます。http://proforma.real.com/real/player/unix/unix.html

RealPlayerとWebブラウザーがパスにない場合に、サーバーからクライアントへのコンテンツリダイレクト機能を有効にするには

1. 構成ファイルwfclient.iniを開きます。
2. [Browser]セクションで、次の設定を変更します。
   Path=path

   Command=command

   ここで<path>は、Webブラウザーの実行ファイルのディレクトリです。また、<command>はリダイレクトされるURLを処理する実行ファイルの名前で、サーバーから送信されるURLに追加されます。次に例を示します。

   $ICAROOT/nslaunch netscape,firefox,mozilla

   このコマンドにより、以下が実行されます。

   - 既存のWebブラウザーウィンドウにURLを渡すnslaunchユーティリティが起動します。
   - リストで指定された各Webブラウザーを順番に試行して、コンテンツを表示します。
3. [Player]セクションで、次の設定を変更します。
   Path=path

   Command=command

   ここで<path>は、RealPlayerの実行ファイルのディレクトリです。また、<command>はリダイレクトされるマルチメディアURLを処理する実行ファイルの名前で、サーバーから送信されるURLに追加されます。

4. ファイルを保存して閉じます。
   注：両方のPath設定においても、WebブラウザーおよびRealPlay実行ファイルがあるディレクトリだけを指定する必要があります。実行ファイルのフルパスは必要ありません。たとえば、[Browser]セクションではPathの値は/usr/X11R6/bin/netscapeではなく、/usr/X11R6/binとなります。また、複数のディレクトリ名をコロンで区切って指定できます。この値を指定しない場合、$PATHが使用されます。

Receiverで、サーバーからクライアントへのコンテンツリダイレクト機能を無効にするには

1. 構成ファイルmodule.iniを開きます。
2. CREnabledの設定をOffに変更します。
3. ファイルを保存して閉じます。

キーボードの構成

Nov 19, 2015

Ctrl+Alt+Delキーを送信するためのキーを設定するには

1. Ctrl+Alt+Delキー操作を送信するために使用するキーの組み合わせを決定します。
2. 適切な構成ファイルを開き、[WFClient]セクションのUseCtrlAltEndで、以下の値を設定します。
   - Trueを指定すると、Ctrl+Alt+Endキーを押すことでリモートのデスクトップにCtrl+Alt+Delキー操作が送信されます。
   - False（デフォルト）を指定すると、Ctrl+Alt+Enterキーを押すことでリモートのデスクトップにCtrl+Alt+Delキー操作が送信されます。

xcaptureの使用

Nov 19, 2015

Receiverのパッケージには、サーバーのクリップボードと、Xデスクトップ上のICCCMに準拠していないX Windowアプリケーション間で画像をコピーおよび貼り付けできる、xcaptureユーティリティが付属しています。xcaptureを使って、次の操作を実行できます。

- ダイアログボックスや画面領域をキャプチャし、コネクションウィンドウ内で実行中のアプリケーションと、ユーザーデバイスデスクトップ（ICCCMに準拠していないX Windowアプリケーションを含む）間でコピーする。
- コネクションウィンドウと、グラフィックを編集するX Windowアプリケーションであるxmagまたはxv間で、画像をコピーする。

コマンドラインからxcaptureを起動するには

コマンドプロンプトで、/opt/Citrix/ICAClient/util/xcaptureと入力して、Enterを押します（ここで、/opt/Citrix/ICAClientはReceiverをインストールしたディレクトリです）。

ユーザーデバイスデスクトップからコピーするには

1. ［xcapture］ダイアログボックスで、［画面から］をクリックします。 カーソルが十字型に変わります。
2. 次のいずれかを選択します。
   - ウィンドウの選択。コピーするウィンドウの上にカーソルを移動し、マウスの中央ボタンをクリックします。
   - 領域の選択。マウスの左ボタンを押したままカーソルをドラッグして、コピーする領域を選択します。
   - 選択の取り消し。マウスの右ボタンをクリックします。ドラッグしているときに中央ボタンまたは左ボタンを押したままマウスの右ボタンをクリックすると、選択が解除されます。
3. ［xcapture］ダイアログボックスで、［ICAへ］をクリックします。 ボタンの色が変わり、情報を処理していることが示されます。
4. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

xvから、ICAセッション内のアプリケーションにコピーするには

1. xvで情報をコピーします。
2. ［xcapture］ダイアログボックスで、［xvから］、［ICAへ］の順にクリックします。 ボタンの色が変わり、情報を処理していることが示されます。
3. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

ICAセッション内のアプリケーションからxvにコピーするには

1. ICAセッション内のアプリケーションで、情報をコピーします。
2. ［xcapture］ダイアログボックスで、［ICAから］、［xvへ］の順にクリックします。 ボタンの色が変わり、情報を処理していることが示されます。
3. 転送が完了したら、コピーした情報をxv内に貼り付けます。

ユーザーの自動再接続

Nov 19, 2015

このトピックでは、HDX Broadcastのクライアント自動再接続機能について説明します。この機能は、HDX Broadcastセッション画面の保持機能と組み合わせて使用することをお勧めします。

ネットワークの状態が不安定であったり、待ち時間が非常に変わりやすかったりする場合、また、無線デバイスの伝送距離に制限がある場合に、セッションが切断されてしまうことがあります。HDX Broadcastのクライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションをReceiverが検出すると、そのセッションに自動的に再接続します。

この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。サーバー側でユーザー認証を要求する設定になっている場合、再接続時にユーザーの資格情報を入力するためのダイアログボックスが開きます。ユーザーがセッションからログオフしないでアプリケーションを終了してセッションを切断した場合、自動再接続は行われません。自動再接続は、ユーザーによる切断以外の理由で切断されたセッションに対してのみ行われます。

デフォルトでは、Receiverは36秒間待機してから切断したセッションに再接続を実行し、またこれを3回試行します。

AccessGatewayを介して接続すると、ACRは使用できません。ネットワークの障害から保護するため、AccessGateway上で構成するだけではなく、サーバーとクライアントの両方でもセッション画面の保持を有効にしておきます。

HDX Broadcastのクライアント自動再接続の構成手順については、XenAppおよびXenDesktopのドキュメントを参照してください。

セッション画面の保持

Nov 19, 2015

このトピックは、デフォルトで有効になっているHDX Broadcastセッション画面の保持機能について説明します。

HDX Broadcastセッション画面の保持を有効にすると、公開アプリケーションへの接続が中断しても、ユーザーのセッション画面には作業中の画面が保持され、表示されたままになります。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、ユーザーデバイス上の画面表示が停止します。トンネルから出るなどして再接続されると、ユーザーはそのまま作業を続行できます。接続が切断している間、ユーザーのデータのすべて、キー入力、およびそのほかの操作は記憶され、アプリケーションは応答しないまま表示されます。接続が再度確立されると、これらすべての操作がアプリケーション内に反映されます。

クライアント自動再接続とセッション画面の保持が構成されている時、接続の問題がある場合にはセッションの画面保持が優先して実行されます。セッション画面の保持は既存のセッションへの接続を再度確立しようとします。接続の問題を検出するには最大で25秒かかることがあり、次に再接続するための構成可能な期間（デフォルトは180秒）を指定します。セッション画面の保持が再接続に失敗すると、クライアント自動再接続が再接続を試みます。

HDX Broadcastセッション画面の保持を有効にすると、セッションの通信に使用されるデフォルトのポートは、1494から2598に変更されます。

重要：HDX Broadcastセッション画面の保持では、サーバー上で（ポリシー設定を使って）Common Gateway Protocolを有効にする必要があります。Common Gateway Protocolを無効にすると、HDX Broadcastセッション画面の保持も無効になります。
Receiverのユーザーには、サーバー側の設定が自動的に適用されます。詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

Receiver通信のセキュリティ保護

Nov 19, 2015

サーバーファームとReceiver間の通信を保護するには、以下の一連のセキュリティ技術を使用します。

- SOCKSプロキシサーバーまたはSecureプロキシサーバー（セキュリティプロキシサーバー、HTTPSプロキシサーバーまたはTLSトンネリングプロキシサーバーとも呼ばれます）。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Receiverとサーバー間の接続を制御できます。Receiverは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。
- Secure GatewayまたはTransport Layer Security（TLS）プロトコルによるSSL Relayソリューション。TLS Version 1.0から1.2がサポートされます。
- ファイアウォール。ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部IPアドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまりNAT（Network Address Translation：ネットワークアドレス変換））を介してReceiverを使用する場合は、外部アドレスを構成します。

プロキシサーバー経由の接続

Nov 19, 2015

プロキシサーバーは、ネットワーク内部から外部への、および外部から内部へのアクセスを制限して、ReceiverとCitrix XenAppやCitrix XenDesktopとの間の接続を制御するために使います。Receiverは、SOCKSプロトコル、Secure GatewayおよびCitrix SSL Relay、Secureプロキシプロトコル、およびWindows NTチャレンジ/レスポンス（NTLM）認証をサポートしています。

サポートされているプロキシの種類の一覧は、Trusted_Regions.iniとUntrusted_Regions.iniの内容によってAuto、None、およびWpadの種類に制限されます。SOCKS、Secure、またはScriptといった種類を使用する必要がある場合は、それらのファイルを編集して、許可された一覧へ追加の種類を追加します。

注：確実に安全な接続を実行するには、TLSを有効にします。

Secureプロキシプロトコルを使用する接続を構成して、Windows NTチャレンジ/レスポンス（NTLM）認証のサポートを有効にできます。このプロトコルを使用できる場合は、追加構成なしで実行時にこれが検出され使用されます。

重要：NTLMをサポートするには、ユーザーデバイスにOpenSSLライブラリのlibcrypto.soをインストールする必要があります。このライブラリは、多くの場合Linuxディストリビューションに含まれていますが、http://www.openssl.org/からダウンロードすることもできます。

Secure GatewayまたはCitrix SSL Relayの使用

Nov 19, 2015

ReceiverをSecure GatewayまたはCitrix SSL（Secure Sockets Layer）Relayと共に使うことができます。ReceiverはTLSプロトコルをサポートします。TLS（Transport Layer Security）は、標準化されたSSLプロトコルの最新版です。IETF（Internet Engineering TaskForce）が、SSLの公開標準規格の開発をNetscape Communications社から引き継いだときに、SSLという名前をTLSに変更しました。TLSは、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信を保護します。米国政府など、データ通信を保護するためにTLSの使用を必須としている組織もあります。このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140は、暗号化の情報処理規格です。

Secure Gatewayを通常モードまたはリレーモードのどちらかで使用して、Receiverとサーバーの間に保護された通信チャネルを提供できます。Secure Gatewayを通常モードで使用し、ユーザーがWeb Interface経由で接続する場合は、Receiver側での構成は不要です。

ReceiverがSecure Gatewayサーバーと通信するときは、リモートのWeb Interfaceサーバーで構成されている設定が使用されます。Receiverをサポートするプロキシサーバー設定の構成については、Web Interfaceのドキュメントを参照してください。

Secure Gateway Proxyがセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Gateway Proxyをリレーモードで使用できます。詳しくは、XenApp（Secure Gateway）のドキュメントを参照してください。

ただし、リレーモードで使用する場合、Secure Gatewayサーバーはプロキシサーバーとして機能するため、Receiverで次の項目を構成する必要があります。

- Secure Gatewayサーバーの完全修飾ドメイン名。
- Secure Gatewayサーバーのポート番号。Secure Gateway, Version 2.xでは、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の3つの要素を順に指定する必要があります。

- Host name
- サブドメイン名
- 最上位ドメイン名

たとえば、my_computer.my_company.comは完全修飾ドメイン名です。ホスト名（my_computer）、サブドメイン名（my_company）、最上位ドメイン名（com）が順に指定されています。一般的には、サブドメイン名と最上位ドメイン名の組み合わせ（my_company.com）をドメイン名といいます。

デフォルトではCitrix SSL Relayのリスナーポートとして、TLSで保護された通信の標準ポートであるXenAppサーバーのTCPポート443が使用されます。Citrix SSL Relayは、SSL/TLS接続要求を受信すると、その要求を解読してからサーバーに転送します。ユーザーがTLS+HTTPSブラウズを選択した場合は、Citrix XML Serviceに転送します。

443以外のリスナーポートを構成する場合、Receiverに対して非標準のリスナーポート番号を指定する必要があります。

Citrix SSL Relayを使用すると、次の通信のセキュリティを保護できます。

- TLSが有効なユーザーデバイスとサーバー間の通信。

- Web InterfaceによるXenAppサーバーとWebサーバー間の通信。

SSL Relayによるセキュリティ機能については、XenAppのドキュメントを参照してください。TLS暗号化を使用するためのWeb Interfaceの構成については、Web Interfaceのドキュメントを参照してください。

SSL Relayによるセキュリティ機能については、XenAppのドキュメントを参照してください。TLS暗号化を使用するためのWeb Interfaceの構成については、Web Interfaceのドキュメントを参照してください。

Receiverが必ずTLSを使用して接続するようにするには、Secure GatewayサーバーまたはCitrix SSL RelayでTLSを指定します。詳しくは、Secure GatewayまたはSSL Relasyサービスのドキュメントを参照してください。
注：このバージョンのReceiver for LinuxではSSLv3プロトコルの使用を無効にしています。
Secure Gateway for WindowsまたはCitrix SSL Relayについて詳しくは、XenAppのドキュメントを参照してください。

TLSを使うには、サーバー証明書の証明機関の署名を確認するためのルート証明書がユーザーデバイスにインストールされている必要があります。Receiverでは、デフォルトで以下の証明書がサポートされます。

Certificate	証明機関
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

これらの証明書を使用する場合は、ルート証明書をユーザーデバイスにインストールする必要はありません。ただし、上記の証明機関以外の証明書を使用する場合は、該当する証明機関からルート証明書を取得して、各ユーザーデバイスにインストールする必要があります。

重要：Receiverでサポートされる証明書のキーの長さは、4096ビットまでです。証明機関のルート証明書と中間証明書、およびお使いのサーバーの証明書は4096ビット長以下である必要があります。
注： Receiver for Linux 13.0は、ローカルデバイスのc_rehashを使用します。バージョン13.1以降は、以降で説明しているようにctx_rehashツールを使用します。
ルート証明書の使用

証明機関により発行され、ユーザーデバイスに信頼されていないサーバー証明書を認証するには、StoreFrontストアを追加する前に以下の手順を行ってください。

1. PEM形式のルート証明書を入手します。
   ヒント：PEM形式の証明書が見つからない場合は、opensslユーティリティを使用してCRT形式の証明書をPEMファイルに

変換できます。

2. パッケージをインストールしたユーザー（通常はルート）が、以下の手順を実行します。
   1. ルート証明書を$ICAROOT/keystore/cacertsにコピーします。
   2. 次のコマンドを実行します。
      $ICAROOT/util/ctx_rehash

中間証明書の使用

1. PEM形式の中間証明書を別途入手します。
   ヒント：PEM形式の証明書が見つからない場合は、opensslユーティリティを使用してCRT形式の証明書をPEMファイルに変換できます。
2. パッケージをインストールしたユーザー（通常はルート）が、以下の手順を実行します。
   1. ファイルを$ICAROOT/keystore/intcertsにコピーします。
   2. パッケージをインストールしたユーザーとして次のコマンドを実行します。
      $ICAROOT/util/ctx_rehash

スマートカードサポートの有効化

Nov 19, 2015

Receiver for Linuxは、さまざまな種類のスマートカードリーダーをサポートしています。サーバーとReceiverの両方でスマートカードのサポートを有効にすると、以下の機能が有効になります。

- スマートカードによるログオン認証。スマートカードを使って、Citrix XenAppサーバーにログオンするユーザーを認証します。
- スマートカード対応アプリケーションのサポート。スマートカード対応の公開アプリケーションを使って、ローカルのスマートカードリーダーにアクセスできます。

スマートカードのデータは機密性の高い情報であるため、TLSなどの信頼された証明機関から認証されたセキュリティアーキテクチャを経由して転送する必要があります。

次に、スマートカードサポートを使用するための条件を示します。

- スマートカードリーダーと公開アプリケーションが、業界標準のPC/SC規格に準拠している必要があります。
- 使用するスマートカードに適切なドライバーをインストールする必要があります。
- PC/SC Liteパッケージをインストールする必要があります。
- ミドルウェアがPC/SCを使ってスマートカードにアクセスするためのpcscdデーモンをインストールして実行する必要があります。
- 64ビットシステムには、64ビットと32ビットの両バージョンの"libpscslite1"パッケージがある必要があります。

重要：SunRayサーバーソフトウェアVersion 2.0以降でSunRayターミナルを使用している場合は、PC/SCバイパスパッケージをインストールする必要があります。このパッケージは、SunのWebサイト（www.sun.com）からダウンロードできます。サーバー上でのスマートカードサポートの構成について詳しくは、XenDesktopおよびXenAppのドキュメントを参照してください。

NetScaler Gateway経由の接続

Nov 19, 2015

Citrix NetScaler Gateway（旧称「Access Gateway」）を使用すると、StoreFrontストアへの接続を保護して、デスクトップやアプリケーションへのユーザーアクセスを詳細に管理できます。

NetScaler Gateway経由でデスクトップやアプリケーションに接続するには

1. 管理者により提供されたNetScaler GatewayのURLを指定します。これを行うには、以下のいずれかの手順に従います。
   - セルフサービスユーザーインターフェイスの初回使用時に、［アカウントの追加］ダイアログボックスでURLを入力します。
   - セルフサービスユーザーインターフェイスの初回使用時以降は、［環境設定］>［アカウント］>［追加］の順に選択します。
   - storebrowseコマンドで接続する場合は、コマンドラインにURLを入力します。

   URLにより、ゲートウェイと、必要に応じて特定のストアが指定されます。

   - Receiverで検出された最初のストアに接続されるようにするには、URLをhttps://gateway.company.com形式で指定します。
   - 特定のストアに接続する場合は、URLをhttps://gateway.company.com?形式で指定します。この動的URLは、非標準の形式です。そのため、=（等号記号）をURLに含めないでください。storebrowseコマンドで特定のストアに接続する場合は、URLを引用符で囲んで指定します。
2. 資格情報の入力を確認するメッセージが表示されたら、ユーザー名、パスワード、およびセキュリティトークンを入力します。手順について詳しくは、NetScaler Gatewayのドキュメントを参照してください。

   認証処理が完了すると、デスクトップまたはアプリケーションが表示されます。

Receiver for Linuxのトラブルシューティング

Nov 19, 2015

このセクションでは、管理者によるReceiver for Linuxのトラブルシューティングに役立つ情報について説明します。

Receiverの実行時に問題が発生した場合、Citrixテクニカルサポートに診断情報の提出を求められる場合があります。この情報は、Citrixテクニカルサポートで問題を調査して修正する目的で使用されます。

Receiverに関する診断情報を取得するには

1. インストールディレクトリに、「util/lurdump」と入力します。Receiverのバージョン、構成ファイルの内容、およびさまざまなシステム変数値などの詳細な診断情報を含むファイルが作成されます。
2. テクニカルサポートにこのファイルを送信する前に、ファイルに機密情報が含まれていないことを確認してください。

接続の問題

Nov 19, 2015

以下の接続関連の問題が確認されています。

Windowsサーバーへの接続を確立しているときに、ダイアログボックスに「サーバーxxxに接続しています」というメッセージが表示された後に、接続画面が何も開かない場合は、サーバーのクライアントアクセスライセンス（CAL）の構成を確認する必要があります。ライセンスについて詳しくは、製品ライセンスの有効化を参照してください。

Receiverからの要求よりも多いウィンドウの色数でセッションを再接続しようとすると、接続に失敗する場合があります。これは、サーバーのメモリ不足が原因です。再接続に失敗した場合、Receiverはセッションで元の色数を使おうとします。再接続した場合は、サーバーは新しいセッションを要求した色数で開始しようとし、元のセッションは切断されたままになります。ただし、サーバーのメモリが依然不足している場合は2つ目のセッションも失敗する可能性があります。

ネットワークでDNS（ドメインネームシステム）を構成すると、接続するサーバー名を解決できるようになります。構成されたDNSがない場合は、サーバー名をIPアドレスに解決することができません。または、接続先サーバーの名前の代わりにIPアドレスを指定することもできます。ただし、TLS接続では、IPアドレスではなく完全修飾ドメイン名の指定が必要です。

コネクションで自動プロキシ検出を使用するように構成されていて、接続時に「プロキシを検出できません。JavaScript エラーです。」というエラーメッセージが表示される場合は、$ICAROOT/util内にwpad.datファイルをコピーします。次のコマンドを実行します。ここで、hostnameは接続するサーバーのホスト名です。

cat wpad.dat | ./pacexec pac.js FindProxyForURL http://hostname hostname 2>&1 | grep “undeclared variable”

コマンドを実行しても出力がない場合は、サーバーのwpad.datファイルに調査が必要な深刻な問題があります。ただし、“assignment to undeclared variable ...”のような出力がある場合は問題を解決できます。pac.jsを開き、出力内に表示されている各変数について、ファイルの最初に次の形式の行を追加します。ここで、“...”は変数名です。

var ...;

マウスを動かすまでセッションが開始されないことがあります。Linuxカーネルでの乱数生成に問題があると、この問題が発生します。この問題を回避するには、run an entropy-generating daemon such as rngd（ハードウェアベース）またはhaveged（Magic Software）などのエントロピー生成デーモンを実行してください。

単一のシリアルポートを構成するには、$ICAROOT/config/module.ini構成ファイルに次のエントリを追加します。

LastComPortNum=1 ComPort1=<デバイス>

複数のシリアルポートを構成するには、$ICAROOT/config/module.ini構成ファイルに次のエントリを追加します。

LastComPortNum=2 ComPort1=<デバイス1> ComPort2=<デバイス2>

表示の問題

Nov 19, 2015

以下の表示関連の問題が確認されています。

英語以外のキーボードを使用している場合、画面表示がキーボード入力と一致しないことがあります。この場合、使用しているキーボードの種類とレイアウトを指定する必要があります。キーボードの指定については、「キーボードの構成」を参照してください。

ウィンドウマネージャーの種類によっては、ウィンドウを移動すると新しいウィンドウ位置が常にサーバーにレポートされるため、再描画が過度に発生することがあります。ウィンドウを移動したときにウィンドウ枠のみを描画するモードに切り替えると、この問題は解決します。

シームレスウィンドウモードでは、タイトルバーや境界線が、ローカルデバイスのウィンドウマネージャーの表示形式ではなく、サーバー側の表示形式で表示されます。ウィンドウマネージャーによって、表示形式を置き換えるメカニズムは異なります。

Receiverはウィンドウマネージャーに、Motifの_MOTIF_DECORATIONSヒントを適用して、表示形式を置き換えます。また、すべてのシームレスウィンドウのクラスが"Wfica_Seamless"に設定されるため、ヒントを認識しないウィンドウマネージャーでも、リソースファイルエントリを介して表示形式が置き換えられます。

Receiverは、ほとんどのウィンドウマネージャーと連携するウィンドウアイコンを作成しますが、ICCCM（Inter-Client Communication Convention Manual：クライアント間通信規約マニュアル）に準拠していません。

ICCCMに完全に準拠するには

1. 構成ファイルwfclient.iniを開きます。
2. [WFClient]セクションで次のように行を編集します。UseIconWindow=True
3. ファイルを保存して閉じます。

カーソルの色が背景色と同じまたは似ている場合には、見分けるのが難しくなることがあります。この問題は、カーソルを黒または白にすることで解決できます。

カーソルの色を変更するには

1. 構成ファイルwfclient.iniを開きます。
2. 次のいずれかの行を[WFClient]セクションに追加します。
   CursorStipple=ffff,ffff （カーソルを黒で表示）

   CursorStipple=0,0 （カーソルを白で表示）
3. ファイルを保存して閉じます。

コネクションウィンドウの内/外にマウスを移動させると、フォーカスのないウィンドウの色がちらつくことがあります。これは、PseudoColor表示でX Windows Systemを使用する場合の制限事項として知られています。可能な場合、問題のあるコネクションではより色数の多いウィンドウを使用してください。

サーバーに接続するとき、ウィンドウの色数として256色を選択できます。256色を選択する場合は、ビデオカードがパレットをサポートしていて、アプリケーションでパレットの色を高速変更し、アニメーション表示が可能であることが前提になります。

True Color表示では、パレットを高速変更してアニメーションを生成する機能はエミュレートできません。ソフトウェアでのこの機能のエミュレーションは相対的に時間がかかり、多くのネットワークトラフィックが費やされます。この問題を解決するために、Receiverは高速パレット変更をバッファーに格納し、数秒ごとに実際のパレットを更新するように設定されています。

Receiverでは、日本語文字にEUC-JPまたはUTF-8文字エンコードが使用されます。一方、サーバー側ではShift-JIS文字エンコードが使用されます。Receiverでは、これらの文字セット間でのエンコーディングが実行されません。このため、ファイルに日本語の名前を使用し、クライアントドライブマッピングを使用してローカルコンピューターにそのファイルを保存する場合、ローカルコンピューターではその日本語ファイル名が正しく表示されません。逆に、ローカルで日本語名のファイルを作成し、クライアントドライブマッピングを使用してサーバーに保存した場合、サーバー上でこのファイル名を正しく表示できません。この問題は、拡張パラメーターパス機能で使用されるパラメーターの日本語でも発生します。

全画面モードのセッションは、すべてのモニターの表示領域全体に表示されます。また、コマンドラインオプションとして-spanを使用することもできます。これにより全画面セッションを複数モニターにまたがって表示できます。

重要：-spanは、シームレスセッションや標準のウィンドウセッション、またそれらが混在するセッションには適用されません。
-spanオプションは、以下のように指定します。

-span [h][o][a | [,[,,]]]

ここでhを指定すると、モニターの一覧がstdoutに出力されます。また、この値のみを指定した場合、モニター一覧の出力後にwficaが終了します。

ここでoを指定すると、セッションウィンドウのリダイレクト属性がoverride-redirectになります。

注意：この値の使用は推奨されません。これは、非協調性のウィンドウマネージャーで使用するための最後の手段です。セッションウィンドウはウィンドウマネージャーで非表示となり、アイコンもなく、再スタックできません。セッションを終了することによってのみウィンドウを削除できます。
ここでaを指定すると、すべてのモニターを使用してセッションが表示されます。

-spanオプションの残りの値は、使用するモニターの番号として処理されます。特定のモニターを使用する場合は単一の値（）を指定します。また、表示領域の左上と右下のモニターを指定（,）したり、上端、下端、左端、および右端のモニターを指定（,,,）したりできます。

ここで、oを指定しない場合、wficaコマンドでは、_NET_FULLSCREEN_MONITORSメッセージによりウィンドウマネージャーから適切なウィンドウレイアウトが取得されます（サポートされる場合）。それ以外の場合は、サイズおよび位置に

するヒントを使用して必要なレイアウトを要求します。

ウィンドウマネージャーがこのクライアントメッセージをサポートするかどうかを確認するには、次のコマンドを実行します。

xprop -root | grep _NET_WM_FULLSCREEN_MONITORS

出力がない場合、サポートされません。サポートされないウィンドウマネージャーでは、ウィンドウリダイレクトの上書き（override-redirect）が必要な場合があります。override-redirectウィンドウをセットアップするには、-span oを使用します。

コマンドラインからセッションを複数のモニターにまたがって実行するには

1. コマンドプロンプトで、次のコマンドを実行します。/opt/Citrix/ICAClient/wfica -span hユーザーデバイスに現在接続しているモニターの番号の一覧がstdoutに出力され、wficaが終了します。
2. これらのモニターの番号をメモしておきます。
3. コマンドプロンプトで、次のコマンドを実行します。/opt/Citrix/ICAClient/wfica -span [w[,x[,y,z]]]ここでw、x、y、およびzは、手順1でメモしたモニターの番号です。特定のモニターを使用する場合は単一の値（w）を指定します。また、表示領域の左上と右下のモニターを指定（w,x）したり、上端、下端、左端、および右端のモニターを指定（w,x,y,z）したりできます。
   重要：selfserviceを起動したりWebブラウザーでWeb interfaceに接続したりする前に、WFICA_OPTS変数を定義しておく必要があります。これを行うには、プロファイルファイル（通常は、$HOME/.bash_profileまたは$HOME/.profile）を編集して、WFICA_OPTS変数を定義する行を追加します。次に例を示します。
   export WFICA_OPTS="-span a"
   この変更は、XenAppおよびXenDesktopセッションの両方に適用されます。

この問題は、クライアント側のシステムUIが非表示になっていて、キーボード透過機能が通常のキーボードコマンド（Alt+Tabなど）を無効にし、代わりにサーバーにコマンドを送るために発生します。

この問題を回避するには、フォーカスがセッションウィンドウに移るまでCtrl+F2キーを押してキーボード透過機能を一時的にオフにします。代替の回避策であるTransparentKeyPassthroughをNoと$ICAROOT/config/module.iniで設定します。これによりキーボード透過機能は無効になりますが、All_regions.iniファイルにこの設定を追加してICAファイルを上書きする必要があります。

Webブラウザーの問題

Nov 19, 2015

以下のWebブラウザー関連の問題が確認されています。

サーバーからクライアントへのコンテンツリダイレクトは、wfclient.iniで有効になっています。このため、ローカルのアプケーションが実行されます。サーバーからクライアントへのコンテンツリダイレクト機能を無効にするは、「サーバーからクライアントへのコンテンツリダイレクトのセットアップ」を参照してください。

FirefoxやChrome以外のWebブラウザーでは、公開リソースに接続するための設定が必要な場合があります。Web Interfaceを介して接続する場合、リソースの一覧が表示されたWeb Interfaceのページにアクセスできる場合があります。公開されているリソースの一覧からアイコンをクリックしてリソースにアクセスしようとすると、ICAファイルの保存を確認するメッセージが表示されることがあります。

Webブラウザーにより詳細は異なりますが、WebブラウザーのMIMEタイプをセットアップして、MIMEタイプapplication/x-icaまたはICAファイルが$ICAROOT/wficaにより実行されるように設定します。

特定のWebブラウザーで問題が生じる場合、setupwfcを実行する前に環境変数BROWSERを設定して必要なWebブラウザーのローカルパスや名前を指定してください。

ICAプラグインを有効にしてください。

ICAプラグインを無効にしてください。

そのほかの問題

Nov 19, 2015

そのほか、以下の問題が確認されています。

設定を適用するには、wfclient.iniの各エントリに対応するエントリがAll_Regions.ini内に存在している必要があります。これに加えて、wfclient.iniの[Thinwire3.0]、[ClientDrive]、および[TCP/IP]セクションについて、実行する設定に対してcanonicalization.ini内に対応するエントリが必要です。詳しくは、$ICAROOT/configディレクトリ内のAll_Regions.iniおよびcanonicalization.iniファイルを参照してください。

公開アプリケーションがシリアルポートにアクセスする必要がある場合、ポートがほかのアプリケーションによりロックされていると元のアプリケーションを実行できません（エラーメッセージの表示または非表示はアプリケーションにより異なる）。このような環境では、シリアルポートを一時的にロックしたり、シリアルポートをロックしたまま解除せずに終了したりしているアプリケーションがないかをチェックします。

この問題を解決するには、シリアルポートをブロックしているアプリケーションを終了します。UUCPスタイルのロックの場合は、アプリケーションの終了後にロックファイルが残る可能性があります。このロックファイルの場所は、使用しているオペレーティングシステムにより異なります。

Receiverを起動できず、「Application default file could not be found or is out of date」というメッセージが表示される場合は、環境変数ICAROOTが適切に定義されていません。デフォルト以外の場所にReceiverをインストールした場合は、環境変数ICAROOTを定義する必要があります。この問題を解決するには、次のいずれかを実行してください。

- ICAROOTをインストールディレクトリとして定義する。

  ICAROOT環境変数が正しく定義されているかどうかをチェックするには、Receiverをターミナルセッションから起動します。エラーメッセージが表示される場合は、ICAROOT環境変数が正しく定義されていません。

- Receiverをデフォルトの場所に再インストールする。Receiverのインストールについて詳しくは、「Receiver for Linuxのインストール」を参照してください。

  以前デフォルトの場所にReceiverをインストールしていた場合は、再インストールする前に/opt/Citrix/ICAClienまたは$HOME/ICAClient/platformディレクトリを削除する必要があります。

ウィンドウマネージャーで同じキーボードショートカットが定義されている場合、セッションでのキーボードショートカットが正しく機能しない場合があります。たとえば、KDEウィンドウマネージャーでデスクトップ13～16に切り替えるためのキーの組み合わせである、Ctrl+Shift+F1～F4キーがこれに該当します。この問題を解決するには、以下の方法を使用します。

- ローカルのキーの組み合わせをサーバー側のキーの組み合わせにマップするトランスレートモードを使用します。たとえば、デフォルトのトランスレートモードでは、Ctrl+Shift+F1がサーバー側のAlt+F1にマップされています。これを変更してほかのローカルキーの組み合わせを使用するには、$HOME/.ICAClient/wfclient.iniの[WFClient]セクションを編集します。たとえば、次の変更によりローカルのAlt+Ctrl+F1がサーバー側のAlt+F1にマップされます。
  - 変更Hotkey1Shift=Ctrl+Shiftこの行を、次のように変更しますHotkey1Shift=Alt+Ctrl。

- キーの組み合わせをすべてサーバー側に直接送信するダイレクトモードを使用します。この場合、キーの組み合わせはローカルでは処理されません。ダイレクトモードを構成するには、$HOME/.ICAClient/wfclient.iniの[WFClient]セクションで、TransparentKeyPassthroughこの行を、Remoteに設定します。
- ウィンドウマネージャー側のキーボードショートカットを再構成して競合を解消します。

クロアチア語キーボードレイアウトでリモートの仮想デスクトップにASCII文字が正しく送信されるようにするには、以下の手順に従います。

1. 適切な構成ファイルを開き、[WFClient]セクションのUseEUKSforASCIIでTrueを指定します。
2. UseEUKSで2を指定します。

実行中のCitrix SSLSDKまたはOpenSSLのバージョン番号を確認するには、次のコマンドを使用できます。
strings libctxssl.so | grep "Citrix SSLSDK"
また、AuthManagerDaemonまたはPrimaryAuthManager上でもこのコマンドを実行できます。

日本語キーボードの使用を構成するには、wfclient.ini構成ファイルで次のエントリを更新します。
KeyboardLayout=Japanese (JIS)

ABNT2キーボードの使用を構成するには、wfclient.ini構成ファイルで次のエントリを更新します。
KeyboardLayout=Brazilian (ABNT2)

$ICAROOT/config/module.iniの一覧で最適のサーバーレイアウトを選択します。

一般的なエラーメッセージ

Nov 19, 2015

このセクションでは、一般的なエラーメッセージについて説明します。

このエラーは、コネクションエントリが適切に構成されていない場合に発生します。

E_MISSING_INI_SECTION - 構成ファイルを検証してください："..." 構成ファイルでセクション"..."が見つかりません。

構成ファイルが直接編集されたか、壊れています。

E_MISSING_INI_ENTRY - 構成ファイルを検証してください："..." セクション"..."にはエントリ"..."が含まれている必要があります。

構成ファイルが直接編集されたか、壊れています。

E_INI_VENDOR_RANGE - 構成ファイルを検証してください："..." 構成ファイルのXサーバーベンダーの範囲"..."が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。Citrixに連絡してください。

これらのエラーは、wfclient.iniの構成が正しくない場合に発生します。

E_CSM_MUST_SPECIFY_SERVER - サーバーを入力する必要があります。

［プロパティ］ダイアログボックスの［ネットワーク］ページで、サーバー名を入力する必要があります。

E_CANNOT_WRITE_FILE - ファイルを書き込めません："..."

コネクションデータベースに保存するときに、空きディスク容量が不足するなどのエラーが発生しました。

E_CANNOT_CREATE_FILE - ファイルを作成できません："..."

新しいコネクションデータベースの作成時にエラーが発生しました。

E_CSM_CONNECTLIST_INVALID - 選択した接続が見つかりません。

構成ファイルが壊れています。新しい構成ファイルを作成してください。

E_CSM_CONNECTION_NOTFOUND - 選択した接続が見つかりません。

構成ファイルが壊れています。新しい構成ファイルを作成してください。

E_CSM_APPSERVERLIST_MISSING - 構成ファイルを検証してください："..."。 セクション"..."がありません。 新しい構成ファイルを作成してください。

構成ファイルが壊れています。新しい構成ファイルを作成してください。

E_CSM_APPSRV_SECTION_MISSING - 構成ファイルを検証してください："..."。 セクション"..."がありません。 新しい構成ファイルを作成してください。

構成ファイルが壊れています。新しい構成ファイルを作成してください。

E_PNAGENT_FILE_UNREADABLE - Citrix XenApp ファイル"..."を読み取れません：そのようなファイルまたはディレクトリはありません。

— または—

Citrix XenApp ファイル"..."を読み取れません：アクセスは拒否されました。

デスクトップアイテムまたはメニューからリソースにアクセスしようとしていますが、そのリソースのXenAppファイルを使用できません。［ビュー］メニューの［アプリケーションの更新］を選択して公開リソースの一覧を更新し、もう一度リソースにアクセスしてみてください。問題が解決されない場合は、デスクトップアイコンまたはメニューのプロパティ、およびアイコンまたはメニューが参照しているXenAppファイルのプロパティを確認します。

E_CSM_DESCRIPTION_NONUNIQUE - 説明フィールドは一意なものである必要があります。 この説明は既に使用されています。

［プロパティ］ダイアログボックスの［ネットワーク］ページの［コネクション名］ボックスに、ほかで使われていない固有の名前を入力する必要があります。

プロキシ自動検出スクリプトファイル（PACファイル）を使用してプロキシ構成を指定する場合、以下のエラーが発生することがあります。

プロキシを検出できません。不正な自動構成URLです。

ブラウザーで指定したアドレスのURLのタイプが無効です。有効なタイプは「http://」および「https://」で、ほかのタイプはサポートされていません。アドレスを有効なURLタイプに変更してもう一度試してください。

プロキシを検出できません。.PACスクリプトHTTPダウンロードに失敗しました。接続できません。

入力した名前またはアドレスが間違っていないかチェックします。間違いがある場合は、それを修正してもう一度入力します。間違いがない場合は、サーバーがダウンしています。しばらくしてから、もう一度試してください。

プロキシを検出できません。.PACスクリプトHTTPダウンロードに失敗しました。パスが見つかりません。

必要なPACファイルがサーバーにありません。サーバー上でこれを変更するか、ブラウザーを再構成してください。

プロキシを検出できません。.PACスクリプトHTTPダウンロードに失敗しました。

PACファイルのダウンロード中に接続が切断しました。再接続してもう一度実行します。

プロキシを検出できません。自動構成スクリプトが無効です。

PACファイルが空です。サーバー上でこれを変更するか、ブラウザーを再構成してください。

プロキシを検出できません。JavaScriptサポートしていません。

PAC実行ファイルまたはpac.jsテキストファイルがありません。Receiverを再起動します。

プロキシを検出できません。JavaScriptエラーです。

PACファイルに含まれているJavaScriptが無効です。サーバーでPACファイルを修正してください。 接続の問題」も参照してください。

プロキシを検出できません。プロキシ自動構成スクリプトから不正な結果が返されました。

サーバーから不正な形式の応答を受信しました。サーバー上でこれを修正するか、ブラウザーを再構成してください。

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

Receiverをコマンドラインから実行するときにこのメッセージが表示される場合は、通常コマンドラインに指定した名前がappsrv.iniにないことを意味します。

E_BAD_OPTION - オプション"..."は無効です。

オプション"..."の引数が指定されていません。

E_BAD_ARG - オプション"..."に無効な引数があります："..."

オプション"..."に無効な引数が指定されています。

E_INI_KEY_SYNTAX - 構成ファイル"..."のキー"..."が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。新しい構成ファイルを作成してください。

E_INI_VALUE_SYNTAX - 構成ファイル"..."の値"..."が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。新しい構成ファイルを作成してください。

E_SERVER_NAMELOOKUP_FAILURE - サーバー"..."に接続できません。

サーバー名を解決できません。

ヘルプデスクに連絡して、次の情報を知らせてください：NDSツリー："..."を参照できません。

ヘルプデスクに連絡して、このエラーメッセージの詳細を知らせてください。

1つ以上のファイルに書き込めません："..." ディスクの空き容量の問題または権限の問題を解決して、もう一度実行してください。

ディスクの空き容量または権限をチェックします。問題が見つかった場合は、これを修正し、エラーのあった操作をもう一度試してください。

サーバー接続がなくなりました。 再接続してもう一度実行します。 これらのファイルにはデータがない可能性があります："..."

コマンドラインパラメーター

Nov 19, 2015

次の表は、Citrix Receiver for Linuxで使用できるコマンドラインパラメーターの一覧です。

注：パラメーターの一覧を次のように入力して取得できます。wficaまたはstorebrowseに、オプション-?、-help、または-hを付加します。

接続ファイルを使用するには、wficaの後にそのファイルの名前を入力します。次のオプションは指定しません。

目的	種類
使用するカスタムコネクションを接続ファイルから選択する。 注：セルフサービスユーザーインターフェイスを使用する場合、この方法でカスタムコネクションをセットアップすることはできません。	-desc description -description description
起動に使用するデスクトップファイルを指定する。	-desktop filename
接続ファイルを指定する。	-file connection filename
代替プロトコルファイルを設定する。別のmodule.iniを使うことができます。	-protocolfile filename
代替クライアント構成ファイルを設定する。別のwfclient.iniを使うことができます。	-clientfile filename
Receiver名として、で指定した名前を表示する。デフォルトではデバイス名がReceiver名として表示されます。ただしSunrayデバイスを使用している場合は、デフォルト名はデバイスのMACアドレスから取得されます。これは、.ICAClient/wfclient.iniのClientNameエントリにより上書きされますが、このエントリも-clientname コマンドで上書きできます。	-clientname name
この表のパラメーター一覧を表示する。	-help
バージョン情報を表示する。	-version
エラーコードおよび文字列を表示する。	-errno
Receiverインストールファイルの場所を設定する。これは、ICAROOT環境変数を設定することと同じです。	-icaroot directory

目的	種類
コネクションダイアログボックスが表示されないようにする。	-quiet
接続処理のログを記録する。	-log
キーロギングを有効にする。	-keylog
セッションのジオメトリを設定する。	-geometry WxH+X+Y
ウィンドウの色数を設定する。	-depth <4 | 8 | 16 | 24 | auto>
マルチモニターの表示を設定する。	-span [h][o] [a|[,[,,]]]
クライアントデバイスのカラーマップを使用する。	-private
共有カラーマップを使用する。	-shared
公開アプリケーションに渡す文字列を指定する。	-param string
公開アプリケーションからクライアントドライブマッピングを使ってアクセスするUNIXパスを指定する。	-fileparam unixpath
ユーザー名を指定する。	-username username
偽装パスワードを指定する。	-password password
クリアテキストのパスワードを指定する。	-clearpassword "<clear password>"
ドメインを指定する。	-domain domain
初期プログラムを指定する。	-program program
使用する初期プログラムのディレクトリを指定する。	-directory directory
サウンドをオンにする。	-sound

目的	種類
サウンドをオフにする。	-nosound
ドライブマッピングの上書きを設定する。A$=形式で指定します。ここでは、環境変数が含まれている場所です（A$=$HOME/tmpなど）。ドライブごとに、このパラメーターを指定してください。上書き設定が正しく適用されるようにするには、上書きする既存のマッピングが存在する必要があります。	-drivemap string

ヒント：すべてのwficaコマンドのオプションは環境変数WFICA_OPTSでも使用できます。これにより、ReceiverのネイティブUIやCitrix StoreFrontでもこれらのオプションを使用できます。

次の表は、storebrowseコマンドのオプションの一覧です。

オプション	説明	説明
-L、--launch	接続先の公開リソースの名前を指定します。これにより、公開リソースへの接続が起動します。セッションは接続されたまま、コマンドが終了します。	
-E、--enumerate	使用可能なリソースが列挙されます。	デフォルトでは、リソース名、表示名、およびそのリソースを格納するフォルダー名が表示されます。ほかの情報を表示するには、--detailsオプションを指定します。
-S、--subscribed	サブスクリプションするリソースを一覧表示します。	デフォルトでは、リソース名、表示名、およびそのリソースを格納するフォルダー名が表示されます。ほかの情報を表示するには、--detailsオプションを指定します。
-M、--details 次の-Eまたは-Sオプションと共に使用します。	列挙する公開アプリケーションの属性を指定できます。引数として、列挙する属性の値の合計値を指定します。属性の値は、Publisher（0x1）、VideoType（0x2）、SoundType（0x4）、AppInStartMenu（0x8）、AppOnDesktop（0x10）、AppIsDesktop（0x20）、AppIsDisabled（0x40）、WindowType（0x80）、WindowScale（0x100）、DisplayName（0x200）、およびAppIsMandatory（0x10000）です。 -S、-s、および-uオプションでは、CreateShortcuts（0x100000）を指定して、サブスクライブしたアプリケーションのメニュー項目を作成できます。-Sオプションでは、RemoveShortcuts（0x200000）を指定して、すべてのメニュー項目を削除できます。	これらの情報の一部は、storebrowseでは使用できません。この場合、0が出力されます。 これらの属性値は、16進数または10進数で指定できます（0x200または512など）。

オプション	説明	説明
-v、--version	storebrowseのバージョン番号が標準出力に出力されます。	
-h、-?、--help	storebrowseの使用方法が表示されます。	この表を簡潔にした内容が表示されます。
-U、--username	ユーザーのユーザー名を指定します。	これらのオプションは廃止予定であり、将来のリリースで削除される場合があります。Program Neighborhoodエージェントサイトで使用でき、StoreFrontサイトでは無視されます。これらのオプションを使用する代わりに、ユーザーに資格情報を入力させることをお勧めします。
-P、--password	ユーザーのパスワードを指定します。	
-D、--domain	ユーザーのドメインを指定します。	
-r、--icaroot	Receiver for Linuxのインストール先のルートディレクトリを指定します。	ディレクトリを指定しない場合は、実行時に値が特定されます。
-i、--icons 次の-E、または-Sオプションと共に使用します。	デスクトップまたはアプリケーションのアイコンをPNG形式で取得します。アイコンのサイズや解像度は、bestまたはsize引数で指定します。 引数bestを使用すると、サーバー上で使用可能な最適なサイズのアイコンが取得されます。取得した後で任意のサイズに変更することができます。引数bestは、ストレージや帯域幅について最も効率的であり、スクリプト化も簡単です。 引数sizeを使用すると、指定のサイズや解像度のアイコンがフェッチされます。 いずれの引数でも、-Eまたは-Sオプションで返されるリソースごとにアイコンファイルが作成されます。	引数bestで取得されるアイコンファイルの名前は、.pngです。 引数sizeは「WxB」形式で指定します。ここで「W」はアイコンの幅（すべてのアイコンは正方形なので幅のみを指定します）で、「B」は色の解像度（1ピクセルあたりのビット数）です。「W」は必須ですが、「B」は省略できます。「B」を省略すると、そのサイズで使用可能なすべての解像度のアイコンが取得されます。作成されるアイコンファイルの名前は、_WxWxB.pngです。
-u、--unsubscribe	指定したストアのリソースのサブスクリプションを解除します。	
-s、--subscribe	指定したストアのリソースをサブスクライブします。	異なるReceiverを使用する場合は、Program Neighborhood Agentサーバーのサブスクリプションは失われます。
-W [r|R]、--reconnect [r|R]	アクティブセッションおよび切断セッションに再接続されます。	rを指定すると、すべての切断セッションに再接続されます。Rを指定すると、すべてのアクティブセッションおよび切断セッションに再接続されます。
-WD、--disconnect	すべてのセッションが切断されます。	指定したストアのセッションにのみ適用されます。
-WT、--logoff	すべてのセッションからログオフされます。	指定したストアのセッションにのみ適用されま

オプション	説明	説明
-l、--liststores	storebrowseで接続可能なStoreFrontストアの一覧を表示します。これらは、ServiceRecordプロキシで登録されたストアです。また、Program Neighborhoodサイトの一覧も表示されます。	す
-a、--addstore	新しいストアをService Recordデーモンに登録します。ゲートウェイやビーコンの情報も登録されます。	ストアの完全なURLを返します。失敗するとエラーが表示されます。
-g、--storegateway	Service Recordデーモンに登録済みのストアのデフォルトのゲートウェイを設定します。	以下の構文で使用します。 ./util/storebrowse --storegateway "" " 重要：ストアのゲートウェイの一覧で、同じゲートウェイ名を使用することはできません。
-d、--deletestore	ストアのService Recordデーモンへの登録を解除します。	
-c、--configselfservice	セルフサービスユーザーインターフェイスの設定を取得および設定します。この設定は、StoreCache.ctxに格納されます。引数は、形式で指定します。「entry」のみを指定すると、現在の設定値が出力されます。「value」を指定すると、その値がセルフサービスユーザーインターフェイスに設定されます。	例：storebrowse --configselfservice SharedUserMode=True 重要：「entry」および「value」では大文字と小文字が区別されます。StoreCache.ctxに格納されている設定と大文字/小文字が異なる場合、そのコマンドは失敗します。
-C、--addCR	Citrix Receiver（CR）ファイルを読み取って、各ストアの追加を確認するメッセージを表示します。	-aオプションと同じ出力が得られますが、複数のストアが含まれる場合があります（各行に1つのストア）。
-K、--killdaemon	storebrowseデーモンプロセスを強制終了します。	すべての資格情報およびトークンがパージされます。

重要：pnabrowseは廃止予定のユーティリティですが、これを使用してWeb InterfaceのProgram Neighborhoodエージェントサイトからサーバーや公開リソースの一覧を照会して、これらに接続することができます。pnabrowseのStoreFrontストアでの使用はお勧めしません。代わりに、storebrowseを使用してください。storebrowseは、サイトおよびストアから資格情報を要求できます。-U、-P、および-Dオプションは、Program Neighborhoodエージェントサイトでのみ動作します。
必要に応じて、接続先サーバーを指定する引数を指定できます。以下のいずれかの方法でサーバーを指定します。

- -Sおよび-Aオプションでは、XenAppサーバーの名前を指定します。
- -Eおよび-Lオプションでは、Web InterfaceサーバーのURLを指定します。

pnabrowseユーティリティは、処理の成功または失敗を示す終了値を返します。XenAppで以下のオプションを使用できます。

オプション	説明

オプション	説明
-S	共有バーの一覧を各行に1つずつ出力します。
-A	公開アプリケーションの一覧を各行に1つずつ出力します。
-m	-Aオプションと一緒に指定して、公開アプリケーションに関するより詳細な情報（Publisher、Video Type、Sound Type、AppInStartMenu、AppOnDesktop、AppIsDesktop、AppIsDisabled、Window Type、WindowScale、およびDisplay Name.）を出力します。
-M	-Aオプションと一緒に指定して、公開アプリケーションに関する特定の情報を出力します。引数として、列挙する属性の値の合計値（1-1023）を指定します。属性の値は、Publisher（1）、VideoType（2）、SoundType（4）、AppInStartMenu（8）、AppOnDesktop（16）、AppIsDesktop（32）、AppIsDisabled（64）、WindowType（128）、WindowScale（256）、およびDisplayName(512)です。
-c	-Aオプションに追加して、クライアントエンジンで公開アプリケーションに接続するための（最低限の）情報（アプリケーション名、ブラウズサーバー、ウィンドウ解像度、色数、オーディオ、および暗号化設定など）を指定するファイルを作成します。作成されるファイルには、/tmp/_1.ica、/tmp/_2.icaなどの名前が設定されます（はpnabrowseプロセスの10進数の識別子）。
-d	-Lと一緒に使用されて、XDGデスクトップファイルを指定します。
-e	エラー数を表示します。
-i	-Aオプションでの出力に、公開アプリケーションのアイコンイメージファイルのパスを追加します。指定するサイズ（WxB）オプションにより、XPMまたはPNGファイルのパスが返されます。 ● 「-i」を指定すると、XPM形式で1ピクセルあたり4ビットの16x16アイコンが返されます。 ● 「-iWxB」を指定すると、PNG形式で1ピクセルあたりBビットのWxWアイコンが返されます。
-f	-Aオプションでの出力に、公開アプリケーションのXenAppでのフォルダー名を追加します。
-u	プロキシサーバーに対するユーザー名を指定します。
-p	プロキシサーバーに対するパスワードを指定します。

次のオプションは、Citrix XenApp（Program Neighborhoodエージェント）サービス機能を提供し、XenAppおよびXenDesktop機能の両方で使用できます。

オプション	説明
-D	Web InterfaceサーバーまたはCitrix XenApp（Program Neighborhoodエージェント）Serviceのサーバーでユーザーを認証するためのドメインを指定します。

オプション	説明
-E	Citrix XenAppに照会して、すべての公開リソースを列挙します。 -Eおよび-Lの両方を指定した場合は、最後のオプションが適用されます。ユーティリティは終了し、コネクションは開いたままになります。 各リソースについて、以下の情報が標準出力に出力されます。各項目は一重引用符で囲まれ、タブ文字で区切られます。 Name：アプリケーションの表示名。Access管理コンソールのアプリケーションのプロパティダイアログボックスに表示されます。 Folder：アプリケーションのProgram Neighborhoodフォルダー名。Access管理コンソールのアプリケーションのプロパティダイアログボックスに表示されます。 Type：アプリケーション（Application）またはコンテンツ（Content）。 Icon：XPM形式のアイコンファイルのフルパス。
-L	接続先の公開リソースの名前を指定します。これによりCitrix XenAppが照会され、公開リソースへの接続が起動します。-Eおよび-Lの両方を指定した場合は、最後のオプションが適用されます。ユーティリティは終了し、コネクションは開いたままになります。
-N	新しいパスワードを指定します。このオプションは、既存の資格情報と一緒に指定する必要があります。また、既存のパスワードの有効期限が切れた場合（終了コード238： E_PASSWORD_EXPIREDで示されます）のみ有効です。
-P	Web InterfaceサーバーまたはCitrix XenApp（Program Neighborhoodエージェント）Serviceのサーバーでユーザーを認証するためのパスワードを指定します。
-U	Web InterfaceサーバーまたはCitrix XenApp（Program Neighborhoodエージェント）Serviceのサーバーでユーザーを認証するためのユーザー名を指定します。
-WD	そのユーザーのすべてのアクティブセッションを切断します。
-WT	そのユーザーのすべてのセッションを終了します。
-Wr	そのユーザーのすべての切断セッションを再接続します。
-WR	そのユーザーのすべてのセッション（アクティブセッションおよび切断セッション）を再接続します。
-k	ユーザー名、パスワード、およびドメインの代わりに、既存のKerberosチケットを使用して認証します。クライアント側およびサーバー側で構成が必要です。詳しくは、「 *— Using Kerberos with Citrix Receiver for Linux Guide*

オプション	説明
-A	を参照してください。このドキュメントは、Citrixより秘密保持契約の下で提供されます。

以下の共通オプションも使用できます。

オプション	説明
-q	サイレントモード。エラーメッセージを出力しません。
-r	-Eまたは-Aオプションでの出力に、公開アプリケーションの生アイコンデータを追加します。
-V	バージョンの詳細を表示します。
-h	各オプションの使用方法を表示します。
-?	各オプションの使用方法を表示します。