リナックス バーチャル デリバリー エージェント 2303

重要:

現在のリリース (CR) および長期サービスリリース (LTSR) の製品ライフサイクル戦略については、Lifecycle Milestonesに記載されています。

Linux Virtual Delivery Agent (VDA) は、Citrix Workspace™アプリがインストールされているあらゆるデバイスからどこからでも、Linux仮想アプリとデスクトップへのアクセスを可能にします。

(/ja-jp/linux-virtual-delivery-agent/current-release/system-requirements.html)に基づいて仮想アプリとデスクトップを配信できます。Linux仮想マシン (VM) にVDAソフトウェアをインストールし、Delivery Controllerを構成し、Citrix Studioを使用してアプリとデスクトップをユーザーに提供します。

新機能

2303の新機能

Linux VDA バージョン 2303 には、次の新機能と機能強化が含まれています。

RHEL 9.1 および Rocky Linux 9.1 のサポート

サポート対象のディストリビューションとして、RHEL 9.1 および Rocky Linux 9.1 を追加しました。詳しくは、「システム要件」を参照してください。

新しい Linux ストリーミングターゲットデバイスのサポート

Linux ストリーミングは、以下のディストリビューションに拡張されました。

- RHEL 9.1
- RHEL 9.0
- ロッキー・リナックス 9.1
- ロッキー・リナックス 9.0

詳しくは、Citrix Provisioning のドキュメントの「Linux ターゲットデバイスのストリーミング」を参照してください。

簡単インストール機能の強化

簡単インストール機能を強化し、サイレントモードと対話モードの両方でユーザーエクスペリエンスを向上させました。主な機能強化のリストを次に示します。

- GUI および ctxinstall.sh に必要なすべての環境変数の値を設定、保存、同期するための簡単インストールの構成ファイルとして、**/opt/Citrix/VDA/sbin/ctxinstall.conf** を追加しました。
- 堅牢性を向上させるために、変数構成の検証を追加しました。
- ctxinstall.sh を実行するためのコマンドオプションを追加しました。詳しくは、ヘルプコマンド **ctxinstall.sh -h** を使用してください。

簡易インストールの使用に関する詳細については、「簡易インストールを使用してドメイン参加済みVDAを作成する」を参照してください。

XDPingの機能強化

XDPingツールに、VDA登録ステータスを確認および分析するための分析モジュールを追加しました。VDA登録ステータスを確認するには、**sudo /opt/Citrix/VDA/bin/xdping -a**コマンドを実行します。

また、**XDPing**テストカテゴリを拡張し、依存関係、Kerberos、PAMのチェックを含めました。特定のチェックを実行するには、**sudo /opt/Citrix/VDA/bin/xdping -T dependency,kerberos,pam**コマンドを実行します。

詳細については、「XDPing」、「フェデレーション認証サービス」、および「スマートカード」を参照してください。

以前のリリースでの新機能

1912 LTSRから2301 CRまでにリリースされたバージョンに含まれる新機能については、「新機能の履歴」を参照してください。

修正された問題

Linux Virtual Delivery Agent 2301以降、以下の問題が修正されました。

- Citrix Cloud™を介して管理されているLinux VDAセッションへの再接続の試行は、次のエラーメッセージとともに失敗する可能性があります。

  ```
  citrix-ctxloginauth: : pam_authenticate err[7],can retry for user
  ```

- Linux VDAセッションの起動時にグレースクリーンが表示されることがあります。
- Ubuntuを実行しているLinux VDAセッションのクリーンアッププロセスが停止したままになることがあります。
- VDAが登録状態であっても、Linux VDAセッションの開始の試行が失敗する可能性があります。
- シームレスではない公開アプリケーションは、起動直後に終了する可能性があります。この問題は、Mutterがmutter-3.28.3-4より新しいバージョンにアップグレードされた後に発生します。この問題を回避するには、mutter-3.28.3-4以前を使用してください。

既知の問題

本リリースで確認されている問題は次のとおりです。

- HDX™ 3D Proが有効な場合、拡張モニター上のセッションはブラックアウトし、プライマリモニターのみがセッションを適切に表示します。この問題を解決するには、VDAでターミナルを開き、必要に応じて次のコマンドを実行します。
  - デュアルモニターの場合、次を実行します。

    ```
    #sed -i "/UseEDID/a \ \ Option \"ConnectedMonitor\" \"DFP, DFP\"" /
    etc/X11/ctx-nvidia-2.conf
    ```

  - トリプルモニターの場合、次を実行します。

    ```
    #sed -i "/UseEDID/a \ \ Option \"ConnectedMonitor\" \"DFP, DFP,
    DFP\"" /etc/X11/ctx-nvidia-3.conf
    ```

  - クアッドモニターの場合、次を実行します。

    ```
    #sed -i "/UseEDID/a \ \ Option \"ConnectedMonitor\" \"DFP, DFP, DFP,
    DFP\"" /etc/X11/ctx-nvidia-4.conf
    ```

- **/var/log/xdl/jproxy.log**で次のLDAP例外がスローされるため、VDA登録が失敗する可能性があります。

  ```
  javax.naming.NamingException: LDAP response read timed out, timeout
  used: 10000 ms.
  ```

  この問題を回避するには、次の手順を実行します。

  - LDAPタイムアウト値を変更します。たとえば、次のコマンドを使用してLDAPタイムアウト値を60秒に変更します。

    ```
    ctxreg create -k "HKLM\Software\Citrix\GroupPolicy\Defaults" -t
    "REG_DWORD" -v "LDAPTimeout" -d "0x000EA60" --force
    ```

  - 検索ベースを設定してLDAPクエリを高速化します。ctxsetup.shでCTX_XDL_SEARCH_BASE変数を使用するか、次のコマンドを使用して検索ベースを設定できます。

```
ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t
"REG_SZ" -v "LDAPComputerSearchBase" -d "<specify a search base
instead of the root of the domain to improve search performance>" --
force
```

- Microsoftは、2022年11月にWindows 10用の累積更新プログラムKB5019966およびKB5019964をリリースしました。これらの更新プログラムにより、ドメイン参加と登録に失敗が発生します。この問題を回避するには、Knowledge Centerの記事CTX474888を参照してください。
- Kerberos で**RC4_HMAC_MD5**暗号化タイプが許可されている場合、Linux VDAがControllerに登録できないことがあり、次のエラーメッセージが表示されます。

  エラー: GSS-APIレベルで指定されていない障害（メカニズムレベル: HMAC付きRC4暗号化タイプはサポートされていません/有効になっていません）

  この問題を回避するには、Active Directoryドメインで**RC4_HMAC_MD5**をグローバルに無効にする（*またはOUで具体的に無効にする*）か、Linux VDAで弱い暗号化タイプを許可します。その後、**klist -li 0x3e4 purge**コマンドを使用してControllerおよびCitrix Cloud Connector™上のキャッシュされたKerberosチケットをクリアし、Linux VDAを再起動します。

  アクティブディレクトリドメインで**RC4_HMAC_MD5**をグローバルに無効にするには、次の手順を実行します。

  a. グループポリシー管理コンソールを開きます。
  b. ターゲットドメインを見つけて、**Default Domain Policy**を選択します。
  c. 「**Default Domain Policy**」を右クリックし、「**Edit**」を選択します。グループポリシー管理エディターが開きます。
  d. 「**コンピューターの構成 > ポリシー > Windows の設定 > セキュリティの設定 > ローカル ポリシー > セキュリティ オプション**」を選択します。
  e. 「**Network security: Configure encryption types allowed for Kerberos**」をダブルクリックします。
  f. 「**DES_CBC_CRC**」、「**DES_CBC_MD5**」、および「**RC4_HMAC_MD5**」のチェックボックスをオフにし、「**AES128_HMAC_SHA1**」、「**AES256_HMAC_SHA1**」、および「**Future encryption types**」を選択します。

  Linux VDAで脆弱な暗号化タイプを許可するには、次の手順を実行します。

  注:

> 脆弱な暗号化タイプを使用すると、展開が攻撃に対して脆弱になります。

a. Linux VDA 上の /etc/krb5.conf ファイルを開きます。

b. ****セクションに次の設定を追加します。

```
allow_weak_crypto= TRUE
```

- Linux VDAは、暗号化にSecureICA 1.0をサポートしていません。Linux VDAでSecureICA 1.0を有効にすると、セッション起動が失敗します。
- ファイルダウンロード中に予期しないウィンドウが表示されます。このウィンドウはファイルダウンロード機能には影響せず、しばらくすると自動的に消えます。
- PulseAudioのデフォルト設定では、20秒間アクティビティがないとサウンドサーバープログラムが終了します。PulseAudioが終了すると、オーディオが機能しなくなります。この問題を回避するには、/etc/pulse/daemon.confファイルでexit-idle-time=-1を設定します。
- SSL暗号化が有効でセッションの信頼性が無効になっている場合、Citrix Workspace™ app for Linuxでセッションを起動できません。
- Ubuntuグラフィック：HDX 3D Proでは、Desktop Viewerのサイズ変更後にアプリケーションの周囲に黒いフレームが表示されたり、背景が黒く表示されたりする場合があります。
- Linux VDAの印刷リダイレクトによって作成されたプリンターは、セッションからログアウトしても削除されない場合があります。
- ディレクトリに多数のファイルやサブディレクトリが含まれている場合、CDMファイルが欠落します。この問題は、クライアント側にファイルやディレクトリが多すぎる場合に発生する可能性があります。
- 非英語言語ではUTF-8エンコーディングのみがサポートされています。
- セッションローミング中に、Android版Citrix WorkspaceアプリのCAPS LOCKの状態が反転する場合があります。既存の接続をAndroid版Citrix Workspaceアプリにローミングすると、CAPS LOCKの状態が失われることがあります。回避策として、拡張キーボードのShiftキーを使用して、大文字と小文字を切り替えてください。
- Mac版Citrix Workspaceアプリを使用してLinux VDAに接続すると、ALTキーを含むショートカットキーが常に機能するとは限りません。Mac版Citrix Workspaceアプリは、デフォルトで左右のOptions/Altキーの両方に対してAltGrを送信します。この動作はCitrix Workspaceアプリの設定内で変更できますが、結果はアプリケーションによって異なります。
- Linux VDAがドメインに再参加すると、登録が失敗します。再参加により、新しいKerberosキーセットが生成されます。しかし、Brokerは以前のKerberosキーセットに基づいた、キャッシュされた古いVDAサービスチケットを使用する可能性があります。VDAがBrokerに接続しよ

うとすると、BrokerはVDAへのリターンセキュリティコンテキストを確立できない場合があります。一般的な症状は、VDA登録の失敗です。

この問題は、VDAサービスチケットの有効期限が切れて更新されると、最終的には自然に解決されます。しかし、サービスチケットは有効期間が長いため、解決には時間がかかる場合があります。

回避策として、Brokerのチケットキャッシュをクリアしてください。Brokerを再起動するか、管理者としてコマンドプロンプトからBrokerで次のコマンドを実行してください。

```
klist -li 0x3e4 purge
```

このコマンドは、Citrix Broker Serviceが実行されているNetwork Serviceプリンシパルによって保持されているLSAキャッシュ内のすべてのサービスチケットをパージします。これにより、他のVDAや潜在的に他のサービスに対するサービスチケットが削除されます。しかし、これは無害です。これらのサービスチケットは、必要に応じてKDCから再取得できます。

- オーディオのプラグアンドプレイはサポートされていません。ICA®セッションでオーディオの録音を開始する前に、オーディオキャプチャデバイスをクライアントマシンに接続できます。オーディオ録音アプリケーションの開始後にキャプチャデバイスが接続された場合、アプリケーションが応答しなくなり、再起動する必要があります。録音中にキャプチャデバイスが取り外された場合も、同様の問題が発生する可能性があります。
- Windows版Citrix Workspaceアプリでは、オーディオ録音中に音声の歪みが発生する場合があります。

サードパーティ通知

Linux Virtual Delivery Agent バージョン 2303 (PDFダウンロード)

このLinux VDAリリースには、ドキュメントで定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれる場合があります。

廃止予定

この記事のお知らせは、段階的に廃止されるプラットフォーム、Citrix®製品、および機能について事前に通知し、お客様がタイムリーなビジネス上の意思決定を行えるようにするものです。Citrixは、いつそれらが廃止されるかを決定するために、顧客の使用状況とフィードバックを監視しています。お知らせは、その後のリリースで変更される可能性があり、すべての非推奨の機能や機能性を含まない場合があります。 製品ライフサイクルサポートの詳細については、製品ライフサイクルサポートポリシーの記事を参照してください。

廃止予定と削除

次の表は、非推奨または削除されたプラットフォーム、Citrix製品、および機能を示しています。**非推奨**の項目は、すぐに削除されるわけではありません。Citrixは、このリリースでは引き続きサポートしますが、将来のCurrent Releaseで削除されます。 **削除済み**の項目は、Linux VDAで削除されたか、またはサポートされなくなっています。

項目	非推奨が発表された時期	削除時期
RHEL 8.4のサポート	2303	2308
Ubuntu 18.04のサポート	2212	2305
SUSE 15.3のサポート	2210	2301
Debian 10.9のサポート	2206	2210
SUSE 15.2のサポート	2206	2209
RHEL 8.2のサポート	2206	2209
RHEL 8.1、RHEL 8.3のサポート	2203	2206
RHEL 7.8、CentOS 7.8のサポート	2203	2204
CentOS 8.xのサポート	2110	2201
SUSE 12.5のサポート	2109	2204
Ubuntu 16.04のサポート	2109	2203
RHEL 7.7、CentOS 7.7のサポート	2006	2009
SUSE 12.3のサポート	2006	2006
RHEL 6.10、CentOS 6.10のサポート	2003	2003
RHEL 6.9、CentOS 6.9のサポート	1909	1909

項目	非推奨が発表された時期	削除時期
RHEL 7.5、CentOS 7.5のサポート	1903	1903
RHEL 7.4、CentOS 7.4のサポート	1811	1811
RHEL 6.8、CentOS 6.8のサポート	1811	1811
RHEL 7.3、CentOS 7.3のサポート	7.18	7.18
RHEL 6.6、CentOS 6.6のサポート	7.16	7.16
SUSE 11.4	7.16	7.16

新機能の履歴

この記事では、1912 LTSRから2301 CRまでにリリースされた新機能に関する情報を提供します。

2301の新機能

Linux VDAバージョン2301には、以下の新機能と機能強化が含まれています。

RHEL 8.7、Rocky Linux 8.7、およびSUSE 15.4のサポート

サポート対象のディストリビューションとして、RHEL 8.7、Rocky Linux 8.7、およびSUSE 15.4を追加しました。詳しくは、「システム要件」を参照してください。

> **注:**
>
> このリリース以降、SUSE 15.3は非推奨となります。SUSE 15.4でLinux VDAを実行するには、VDAを新規インストールしてください。

Waylandのサポート（実験的）

実験的な機能として、Linux VDAはRHEL 9.0、Rocky Linux 9.0、およびUbuntu 22.04のGNOMEでWaylandをサポートするようになりました。詳しくは、「Wayland（実験的）」を参照してください。

すべてのクライアントプリンターをLinux VDAセッションにマップできるようになりました

以前は、クライアントデバイスのデフォルトプリンターのみをLinux VDAセッションにマップできました。このリリース以降、クライアントデバイスのすべてのプリンターをLinux VDAセッションにマップできます。詳しくは、「印刷のベストプラクティス」および「PDF印刷」を参照してください。

動的なクライアントドライブマッピングとクライアントフォルダーリダイレクト

以前は、セッション開始後にクライアントに接続されたドライブはセッションにマップされませんでした。これらのドライブをセッションでアクセス可能にするには、セッションを切断して再接続する必要がありました。このリリース以降、セッション中にいつでもクライアントに接続されたドライブは自動的にマップできます。さらに、このリリースでは、クライアント上のローカルドライブのカスタム部分をセッションに動的にリダイレクトできるクライアントフォルダーリダイレクトが導入されました。詳しくは、「クライアントドライブマッピング」を参照してください。

2212 の新機能

Linux VDAバージョン2212には、以下の新機能と機能強化が含まれています。

RHEL 9.0およびRocky Linux 9.0のサポート

サポート対象のディストリビューションとして、RHEL 9.0およびRocky Linux 9.0を追加しました。詳しくは、「システム要件」を参照してください。

USBデバイスリダイレクトの機能強化

USBデバイスリダイレクトについて、以下の機能強化を行いました。

- USBデバイスリダイレクトの新しい仮想ホストコントローラーとして、USB/IPを使用するようになりました。ほとんどの場合、USB/IPカーネルモジュールはLinuxカーネルバージョン3.17以降でリリースされているため、デフォルトでカーネルモジュールをビルドする必要はありません。
- USB 3.0ポートのサポートを追加しました。クライアントデバイスのUSB 3.0ポートにUSB 3.0デバイスを挿入できるようになりました。

- バルク転送を最適化し、転送速度を向上させました。この向上は、高遅延環境でより顕著になります。
- USBデバイスリダイレクトを、**TD-RDF5A Transcend USBデバイス**や複合USBデバイスの**Yubico YubiKey OTP+FIDO+CCID**など、より多くのUSBデバイスに拡張しました。

詳しくは、「USBデバイスリダイレクト」を参照してください。

NVIDIA製特定の非仮想化GPUのハードウェアアクセラレーション

Linux VDAのドキュメントでは、非仮想化GPUとは以下を指します。

- リモートPCアクセスシナリオで使用されるGPU
- ハイパーバイザーからパススルーされたGPU

HDX 3D Proグラフィックを優れたパフォーマンスでレンダリングするために、NVIDIA製特定の非仮想化GPUのハードウェアアクセラレーションを有効にしました。特定の非仮想化GPUについては、NVIDIA Linux Capture SDKのリリースノートのサポートされるハードウェアのセクションを参照してください。

詳しくは、「非仮想化GPU」を参照してください。

スマートカードおよびFAS認証におけるpam_krb5のSSSDへの置き換え

以前は、RHEL 8およびRocky Linux 8でスマートカードまたはフェデレーション認証サービス (FAS) 認証を使用するには、pam_krb5モジュールを手動でビルドする必要がありました。このリリース以降、VDIモードで提供されるRHEL 8およびRocky Linux 8マシンでは、この手動の手順は不要になりました。詳しくは、「フェデレーション認証サービス」および「スマートカード」を参照してください。

簡単インストールGUIをMCS構成を含むように拡張

以前は、MCS変数は`/etc/xdl/mcs/mcs.conf`ファイルを編集することによってのみ構成できました。このリリースでは、簡単インストールGUIがMCS構成を含むように拡張され、GUIを使用してMCS変数を構成することもできるようになりました。GUIで**展開**をクリックすると、GUIで設定した変数が`/etc/xdl/mcs/mcs.conf`ファイルで設定した変数を上書きします。詳細については、「ステップ3：マスターイメージの準備」を参照してください。

Linuxセッションの記録のサポート（実験的）

実験的な機能として、Linux VDAでホストされているセッションを記録および再生できるようになりました。詳細については、「セッション記録（実験的）」を参照してください。

データベースオプションが利用可能になりました（実験的）

実験的な機能として、PostgreSQLに加えてSQLiteを使用できるようになりました。Linux VDAパッケージのインストール後に`/etc/xdl/db.conf`を編集することで、SQLiteとPostgreSQLを切り替えることもできます。そのためには、次の手順を実行します。

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh`を実行します。新規インストールの場合、この手順は省略してください。
2. `/etc/xdl/db.conf`を編集して、使用するデータベースを指定します。
3. インストール方法に基づいて、次のいずれかのスクリプトを実行します。

- 簡単インストールを使用している場合は、`/opt/Citrix/VDA/sbin/ctxinstall.sh`または`/opt/Citrix/VDA/bin/easyinstall`
- Linux VDAを手動でインストールしている場合は、`/opt/Citrix/VDA/sbin/ctxsetup.sh`
- MCSを使用してLinux VDAを作成している場合は、`/opt/Citrix/VDA/sbin/deploymcs.sh`

注:

- VDIモードでのみSQLiteを使用することをお勧めします。
- 手動インストールの場合、SQLiteとPostgreSQLを切り替えるには、それらを事前に手動でインストールする必要があります。簡単インストールおよびMCSの場合、手動でインストールすることなくSQLiteとPostgreSQLを切り替えることができます。
- PostgreSQLのポート番号を構成するには、`/etc/xdl/db.conf`を使用することもできます。

詳細については、インストール記事を参照してください。

2210の新機能

Linux VDAバージョン2210には、以下の新機能と機能強化が含まれています。

HDX™ 3D Pro向けGPUハードウェアアクセラレーションの強化

GPUとLinuxシステムメモリ間のデータ転送効率を改善しました。また、3Dグラフィックレンダリングとハードウェアエンコードにおける遅延を削減しました。これらの機能強化により、ハードウェアリソースの利用が最適化され、フレーム/秒（FPS）のパフォーマンスが大幅に向上します。詳細については、H.264ハードウェアエンコードを参照してください。

クリップボードを介したデータ転送のサイズ制限のサポート

ユーザーが1回のコピー＆ペースト操作でクライアントとLinux仮想セッション間で転送できるクリップボードデータの最大サイズ（KB単位）を指定できます。これを行うには、以下のポリシー設定を使用します。

- クリップボードのクライアントからセッションへの転送サイズを制限する
- クリップボードのセッションからクライアントへの転送サイズを制限する

ポリシー設定の詳細については、ICAポリシー設定のクライアントクリップボードリダイレクトセクションを参照してください。

Linux VDAがサポートするポリシー設定については、ポリシーサポートリストを参照してください。

新しいLinuxストリーミングターゲットデバイスのサポート

Linuxストリーミングは、以下のディストリビューションに拡張されました。

- RHEL 8.6
- ロッキー・リナックス 8.6
- ウブンツ 22.04

詳細については、Citrix ProvisioningドキュメントのLinuxターゲットデバイスのストリーミングを参照してください。

シェルスクリプトの機能強化

シェルスクリプトを保守しやすいように機能強化し、以下の構成テンプレートを `/etc/xdl/mcs/` から `/etc/xdl/ad_join/` に移動しました。

- winbind_krb5.conf.tmpl
- winbind_smb.conf.tmpl
- sssd.conf.tmpl
- sssd_krb5.conf.tmpl
- sssd_smb.conf.tmpl
- centrify_krb5.conf.tmpl
- centrify_smb.conf.tmpl

簡単インストールでは、特定のドメイン参加方法に関連する構成テンプレートも使用されます。

2209 の新機能

Linux VDAバージョン2209には、以下の新機能と機能強化が含まれています。

RHEL 8.6、Rocky Linux 8.6、およびUbuntu 22.04のサポート

サポート対象のディストリビューションとして、RHEL 8.6、Rocky Linux 8.6、およびUbuntu 22.04を追加しました。

SSSDおよびPBISに参加しているUbuntuおよびSUSE VDAのフェデレーション認証のサポート

フェデレーション認証サービス（FAS） のサポートを以下の種類のVDAに拡張しました。

- SSSDとPBISを使用してドメインに参加しているUbuntu VDA
- SSSDを使用してドメインに参加しているSUSE VDA。

これらのVDAにログオンするユーザーの認証にFASを使用できるようになりました。詳細については、「フェデレーション認証サービス」を参照してください。

セッションユーザーによるカスタムデスクトップ環境

セッションユーザーはデスクトップ環境をカスタマイズできるようになりました。この機能を有効にするには、VDAにデスクトップ環境を事前にインストールする必要があります。詳細については、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

GPG署名

公開キーを使用してLinux VDAパッケージの整合性を検証できるように、GPGを使用してLinux VDAパッケージに署名しました。

公開キーを取得するには：

1. Citrix Virtual Apps and Desktopsダウンロードページにアクセスします。
2. Citrix Virtual Apps and Desktopsの適切なバージョンを展開します。
3. **［Components］**をクリックして、公開キーを見つけてダウンロードします。

公開キーを使用してLinux VDAパッケージの整合性を検証するには：

- RPMパッケージの場合は、公開キーをRPMデータベースにインポートし、次のコマンドを実行します。

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

- DEBパッケージの場合は、公開キーをDEBデータベースにインポートし、次のコマンドを実行します。

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

2207の新機能

Linux VDAバージョン2207には、以下の新機能と機能強化が含まれています。

非SSOシナリオでのより多くのユーザー認証方法のサポート

以前は、シングルサインオン（SSO）が無効になっている場合、ユーザーはCitrix Workspaceアプリとセッションに異なるユーザー名を使用してログオンできました。このリリース以降、ユーザーはユーザー名またはスマートカードを使用してログオンできます。詳しくは、「非SSO認証」を参照してください。

セッションウォーターマークを構成するための追加オプション

セッションウォーターマークをさらにカスタマイズできるように、**ウォーターマークカスタムテキスト**ポリシーに新しいオプションを追加しました。たとえば、PNGウォーターマークを作成するには、**ウォーターマークカスタムテキスト**を**<image=VDA上のPNG画像へのパス>**に設定します。詳しくは、「セッションウォーターマーク」を参照してください。

KVMハイパーバイザーのサポート

Kernel-based Virtual Machine（KVM）は、Linux向けの主要なオープンソース仮想化テクノロジーです。Linuxの一部であり、Linuxマシンをハイパーバイザーに変えて、複数の分離された仮想マシン（VM）をホストできるようにします。Linux VDAはKVMハイパーバイザーで適切に動作します。ただし、KVMハイパーバイザーは、MCSを使用して仮想マシンを作成する目的ではサポートされていません。

サポートされているすべてのLinuxディストリビューションでファイルコピーと貼り付けが可能に

以前は、**ファイルコピーと貼り付け機能**はDebian 10、RHEL 7.9、およびUbuntu 18.04でのみ利用可能でした。このリリース以降、この機能はLinux VDAがサポートするすべてのLinuxディストリビューションに拡張されました。詳しくは、「ファイルコピーと貼り付け」を参照してください。

2206の新機能

Linux VDAバージョン2206には、以下の新機能と機能強化が含まれています。

Debian 11.3のサポート

サポート対象のディストリビューションとしてDebian 11.3を追加しました。

Azure AD資格情報を使用したユーザー認証のサポート

Linux VDAはAzure Active Directory（AD）と統合してユーザー認証を提供できるようになりました。この機能により、ユーザーはAzure AD資格情報を使用して、ドメインに参加していないLinuxデスクトップにログオンできます。詳しくは、「Azure Active Directoryでの認証」を参照してください。

クライアントバッテリーステータスの表示

Linux VDA は、仮想デスクトップ内のクライアントデバイスのバッテリー状態をリダイレクトして表示できるようになりました。この機能はデフォルトで有効になっています。詳細については、「クライアントのバッテリー状態の表示」を参照してください。

非vGPUグラフィックカードを使用するRemote PC Access VDAのマルチモニター機能強化

このリリースでは、ユーザーがRemote PC Accessセッションにアクセスする際に発生する以下の問題に対処しています。

- リモートPCのモニターをブラックアウトできません。セッションコンテンツを表示すると、セキュリティリスクが生じる可能性があります。
- 複数のモニターを使用してRemote PC Accessセッションにアクセスすると、モニターにアーティファクトが表示されることがあります。

詳細については、「非vGPUグラフィックカード」を参照してください。

セッションログオン画面のカスタム背景とバナーメッセージ

カスタム背景とバナーメッセージを使用して、セッションログオン画面をカスタマイズできるようになりました。詳細については、「セッションログオン画面のカスタム背景とバナーメッセージ」を参照してください。

自動DPIスケーリング

Linux VDAは、自動DPIスケーリングをサポートするようになりました。ユーザーが仮想デスクトップまたはアプリケーションセッションを開くと、セッション内のDPI値はクライアント側のDPI設定と一致するように自動的に変更されます。詳細については、「自動DPIスケーリング」を参照してください。

LDAPクエリの高速化

ポーリングモードで各LDAPサーバーをクエリするだけでなく、Linux VDAはマルチドメインフォレスト内のLDAPサーバーを同時にクエリできるようになりました。LDAPクエリを高速化するには、ドメインコントローラーで**グローバルカタログ**を有効にし、関連するLDAPポート番号を3268として指定します。LDAPサーバーとLDAPポートの指定方法については、お使いのディストリビューションに基づいたLinux VDAインストール記事のCTX_XDL_LDAP_LIST変数の説明を参照してください。

カスタムFASポート

以前は、Linux VDAはポート80を介してFASサーバーと通信するようにハードコードされていました。このリリース以降、ctxsetup.shのCTX_XDL_FAS_LISTを介してLinux VDA側でFASポートをカスタマイズできます。詳細については、お使いのディストリビューションに基づいたLinux VDAインストール記事を参照してください。

2204の新機能

Linux VDA のバージョン 2204 には、次の新機能と機能強化が含まれています。

ハードウェアエンコードが選択的コーデックに拡張されました

以前は画面全体でのみ利用可能でしたが、H.264 ハードウェアエンコードは、アクティブに変化する領域での選択的な使用をサポートするようになりました。この機能により、CPU のビデオ圧縮処理がハードウェアにオフロードされ、画質と 1 秒あたりのフレーム数 (FPS) が向上します。この機能を有効にする方法については、「グラフィックの構成と微調整」を参照してください。

一時ホームディレクトリを使用したログオンのサポート

このリリース以降、Linux VDA 上のマウントポイントが失敗した場合に備えて、一時ホームディレクトリを指定できます。一時ホームディレクトリが指定されている場合、マウントポイントが失敗

すると、セッションログオン中にプロンプトが表示されます。ユーザーデータは一時ホームディレクトリに保存されます。詳細については、「一時ホームディレクトリを使用したログオン」を参照してください。

Rendezvous HDX トラフィックの SOCKS5 プロキシサポート

Linux VDA は、Rendezvous 接続を確立するための SOCKS5 プロキシサポートを拡張しました。詳細については、「Rendezvous V1」および「Rendezvous V2」を参照してください。

Rendezvous の透過型プロキシサポート

Rendezvous で透過型 HTTP プロキシがサポートされるようになりました。ネットワークで透過型プロキシを使用している場合、VDA で追加の構成は必要ありません。

GNOME Classic デスクトップのサポート

このリリースでは、ctxsetup.sh の `CTX_XDL_DESKTOP _ENVIRONMENT` を介して指定できるデスクトップオプションとして GNOME Classic が追加されました。詳細については、お使いのディストリビューションに基づいた Linux GNOME Classic VDA インストール記事を参照してください。

アプリケーションのタスクバーボタンのグループ化

以前は、同じセッションで実行されている公開アプリケーションのすべてのタスクバーボタンが 1 つのグループにまとめられていました。このリリース以降、アプリケーションの複数のウィンドウが開いている場合でも、各アプリケーションは単一のタスクバーボタンとして表示されます。

2203の新機能

Linux VDA のバージョン 2203 には、次の新機能と機能強化が含まれています。

Rendezvous V2 の完全サポート

Citrix Gatewayサービスを使用する場合、Rendezvousプロトコルにより、トラフィックはCitrix Cloud™ Connectorsをバイパスし、Citrix Cloudコントロールプレーンに直接かつ安全に接続できます。

考慮すべきトラフィックには、次の2種類があります。1) VDA登録およびセッションブローカリングのための制御トラフィック、2) HDXトラフィック。

Rendezvous V1では、HDXトラフィックがCloud Connectorsをバイパスできますが、VDA登録およびセッションブローカリングのためのすべての制御トラフィックをプロキシするには、Cloud Connectorsが引き続き必要です。

シングルセッションおよびマルチセッションのLinux VDAでRendezvous V2を使用する場合、標準のADドメイン参加マシンと非ドメイン参加マシンがサポートされます。非ドメイン参加マシンでは、Rendezvous V2により、HDXトラフィックと制御トラフィックの両方がCloud Connectorsをバイパスできます。

詳しくは、「Rendezvous V2」を参照してください。

Easy install GUIが利用可能になりました

以前は、easy installを使用するためにコマンドラインインターフェイスしか操作できませんでした。このリリースでは、次の操作をガイドするeasy install GUIが提供されます。

- システム環境を確認する
- 依存関係のインストール
- VDAを指定されたドメインに参加させる
- ランタイム環境を構成する

easy install GUIを使用するには、VDAのデスクトップ環境で `/opt/Citrix/VDA/bin/easyinstall` コマンドを実行します。詳しくは、「easy installを使用したクイックインストール（推奨）」の記事の「**対話モード**」セクションを参照してください。

HDXグラフィックの改善

Thinwireは、特定のタスクを並列化することで、1秒あたりのフレーム数（FPS）を向上させることができるようになりましたが、全体的なCPU消費量がわずかに増加するというオーバーヘッドがあります。この機能はデフォルトで無効になっています。詳しくは、「グラフィックの構成」の記事の「並列処理」セクションを参照してください。

2201の新機能

Linux VDAのバージョン2201には、次の新機能と機能強化が含まれています。

SUSE 15.3およびSUSE 15.2でのMATEデスクトップのサポート

SUSE 15.3およびSUSE 15.2セッションのデフォルトデスクトップとしてMATEを指定できるようになりました。デスクトップ環境の詳細については、インストール記事を参照してください。

セッションシャドウイング機能がすべてのサポート対象ディストリビューションに拡張されました

セッションシャドウイング機能を使用すると、ドメイン管理者はイントラネット内でユーザーのICAセッションを表示できます。以前はRHEL 7.xおよびUbuntu 16.04でのみ利用可能でしたが、こ

の機能はLinux VDAがサポートするすべてのディストリビューションに拡張されました。 詳細については、「セッションのシャドウイング」を参照してください。

ドメインに参加していないVDAで指定された属性を持つローカルユーザーを作成する

ドメインに参加していないVDAでホストされているセッションを開くと、VDAはデフォルト属性を持つローカルユーザーを自動的に作成します。VDAは、Citrix Workspaceアプリへのログオンに使用したユーザー名に基づいてローカルユーザーを作成します。ユーザーのユーザー識別子（UID）、グループID（GID）、ホームディレクトリ、ログインシェルなどのユーザー属性を指定できるようになりました。詳細については、「ドメインに参加していないVDA」を参照してください。

Transport Layer Security (TLS) 1.3のサポート

Linux VDAはTLS 1.3をサポートするようになりました。/opt/Citrix/VDA/sbinディレクトリにある `enable_vdassl.sh` スクリプトを使用すると、TLSを有効にし、最小TLSバージョンを設定できます。詳細については、「TLSを使用したユーザーセッションの保護」を参照してください。

> **注:**
>
> このリリース以降、Linux VDAをインストールする前に.NET Runtime 6.0をインストールする必要があります。

2112の新機能

Linux VDAバージョン2112には、以下の新機能と機能強化が含まれています。

Amazon Linux 2のサポート（実験的）

実験的機能として、Amazon Linux 2をサポート対象ディストリビューションに追加しました。詳細については、「システム要件」を参照してください。

HDX画面共有の完全サポート

以前は実験的機能として提供されていたHDX画面共有が、完全にサポートされるようになりました。仮想デスクトップの画面を、他の仮想デスクトップ上のセッションユーザーと共有できます。画面共有機能はデフォルトで無効になっています。詳細については、「HDX画面共有」を参照してください。

HTTPプロキシ経由のRendezvous接続

Linux VDAは、ICAのトランスポートプロトコルとしてTCPを使用するHTTPプロキシを介したRendezvous接続の確立をサポートするようになりました。詳細については、「Rendezvousプロトコル」を参照してください。

Rendezvousプロキシ認証

ドメイン参加済みのLinux VDAは、Rendezvous接続のためにプロキシサーバーに対して認証できるようになりました。詳細については、「Rendezvousプロトコル」を参照してください。

アダプティブオーディオのサポート

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、ネットワークの状態に基づいてオーディオサンプリングビットレートを動的に調整し、プレミアムなオーディオエクスペリエンスを提供します。詳細については、「アダプティブオーディオ」を参照してください。

新しいLinuxストリーミングターゲットデバイスのサポート

Linuxストリーミングでは、以下のオペレーティングシステムがサポートされるようになりました。

- スーゼ Linux エンタープライズ サーバー 15 SP2 (スーゼ 15.2)
- スーゼ Linux エンタープライズ サーバー 15 SP3 (スーゼ 15.3)

詳細については、Citrix Provisioningのドキュメントの「Linuxターゲットデバイスのストリーミング」を参照してください。

キーボードレイアウト同期の機能強化

WFCLIENT.iniファイルで**KeyboardLayout**を**Server Default**に設定すると、セッションに再接続した後も以前に選択したキーボードレイアウトが保持されます。

キーボード入力の機能強化

いくつかの問題に対処し、より多くの特殊文字とショートカットのサポートを追加しました。

2110の新機能

Linux VDAのバージョン2110には、以下の新機能と機能強化が含まれています。

SUSE 15.3 および SUSE 15.2 のサポート

SUSE Linux Enterprise Server 15 SP3 (SUSE 15.3) および SUSE Linux Enterprise Server 15 SP2 (SUSE 15.2) をサポート対象のディストリビューションとして追加しました。詳しくは、「システム要件」を参照してください。

SUSE 15.3、SUSE 15.2、および SUSE 12.5 の HDX Web カメラビデオ圧縮のサポート

SUSE 15.3、SUSE 15.2、および SUSE 12.5 セッションで実行されているビデオ会議アプリケーションのユーザーは、HDX Web カメラビデオ圧縮を使用して Web カメラを使用できるようになりました。詳しくは、「HDX Web カメラビデオ圧縮」を参照してください。

PowerBroker Identity Services (PBIS) を使用する MCS 作成 VM の FAS サポート

PBIS を使用して Windows ドメインに参加した MCS 作成の Linux VDA にログオンするユーザーを認証するために、FAS を使用できるようになりました。詳しくは、「フェデレーション認証サービスを構成する」および「MCS 作成 VM で FAS を有効にする」を参照してください。

ctxfascfg.sh に 2 つの環境変数が追加されました

ctxfascfg.sh に次の変数を追加しました。

- CTX_FAS_KDC_HOSTNAME: PBIS を選択した場合の Key Distribution Center (KDC) のホスト名を指定します。
- CTX_FAS_PKINIT_KDC_HOSTNAME: PKINIT KDC ホスト名を指定します。特に指定がない限り、CTX_FAS_KDC_HOSTNAME と同じです。

詳しくは、「ctxfascfg.sh を実行する」を参照してください。

Citrix Workspace™ アプリへのログオンに使用した資格情報とは異なる資格情報でのセッション起動

Citrix Workspace アプリにログオンした後、異なる資格情報を使用して Citrix Virtual Apps™ and Desktops セッションを起動できます。この機能を有効にするには、Linux VDA で次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

この機能を有効にすると、セッションの起動時に資格情報の入力を求められます。この機能は、次のディストリビューションでサポートされています。

- RHEL 8.4 / CentOS 8 (2105)
- RHEL 7.9 / CentOS 7.9
- ウブントゥ 16.04
- デビアン 10.9
- SUSE 15.3
- SUSE 15.2

2109の新機能

Linux VDAのバージョン2109には、以下の新機能と機能強化が含まれています。

HDX画面共有のサポート（実験的）

Linux VDAでは、仮想デスクトップの画面を他の仮想デスクトップのセッションユーザーと共有できるようになりました。画面共有機能はデフォルトで無効になっています。詳しくは、「HDX画面共有」を参照してください。

Linux VDA 用 Citrix Virtual Channel ソフトウェア開発キット (SDK)（実験的）

Linux VDA用Citrix Virtual Channel SDKが利用可能になりました。Virtual Channel SDKを使用すると、VDAで実行するサーバー側アプリケーションを作成できます。詳しくは、「Linux VDA用Citrix Virtual Channel SDKドキュメント」を参照してください。

Linux VDA用Citrix Virtual Channel SDKは、Citrix Virtual Apps and Desktopsダウンロードページからダウンロードできます。Citrix Virtual Apps and Desktopsの適切なバージョンを展開し、**Components**をクリックしてLinux VDAのダウンロードを選択します。

PBISを使用するVDAのFASサポート

PowerBroker Identity Services (PBIS)を使用してWindowsドメインに参加したLinux VDAにログオンするユーザーを認証するために、FASを使用できるようになりました。ctxfascfg.shの実行中にPBISを選択すると、スクリプトの指示に従ってKey Distribution Center (KDC)のホスト名を入力します。詳しくは、「フェデレーション認証サービスを構成する」を参照してください。

RHEL 8.4、RHEL 7.9、SUSE 12.5のLinuxストリーミングサポート

Citrix ProvisioningのLinuxストリーミング機能を使用すると、Citrix Virtual Apps and Desktops環境でLinux仮想デスクトップを直接プロビジョニングできます。詳細については、「Citrix Provisioningを使用してLinux VMを作成する」を参照してください。

MATEデスクトップのキーボードレイアウト同期サポート

キーボードレイアウト同期サポートをMATEデスクトップに拡張しました。クライアントデバイスのキーボードレイアウトが変更されると、MATEデスクトップ環境がインストールされているVDAのレイアウトもそれに従います。詳細については、「動的キーボードレイアウト同期」を参照してください。

セッションデータクエリユーティリティ

各Linux VDAでセッションデータを照会するために使用できるユーティリティ (`ctxsdcutil`) を提供するようになりました。VDAでホストされているすべてのセッションまたは特定のセッションの次のデータを照会するには、`/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` コマンドを実行します。`[-c]` 引数は、1秒ごとにデータを照会することを意味します。

- **入力セッション帯域幅**
- **出力セッション帯域幅**
- **出力セッション回線速度**
- **待機時間 - 最終記録**
- **ラウンドトリップタイム**
- **出力ThinWire帯域幅**
- **出力オーディオ帯域幅**
- **出力プリンター帯域幅**
- **入力ドライブ帯域幅**
- **出力ドライブ帯域幅**

新しいLinuxセッションメトリックが利用可能になりました

Linuxセッションのパフォーマンスを追跡、集計、視覚化するために、次のメトリックを追加しました。

- ログオン期間

  ログオン期間とは、ユーザーがCitrix Workspaceアプリから接続してからセッションが使用可能になるまでのログオンプロセスの測定値です。このメトリックは、Citrix DaaSのMonitorタブで確認できます。Monitorは、Citrix Virtual Apps and DesktopsのCurrent ReleaseおよびLTSR展開を監視およびトラブルシューティングするためのDirectorコンソールとして利用できます。

- セッションの自動再接続数

Citrix DirectorとMonitorの両方の**トレンド**ビューで、Linuxセッションにおける自動再接続の数を表示できるようになりました。自動再接続は、**セッションの信頼性**または**クライアントの自動再接続**ポリシーが有効な場合に有効になります。セッションの再接続について詳しくは、セッションを参照してください。ポリシーについて詳しくは、クライアントの自動再接続ポリシー設定およびセッションの信頼性ポリシー設定を参照してください。

詳しくは、「Linux VMとLinuxセッションの監視」を参照してください。

2107の新機能

Linux VDAバージョン2107には、次の新機能と機能強化が含まれています。

MCSで作成されたRHEL 7/CentOS 7およびRHEL 8/CentOS 8マシンに対するCentrifyのサポート

MCSで作成されたRHEL 7/CentOS 7およびRHEL 8/CentOS 8マシンをWindowsドメインに参加させるためのCentrifyサポートを追加しました。詳しくは、「Machine Creation Services（MCS）を使用してLinux VMを作成する」を参照してください。

USBリダイレクトのカーネルモジュール再構築の簡素化

Linux VDAソースコードファイルcitrix-linux-vda-sources.zipに`ctxusbcfg.sh`を提供するようになりました。このスクリプトは、Dynamic Kernel Module Support（DKMS）オプションの有無にかかわらず、VHCIカーネルモジュール（`usb-vhci-hcd.ko`および`usb-vhci-iocif.ko`）のビルドを簡素化するのに役立ちます。DKMSは、カーネルがアップグレードされたときにVHCIカーネルモジュールを自動的に再構築するのに役立ちます。詳しくは、「USBリダイレクトの構成」を参照してください。

RHEL 8.4およびCentOS 8（2105）のサポート

RHEL 8.4およびCentOS 8（2105）をサポート対象のディストリビューションとして追加しました。詳しくは、「システム要件」を参照してください。

Debian向けスマートカードサポート

クライアントデバイスに接続されたスマートカードを使用して、Linux仮想デスクトップセッションにログオンする際の認証を行うことができます。このリリースでは、Debian 10.7セッションでスマートカードを使用できるようになりました。詳細については、「スマートカードのサポート」を参照してください。

2106の新機能

Linux VDAバージョン2106には、以下の新機能と機能強化が含まれています。

Linux VDAのセルフアップデート

この機能は、Linux VDAソフトウェアを即時またはスケジュールされた時間に自動的に更新するのに役立ちます。AzureのVMに対する管理者権限がない場合に特に便利です。詳細については、「Linux VDAのセルフアップデート」を参照してください。

Nutanix AHVでのMachine Creation Services™ (MCS)のサポート

MCSを使用してNutanix AHV上にLinux VMを作成できるようになりました。詳細については、「MCSを使用してNutanix AHV上にLinux VMを作成する」を参照してください。

MCSで作成されたマシンをWindowsドメインに参加させるためのPBISサポート

MCSで作成されたマシンをWindowsドメインに参加させるためのPBISサポートを追加しました。詳細については、「Machine Creation Services (MCS)を使用してLinux VMを作成する」を参照してください。

HDXウェブカメラビデオ圧縮のサポート

Linux VDAセッションで実行されているビデオ会議アプリケーションのユーザーは、HDXウェブカメラビデオ圧縮を使用してウェブカメラを使用できるようになりました。HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオを傍受し、トランスコードして圧縮します。この機能はデフォルトで有効になっています。可能な場合は常にHDXウェブカメラビデオ圧縮を使用することをお勧めします。詳細については、「HDXウェブカメラビデオ圧縮」を参照してください。

グラフィック品質スライダー

仮想Linuxセッションで実行されるグラフィックステータスインジケーターツールに、グラフィック品質スライダーを含めました。このスライダーは、画質とインタラクティブ性の適切なバランスを見つけるのに役立ちます。詳細については、「グラフィック品質スライダー」を参照してください。

CGPセッション再接続中のSecure Browserログオンユーザーに対するポリシー評価のサポート

Linux VDA は、Secure Browser サービスで設定したユーザー固有のポリシーを、CGP セッションの再接続中に評価および適用できるようになりました。以下のポリシーがサポートされています。

- クリップボード
  - クライアントクリップボードリダイレクト
  - クリップボード選択更新モード
  - プライマリ選択更新モード
- 印刷
  - クライアントプリンターリダイレクト
  - PDF ユニバーサルプリンターの自動作成
- ファイル転送
  - デスクトップとクライアント間のファイル転送を許可する
  - デスクトップからファイルをダウンロード
  - デスクトップにファイルをアップロード

RHEL 8.3 および Ubuntu 18.04 の Linux ストリーミングのサポート

以前は実験的機能として提供されていましたが、RHEL 8.3 および Ubuntu 18.04 の Linux ストリーミングが完全にサポートされるようになりました。Citrix Provisioning で Linux ストリーミング機能を使用すると、Citrix Virtual Apps and Desktops 環境に Linux 仮想デスクトップを直接プロビジョニングできます。詳しくは、「Citrix Provisioning を使用して Linux VM を作成する」を参照してください。

2104 の新機能

Linux VDA のバージョン 2104 には、以下の新機能と機能強化が含まれています。

Citrix DaaS™ でのドメインに参加していない Linux VDA のサポート

MCS を使用して、Citrix DaaS (旧 Citrix Virtual Apps and Desktops サービス) でドメインに参加していない Linux VDA を作成できるようになりました。

OpenJDK 11 が必須に

Linux VDA では、OpenJDK 11 が必要になりました。Linux VDA がサポートする Linux ディストリビューションのうち、Ubuntu 16.04 のみ OpenJDK 11 を手動でインストールする必要があります。その他のサポートされているディストリビューションでは、Linux VDA のインストール時に依存関係として OpenJDK 11 が自動的にインストールされます。

XDPing の変更点

`ctxsetup.sh`を実行しても`XDPing`はインストールされなくなりました。`XDPing`をインストールするには、`sudo /opt/Citrix/VDA/bin/xdping`を実行します。このコマンドは、`XDPing`に必要なPython3仮想環境も作成します。詳しくは、「XDPing」を参照してください。

Ubuntuのスマートカードサポート

ユーザーは、Linux仮想デスクトップセッションにログオンする際に、クライアントデバイスに接続されたスマートカードを認証に使用できます。このリリースでは、Ubuntu 20.04、Ubuntu 18.04、およびUbuntu 16.04セッションでスマートカードパススルー認証を使用できるようになりました。詳しくは、「スマートカードを使用したパススルー認証」を参照してください。

MATEデスクトップのサポート

CentOS、RHEL、Ubuntu、Debianで軽量のMATEデスクトップのサポートを追加しました。ctxinstall.sh、ctxsetup.sh、deploymcs.shスクリプトで利用可能な新しい変数を使用して、MATEまたはGNOMEデスクトップを指定できるようになりました。変数を指定しない場合、VDAに現在インストールされているデスクトップが使用されます。ただし、現在インストールされているデスクトップがMATEである場合は、この変数の値をmateに設定する必要があります。詳しくは、「簡易インストール」および「RHEL/CentOS用Linux Virtual Delivery Agentのインストール」などの手動インストールに関する記事を参照してください。

RHEL 8、CentOS 8、SUSE 12.5でのPBISサポート

RHEL 8、CentOS 8、SUSE 12.5マシンをWindowsドメインに参加させるためのPBISサポートを追加しました。

2103の新機能

Linux VDAバージョン2103には、次の新機能と機能強化が含まれています。

Debian 10.7およびCentOS 8.3のサポート

サポート対象のディストリビューションとしてDebian 10.7およびCentOS 8.3を追加しました。詳しくは、「システム要件」、「Debian用Linux Virtual Delivery Agentのインストール」、および「RHEL/CentOS用Linux Virtual Delivery Agentのインストール」を参照してください。

SUSEマシンをWindowsドメインに参加させるためのSSSDサポート

SUSEマシンをWindowsドメインに参加させるためのSSSDサポートを追加しました。

ドメイン参加済みおよび非ドメイン参加済みユースケース向けの単一Linux VDAイメージ

Citrix Virtual Apps and Desktops Standard for Azureで、ドメイン参加済みと非ドメイン参加済みの両方のLinux VDAを作成するための単一イメージを提供するようになりました。この機能により、イメージの準備とメンテナンスが簡素化されます。詳しくは、「Citrix Virtual Apps and Desktops Standard for AzureでLinux VDAを作成する」を参照してください。

ファイル転送の機能強化

プログレスバーの再設計、ダウンロード速度の高速化、およびいくつかのバグの解決により、ファイル転送機能を強化しました。また、一度に転送できるファイルの数を10個から100個に増やしました。詳細については、「ファイル転送」を参照してください。

Citrix Studioでのセッション接続タイマー構成のサポート

以前は、アイドルセッションと切断されたセッションの制限時間は、各VDAで個別に`/opt/Citrix/VDA/bin/ctxcfg`を介してのみ構成できました。このリリースでは、Citrix Studioでセッション接続タイマーを構成するための以下のポリシーが追加されています。

- **セッションアイドルタイマー**: アイドルセッションに時間制限を適用するかどうかを決定します。
- **セッションアイドルタイマー間隔**: アイドルセッションの時間制限を設定します。**セッションアイドルタイマー**が**有効**で、設定された時間内にアクティブなセッションがユーザー入力を受信しなかった場合、セッションは切断されます。
- **切断セッションタイマー**: 切断されたセッションに時間制限を適用するかどうかを決定します。
- **切断セッションタイマー間隔**: 切断されたセッションがログオフされるまでの間隔を設定します。

ポリシー設定を更新する際は、展開全体で一貫性があることを確認してください。ポリシーの詳細については、「ポリシーサポートリスト」を参照してください。

アイドルセッションの時間制限が切れると、警告メッセージが表示されます。例については、以下のスクリーンショットを参照してください。**OK**を押すと警告メッセージは閉じますが、セッションをアクティブに保つことはできません。セッションをアクティブに保つには、ユーザー入力を提供してアイドルタイマーをリセットしてください。

警告メッセージ(/en-us/linux-virtual-delivery-agent/2103/media/warning-message-idle-session-timeout.png)

Citrix DirectorでLinux VMおよびLinuxセッションの新しいメトリックが利用可能に

このリリースでは、Citrix DirectorにLinux VMおよびLinuxセッションの新しいメトリックが追加されています。

各Linux VMの新しいメトリック:

- CPUコア数
- メモリサイズ
- ハードディスク容量
- 現在および過去のCPUとメモリの使用率

各Linuxセッションの新しいメトリック:

- アイドル時間

詳細については、「Citrix DirectorでLinux VMとLinuxセッションを監視する」を参照してください。

Linux VDAのFAS機能強化

ctxfascfg.shスクリプトを実行する際に、より詳細なログ出力を提供し、ルート証明書とすべての中間証明書の両方を含むパスを指定できるようになりました。構成情報については、「フェデレーション認証サービスを構成する」を参照してください。

RHEL 8.3およびUbuntu 18.04.5のLinuxストリーミングサポート - 実験的機能

Citrix ProvisioningのLinuxストリーミング機能を使用すると、Citrix Virtual Apps and Desktops環境でLinux仮想デスクトップを直接プロビジョニングできます。詳細については、「Linuxストリーミング」を参照してください。

2012年の新機能

Linux VDAバージョン2012には、以下の新機能と機能強化が含まれています:

エンライトンド データ トランスポート (EDT) MTU 検出

EDTは、セッション確立時に最大伝送単位（MTU）を自動的に決定します。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットのフラグメンテーションを防ぎます。詳細については、「EDT MTU検出」を参照してください。

LDAPチャネルバインディングのサポート

以前は、Active Directoryでチャネルバインディングが有効になっている場合、Linux VDAはDelivery Controller™に登録できませんでした。このLinux VDAリリースでは、Active Directoryドメインコントローラーとの通信のセキュリティを強化するためにチャネルバインディングをサポートしています。Linux VDAでチャネルバインディングを有効にする前に、Python3仮想環境を作成してください。

Linux VDAに統合されたXDPing

Linux **XDPing**ツールは、Linux VDA環境における一般的な構成の問題を自動的にチェックするコマンドラインベースのアプリケーションです。以前は、CTX202015ページから**XDPing**をダウンロードし、Linux VDAとは別にツールをインストールする必要がありました。このリリース以降、`XDPing`はLinux VDAに統合され、Linux VDAのインストール時に自動的にインストールできます。

RHEL 7.9、RHEL 8.3のサポート

RHEL 7.9とRHEL 8.3をサポート対象のディストリビューションとして追加しました。

Ubuntu 20.04のサポート

以前は実験的な機能として提供されていましたが、このリリースではUbuntu 20.04が完全にサポートされます。

Rendezvousプロトコルのサポート

Linux VDAはRendezvousプロトコルをサポートするようになりました。Citrix Gatewayサービスを使用する環境では、Rendezvousプロトコルにより、HDXセッションはCitrix Cloud Connector™をバイパスし、Citrix Gatewayサービスに直接かつ安全に接続できます。

グーグル クラウド プラットフォーム (GCP) での マシン クリエーション サービス (MCS) のサポート

GCPでMCSを使用してLinux VMを作成できるようになりました。詳しくは、「Machine Creation Services (MCS)を使用してLinux VMを作成する」を参照してください。

LinuxマシンでWake on LANが利用可能に

統合されたWake on LAN機能がLinuxマシンで利用可能になりました。

> **注:**

> このリリース以降、Linux VDAをインストールする前に、.NET Core Runtime 3.1をインストールする必要があります。

2009の新機能

Linux VDAバージョン2009には、次の新機能と機能強化が含まれています。

RHEL 8.2のサポート

CitrixはRHEL 8.2をサポート対象のディストリビューションとして追加しました。

(実験的) Ubuntu 20.04のサポート

実験的な機能として、Ubuntu 20.04でLinux VDAを配布できます。

ブラウザコンテンツリダイレクトのサポート

このリリースから、Linux VDAはGoogle Chromeでのブラウザコンテンツリダイレクトをサポートします。ブラウザコンテンツリダイレクトは、許可リストにあるウェブページをクライアント側でレンダリングする機能を提供します。詳細については、「ブラウザコンテンツリダイレクト」を参照してください。

セッションウォーターマークのサポート

Linux VDAはセッションウォーターマークをサポートするようになりました。元のドキュメントの内容を変更せずに、セッション画面全体に表示するテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む人々への抑止力として、セッションデスクトップに表示されます。詳細については、「セッションウォーターマーク」を参照してください。

Citrix Virtual Apps and Desktops Standard for Azureにおけるドメイン非参加Linux VDAのサポート

Microsoft Azureから任意のデバイスに仮想アプリとデスクトップを配信するために、Citrix Virtual Apps and Desktops Standard for Azureでドメイン非参加Linux VDAを作成できるようになりました。詳細については、「Citrix DaaS Standard for AzureでLinux VDAを作成する」および「Citrix DaaS Standard for Azure」を参照してください。

動的キーボードレイアウト同期とクライアントIMEユーザーインターフェイス同期を設定するためのポリシーが利用可能に

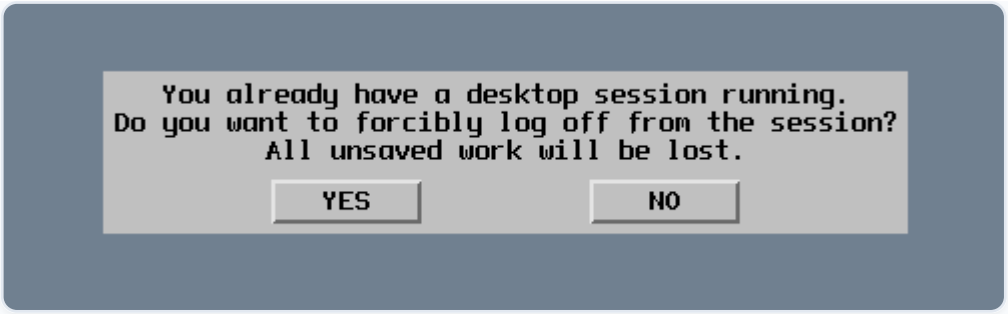
以前は、動的キーボードレイアウト同期とクライアントIMEユーザーインターフェイス同期機能を有効または無効にするには、各ターゲットVDAのレジストリを編集する必要がありました。このリリースから、**クライアントキーボードレイアウト同期とIMEの改善**ポリシーを使用してこれらの機能を設定できます。このポリシーはレジストリ設定よりも優先され、指定したユーザーおよびマシンオブジェクト、またはサイト内のすべてのオブジェクトに適用できます。詳細については、「動的キーボードレイアウト同期」および「クライアントIMEユーザーインターフェイス同期」を参照してください。

VDAから追加のデスクトップセッションを開くときに表示されるプロンプト

Citrix HDX、RDP、および直接コンソール接続を介してVDAからデスクトップセッションを開くことができます。ただし、このリリース以前は、同じUbuntu VDAから追加のHDXデスクトップセッションを開こうとすると失敗していました。この問題は、GNOMEデスクトップがインストールされているUbuntu VDAで発生していました。機能強化として、次のプロンプトで現在のデスクトップセッションから強制的にログオフすることで、新しいデスクトップセッションを続行できるようになりました。このプロンプトは、VDAがインストールされているLinuxプラットフォームに関係なく、VDAから追加のデスクトップセッションを開くたびに表示されます。

注:

- gdm3を介してVDAにログインする際にプロンプトで**はい**をクリックすると、コンソールデスクトップの画面が黒くなり、応答しないように見えます。Ctrl+Alt+F1を使用してVDAログインウィンドウに戻ることができます。
- プロンプトは30秒間表示されます。その後、回答は自動的に**いいえ**に設定されます。



2006の新機能

Linux VDAバージョン2006には、以下の新機能と機能強化が含まれています。

言語サポート

Linux VDAはイタリア語で利用できるようになりました。詳細については、Citrix製品の言語サポートを参照してください。

SUSE 12 SP5のサポート

このリリースから、Citrixはサポート対象のディストリビューションとしてSUSE 12 SP5を追加しました。

クライアントドライブマッピングの機能強化

このリリースでは、Linux VDAとクライアントデバイス間のファイル転送を高速化するために、クライアントドライブマッピングが強化されています。特にネットワーク遅延が大きい状況で効果を発揮します。

セッションとクライアント間でのファイルコピー＆ペーストのサポート

Citrix Virtual Apps and Desktops 2006およびWindows用Citrix Workspaceアプリ1903以降を使用すると、ユーザーはセッションとローカルクライアント間でファイルをコピー＆ペーストできるようになりました。コピー＆ペースト機能は、右クリックメニューまたはキーボードショートカットを使用して実行できます。詳細については、「ファイルコピー＆ペースト」(/ja-jp/linux-virtual-delivery-agent/2303/configure/file/file-copy-and-paste.html)を参照してください。

> **注:**
>
> このリリースから、Linux VDAをインストールする前に.NET Core Runtime 2.1をインストールする必要があります。

2003の新機能

Linux VDAバージョン2003には、以下の新機能と機能強化が含まれています。

RHEL 8のサポート

このリリースから、CitrixはサポートRHEL 8を追加しました。

Citrix Telemetry Serviceとの統合

Citrix Telemetry Service (**ctxtelemetry**)は、Linux VDAソフトウェアと統合されています。これで、Delivery ControllerからCitrix Scoutを実行して、Linux VDAに関するログを収集できます。詳しくは、Citrix Scoutを参照してください。

軽量NSAP仮想チャネルのサポート

Linux VDAはNSAP仮想チャネルのサポートを追加します。すべてのHDX Insightデータは、NSAP仮想チャネルからのみ取得され、非圧縮で送信されるため、スケーラビリティとパフォーマンスが向上します。詳しくは、HDX Insightを参照してください。

自動ダウンロード

Citrixは、ファイル転送の機能強化として自動ダウンロードを追加しました。これは、HTML5用Citrix WorkspaceアプリおよびChrome用Citrix Workspaceアプリで利用できます。この機能強化により、VDA上に**Save to My Device**ディレクトリが提供されます。**Save to My Device**ディレクトリにダウンロードまたは移動したファイルは、クライアントデバイスに自動的に転送されます。詳しくは、ファイル転送を参照してください。

NVIDIA Tesla T4のサポート

NVIDIA Tesla T4がサポートされています。

システム要件

Linux VDAのCurrent Releaseは、Citrix Virtual Apps and Desktopsと連携しています。また、ライフサイクルが終了していない以前のバージョンのCitrix Virtual Apps and Desktopsとも下位互換性があります。Citrix製品のライフサイクルに関する情報、およびCitrixが特定のバージョンの製品のサポートを終了する時期については、Citrix製品ライフサイクルマトリックスを参照してください。

Linux VDAの構成プロセスは、Windows VDAとは若干異なります。どのDelivery Controller™ ファームでも、WindowsデスクトップとLinuxデスクトップの両方を仲介できます。

ここで説明されていないコンポーネント（Citrix Workspace™アプリなど）のシステム要件は、それぞれのドキュメントセットで説明されています。

Long Term Service (LTSR) 環境でのCurrent Release (CR) の使用に関する情報、およびその他のFAQについては、Knowledge Centerの記事を参照してください。

サポートされているLinuxディストリビューション、Xorg バージョン、およびデスクトップ環境

このバージョンのLinux VDAがサポートするLinuxディストリビューション、Xorgバージョン、およびデスクトップ環境の表については、以下の表を参照してください。詳細については、XorgModuleABIVersionsを参照してください。

LINUXディストリビューション	XORGバージョン	サポートされているデスクトップ
アマゾン リナックス 2	1.20	グノーム、グノーム クラシック、マテ
デビアン 11.3	1.20	グノーム、グノーム クラシック、KDE、マテ
RHEL 9.1/9.0	1.20	GNOME
RHEL 8.7/8.6/8.4	1.20	ノーム、ノームクラシック、マテ

LINUXディストリビューション	XORGバージョン	サポートされているデスクトップ
RHEL 7.9, CentOS 7.9	1.20	ノーム、ノームクラシック、KDE、マテ
ロッキーリナックス 9.1/9.0	1.20	GNOME
ロッキーリナックス 8.7/8.6	1.20	ノーム、ノームクラシック、KDE、マテ
SUSE 15.4	1.20	グノーム、グノーム クラシック、マテ
ウブンツ 22.04	1.21	グノーム、グノーム クラシック、ケーディーイー、マテ
ウブントゥ 20.04	1.20	グノーム、グノーム クラシック、ケーディーイー、マテ
ウブントゥ 18.04	1.19	GNOME、GNOME クラシック、KDE、MATE

注:

- OSベンダーからのサポートが終了すると、Citrixが問題の修復にできることは限られる可能性があります。非推奨または削除されたプラットフォームについては、非推奨を参照してください。
- CentOSプロジェクトはCentOS Streamに焦点を移します。RHEL 8のリビルドであるCentOS Linux 8は、2021年末に終了します。CentOS Streamはそれ以降も継続され、Red Hat Enterprise Linuxのアップストリーム（開発）ブランチとして機能します。詳細については、`<https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux>`を参照してください。
- 少なくとも1つのデスクトップがインストールされている必要があります。セッションで使用するGNOME、GNOME Classic、またはMATEデスクトップ環境は、ctxinstall.shまたはctxsetup.shスクリプトを介して指定できます。
- Red Hat Enterprise Linuxのドキュメントによると、RHEL 9で利用可能なデスクトップ環境はGNOMEのみです。

- Ubuntuで`HWE kernel`または`HWE Xorg`を使用しないでください。
- ユーザー名の形式は、現在のディスプレイマネージャーの`systemd`構文規則に準拠している必要があります。`systemd`ユーザー名構文の詳細については、「User/Group Name Syntax」を参照してください。

サポートされているホストプラットフォームと仮想化環境

- ベアメタルサーバー
- アマゾン ウェブ サービス (AWS)
- シトリックス ハイパーバイザー™
- グーグル クラウド プラットフォーム (GCP)
- カーネルベース仮想マシン (KVM)
- マイクロソフト アジュール
- マイクロソフト Hyper-V
- VMware vSphere ハイパーバイザー
- ニュータニックス AHV

注:

すべての場合において、サポートされるプロセッサアーキテクチャはx86-64です。

2203リリース以降、Citrix Virtual Apps and DesktopsおよびCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）向けに、Microsoft Azure、AWS、GCPでLinux VDAをホストできます。これらのパブリッククラウドホスト接続をCitrix Virtual Apps and Desktops展開に追加するには、Citrix Universal SubscriptionまたはHybrid Rightsライセンスが必要です。Universal SubscriptionおよびHybrid Rightsライセンスの詳細については、「Transition and Trade Up (TTU) with Citrix Universal Subscription」を参照してください。

Active Directory統合パッケージ

Linux VDAは、次のActive Directory統合パッケージと製品をサポートしています。

	ウィンバインド	SSSD	セントリファイ	PBIS	クエスト
アマゾン Linux 2	はい	はい	はい	はい	いいえ
デビアン 11.3	はい	はい	はい	はい	いいえ
RHEL 9.1/9.0 バージョン、Rocky Linux 9.1/9.0/8.7/8.6 バージョン	はい	はい	いいえ	いいえ	いいえ
RHEL 8.7/8.6/8.4	はい	はい	はい	はい	いいえ
RHEL 7.9, CentOS 7.9	はい	はい	はい	はい	はい (Quest v4.1 以降)
SUSE 15.4	はい	はい	はい	はい	いいえ
ウブントゥ 22.04/20.04/18.04	はい	はい	はい	はい	はい (Quest v4.1 以降)

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™ の HDX 3D Pro を使用すると、ハードウェアアクセラレーションのためにグラフィックス処理ユニット (GPU) を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。

ハイパーバイザー

Linux VDA では、HDX 3D Pro は以下のハイパーバイザーと互換性があります。

- シトリックス ハイパーバイザー
- VMware vSphere ハイパーバイザー
- ニュータニックス AHV

- マイクロソフト アジュール
- アマゾン ウェブ サービス (AWS)
- グーグル クラウド プラットフォーム (GCP)

> **注:**
>
> ハイパーバイザーは特定のLinuxディストリビューションと互換性があります。 Amazon Linux 2でHDX 3D Proを使用するには、NVIDIAドライバー470をインストールすることをお勧めします。

GPU

お使いのLinuxディストリビューションがどのNVIDIA GPUカードをサポートしているかを確認するには、NVIDIA製品サポートマトリックスにアクセスし、**ハイパーバイザーまたはベアメタルOS**、**ソフトウェア製品の展開**、**サポートされているハードウェア**、および**ゲストOSのサポート**の列を確認してください。

GPUカード用の最新のvGPUドライバーをインストールしてください。現在、Linux VDAはvGPU 14までをサポートしています。詳細については、NVIDIA Virtual GPU Software Supported GPUsを参照してください。

インストールの概要

このセクションでは、以下の手順について説明します。

- 簡単なインストールを使用してドメイン参加済みVDAを作成する
- MCSを使用してドメインに参加していないLinux VDAを作成する
- MCSを使用してLinux VDAを作成する
- Citrix Provisioningを使用してLinux VDAを作成する
- Citrix DaaS Standard for AzureでLinux VDAを作成する
- Linux VDAを手動でインストールする
  - Amazon Linux 2、CentOS、RHEL、およびRocky LinuxにLinux VDAを手動でインストールする
  - SUSEにLinux VDAを手動でインストールする
  - UbuntuにLinux VDAを手動でインストールする
  - DebianにLinux VDAを手動でインストールする

easy install を使用してドメイン参加済み VDA を作成する

> **重要:**

> - 新規インストールの場合、迅速なインストールについてはこの記事を参照することをお勧めします。この記事では、easy install を使用して Linux VDA をインストールおよび構成する方法を順を追って説明します。easy install は、手動インストールよりも時間と労力を節約でき、エラーが発生しにくいです。必要なパッケージをインストールし、構成ファイルを自動的にカスタマイズすることで、Linux VDA の実行環境をセットアップするのに役立ちます。
> - easy install は、Quest を使用したドメイン参加をサポートしていません。

- ドメインに参加していない VDA を作成するには、Machine Creation Services (MCS) を使用する必要があります。詳細については、「ドメインに参加していない Linux VDA の作成」を参照してください。
- ドメインに参加していない VDA で利用可能な機能については、「ドメインに参加していない VDA」を参照してください。

ステップ 1：構成情報と Linux マシンを準備する

easy install に必要な以下の構成情報を収集します。

- ホスト名 – Linux VDA をインストールするマシンのホスト名。
- ドメインネームサーバーの IP アドレス。
- NTP サーバーの IP アドレスまたは文字列名。
- ドメイン名 – ドメインの NetBIOS 名。
- レルム名 – Kerberos レルム名。
- ドメインの完全修飾ドメイン名 (FQDN)。
- AD 統合方法 - Active Directory 統合方法。現在、easy install は Winbind、SSSD、Centrify、および PBIS をサポートしています。
- ユーザー名 – マシンをドメインに参加させるユーザーの名前。
- パスワード - マシンをドメインに参加させるユーザーのパスワード。
- ワークグループ名 – ワークグループ名。オプション。特に指定がない限り、ドメイン名と同じ値になります。
- OU – 組織単位。オプション。

重要:

- Linux VDAをインストールするには、リポジトリがLinuxマシンに正しく追加されていることを確認してください。
- セッションを起動するには、X Windowシステムとデスクトップ環境がインストールされていることを確認してください。
- セキュリティのため、簡易インストールではドメイン参加パスワードは保存されません。インタラクティブモードで簡易インストールスクリプト (ctxinstall.sh) を実行するたびに、ドメイン参加パスワードを手動で入力する必要があります。サイレントモードで

> は、ドメイン参加パスワードを **/Citrix/VDA/sbin/ctxinstall.conf** で設定するか、パスワードをエクスポートする必要があります。ドメイン参加には管理者アカウントを使用しないことをお勧めします。代わりに、管理者アカウント以外のActive Directoryユーザーにドメイン参加権限を委任してください。これを行うには、**Delegation of Control Wizard** を使用してドメインコントローラーで制御を委任します。

ステップ2：ハイパーバイザーを準備する

サポートされているハイパーバイザー上でLinux VDAを仮想マシンとして実行する場合、いくつかの変更が必要です。使用しているハイパーバイザープラットフォームに基づいて、以下の変更を行ってください。Linuxマシンをベアメタルハードウェアで実行している場合、変更は不要です。

Citrix Hypervisor™ で時刻同期を修正する

Citrix Hypervisorの時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとCitrix Hypervisorの両方がシステムクロックを管理しようとするため、問題が発生します。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。HVMモードでは変更は不要です。

Citrix VM Toolsがインストールされた準仮想化Linuxカーネルを実行している場合、Linux VM内からCitrix Hypervisorの時刻同期機能が存在し、有効になっているかを確認できます。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは0または1を返します。

- 0 - 時刻同期機能が有効になっており、無効にする必要があります。
- 1 - 時刻同期機能は無効になっており、それ以上の操作は不要です。

/proc/sys/xen/independent_wallclock ファイルが存在しない場合、以下の手順は不要です。

有効になっている場合、ファイルに1を書き込むことで時刻同期機能を無効にします。

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

この変更を再起動後も永続的に適用するには、**/etc/sysctl.conf** ファイルを編集し、次の行を追加します。

`xen.independent_wallclock = 1`

これらの変更を確認するには、システムを再起動します。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは値1を返します。

Microsoft Hyper-Vでの時刻同期の修正

Hyper-V Linux Integration Servicesがインストールされ ているLinux VMは、Hyper-V時刻同期機能を使用してホストオペレーティングシステムの時刻を使用できます。システムクロックが正確であることを保証するために、NTPサービスと並行してこの機能を有効にする必要があります。

管理オペレーティングシステムから：

1. Hyper-Vマネージャーコンソールを開きます。
2. Linux VMの設定で、**統合サービス**を選択します。
3. **時刻同期**が選択されていることを確認します。

> **注:**
>
> このアプローチは、NTPとの競合を避けるためにホスト時刻同期が無効になっているVMwareおよびCitrix Hypervisorとは異なります。Hyper-V時刻同期はNTP時刻同期と共存し、補完することができます。

ESXおよびESXiでの時刻同期の修正

VMware時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとハイパーバイザーとの間で問題が発生します。両方ともシステムクロックを同期しようとします。クロックが他のサーバーと同期しなくなるのを避けるために、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホスト時刻同期を無効にする必要があります。

VMware Toolsがインストールされた準仮想化Linuxカーネルを実行している場合：

1. vSphere Clientを開きます。
2. Linux VMの設定を編集します。
3. **仮想マシンプロパティ**ダイアログで、**オプション**タブを開きます。
4. **VMware Tools**を選択します。
5. **詳細設定**ボックスで、**ゲストの時刻をホストと同期**のチェックを外します。

ステップ3：.NET Runtime 6.0をインストールする

Linux VDAをインストールする前に、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>`の指示に従って.NET Runtime 6.0をインストールします。

.NET Runtime 6.0のインストール後、**which dotnet**コマンドを実行してランタイムパスを見つけます。

コマンドの出力に基づいて、.NETランタイムバイナリパスを設定します。たとえば、コマンドの出力が/aa/bb/dotnetの場合、/aa/bbを.NETバイナリパスとして使用します。

ステップ4：Linux VDAパッケージをダウンロードする

1. Citrix Virtual Apps and Desktopsダウンロードページにアクセスします。
2. 適切なバージョンのCitrix Virtual Apps and Desktopsを展開します。
3. **コンポーネント**をクリックして、お使いのLinuxディストリビューションに一致するLinux VDAパッケージと、Linux VDAパッケージの整合性を検証するために使用できるGPG公開キーをダウンロードします。

   公開キーを使用してLinux VDAパッケージの整合性を検証するには：

   - RPMパッケージの場合、公開キーをRPMデータベースにインポートし、次のコマンドを実行します。

     ```
     rpmkeys --import <path to the public key>

     rpm --checksig --verbose <path to the Linux VDA package>
     ```

   - DEBパッケージの場合、公開キーをDEBデータベースにインポートし、次のコマンドを実行します。

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

ステップ 5: Linux VDA パッケージをインストールする

Linux VDA の環境をセットアップするには、次のコマンドを実行します。

Amazon Linux 2、CentOS、RHEL、および Rocky Linux ディストリビューションの場合:

注:

- RHEL および CentOS の場合、Linux VDA を正常にインストールする前に EPEL リポジトリをインストールしてください。EPEL のインストール方法については、`<https://docs.fedoraproject.org/ja-jp/epel/>` の手順を参照してください。
- RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 に Linux VDA をインストールする前に、**libsepol** パッケージをバージョン 3.4 以降に更新してください。

```
sudo yum  -y localinstall   <PATH>/<Linux VDA RPM>
```

注:

GCP でホストされている RHEL 8.x/9.x および Rocky Linux 8.x/9.x に Linux VDA をインストールした後、VM の再起動後にイーサネット接続が失われ、Linux VDA に到達できなくなる可能性があります。この問題を回避するには、VM を再起動する前に次のコマンドを実行します。

```
nmcli dev connect eth0

service NetworkManager restart
```

Ubuntu/Debian ディストリビューションの場合:

```
sudo dpkg -i <PATH>/<Linux VDA deb>

sudo apt-get install -f
```

注:

- Debian 11.3 ディストリビューションに必要な依存関係をインストールするには、/etc/apt/sources.list ファイルに `deb http://deb.debian.org/debian/ bullseye main` の行を追加します。
- GCP 上の Ubuntu 20.04 の場合、RDNS を無効にします。そのためには、/etc/krb5.conf の の下に **rdns = false** の行を追加します。

SUSE ディストリビューションの場合:

1. AWS、Azure、および GCP 上の SUSE 15.4 の場合、以下を確認してください。
   - **libstdc++6** バージョン 12 以降を使用していること。
   - **/etc/sysconfig/windowmanager** の **Default_WM** パラメーターが **"gnome"** に設定されていること。
2. Linux VDA をインストールするには、次のコマンドを実行します。

   ```
   zypper -i install <PATH>/<Linux VDA RPM>
   ```

ステップ 6: NVIDIA GRID ドライバーをインストールする

HDX™ 3D Pro を有効にするには、ハイパーバイザーと VDA マシンに NVIDIA GRID ドライバーをインストールする必要があります。

特定のハイパーバイザーに NVIDIA GRID Virtual GPU Manager (ホストドライバー) をインストールして構成するには、次のガイドを参照してください。

- シトリックス ハイパーバイザー
- ヴイエムウェア ESX
- ニュータニックス AHV

NVIDIA GRID ゲスト VM ドライバーをインストールして構成するには、次の一般的な手順を実行します。

1. ゲスト VM がシャットダウンされていることを確認します。
2. ハイパーバイザーのコントロールパネルで、VM に GPU を割り当てます。
3. VM を起動します。
4. VM にゲスト VM ドライバーをインストールします。

手順 7：使用するデータベースを指定する

実験的な機能として、PostgreSQL に加えて SQLite を使用できます。Linux VDA パッケージのインストール後に `/etc/xdl/db.conf` を編集することで、SQLite と PostgreSQL を切り替えることもできます。

そのためには、`sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` または `/opt/Citrix/VDA/bin/easyinstall` を実行する前に `etc/xdl/db.conf` を編集します。

> **注:**

- SQLite は VDI モードでのみ使用することをお勧めします。
- 簡易インストールと MCS の場合、手動でインストールすることなく SQLite と PostgreSQL を切り替えることができます。`/etc/xdl/db.conf` で特に指定がない限り、Linux VDA はデフォルトで PostgreSQL を使用します。
- `/etc/xdl/db.conf` を使用して PostgreSQL のポート番号を構成することもできます。

手順 8：インストールを完了するためのランタイム環境をセットアップする

Linux VDAパッケージのインストール後、ctxinstall.shスクリプトまたはGUIを使用して実行環境を構成します。

> **注:**

ランタイム環境をセットアップする前に、OSに**en_US.UTF-8**ロケールがインストールされていることを確認してください。ロケールがOSで利用できない場合は、**sudo locale-gen en_US.UTF-8**コマンドを実行します。Debianの場合、**/etc/locale.gen**ファイルを編集して

 # en_US.UTF-8 UTF-8の行のコメントを解除し、**sudo locale-gen**コマンドを実行します。

ctxinstall.sh

ctxinstall.shは、Linux VDAのランタイム環境を構成する簡易インストールスクリプトです。詳細については、ヘルプコマンド**ctxinstall.sh -h**を使用してください。

簡易インストールでは、GUIおよびctxinstall.shに必要なすべての環境変数の値を設定、保存、同期するための構成ファイルとして**/opt/Citrix/VDA/sbin/ctxinstall.conf**を使用します。構成ファイルを初めて作成する場合は、次のいずれかの方法を使用します。

- **/opt/Citrix/VDA/sbin/ctxinstall.conf.tmpl**テンプレートファイルをコピーし、**/opt/Citrix/VDA/sbin/ctxinstall.conf**として保存します。
- ctxinstall.shを実行します。ctxinstall.shを実行するたびに、入力は**/opt/Citrix/VDA/sbin/ctxinstall.conf**に保存されます。

注:

- 最小特権の原則に従い、ドメイン参加パスワードがファイルに設定されている可能性があるため、rootユーザーのみが**/opt/Citrix/VDA/sbin/ctxinstall.conf**を読み取れるようにしてください。
- Linux VDA をアンインストールすると、**/opt/Citrix/VDA** 以下のファイルが削除されます。VDA をアンインストールする前に、**/opt/Citrix/VDA/sbin/ctxinstall.conf** をバックアップすることをお勧めします。

ctxinstall.shは、対話モードまたはサイレントモードで実行できます。スクリプトを実行する前に、次の環境変数を設定します。

- **CTX_EASYINSTALL_HOSTNAME=host-name** – Linux VDAサーバーのホスト名。
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** – DNSのIPアドレス。
- **CTX_EASYINSTALL_NTPS=address-of-ntps** – NTPサーバーのIPアドレスまたは文字列名。
- **CTX_EASYINSTALL_DOMAIN=domain-name** – ドメインのNetBIOS名。
- **CTX_EASYINSTALL_REALM=realm-name** – Kerberosレルム名。

- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_USERNAME=domain-user-name** – マシンをドメインに参加させるユーザーの名前。
- **CTX_EASYINSTALL_PASSWORD=password** – マシンをドメインに参加させるユーザーのパスワード。

> **注:**
>
> ドメイン参加には管理者アカウントを使用しないことをお勧めします。代わりに、管理者アカウント以外のActive Directoryユーザーにドメイン参加権限を委任してください。これを行うには、**Delegation of Control Wizard**を使用してドメインコントローラーで制御を委任します。

以下の4つの変数はオプションです。これらが設定されていなくても、ctxinstall.shはサイレントモードで中断せず、インタラクティブモードでユーザー入力を求められることもありません。これらの変数は、値をエクスポートするか、**/Citrix/VDA/sbin/ctxinstall.conf**を編集することによってのみ設定できます。

- **CTX_EASYINSTALL_WORKGROUP=workgroup-name** – ワークグループ名はデフォルトでドメイン名です。ニーズに合わせてワークグループをカスタマイズできます。この変数はオプションです。
- **CTX_EASYINSTALL_OU=ou-value** – OU値はADメソッドによって異なります。OU値の例については、この記事の考慮事項セクションの表を参照してください。この変数はオプションです。
- **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=centrify-local-path** – Easy installは、インターネットからCentrifyパッケージをダウンロードするのに役立ちます。ただし、Centrifyがすでにインストールされている場合は、この変数で定義されたローカルディレクトリからCentrifyパッケージを取得できます。この変数はオプションです。
- **CTX_EASYINSTALL_PBIS_LOCAL_PATH= pbis-local-path** – Easy installは、インターネットからPBISパッケージをダウンロードするのに役立ちます。ただし、PBISがすでにインストールされている場合は、この変数で定義されたローカルディレクトリからPBISパッケージを取得できます。この変数はオプションです。

ctxinstall.shを実行すると、別のスクリプトであるctxsetup.shが呼び出されます。ctxsetup.shは以下の変数を使用します。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Linux VDAは、DNS CNAMEレコードを使用してDelivery Controller名を指定することをサポートしています。
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Linux VDAは、Delivery Controllerに登録するために使用する、スペースで区切られたDelivery Controllerの完全修飾ドメイン名（FQDN）のリストを必要とします。少なくとも1つのFQDNまたはCNAMEを指定する必要があります。
- **CTX_XDL_VDA_PORT=port-number** – Linux VDAは、TCP/IPポートを介してDelivery Controllerと通信します。
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Linux Virtual Desktopサービスは、マシンの起動後に開始されます。
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Linux VDAサービスは、システムファイアウォールを介した受信ネットワーク接続が許可されている必要があります。Linux Virtual Desktopの場合、必要なポート（デフォルトではポート80と1494）をシステムファイアウォールで自動的に開くことができます。
- **CTX_XDL_AD_INTEGRATION=winbind \| sssd \| centrify \| pbis** – Linux VDAがDelivery Controllerで認証するには、Kerberos構成設定が必要です。Kerberos構成は、システムにインストールおよび構成されているActive Directory統合ツールから決定されます。
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Linux VDAは、リッチグラフィックアプリケーションの仮想化を最適化するために設計されたGPUアクセラレーションテクノロジーのセットであるHDX 3D Proをサポートしています。HDX 3D Proが選択されている場合、VDAはVDIデスクトップ（シングルセッション）モード（つまり、CTX_XDL_VDI_MODE=Y）用に構成されます。
- **CTX_XDL_VDI_MODE=Y \| N** – マシンを専用デスクトップ配信モデル（VDI）として構成するか、ホスト型共有デスクトップ配信モデルとして構成するかを決定します。HDX 3D Pro環境の場合は、値をYに設定します。
- **CTX_XDL_SITE_NAME=dns-name** – Linux VDAはDNSを介してLDAPサーバーを検出します。DNS検索結果をローカルサイトに制限するには、DNSサイト名を指定します。不要な場合は、**\<none\>**に設定します。
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Linux VDAはDNSにクエリを実行してLDAPサーバーを検出します。DNSがLDAPサービスレコードを提供できない場合、LDAPポートを持つLDAP FQDNのスペース区切りリストを提供できます。たとえば、ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268。LDAPポート番号を389として指定すると、Linux VDAは指定されたドメイン内の各LDAPサーバーをポーリングモードでクエリします。ポリシーの数がx、LDAPサーバーの数がyの場合、Linux VDAは合計XかけるYのクエリを実行します。ポーリング時間がしきい値を超えると、セッションログオンが失敗する可能性があります。より高速なLDAPクエリを有効にするには、ドメインコ

ントローラーで**Global Catalog**を有効にし、関連するLDAPポート番号を3268として指定します。この変数はデフォルトで**\<none\>**に設定されています。

- **CTX_XDL_SEARCH_BASE=search-base-set** – Linux VDAは、Active Directoryドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを介してLDAPにクエリを実行します。検索パフォーマンスを向上させるために、検索ベース（例：OU=VDI,DC=mycompany,DC=com）を指定できます。不要な場合は、**\<none\>**に設定します。
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Federated Authentication Service (FAS)サーバーは、ADグループポリシーを介して構成されます。Linux VDAはADグループポリシーをサポートしていませんが、代わりにFASサーバーのセミコロン区切りリストを提供できます。シーケンスはADグループポリシーで構成されているものと同じである必要があります。サーバーアドレスが削除された場合は、その空白を**\<none\>**テキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。FASサーバーと適切に通信するには、FASサーバーで指定されているものと一致するポート番号を追加してください。例：CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – 新しいブローカーエージェントサービス（`ctxvda`）をサポートするための.NET Runtime 6.0のインストールパス。デフォルトパスは/usr/binです。
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** – セッションで使用するGNOME、GNOME Classic、またはMATEデスクトップ環境を指定します。この変数を指定しない場合、VDAに現在インストールされているデスクトップが使用されます。ただし、現在インストールされているデスクトップがMATEである場合は、変数の値を**mate**に設定する必要があります。
- **CTX_XDL_START_SERVICE=Y \| N** – 構成完了時にLinux VDAサービスを開始するかどうかを決定します。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scoutのリッスン用ソケットポート。デフォルトポートは7503です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scoutとの通信用ポート。デフォルトポートは7502です。

考慮事項

- ワークグループ名はデフォルトでドメイン名です。環境内でワークグループをカスタマイズするには、**/opt/Citrix/VDA/sbin/ctxinstall.conf**で環境変数**CTX_EASYINSTALL_WORKGROUP**を設定します。

- VDAを特定のOUに参加させるには、次の手順を実行します。

  a. 特定のOUがドメインコントローラーに存在することを確認します。

     OU の例については、次のスクリーンショットを参照してください

     OU の例(/en-us/linux-virtual-delivery-agent/2303/media/example-ou.png)

  b. 環境変数 **CTX_EASYINSTALL_OU** を **/opt/Citrix/VDA/sbin/ctxinstall.conf** で設定します。

     OU の値は AD の方法によって異なります。次の表は、前のスクリーンショットの OU 名の例を示しています。組織内で他の OU 名を使用することもできます。

OS	ウィンバインド	SSSD	セントリファイ	PBIS
アマゾン リナックス 2	`"Linux/amazon"`	`"Linux/amazon"`	`"XD.LOCAL/Linux/amazon"`	`"Linux/amazon"`
デビアン	`"Linux/debian"`	`"Linux/debian"`	`"XD.LOCAL/Linux/debian"`	`"Linux/debian"`
RHEL 9.1/9.0、ロッキーLinux 9.1/9.0	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	該当なし	該当なし
RHEL 8.x	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`
ロッキーLinux 8.x	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	該当なし	該当なし
RHEL 7	`"Linux/redhat"`	`"Linux/redhat"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`
SUSE	`"Linux/suse"`	`"Linux/suse"`	`"XD.LOCAL/Linux/suse"`	`"Linux/suse"`

OS	ウィンバインド	SSSD	セントリファイ	PBIS
ウブントゥ	`"Linux/ubuntu"`	`"Linux/ubuntu"`	`"XD.LOCAL/Linux/ubuntu"`	`"Linux/ubuntu"`

- Centrifyは純粋なIPv6 DNS構成をサポートしていません。**adclient**がADサービスを適切に検出するには、/etc/resolv.confにIPv4を使用するDNSサーバーが少なくとも1つ必要です。

  ログ:

  ```
  ADSITE   : Check that this machine's subnet is in a site known by AD
    : Failed

          : This machine's subnet is not known by AD.

          : We guess you should be in the site Site1.
  ```

  この問題はCentrifyとその構成に固有のものです。この問題を解決するには、次の手順を実行します。

  a. ドメインコントローラーで**管理ツール**を開きます。

  b. **Active Directoryサイトとサービス**を選択します。 c. **サブネット**に適切なサブネットアドレスを追加します。

- Easy installは、Linux VDA 7.16以降で純粋なIPv6をサポートしています。以下の前提条件と制限が適用されます。

  - マシンが純粋なIPv6ネットワーク経由で必要なパッケージをダウンロードできるように、Linuxリポジトリを構成する必要があります。
  - Centrifyは純粋なIPv6ネットワークではサポートされていません。

  注:

  ネットワークが純粋なIPv6であり、すべての入力が適切なIPv6形式である場合、VDAはIPv6を介してDelivery Controller™に登録されます。ネットワークがIPv4とIPv6のハイブリッド構成である場合、最初のDNS IPアドレスのタイプによって、登録にIPv4とIPv6のどちらが使用されるかが決まります。

- ターゲットセッションユーザーのデスクトップ環境は、次の手順を実行して変更することもできます。

  a. VDA上の**$HOME/<username\>**ディレクトリの下に`.xsession`または`.Xclients`ファイルを作成します。Amazon Linux 2を使用している場合は、`.Xclients`ファイルを作成します。他のディストリビューションを使用している場合は、`.xsession`ファイルを作成します。

  b. ディストリビューションに基づいてデスクトップ環境を指定するために、`.xsession`または`.Xclients`ファイルを編集します。

  - **MATEデスクトップの場合**

```
MSESSION="$(type -p mate-session)"

if [ -n "$MSESSION" ]; then

exec mate-session

fi
```

  - **GNOME Classicデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"

if [ -n "$GSESSION" ]; then

export GNOME_SHELL_SESSION_MODE=classic

exec gnome-session --session=gnome-classic

fi
```

  - **GNOMEデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"

if [ -n "$GSESSION" ]; then

exec gnome-session
```

```
fi
```

c. ターゲットセッションユーザーと700ファイル権限を共有します。

バージョン2209以降、セッションユーザーはデスクトップ環境をカスタマイズできます。この機能を有効にするには、VDAに切り替え可能なデスクトップ環境を事前にインストールする必要があります。詳しくは、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

- ドメイン参加の方法としてCentrifyを選択した場合、ctxinstall.shスクリプトにはCentrifyパッケージが必要です。ctxinstall.shがCentrifyパッケージを取得する方法は次のとおりです。
  - 簡易インストールは、インターネットからCentrifyパッケージを自動的にダウンロードするのに役立ちます。各ディストリビューションのURLは次のとおりです。

    アマゾン Linux 2/RHEL: wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz>`

    CentOSの場合：wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz>`

    SUSEの場合：wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-suse12-x86_64.tgz>`

    Ubuntu/Debian の場合： wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz>`
  - Centrifyがすでにインストールされている場合は、ローカルディレクトリからCentrifyパッケージをフェッチします。Centrifyパッケージのディレクトリを指定するには、**/opt/Citrix/VDA/sbin/ctxinstall.conf**で**CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=/home/mydir**を設定します。例：

```
ls  -ls  /home/mydir

    9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016 adcheck-
rhel4-x86_64

    4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
centrifyda-3.3.1-rhel4-x86_64.rpm

    33492 -r--r--r--. 1 root root 34292673 May 13  2016
centrifydc-5.3.1-rhel4-x86_64.rpm
```

```
    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015 centrifydc-
install.cfg

    756 -r--r--r--. 1 root root   770991 May 13  2016 centrifydc-
ldapproxy-5.3.1-rhel4-x86_64.rpm

    268 -r--r--r--. 1 root root   271296 May 13  2016 centrifydc-
nis-5.3.1-rhel4-x86_64.rpm

    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016 centrifydc-
openssh-7.2p2-5.3.1-rhel4-x86_64.rpm

    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016 centrify-
suite.cfg

    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
express.sh -> install.sh

    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install.sh

    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-notes-
agent-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-notes-
da-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-notes-
nis-rhel4-x86_64.txt

    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-notes-
openssh-rhel4-x86_64.txt
```

- ドメイン参加の方法としてPBISを選択した場合、ctxinstall.shスクリプトにはPBISパッケージが必要です。ctxinstall.shがPBISパッケージを取得する方法は次のとおりです。
    - 簡易インストールは、インターネットからPBISパッケージを自動的にダウンロードするのに役立ちます。たとえば、各ディストリビューションのURLは次のとおりです。

      アマゾン Linux 2、CentOS 7、RHEL 8、RHEL 7、SUSE 15.4: wget `<https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh>`

デビアン、ウブントゥ: wget `<https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh>`

- インターネットから特定のバージョンのPBISパッケージをフェッチします。これを行うには、/opt/Citrix/VDA/sbin/ctxinstall.shファイル内の「pbisDownloadRelease」および「pbisDownloadExpectedSHA256」の行を変更します。

  例については、次のスクリーンショットを参照してください。

  
  ```
  local pbisDownloadURL="https://github.com/BeyondTrust/pbis-open/releases/download"
  local pbisDownloadExpectedSHA256="f37555abf22f453c3865f06eba3c5f913605c300917be29663b23941087137f6"
  local pbisDownloadFMT="rpm"
  local pbisDownloadRelease="9.1.0"
  local pbisDonwloadBuild="551"
  ```

- PBISが既にインストールされている場合、ローカルディレクトリからPBISパッケージを取得します。PBISパッケージのディレクトリを指定するには、**/opt/Citrix/VDA/sbin/ctxinstall.conf**で環境変数**CTX_EASYINSTALL_PBIS_LOCAL_PATH**を設定します。

対話モード

ctxinstall.shスクリプトを対話モードで実行するには、**-S**オプションなしで**sudo /opt/Citrix/VDA/sbin/ctxinstall.sh**コマンドを実行します。コマンドラインインターフェイスの各プロンプトで関連する変数値を入力します。変数が既に設定されている場合、ctxinstall.shは変更するかどうか確認を求めます。

サイレントモード

サイレントモードでは、**/opt/Citrix/VDA/sbin/ctxinstall.conf**またはexportコマンドを使用して、前述の変数を設定する必要があります。その後、**ctxinstall.sh -S**を実行します。必要な変数がすべて設定されていないか、一部の値が無効な場合、デフォルト値がない限り、ctxinstall.shは実行を中止します。

各変数のエクスポートされた値は、設定されていない場合を除き、**/Citrix/VDA/sbin/ctxinstall.conf**の値よりも優先されます。ドメイン参加パスワードを除くすべての更新された値は、**/Citrix/VDA/sbin/ctxinstall.conf**に保存されます。したがって、サイレントモードでは、**/Citrix/VDA/sbin/ctxinstall.conf**でドメイン参加パスワードを設定するか、パスワードをエクスポートする必要があります。

```
export CTX_EASYINSTALL_HOSTNAME=host-name



export CTX_EASYINSTALL_DNS=ip-address-of-dns
```

```
export CTX_EASYINSTALL_NTPS=address-of-ntps

export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N
```

```
export CTX_XDL_AD_INTEGRATION=winbind | centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate |
'<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number
```

```
export CTX_XDL_START_SERVICE=Y | N

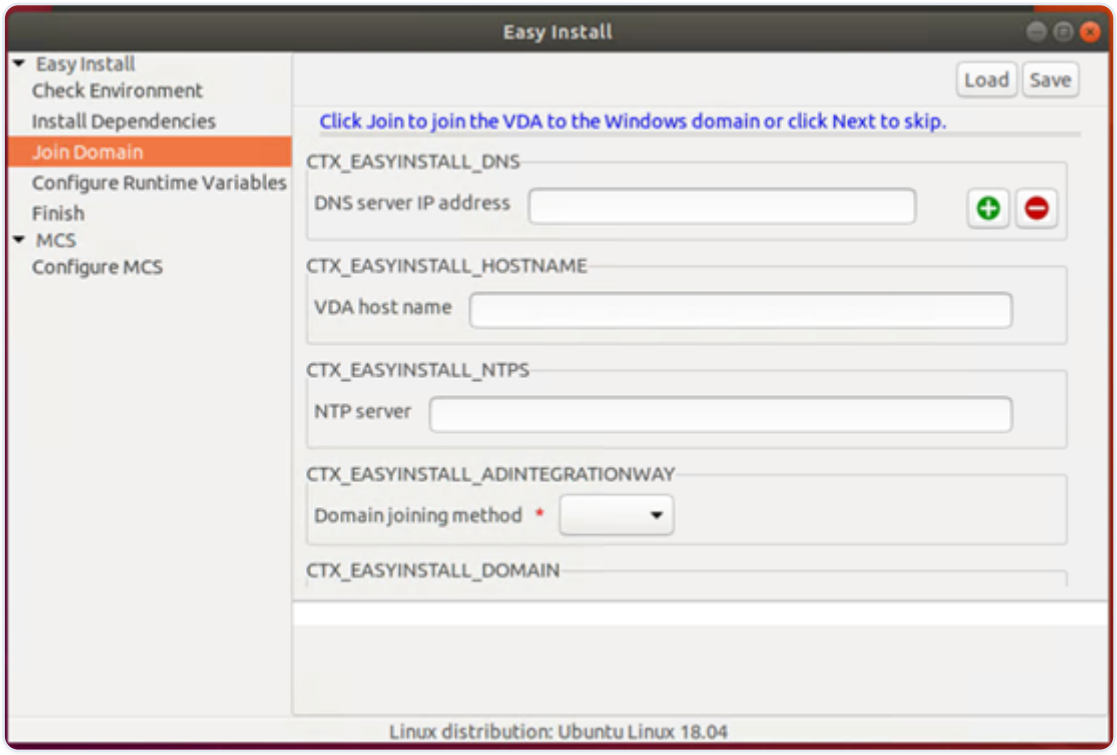

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S
```

sudoコマンドを実行するときは、既存の環境変数を新しく作成されるシェルに渡すために**-E**オプションを入力します。前述のコマンドから、最初の行に**#\!/bin/bash**を含むシェルスクリプトファイルを作成することをお勧めします。

または、単一のコマンドを使用してすべての変数を指定することもできます。

GUI

ドメイン参加方法としてSSSDまたはWinbindを使用する場合、GUIを介して簡易インストールを使用できます。VDAのデスクトップ環境で**/opt/Citrix/VDA/bin/easyinstall**コマンドを実行し、簡易インストールGUIの指示に従います。



簡易インストールGUIは、以下の操作をガイドします。

- システム環境の確認
- 依存関係のインストール
- VDAを指定されたドメインに参加させる

- ランタイム環境の構成

> **ヒント:**
>
> - 指定したパスのローカルファイルに変数設定を保存するには、**Save**をクリックします。指定したファイルから変数設定を読み込むには、**Load**をクリックします。MCS変数の構成については、「ステップ3：マスターイメージの準備」を参照してください。
> - ctxinstall.sh スクリプトは、ドメイン参加パスワードを除くすべての変数設定を **/Citrix/VDA/sbin/ctxinstall.conf** に保存します。

ステップ9：XDPing を実行する

Linux VDA 環境における一般的な構成の問題を確認するには、`sudo /opt/Citrix/VDA/bin/xdping` を実行します。詳細については、「XDPing」を参照してください。

ステップ10：Linux VDA を実行する

Linux VDA を開始する：

Linux VDA サービスを開始するには：

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDA を停止する：

Linux VDA サービスを停止するには：

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **注:**

> `ctxvda` および `ctxhdx` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止してください。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

> **Linux VDA を再起動する：**

Linux VDA サービスを再起動するには：

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Linux VDA のステータスを確認する：

Linux VDA サービスの実行ステータスを確認するには：

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

ステップ11：マシンカタログを作成する

マシンカタログを作成し、Linux VDA マシンを追加するプロセスは、従来の Windows VDA のアプローチと似ています。これらのタスクを完了する方法の詳細については、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

Linux VDAマシンを含むマシンカタログを作成する場合、Windows VDAマシン用のマシンカタログを作成するプロセスとは異なるいくつかの制限があります。

- オペレーティングシステムについては、以下を選択します。
    - ホストされた共有デスクトップ配信モデルの場合は、**Multi-session OS**オプション。

    - VDI専用デスクトップ配信モデルの場合は、**Single-session OS**オプション。

- 同じマシンカタログ内でLinux VDAマシンとWindows VDAマシンを混在させないでください。

> **注:**
>
> Citrix Studioの初期バージョンでは、「Linux OS」という概念はサポートされていませんでした。ただし、**Windows Server OS**または**Server OS**オプションを選択すると、同等のホストされた共有デスクトップ配信モデルが意味されます。**Windows Desktop OS**または**Desktop OS**オプションを選択すると、マシンごとに1人のユーザーという配信モデルが意味されます。

> **ヒント:**
>
> マシンをActive Directoryドメインから削除して再参加させる場合は、そのマシンをマシンカタログから削除して再度追加する必要があります。

ステップ12：デリバリーグループを作成する

デリバリーグループを作成し、Linux VDAマシンを含むマシンカタログを追加するプロセスは、Windows VDAマシンとほぼ同じです。これらのタスクを完了する方法の詳細については、「デリバリーグループの作成」を参照してください。

Linux VDAマシンカタログを含むデリバリーグループを作成する場合、以下の制限が適用されます。

- 選択したADユーザーとグループが、Linux VDAマシンにログオンできるように適切に構成されていることを確認してください。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- デリバリーグループとWindowsマシンを含むマシンカタログを混在させないでください。

> **重要:**
>
> アプリケーションの公開はLinux VDAバージョン1.4以降でサポートされています。ただし、Linux VDAはデスクトップとアプリを同じマシンに配信することをサポートしていません。

> マシンカタログとデリバリーグループの作成方法については、「Citrix Virtual Apps and Desktops 7 2303」を参照してください。

ステップ 13: Linux VDA のアップグレード (オプション)

既存のインストールを、以前の2つのバージョンおよびLTSRリリースからアップグレードできます。

RHEL 7 および CentOS 7 の場合:

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

RHEL 8 および Rocky Linux 8 の場合:

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の場合:

> **注:**
>
> RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 でLinux VDAをアップグレードする前に、**libsepol** パッケージをバージョン3.4以降に更新してください。

```
sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
```

SUSE の場合:

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Ubuntu 18.04 の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Ubuntu 20.04 の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

Ubuntu 22.04 の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

トラブルシューティング

このセクションの情報を使用して、簡易インストール機能の使用によって発生する可能性のある問題をトラブルシューティングします。

SSSD を使用したドメイン参加に失敗する

ドメインに参加しようとするとエラーが発生する場合があります。出力は次のようになります (画面出力についてはログを確認してください):

`Step 6: join Domain!Enter ctxadmin's password:Failed to join domain: failed to lookup DC info for domain 'CITRIXLAB.LOCAL' over rpc: The network name cannot be found`

/var/log/xdl/vda.log:

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service successfully
obtained the following list of 1 delivery controller(s) with which to
register: 'CTXDDC.citrixlab.local (10.158.139.214)'.

2016-11-04 02:11:52.362 [ERROR] -
RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register
with http://CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar.
Error: General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))

2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
connect to the delivery controller 'http://CTXDDC.citrixlab.local:80/
Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')

Check the following:- The system clock is in sync between this machine and
the delivery controller.

-  The Active Directory provider (e.g. winbind daemon) service is running
and correctly configured.

-  Kerberos is correctly configured on this machine.
```

```
If the problem persists, please refer to Citrix Knowledge Base article
CTX117248 for further information.

Error Details:

Exception 'General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))' of type 'class
javax.xml.ws.soap.SOAPFaultException'.

2016-11-04 02:11:52.362 [INFO ] -
RegistrationManager.AttemptRegistrationWithSingleDdc: The current time for
this VDA is Fri Nov 04 02:11:52 EDT 2016.

Ensure that the system clock is in sync between this machine and the
delivery controller.

Verify the NTP daemon is running on this machine and is correctly
configured.

2016-11-04 02:11:52.364 [ERROR] - Could not register with any controllers.
Waiting to try again in 120000 ms. Multi-forest - false

2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
register with any controllers in the last 470 minutes.
```

/var/log/messages:

`Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Failed to initialize credentials using keytab [MEMORY:/etc/krb5.keytab]: Client 'RH-WS-68$@CITRIXLAB.LOCAL' not found in Kerberos database. Unable to create GSSAPI-encrypted LDAP connection.Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Client 'RH-WS-68$@CITRIXLAB.LOCAL' not found in Kerberos database`

この問題を解決するには:

1. `rm -f /etc/krb5.keytab`コマンドを実行します。
2. `net ads leave $REALM -U $domain-administrator`コマンドを実行します。
3. Delivery Controller上のマシンカタログとデリバリーグループを削除します。
4. /opt/Citrix/VDA/sbin/ctxinstall.shを実行します。
5. Delivery Controller上にマシンカタログとデリバリーグループを作成します。

Ubuntuデスクトップセッションでグレースクリーンが表示される

この問題は、セッションを起動した後に空白のデスクトップでブロックされる場合に発生します。さらに、ローカルユーザーアカウントを使用してログオンすると、マシンのコンソールにもグレースクリーンが表示されます。

この問題を解決するには:

1. `sudo apt-get update`コマンドを実行します。
2. `sudo apt-get install unity lightdm`コマンドを実行します。
3. `/etc/lightdm/lightdm.conf`に次の行を追加します:

   `greeter-show-manual-login=true`

ホームディレクトリがないため、Ubuntuデスクトップセッションの起動に失敗する

/var/log/xdl/hdx.log:

```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)



2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent: Session
started for user ctxadmin.



2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
Login Process died: normal.



2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting normally.
```

ヒント:

この問題の根本原因は、ドメイン管理者のホームディレクトリが作成されていないことです。

この問題を解決するには:

1. コマンドラインから、「**pam-auth-update**」と入力します。
2. 表示されたダイアログで、「**Create home directory login**」が選択されていることを確認します。

Ubuntuがセッションを起動できません(/en-us/linux-virtual-delivery-agent/2303/media/ubuntu-cannot-launch-session.png)

セッションが起動しない、またはdbusエラーで短時間で終了する

/var/log/messages (RHELまたはCentOSの場合):

```
Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
CITRIXLAB\ctxadmin.



Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0



Oct 27 04:17:18 CentOS7 gnome-session[19146]: ERROR: Failed to connect to
system bus: Exhausted all available authentication mechanisms (tried:
EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available: EXTERNAL,
DBUS_COOKIE_SHA1, ANONYMOUS)#012aborting...



Oct 27 04:17:18 CentOS7 gnome-session: gnome-session[19146]: ERROR: Failed
to connect to system bus: Exhausted all available authentication
mechanisms (tried: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available:
EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS)



Oct 27 04:17:18 CentOS7 gnome-session: aborting...



Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.
```

```
Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
CITRIXLAB\ctxadmin.
```

または、Ubuntuディストリビューションの場合は、ログ/var/log/syslogを使用します:

```
Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
Stale PID file, overwriting.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
util.c: Failed to get D-Bus connection: Did not receive a reply. Possible
causes include: the remote application did not send a reply, the message
bus security policy blocked the reply, the reply timeout expired, or the
network connection was broken.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap.c:
Assertion 'h' failed at pulsecore/hashmap.c:116, function
pa_hashmap_free(). Aborting.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
util.c: Failed to connect to system bus: Did not receive a reply. Possible
causes include: the remote application did not send a reply, the message
bus security policy blocked the reply, the reply timeout expired, or the
network connection was broken.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
times: [ [pulseaudio] core-util.c: Failed to connect to system bus: Did
not receive a reply. Possible causes include: the remote application did
not send a reply, the message bus security policy blocked the reply, the
reply timeout expired, or the network connection was broken.]



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
```

```
Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-
ctxgfx[24693]: Exiting normally
```

一部のグループまたはモジュールは、再起動するまで有効になりません。ログに**dbus**エラーメッセージが表示される場合は、システムを再起動して再試行することをお勧めします。

SELinuxがSSHDのホームディレクトリへのアクセスを妨げる

ユーザーはセッションを起動できますが、ログオンできません。

/var/log/xdl/ctxinstall.log:

```
Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing /
usr/sbin/sshd from setattr access on the directory /root. For complete
SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698-963a79f16b81



Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/sbin/
sshd from setattr access on the directory /root.



*****  Plugin catchall_boolean (89.3 confidence) suggests
******************



If you want to allow polyinstantiation to enabled



   Then you must tell SELinux about this by enabling the
'polyinstantiation_enabled' boolean.



You can read 'None' man page for more details.



    Do
```

```
       setsebool -P polyinstantiation_enabled 1


*****  Plugin catchall (11.6 confidence) suggests
**************************


If you believe that sshd should be allowed setattr access on the root
directory by default.


Then you should report this as a bug.


You can generate a local policy module to allow this access.


      Do


       allow this access for now by executing:


       # grep sshd /var/log/audit/audit.log | audit2allow -M mypol


# semodule -i mypol.pp
```

この問題を解決するには:

1. /etc/selinux/configに次の変更を加えてSELinuxを無効にします。

   SELINUX=無効

2. VDA を再起動します。

ドメインに参加していないLinux VDAを作成する

この記事では、Machine Creation Services™ (MCS) を使用して、Citrix DaaSでドメインに参加していないLinux VDAを作成する方法について説明します。

重要:

- ドメインに参加していないVDAは、Citrix DaaSでサポートされています。
  - コントロールプレーンはCitrix DaaS上に展開する必要があります。
  - ドメインに参加していないVDAは、パブリッククラウドまたはオンプレミスのデータセンターに展開できます。ドメインに参加していないVDAは、Citrix DaaSのコントロールプレーンによって管理されます。
  - Citrix Cloud ConnectorsをバイパスするようにRendezvous V2を構成できます。そうしないと、VDAをコントロールプレーンに接続するためにCloud Connectorsをインストールする必要があります。
- ドメインに参加していないVDAを作成するには、MCSを使用する必要があります。
  - ベアメタルサーバーはMCSではサポートされていません。
- ドメインに参加していないLinux VDAでは、次の機能が利用できます。
  - ドメインに参加していないVDAで指定された属性を持つローカルユーザーを作成する
  - 非SSO認証
  - Azure Active Directoryによる認証
  - ランデブー V2

(Nutanixのみ) ステップ1：Nutanix AHVプラグインをインストールして登録する

NutanixからNutanix AHVプラグインパッケージを入手します。Citrix Virtual Apps and Desktops環境にプラグインをインストールして登録します。詳細については、Nutanix Support Portalで入手できるNutanix Acropolis MCSプラグインインストールガイドを参照してください。

ステップ1a: オンプレミスのDelivery Controller用Nutanix AHVプラグインのインストールと登録

Citrix Virtual Apps and Desktops™をインストールした後、Delivery Controllerに**XD MCS AHV Plugin**を選択してインストールします。

オンプレミスのDelivery Controller用Nutanix AHVプラグイン(/en-us/linux-virtual-delivery-agent/2303/media/nutanix-plug-in-for-cvad.png)

ステップ1b: クラウドDelivery Controller用Nutanix AHVプラグインのインストールと登録

Citrix Cloud™ Connector用の**CWA MCS AHV Plugin**を選択してインストールします。Citrix Cloudテナントに登録されているすべてのCitrix Cloud Connectorにプラグインをインストールします。AHVのないリソースの場所を提供するCitrix Cloud Connectorであっても、登録する必要があります。

ステップ1c: プラグインのインストール後に次の手順を完了する

- `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`にNutanix Acropolisフォルダーが作成されていることを確認します。
- `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`コマンドを実行します。
- オンプレミスのDelivery ControllerでCitrix Host、Citrix Broker、およびCitrix Machine Creation Servicesを再起動するか、Citrix Cloud ConnectorでCitrix RemoteHCLServer Serviceを再起動します。

> **ヒント:**
>
> Nutanix AHVプラグインをインストールまたは更新する際は、Citrix Host、Citrix Broker、およびMachine Creation Servicesを停止してから再起動することをお勧めします。

ステップ2: ホスト接続を作成する

ホストとは、リソースの場所で使用されているハイパーバイザーまたはクラウドサービスです。この手順では、DaaSがホスト上のVMと通信するために使用する情報を指定します。詳細情報には、リソースの場所、ホストの種類、アクセス資格情報、使用するストレージ方法、およびホスト上のVMが使用できるネットワークが含まれます。

> **重要:**
>
> 接続を作成する前に、リソースの場所にあるホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、**My Services > DaaS**を選択します。
3. **Manage > Full Configuration**から、左ペインで**Hosting**を選択します。
4. アクションバーで を選択します。
5. ウィザードは次のページに沿って進みます。特定のページの内容は、選択した接続の種類によって異なります。各ページを完了したら、**Next**を選択して**Summary**ページに到達します。

ステップ 2a: 接続

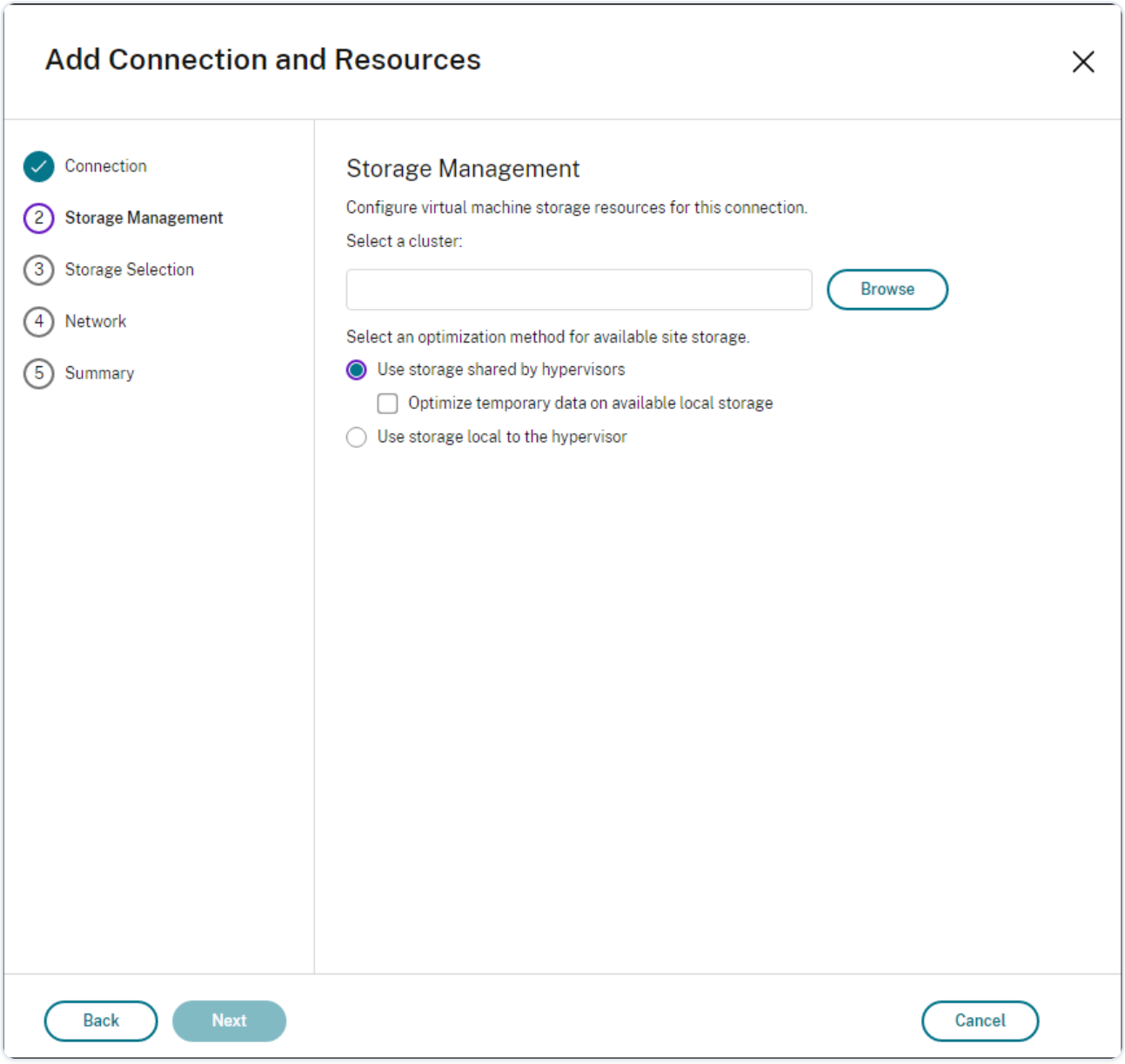
接続の追加イメージ(/en-us/linux-virtual-delivery-agent/2303/media/add-conn-connection.png)

「**接続**」ページで：

- 接続を作成するには、 を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、 を選択し、関連する接続を選択します。
- 「**ゾーン名**」フィールドでゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
- 「**接続の種類**」フィールドでハイパーバイザーまたはクラウドサービスを選択します。オプションは、ゾーンにプラグインが適切にインストールされているハイパーバイザーとクラウドサービスです。 または、PowerShellコマンド `Get-HypHypervisorPlugin -ZoneUid` を使用して、選択したゾーンで利用可能なハイパーバイザープラグインのリストを取得できます。
- 接続名を入力します。この名前は、**管理**表示に表示されます。
- 仮想マシンを作成するツールとして、Machine Creation ServicesまたはCitrix Provisioningを選択します。

接続ページの情報は、使用しているホスト（接続の種類）によって異なります。たとえば、Azure Resource Managerを使用している場合、既存のサービスプリンシパルを使用するか、新しいものを作成できます。

ステップ 2b: ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

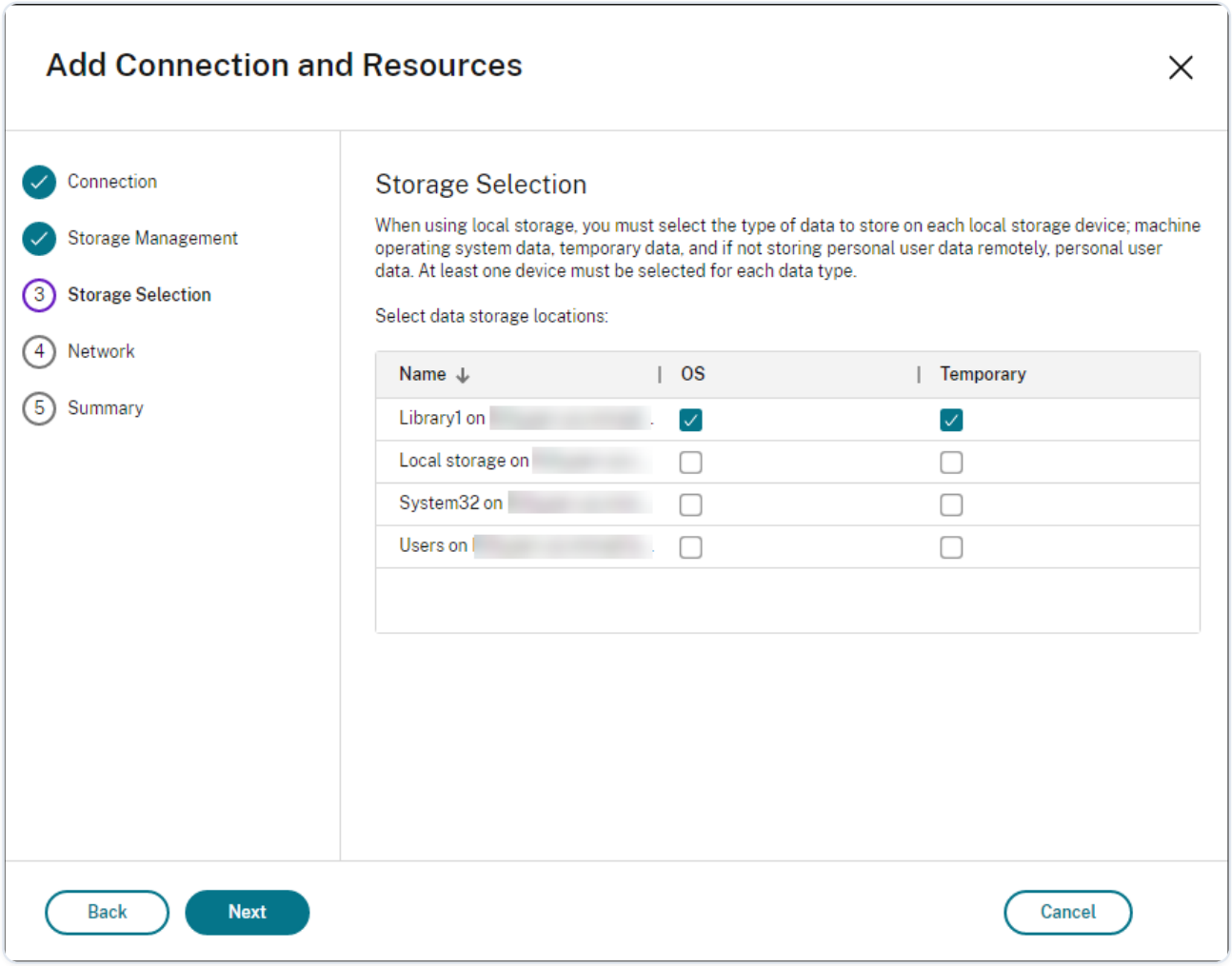
ストレージ管理方法を選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デ

フォルト以外のサイズの一時ストレージを指定できます。）**例外：** クラスター共有ボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerでは、ローカルストレージに一時データキャッシュディスクを作成できません。**管理**コンソールでそのストレージ管理設定を構成しようとすると失敗します。

Citrix Hypervisorプールで共有ストレージを使用する場合、共有ストレージデバイスの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。「Citrix Hypervisor仮想化環境」を参照してください。

ステップ 2c: ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択する必要があります。

ストレージの選択ページの下部には、ハイパーバイザーで共有されるストレージを選択し、**利用可能なローカルストレージ上の一時データを最適化**を有効にした場合に、さらに多くの構成オプションが含まれます。一時データに使用するローカルストレージデバイス（同じハイパーバイザープール内）を選択できます。

現在選択されているストレージデバイスの数が表示されます（グラフィックでは「1 storage device selected」）。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます（デバイスが構成されていない場合を除く）。

1. 使用するストレージデバイスを変更するには、**「選択」**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにしてから、**OK**を選択します。

ステップ 2d: リージョン

（一部のホストタイプでのみ表示されます。）リージョンの選択は、VMが展開される場所を示します。理想的には、ユーザーがアプリケーションにアクセスする場所に近いリージョンを選択してください。

ステップ 2e: ネットワーク

リソースの名前を入力します。この名前は、接続に関連付けられているストレージとネットワークの組み合わせを識別するために、**管理**コンソールに表示されます。 VMが使用するネットワークを1つ以上選択します。

一部の接続タイプ（Azure Resource Managerなど）では、VMが使用するサブネットも表示されます。1つ以上のサブネットを選択します。

ステップ2f：概要

選択内容を確認します。変更する場合は、前のウィザードページに戻ります。確認が完了したら、**「完了」**を選択します。

注意: 一時データをローカルに保存する場合、この接続を使用するマシンを含むカタログを作成するときに、一時データストレージの非デフォルト値を構成できます。

> **注:**
>
> フルアクセス管理者にはスコープは表示されません。詳細については、「管理者、役割、およびスコープ」を参照してください。

詳細については、「接続の作成と管理」を参照してください。

ステップ3：マスターイメージの準備

ヒント:

ドメイン参加済みVDAとドメイン非参加VDAの両方を作成するために、単一のイメージを使用できます。

（Citrix Hypervisor™のみ）ステップ3a：Citrix VM Toolsのインストール

xe CLIまたはXenCenterを使用する各VMのテンプレートVMにCitrix VM Toolsをインストールします。ツールをインストールしないと、VMのパフォーマンスが低下する可能性があります。ツールがないと、次の操作を実行できません。

- VMを正常にシャットダウン、再起動、または一時停止する。
- XenCenterでVMのパフォーマンスデータを表示する。
- 実行中のVMを移行する（`XenMotion`経由）。
- スナップショットまたはメモリ付きスナップショット（チェックポイント）を作成し、スナップショットに戻す。
- 実行中のLinux VMのvCPU数を調整する。

1. guest-tools.isoという名前のCitrix VM Toolsをマウントするには、次のコマンドを実行します。

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. Linuxディストリビューションに基づいて`xe-guest-utilities`パッケージをインストールするには、次のコマンドを実行します。

   RHEL/CentOS/Rocky Linuxの場合:

   ```
   sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
   ```

   Ubuntu/Debianの場合:

   ```
   sudo dpkg -i /mnt/Linux/xe-guest-utilities_{package-version}_all.deb
   ```

SUSEの場合:

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
```

3. XenCenterの**全般**タブで、テンプレートVMの仮想化状態を確認します。Citrix VM Toolsが正しくインストールされている場合、仮想化状態は**最適化済み**になります。

(Azure、AWS、GCPの場合) 手順3b：Ubuntu 18.04向けにcloud-initを構成する

1. VMの再起動または停止時にVDAホスト名を保持するには、次のコマンドを実行します。

```
echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
```

/etc/cloud/cloud.cfgファイルの**system_info**セクションに次の行が存在することを確認します。

```
system_info:

   network:

       renderers: ['netplan', 'eni', 'sysconfig']
```

2. AWSでMCSによって作成されたVMにリモートでアクセスするためにSSHを使用するには、これらのVMにはキー名がアタッチされていないため、パスワード認証を有効にします。必要に応じて、次の操作を行います。

   - `cloud-init`構成ファイル（/etc/cloud/cloud.cfg）を編集します。**ssh_pwauth: true**の行が存在することを確認します。**set-password**の行と、それに続く行が存在する場合は、削除またはコメントアウトします。

     ```
     users:

     - default
     ```

   - `cloud-init`によって作成されたデフォルトユーザー`ec2-user`または`ubuntu`を使用する予定がある場合は、`passwd`コマンドを使用してユーザーパスワードを変更できます。MCSで作成されたVMにログインするために、新しいパスワードを覚えておいてください。
   - `/etc/ssh/sshd_config`ファイルを編集して、次の行が存在することを確認します。

```
PasswordAuthentication yes
```

ファイルを保存し、`sudo service sshd restart`コマンドを実行します。

手順3c：テンプレートVMにLinux VDAパッケージをインストールする

注:

現在実行中のVDAをテンプレートVMとして使用する場合は、この手順をスキップしてください。

テンプレートVMにLinux VDAパッケージをインストールする前に、.NET Runtime 6.0をインストールしてください。

お使いのLinuxディストリビューションに基づいて、Linux VDAの環境をセットアップするために次のコマンドを実行します。

RHEL/CentOS/Rocky Linuxの場合:

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
```

注:

RHELおよびCentOSの場合、Linux VDAをインストールして`deploymcs.sh`を正常に実行する前に、EPELリポジトリをインストールしてください。EPELのインストール方法については、`<https://docs.fedoraproject.org/ja-jp/epel/>`の指示を参照してください。

- GCPでホストされているRHEL 8.x/9.xおよびRocky Linux 8.x/9.xにLinux VDAをインストールした後、VMの再起動後にイーサネット接続が失われ、Linux VDAに到達できなくなる可能性があります。この問題を回避するには、VMを再起動する前に次のコマンドを実行します。

```
nmcli dev connect eth0

service NetworkManager restart
```

Ubuntu/Debianの場合:

```
sudo dpkg –i  <PATH>/<Linux VDA DEB>



apt-get install -f
```

SUSEの場合:

```
sudo zypper –i install <PATH>/<Linux VDA RPM>
```

ステップ3d: tdb-toolsパッケージをインストールするためのリポジトリを有効にする（RHEL 7のみ）

RHEL 7サーバーの場合:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

RHEL 7ワークステーションの場合:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

ステップ3e: （SUSEの場合）ntfs-3gを手動でインストールする

SUSEプラットフォームでは、ntfs-3gを提供するリポジトリがありません。ソースコードをダウンロードし、コンパイルして、ntfs-3gを手動でインストールします。

1. GNU Compiler Collection (GCC) コンパイラシステムとmakeパッケージをインストールします。

```
sudo zypper install gcc

sudo zypper install make
```

2. ntfs-3gパッケージをダウンロードします。
3. ntfs-3gパッケージを解凍します。

```
sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
```

4. ntfs-3gパッケージへのパスを入力します。

```
sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. ntfs-3g をインストールします:

```
./configure

make

make install
```

ステップ 3f: 使用するデータベースを指定します

実験的機能として、PostgreSQL に加えて SQLite を使用できます。Linux VDA パッケージのインストール後に、SQLite と PostgreSQL を切り替えることもできます。これを行うには、次の手順を完了します:

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh` を実行します。新規インストールである場合は、この手順を省略します。
2. `deploymcs.sh` を実行する前に、`/etc/xdl/db.conf` を編集します。

注:

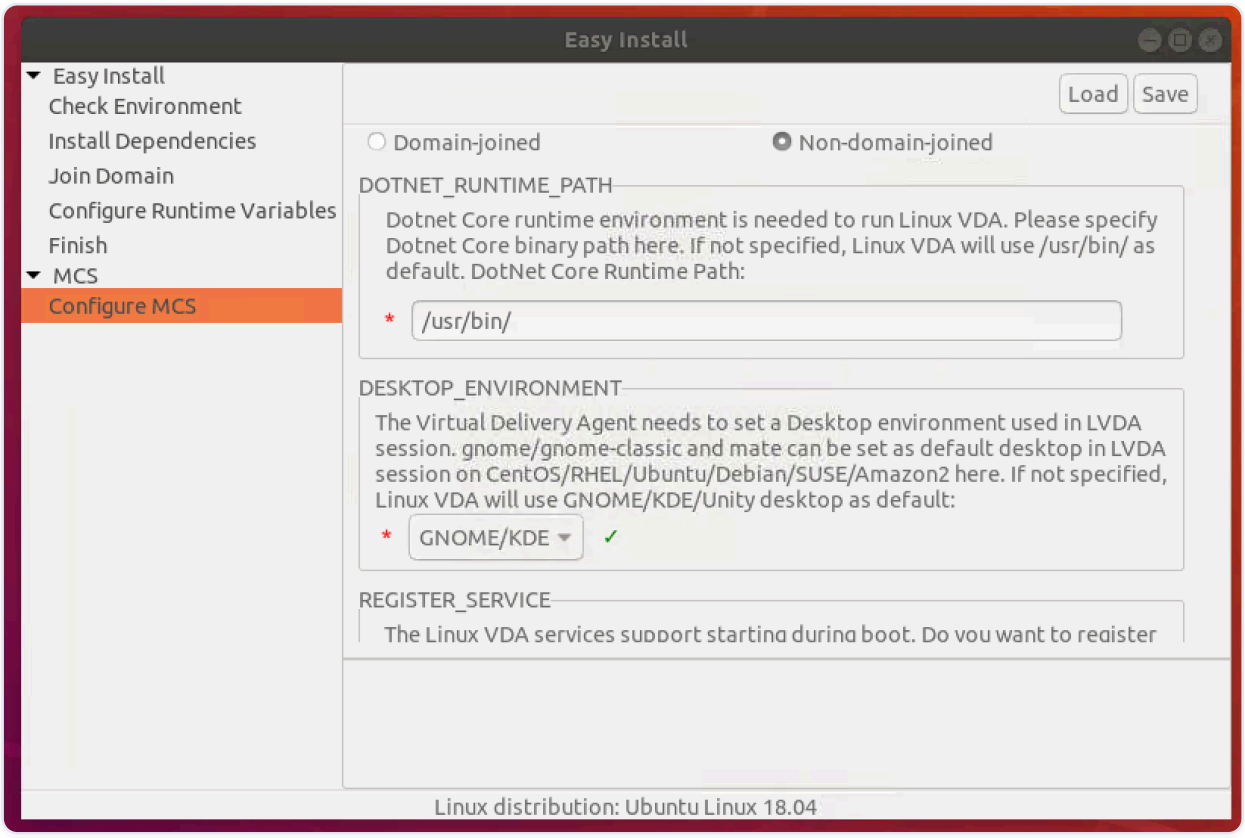
- VDI モードでのみ SQLite を使用することをお勧めします。

- 簡易インストールおよび MCS の場合、SQLite と PostgreSQL を手動でインストールすることなく切り替えることができます。`/etc/xdl/db.conf` を介して別途指定しない限り、Linux VDA はデフォルトで PostgreSQL を使用します。
- `/etc/xdl/db.conf` を使用して、PostgreSQL のポート番号を構成することもできます。

ステップ 3g: MCS 変数を構成します

MCS 変数を構成するには、次の 2 つの方法があります:

- `/etc/xdl/mcs/mcs.conf` ファイルを編集します。
- 簡易インストール GUI を使用します。簡易インストール GUI を開くには、Linux VDA のデスクトップ環境で `/opt/Citrix/VDA/bin/easyinstall` コマンドを実行します。



ヒント:

保存 をクリックして、指定したパスのローカルファイルに変数の設定を保存します。**読み込み** をクリックして、指定したファイルから変数の設定を読み込みます。

以下は、ドメインに参加していないシナリオ用に構成できる MCS 変数です。デフォルトの変数値を使用するか、必要に応じて変数をカスタマイズできます (オプション):

`DOTNET_RUNTIME_PATH` =*dotnet ランタイムのインストールパス *

`DESKTOP_ENVIRONMENT` = *gnome | mate ** `REGISTER_SERVICE` =**Y | N**

`ADD_FIREWALL_RULES` =**Y | N** `VDI_MODE` =**Y | N**

`START_SERVICE` =**Y | N**

ステップ 3h: MCS のレジストリ値を書き込むか更新する (オプション)

テンプレートマシンで、必要に応じてレジストリ値を書き込んだり更新したりするためのコマンドラインを `/etc/xdl/mcs/mcs_local_setting.reg` ファイルに追加します。この操作により、MCS でプロビジョニングされたマシンが再起動するたびにデータと設定が失われるのを防ぎます。

`/etc/xdl/mcs/mcs_local_setting.reg` ファイルの各行は、レジストリ値を設定または更新するためのコマンドです。

たとえば、レジストリ値を書き込んだり更新したりするために、次のコマンドラインを `/etc/xdl/mcs/mcs_local_setting.reg` ファイルに追加できます。

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

ステップ 3i: マスターイメージを作成する

1. `/etc/xdl/mcs/mcs.conf` を編集して MCS 変数を構成する場合は、`/opt/Citrix/VDA/sbin/deploymcs.sh` を実行します。GUI を使用して MCS 変数を構成する場合は、 をクリックします。

   簡易インストール GUI の ボタン(/en-us/linux-virtual-delivery-agent/2303/media/deploy-button-on-easy-install-gui.png)

GUI で をクリックすると、GUI で設定した変数が `/etc/xdl/mcs/mcs.conf` ファイルで設定した変数を上書きします。

2. 使用しているパブリッククラウドに基づいて、マスターイメージのスナップショットを作成し、名前を付けます。

   - **(Citrix Hypervisor、GCP、および VMware vSphere の場合)** テンプレート VM にアプリケーションをインストールし、テンプレート VM をシャットダウンします。マスターイメージのスナップショットを作成して名前を付けます。
   - **(Azure の場合)** テンプレート VM にアプリケーションをインストールし、Azure ポータルからテンプレート VM をシャットダウンします。テンプレート VM の電源状態が **Stopped (deallocated)** であることを確認します。ここでリソースグループの名前を覚えておいてください。Azure でマスターイメージを見つけるには、この名前が必要です。

     テンプレート VM の停止済み電源状態(/en-us/linux-virtual-delivery-agent/2303/media/stopped-deallocated2.png)
   - **(AWS の場合)** テンプレート VM にアプリケーションをインストールし、AWS EC2 ポータルからテンプレート VM をシャットダウンします。テンプレート VM のインスタンス状態が **Stopped** であることを確認します。テンプレート VM を右クリックし、**Image > Create Image** を選択します。必要に応じて情報を入力し、設定を行います。**Create Image** をクリックします。

     EBS イメージの作成(/en-us/linux-virtual-delivery-agent/2303/media/create-ebs-image.png)
   - **(Nutanixの場合)** Nutanix AHVで、テンプレートVMをシャットダウンします。マスターイメージのスナップショットを作成し、名前を付けます。

     > **注:**
     >
     > Citrix Virtual Apps™ and Desktopsで使用するには、Acropolisスナップショット名に `XD_` をプレフィックスとして付ける必要があります。必要に応じてAcropolisコンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した後、**カタログの作成**ウィザードを再起動して、更新されたリストを取得します。

ステップ4：マシンカタログを作成する

1. Citrix Cloudにサインインします。
2. 左上のメニューで、**マイサービス > DaaS**を選択します。

3. **管理 > 完全な構成**から、**マシンカタログ**を選択します。
4. ウィザードの指示に従ってマシンカタログを作成します。

   Nutanix固有の**コンテナ**ページで、以前にテンプレートVMに指定したコンテナを選択します。

   マスターイメージページで、イメージスナップショットを選択します。

   仮想マシンページで、仮想CPUの数とvCPUあたりのコア数を確認します。マシン展開方法としてMCSを選択し、カタログで作成するマシンのIDとして**ドメイン非参加**を選択します。

   必要に応じて、その他の構成タスクを実行します。詳しくは、「マシンカタログの作成」を参照してください。

> **注:**
>
> Delivery Controller™でのマシンカタログ作成プロセスにかなりの時間がかかる場合は、Nutanix Prismに移動し、**Preparation**というプレフィックスが付いたマシンを手動で電源オンにします。この方法により、作成プロセスを続行できます。

ステップ5：デリバリーグループを作成する

デリバリーグループは、1つ以上のマシンカタログから選択されたマシンのコレクションです。どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。詳しくは、「デリバリーグループの作成」を参照してください。

Machine Creation Services™ (MCS) を使用して Linux VDA を作成する

MCS を使用して、ドメイン参加済みおよび非ドメイン参加済み VDA を作成できます。

> **重要:**
>
> 2212 リリース以降、以下の重要な変更点があります。

- /etc/xdl/mcs/mcs.conf ファイルまたは簡易インストール GUI の **AD_INTEGRATION** 変数にはデフォルト値がなくなりました。必要に応じて値を設定する必要があります。詳細については、この記事の 手順 3h: MCS 変数の構成 セクションを参照してください。
- /etc/xdl/mcs/mcs.conf の **UPDATE_MACHINE_PW** エントリの有効な値は、**enabled** または **disabled** ではなく、**Y** または **N** になりました。詳細については、この記事の マシンアカウントパスワードの自動更新 セクションを参照してください。

サポートされているディストリビューション

	ウィンバインド	SSSD	セントリファイ	PBIS
デビアン 11.3	はい	はい	いいえ	はい
RHEL 9.1/9.0	はい	いいえ	いいえ	いいえ
RHEL 8.7/8.6/8.4	はい	いいえ	はい	はい
ロッキー Linux 9.1/9.0	はい	いいえ	いいえ	いいえ
ロッキー Linux 8.7/8.6	はい	いいえ	いいえ	いいえ
RHEL 7.9, CentOS 7.9	はい	はい	はい	はい
SUSE 15.4	はい	はい	いいえ	はい
ウブントゥ 22.04、ウブントゥ 20.04、ウブントゥ 18.04	はい	はい	いいえ	はい

サポートされているハイパーバイザー

- AWS
- シトリックス ハイパーバイザー™
- GCP
- マイクロソフト アジュール

- ニュータニックス AHV
- ヴイエムウェア ブイスフィア

サポートされているもの以外のハイパーバイザーでマスターイメージを準備しようとすると、予期しない結果が発生する可能性があります。

MCSを使用してLinux VMを作成する

考慮事項

- 2203リリース以降、Citrix Virtual Apps and DesktopsおよびCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）向けに、Microsoft Azure、AWS、GCPでLinux VDAをホストできます。これらのパブリッククラウドホスト接続をCitrix Virtual Apps and Desktops展開に追加するには、Citrix Universal SubscriptionまたはHybrid Rightsライセンスが必要です。Universal SubscriptionおよびHybrid Rightsライセンスの詳細については、Transition and Trade Up (TTU) with Citrix Universal Subscriptionを参照してください。
- 仮想マシンを作成するためのMCSでのベアメタルサーバーの使用はサポートされていません。
- Citrix®は、関連するLinuxディストリビューションでの初期機能検証のために、以下のCentrifyバージョンを使用します。

LINUXディストリビューション	CENTRIFYバージョン
RHEL 7/8	5.8.0
SUSE	5.7.1
デビアン、ウブントゥ	5.6.1

  Centrifyの他のバージョンを使用すると、エラーが発生する可能性があります。テンプレートマシンをドメインに参加させるためにCentrifyを使用しないでください。
- MCSで作成されたマシンをWindowsドメインに参加させるためにPBISまたはCentrifyを使用している場合は、次のタスクを完了してください。
  - テンプレートマシンで、`/etc/xdl/mcs/mcs.conf`ファイルにPBISまたはCentrifyパッケージのダウンロードパスを構成するか、PBISまたはCentrifyパッケージを直接インストールします。
  - `/opt/Citrix/VDA/sbin/deploymcs.sh`を実行する前に、その配下にあるすべてのMCSで作成されたマシンに対して書き込み権限とパスワードリセット権限を持つ組織単位 (OU) を作成します。

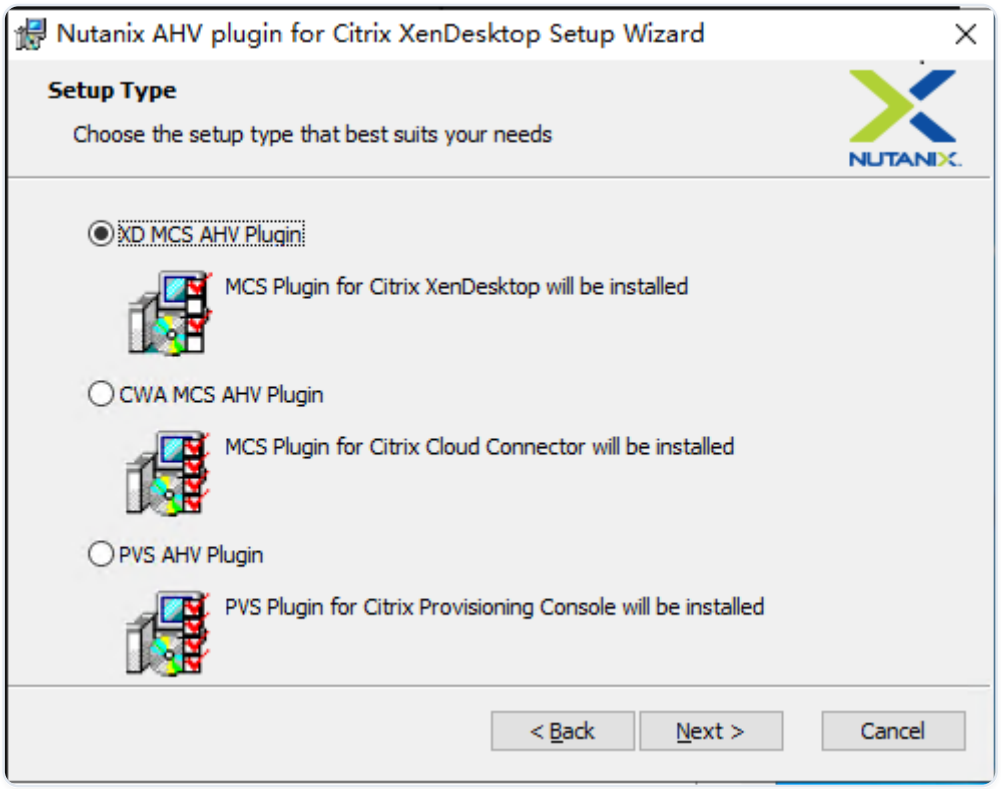
- `/opt/Citrix/VDA/sbin/deploymcs.sh`の実行が完了した後、MCSで作成されたマシンを再起動する前に、展開に応じて、Delivery ControllerまたはCitrix Cloud Connectorで`klist -li 0x3e4 purge`を実行します。

(Nutanixのみ) ステップ1：Nutanix AHVプラグインをインストールして登録する

NutanixからNutanix AHVプラグインパッケージを入手します。Citrix Virtual Apps and Desktops環境にプラグインをインストールして登録します。詳細については、Nutanixサポートポータルで入手できるNutanix Acropolis MCSプラグインインストールガイドを参照してください。

ステップ1a：オンプレミスのDelivery Controller向けNutanix AHVプラグインをインストールして登録する

Citrix Virtual Apps and Desktops™をインストールした後、Delivery Controllerで**XD MCS AHV Plugin**を選択してインストールします。



ステップ1b：クラウドDelivery Controller向けNutanix AHVプラグインをインストールして登録する

Citrix Cloud™ Connector向けに**CWA MCS AHV Plugin**を選択してインストールします。Citrix Cloudテナントに登録されているすべてのCitrix Cloud Connectorにプラグインをインストールします。AHVのないリソースの場所を提供するCitrix Cloud Connectorであっても、登録する必要があります。

ステップ1c：プラグインのインストール後に次の手順を完了します

- `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` にNutanix Acropolisフォルダーが作成されていることを確認します。
- `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` コマンドを実行します。
- オンプレミスのDelivery ControllerでCitrix Host、Citrix Broker、Citrix Machine Creation Servicesを再起動するか、Citrix Cloud ConnectorsでCitrix RemoteHCLServer Serviceを再起動します。

> **ヒント:**
>
> Nutanix AHVプラグインをインストールまたは更新する際は、Citrix Host、Citrix Broker、およびMachine Creation Servicesを停止してから再起動することをお勧めします。

ステップ2：ホスト接続を作成する

このセクションでは、Azure、AWS、GCP、Nutanix AHV、およびVMware vSphereへのホスト接続の作成について説明します。

- Citrix StudioでAzureへのホスト接続を作成する
- Citrix StudioでAWSへのホスト接続を作成する
- Citrix StudioでGCPへのホスト接続を作成する
- Citrix StudioでNutanixへのホスト接続を作成する
- Citrix StudioでVMwareへのホスト接続を作成する

Citrix StudioでAzureへのホスト接続を作成する

1. Citrix Cloudにサインインします。
2. 左上のメニューで、 **>** を選択します。
3. **>** から、左側のペインで を選択します。
4. アクションバーで**「接続とリソースの追加」**を選択します。

   接続の追加イメージ(/en-us/linux-virtual-delivery-agent/2303/media/add-conn-connection.png)

5. 接続の種類としてMicrosoft Azureを選択します。
6. ウィザードがページを案内します。特定のページコンテンツは、選択した接続の種類によって異なります。各ページを完了したら、 を選択して ページに進みます。詳細については、ドメインに参加していないLinux VDAを作成するの記事のステップ2：ホスト接続を作成するを参照してください。

Citrix StudioでAWSへのホスト接続を作成する

1. Citrix Studioで、**構成** > **ホスティング** > **接続とリソースの追加** の順に選択します。
2. 接続の種類として **Amazon EC2** を選択します。

   Amazon EC2の選択(/en-us/linux-virtual-delivery-agent/2210/media/choose-amazon-ec2.png)
3. AWSアカウントのAPIキーとシークレットキーを入力し、接続名を入力します。

   アクセスキーペア(/en-us/linux-virtual-delivery-agent/2210/media/access-key-pair.png)

   APIキー はアクセスキーIDであり、**シークレットキー** はシークレットアクセスキーです。これらはアクセスキーペアと見なされます。シークレットアクセスキーを紛失した場合は、アクセスキーを削除して別のキーを作成できます。アクセスキーを作成するには、次の手順を実行します。

   a. AWSサービスにサインインします。
   b. Identity and Access Management (IAM) コンソールに移動します。
   c. 左側のナビゲーションペインで、**ユーザー** を選択します。
   d. 対象ユーザーを選択し、下にスクロールして **セキュリティ認証情報** タブを選択します。
   e. 下にスクロールして **アクセスキーの作成** をクリックします。新しいウィンドウが表示されます。
   f. **.csvファイルのダウンロード** をクリックし、アクセスキーを安全な場所に保存します。
4. ウィザードは複数のページにわたって案内します。特定のページの内容は、選択した接続の種類によって異なります。各ページを完了したら、**次へ** を選択して **概要** ページに到達するまで進みます。

Citrix StudioでGCPへのホスト接続を作成する

GCP環境を(/ja-jp/citrix-virtual-apps-desktops-service/install-configure/resource-location/google.html)に従って設定し、GCPへのホスト接続を作成するために以下の手順を完了します。

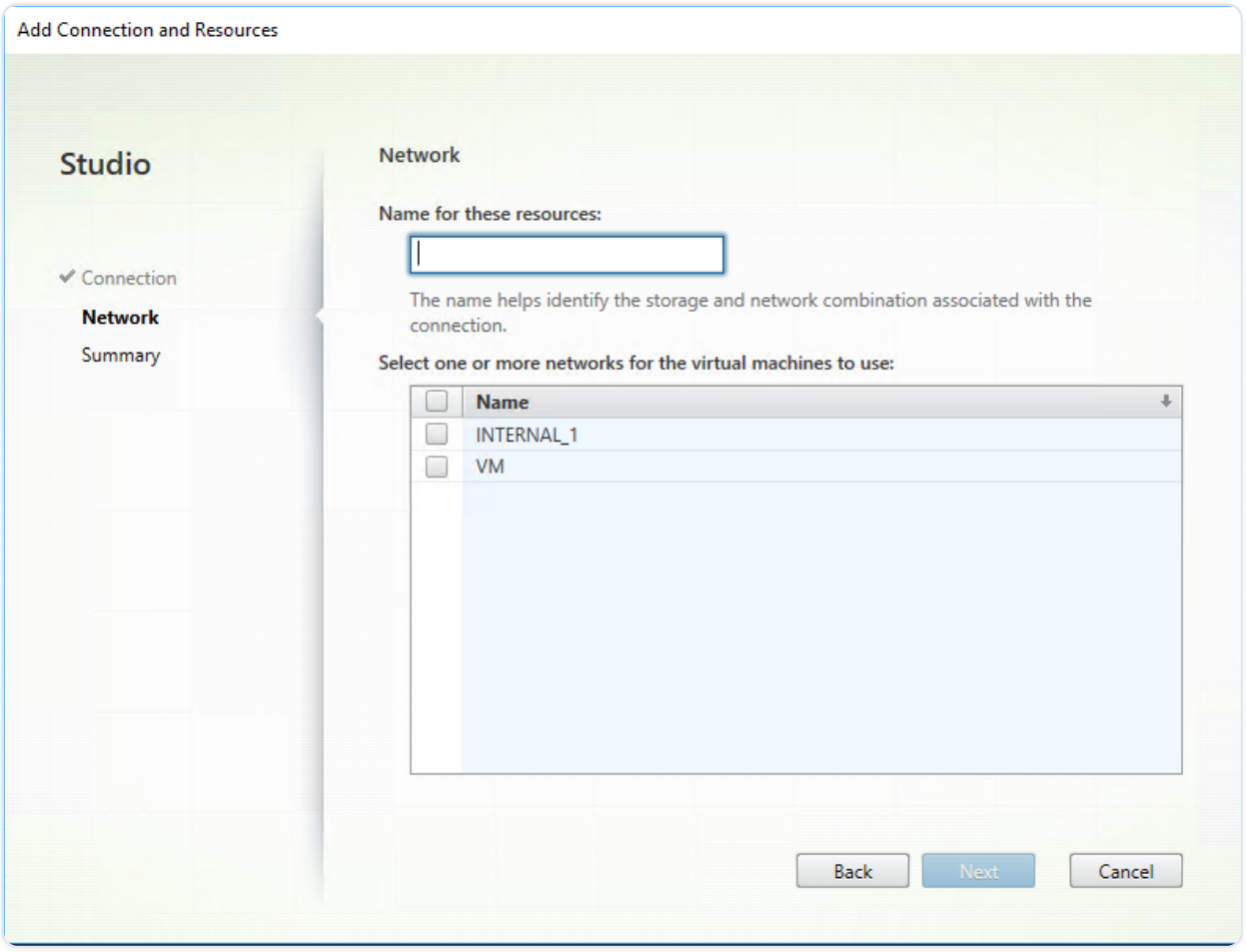
1. Citrix Cloudにサインインします。
2. 左上のメニューで、**My Services > DaaS**を選択します。

3. **Manage > Full Configuration**から、左ペインで**Hosting**を選択します。
4. アクションバーで**「接続とリソースの追加」**を選択します。
5. 接続タイプとして**Google Cloud Platform**を選択します。
6. GCPアカウントのサービスアカウントキーをインポートし、接続名を入力します。
7. ウィザードはページを案内します。特定のページの内容は、選択した接続タイプによって異なります。各ページを完了したら、**Summary**ページに到達するまで**Next**を選択します。詳細については、Create non-domain-joined Linux VDAs記事のStep 2: Create a host connectionを参照してください。

Citrix StudioでNutanixへのホスト接続を作成する

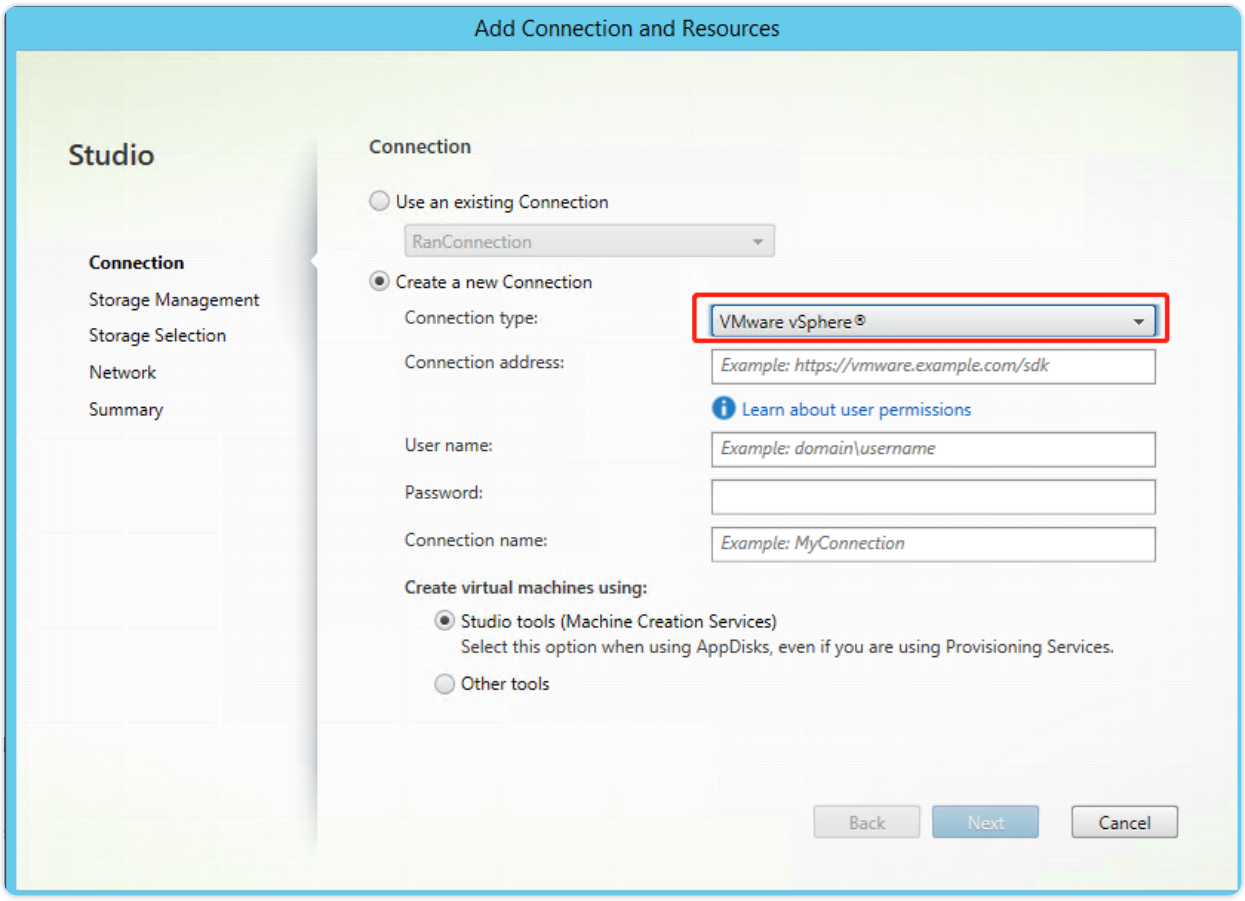
1. オンプレミスのDelivery Controllerの場合、オンプレミスのCitrix Studioで**Configuration > Hosting > Add Connection and Resources**を選択します。クラウドDelivery Controllerの場合、Citrix CloudのWebベースのStudioコンソールで**Manage > Hosting > Add Connection and Resources**を選択して、Nutanixハイパーバイザーへの接続を作成します。
2. **Add Connection and Resources**ウィザードで、**Connection**ページで接続タイプとしてNutanix AHVを選択し、ハイパーバイザーのアドレス、資格情報、および接続名を指定します。**Network**ページで、ユニットのネットワークを選択します。

   例として、オンプレミスのCitrix Studioでは次のようになります。

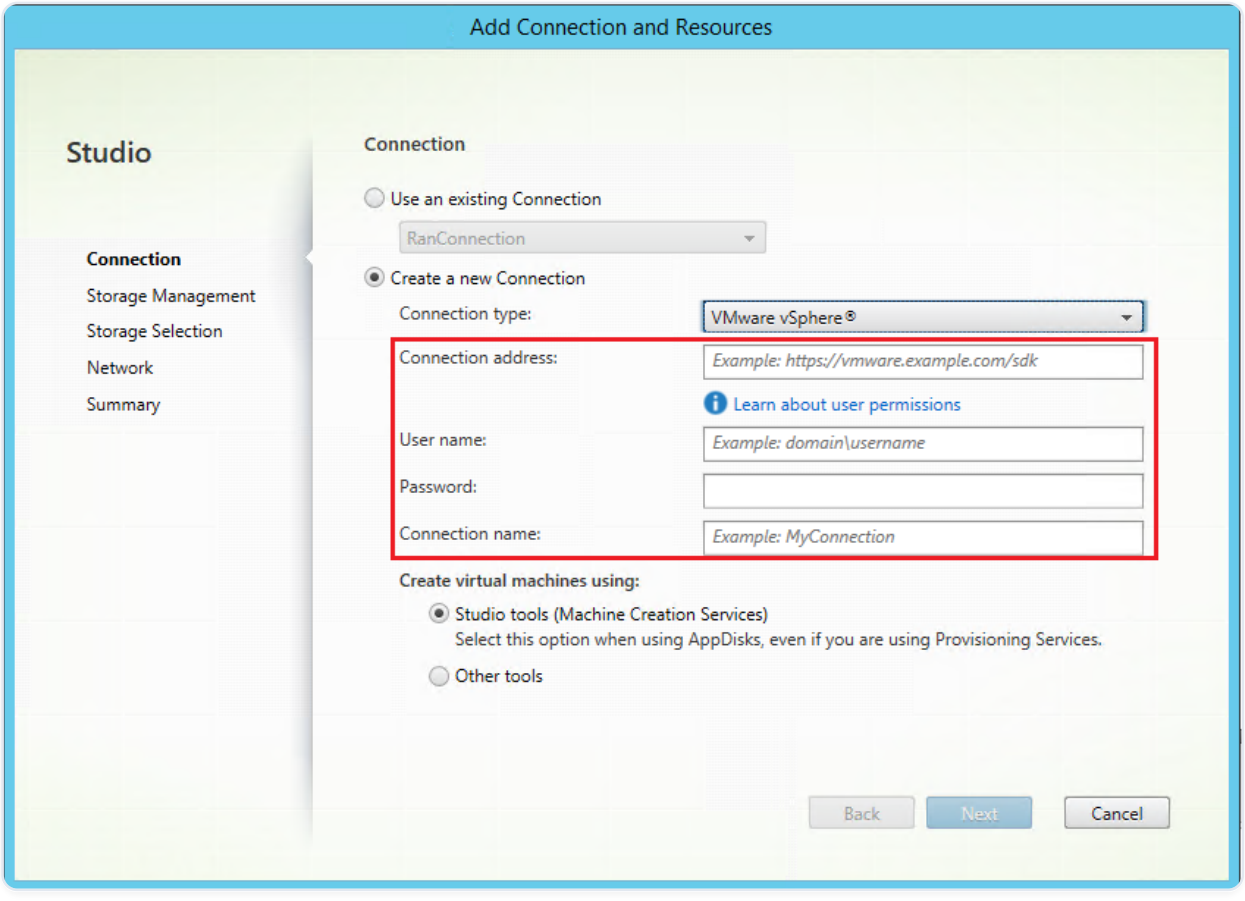


Citrix StudioでVMwareへのホスト接続を作成する

1. vSphere環境にvCenter Serverをインストールします。詳細については、VMware vSphereを参照してください。
2. Citrix Studioで、**［構成］>［ホスト］>［接続とリソースの追加］**を選択します。
3. 接続タイプとしてVMware vSphereを選択します。



4. VMwareアカウントの接続アドレス（vCenter ServerのURL）、ユーザー名とパスワード、および接続名を入力します。



ステップ3：マスターイメージを準備する

（Citrix Hypervisorのみ）ステップ3a：Citrix VM Toolsをインストールする

各VMがxe CLIまたはXenCenterを使用できるように、テンプレートVMにCitrix VM Toolsをインストールします。ツールをインストールしないと、VMのパフォーマンスが低下する可能性があります。ツールがないと、次のいずれも実行できません。

- VMをクリーンにシャットダウン、再起動、または一時停止する。
- XenCenterでVMのパフォーマンスデータを表示する。
- 実行中のVMを移行する（`XenMotion`経由）。
- スナップショットまたはメモリ付きスナップショット（チェックポイント）を作成し、スナップショットに戻す。
- 実行中のLinux VMのvCPU数を調整する。

1. guest-tools.isoという名前のCitrix VM Toolsをマウントするには、次のコマンドを実行します。

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. お使いのLinuxディストリビューションに基づいて、`xe-guest-utilities`パッケージをインストールするには、次のコマンドを実行します。

   RHEL/CentOS/Rocky Linuxの場合：

   ```
   sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
   ```

   Ubuntu/Debianの場合：

   ```
   sudo dpkg -i /mnt/Linux/xe-guest-utilities_{package-version}_all.deb
   ```

   SUSEの場合:

   ```
   sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
   ```

3. XenCenterの**General**タブで、テンプレートVMの仮想化状態を確認します。Citrix VM Toolsが正しくインストールされている場合、仮想化状態は**Optimized**になります。

ステップ3b：AWS、Azure、GCP上のSUSE 15.4の構成を確認する

AWS、Azure、GCP上のSUSE 15.4については、以下を確認してください。

- **libstdc++6**バージョン12以降を使用していること。
- **/etc/sysconfig/windowmanager** 内の **Default_WM** パラメーターが **"gnome"** に設定されていること。

ステップ3c：Azure、AWS、GCP上のUbuntu 18.04向けにcloud-initを構成する

1. VMの再起動時または停止時にVDAホスト名が保持されるようにするには、次のコマンドを実行します。

   ```
   echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
   ```

   /etc/cloud/cloud.cfgファイルの**system_info**セクションに以下の行が存在することを確認します。

   ```
   system_info:

      network:

          renderers: ['netplan', 'eni', 'sysconfig']
   ```

2. AWS上のMCSで作成されたVMにリモートでアクセスするためにSSHを使用するには、それらのVMにはキー名がアタッチされていないため、パスワード認証を有効にします。必要に応じて、次の操作を行います。

   - `cloud-init`構成ファイル /etc/cloud/cloud.cfg を編集します。**ssh_pwauth: true**の行が存在することを確認します。**set-password**の行とそれに続く行が存在する場合は、削除またはコメントアウトします。

     ```
     users:

     - default
     ```

   - `cloud-init`によって作成されたデフォルトユーザー`ec2-user`または`ubuntu`を使用する予定がある場合は、`passwd`コマンドを使用してユーザーパスワードを変更できます。新しいパスワードは、後でMCSで作成されたVMにログインするために覚えておいてください。
   - `/etc/ssh/sshd_config`ファイルを編集して、次の行が存在することを確認します。

```
PasswordAuthentication yes
```

ファイルを保存し、`sudo service sshd restart`コマンドを実行します。

ステップ3d：GCP上のUbuntu 20.04でRDNSを無効にする

テンプレートVMで、/etc/krb5.conf の の下に **rdns = false** の行を追加します。

ステップ3e: テンプレートVMにLinux VDAパッケージをインストールする

> **注:**
>
> 現在実行中のVDAをテンプレートVMとして使用する場合は、この手順をスキップしてください。

> テンプレートVMにLinux VDAパッケージをインストールする前に、.NET Runtime 6.0をインストールしてください。

> お使いのLinuxディストリビューションに基づいて、Linux VDAの環境をセットアップするために次のコマンドを実行します。

RHEL/CentOS/Rocky Linuxの場合:

> **注:**
>
> - RHELおよびCentOSの場合、Linux VDAをインストールして`deploymcs.sh`を正常に実行する前に、EPELリポジトリをインストールしてください。EPELのインストール方法については、`<https://docs.fedoraproject.org/ja-jp/epel/>`の指示を参照してください。
> - RHEL 9.1/9.0およびRocky Linux 9.1/9.0にLinux VDAをインストールする前に、**libsepol** パッケージをバージョン3.4以降に更新してください。

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
```

Ubuntu/Debianの場合:

```
sudo dpkg –i  <PATH>/<Linux VDA DEB>



apt-get install -f
```

SUSEの場合:

```
sudo zypper –i install <PATH>/<Linux VDA RPM>
```

ステップ3f: tdb-toolsパッケージをインストールするためのリポジトリを有効にする（RHEL 7のみ）

RHEL 7サーバーの場合:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

RHEL 7ワークステーションの場合:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

ステップ3g: (SUSEの場合) ntfs-3gを手動でインストールする

SUSEプラットフォームでは、ntfs-3gを提供するリポジトリはありません。ソースコードをダウンロードし、コンパイルして、ntfs-3gを手動でインストールしてください。

1. GNU Compiler Collection (GCC) コンパイラシステムとmakeパッケージをインストールします。

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. ntfs-3gパッケージをダウンロードします。
3. ntfs-3gパッケージを解凍します。

   ```
   sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
   ```

4. ntfs-3gパッケージへのパスを入力します。

```
sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. ntfs-3gをインストールします。

```
./configure

make

make install
```

手順3h：使用するデータベースを指定する

実験的な機能として、PostgreSQLに加えてSQLiteを使用できます。Linux VDAパッケージのインストール後も、SQLiteとPostgreSQLを切り替えることができます。これを行うには、次の手順を完了します。

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh`を実行します。新規インストールの場合、この手順は省略してください。
2. `deploymcs.sh`を実行する前に、`/etc/xdl/db.conf`を編集します。

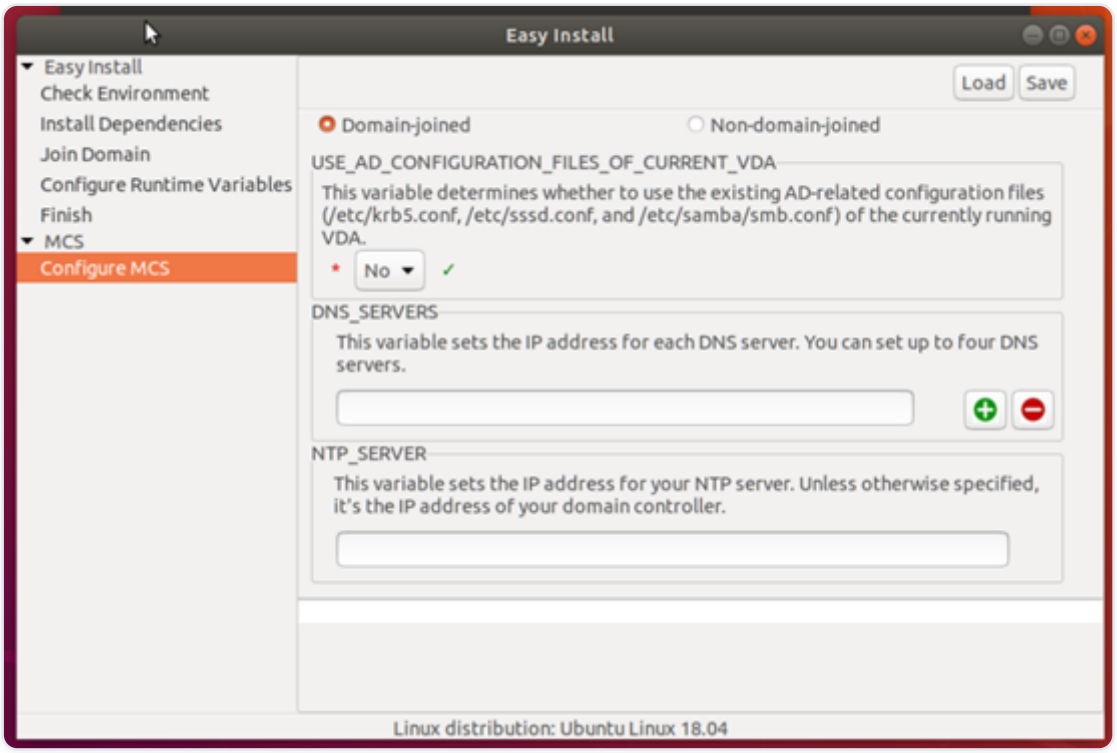
注:

- VDIモードでのみSQLiteを使用することをお勧めします。
- 簡単なインストールとMCSの場合、手動でインストールすることなくSQLiteとPostgreSQLを切り替えることができます。`/etc/xdl/db.conf`で特に指定がない限り、Linux VDAはデフォルトでPostgreSQLを使用します。
- PostgreSQLのポート番号を構成するには、`/etc/xdl/db.conf`を使用することもできます。

手順3i：MCS変数を構成する

MCS変数を構成する方法は2つあります。

- `/etc/xdl/mcs/mcs.conf`ファイルを編集します。
- 簡易インストールGUIを使用します。簡易インストールGUIを開くには、Linux VDAのデスクトップ環境で`/opt/Citrix/VDA/bin/easyinstall`コマンドを実行します。



> **ヒント:**
>
> **保存**をクリックすると、指定したパスのローカルファイルに変数の設定が保存されます。**読み込み**をクリックすると、指定したファイルから変数の設定が読み込まれます。

以下は、ドメインに参加していないシナリオとドメインに参加しているシナリオで構成できるMCS変数です。

- **ドメインに参加していないシナリオの場合**

  デフォルトの変数値を使用するか、必要に応じて変数をカスタマイズできます（オプション）。

  `DOTNET_RUNTIME_PATH` =*path-to-install-dotnet-runtime **

  `DESKTOP_ENVIRONMENT` = *gnome | mate ** `REGISTER_SERVICE` =**Y | N**

  `ADD_FIREWALL_RULES` =**Y | N** `VDI_MODE` =**Y | N**

  `START_SERVICE` =**Y | N**

- **ドメインに参加しているシナリオの場合**

  - `Use_AD_Configuration_Files_Of_Current_VDA`: 現在実行中のVDAの既存のAD関連構成ファイル（/etc/krb5.conf、/etc/sssd.conf、および/etc/samba/smb.conf）を使用するかど

うかを決定します。Yに設定すると、MCSで作成されたマシンの構成ファイルは、現在実行中のVDAの対応するファイルと同じになります。ただし、`dns`変数と`AD_INTEGRATION`変数は引き続き構成する必要があります。デフォルト値はNで、これはマスターイメージの構成テンプレートがMCSで作成されたマシンの構成ファイルを決定することを意味します。

- `dns`: 各DNSサーバーのIPアドレスを設定します。最大4つのDNSサーバーを設定できます。
- `NTP_SERVER`: NTPサーバーのIPアドレスを設定します。特に指定がない限り、これはドメインコントローラーのIPアドレスです。
- `WORKGROUP`: ADで構成したNetBIOS名（大文字と小文字を区別）にワークグループ名を設定します。そうでない場合、MCSはマシンホスト名の直後にあるドメイン名の一部をワークグループ名として使用します。たとえば、マシンアカウントが**user1.lvda.citrix.com**の場合、MCSは**lvda**をワークグループ名として使用しますが、**citrix**が正しい選択です。ワークグループ名を正しく設定してください。
- `AD_INTEGRATION`: Winbind、SSSD、PBIS、またはCentrifyを設定します。MSCがサポートするLinuxディストリビューションとドメイン参加方法の対応表については、この記事のサポートされているディストリビューションを参照してください。
- `CENTRIFY_DOWNLOAD_PATH`: Server Suite Free（旧Centrify Express）パッケージをダウンロードするためのパスを設定します。この値は、`AD_INTEGRATION`変数をCentrifyに設定した場合にのみ有効になります。
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Centrify Sambaパッケージをダウンロードするためのパスを設定します。この値は、`AD_INTEGRATION`変数をCentrifyに設定した場合にのみ有効になります。
- `PBIS_DOWNLOAD_PATH`: PBISパッケージをダウンロードするためのパスを設定します。この値は、`AD_INTEGRATION`変数をPBISに設定した場合にのみ有効になります。
- `UPDATE_MACHINE_PW`: マシンアカウントのパスワード更新の自動化を有効または無効にします。詳細については、「マシンアカウントのパスワード更新を自動化する」を参照してください。
- Linux VDA構成変数:

  `DOTNET_RUNTIME_PATH`=*dotnet ランタイムのインストールパス **

  `DESKTOP_ENVIRONMENT`= *gnome | mate ** `SUPPORT_DDC_AS_CNAME`=**Y | N**

  `VDA_PORT`=**ポート番号** `REGISTER_SERVICE`=**Y | N**

`ADD_FIREWALL_RULES`=**Y | N** `HDX_3D_PRO`=**Y | N**

`VDI_MODE`=**Y | N** `SITE_NAME`=**DNSサイト名 | '<none\>'**

`LDAP_LIST`=**'LDAPサーバーのリスト' | '<none\>'** `SEARCH_BASE`=**検索ベース設定 | '<none\>'**

`FAS_LIST`=**'FASサーバーのリスト' | '<none\>'** `START_SERVICE`=**Y | N**

`TELEMETRY_SOCKET_PORT`=**ポート番号** `TELEMETRY_PORT`=**ポート番号**

ステップ3j: MCSのレジストリ値を書き込むか更新する

テンプレートマシンで、必要に応じてレジストリ値を書き込むまたは更新するために、`/etc/xdl/mcs/mcs_local_setting.reg`ファイルにコマンドラインを追加します。この操作により、MCSでプロビジョニングされたマシンが再起動するたびにデータと設定が失われるのを防ぎます。

`/etc/xdl/mcs/mcs_local_setting.reg`ファイルの各行は、レジストリ値を設定または更新するためのコマンドです。

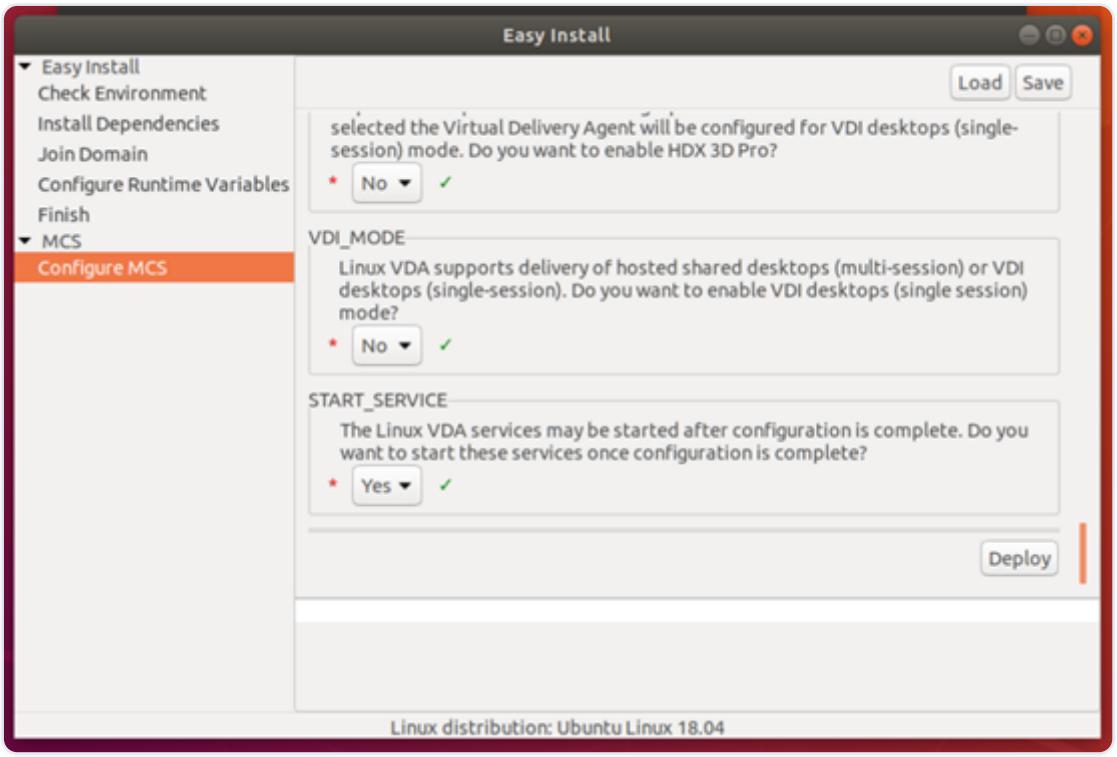
たとえば、`/etc/xdl/mcs/mcs_local_setting.reg`ファイルに次のコマンドラインを追加して、レジストリ値をそれぞれ書き込むまたは更新できます。

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

ステップ3k: マスターイメージを作成する

1. `/etc/xdl/mcs/mcs.conf`を編集してMCS変数を構成する場合は、`/opt/Citrix/VDA/sbin/deploymcs.sh`を実行します。GUIを使用してMCS変数を構成する場合は、**Deploy**をクリックします。



GUIで**Deploy**をクリックすると、GUIで設定した変数が`/etc/xdl/mcs/mcs.conf`ファイルで設定した変数を上書きします。

2. (現在実行中のVDAをテンプレートVMとして使用している場合、またはドメインに参加していないシナリオの場合は、この手順をスキップしてください。) テンプレートVMで、構成テンプレートを更新して、作成されたすべてのVM上の関連する`/etc/krb5.conf`、`/etc/samba/smb.conf`、および`/etc/sssd/sssd.conf`ファイルをカスタマイズします。

   Winbindユーザーの場合は、`/etc/xdl/ad_join/winbind_krb5.conf.tmpl`および`/etc/xdl/ad_join/winbind_smb.conf.tmpl`テンプレートを更新します。

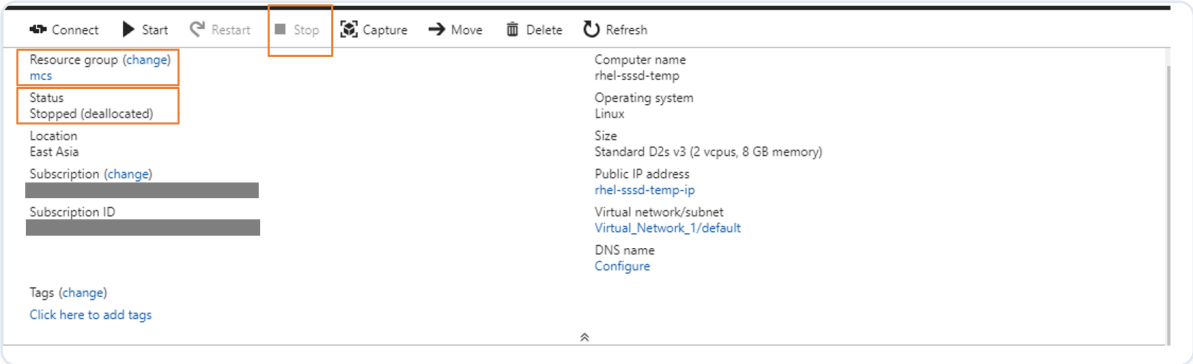
   SSSDユーザーの場合は、`/etc/xdl/ad_join/sssd.conf.tmpl`、`/etc/xdl/ad_join/sssd_krb5.conf.tmpl`、および`/etc/xdl/ad_join/sssd_smb.conf.tmpl`テンプレートを更新します。

   Centrifyユーザーの場合、`/etc/xdl/ad_join/centrify_krb5.conf.tmpl`と`/etc/xdl/ad_join/centrify_smb.conf.tmpl`テンプレートを更新します。

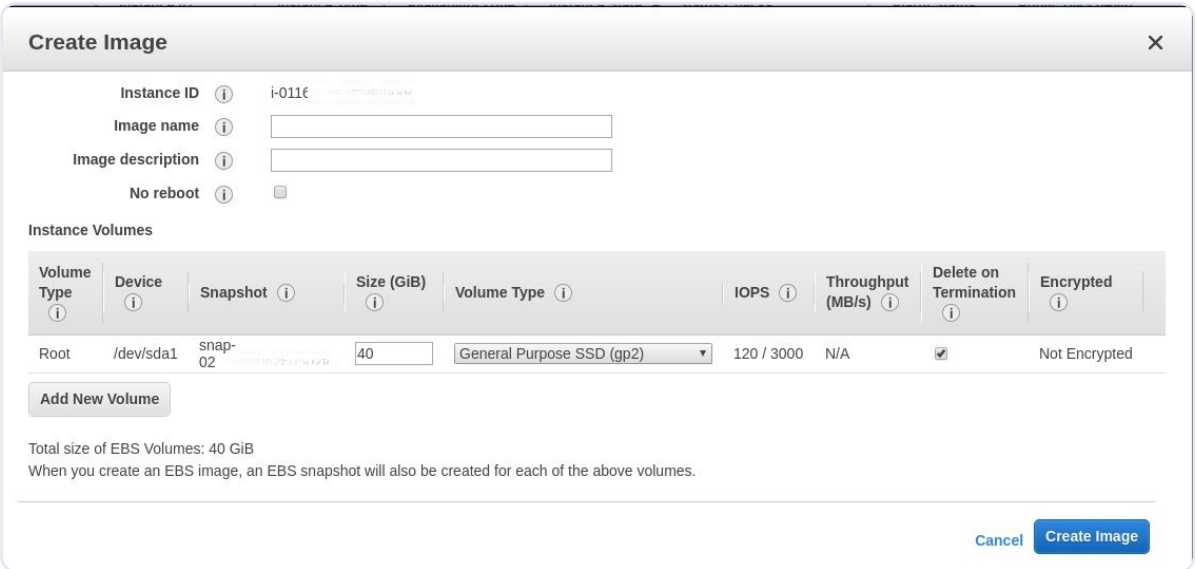
   > **注:**
   >
   > テンプレートファイルで使用されている既存の形式を維持し、$WORKGROUP、$REALM、$realm、${new_hostname}、および$AD_FQDNなどの変数を使用します。

3. 使用しているパブリッククラウドに基づいて、マスターイメージのスナップショットを作成し、名前を付けます。

   - **(Citrix Hypervisor、GCP、およびVMware vSphereの場合)** テンプレートVMにアプリケーションをインストールし、テンプレートVMをシャットダウンします。マスターイメージのスナップショットを作成し、名前を付けます。
   - **(Azureの場合)** テンプレートVMにアプリケーションをインストールし、Azureポータルからテンプレートを VMをシャットダウンします。テンプレートVMの電源ステータスが**停止済み (割り当て解除済み)**であることを確認します。ここでリソースグループの名前を覚えておいてください。Azureでマスターイメージを見つけるには、この名前が必要です。



   - **(AWSの場合)** テンプレートVMにアプリケーションをインストールし、AWS EC2ポータルからテンプレートを VMをシャットダウンします。テンプレートVMのインスタンスの状態が**停止済み**であることを確認します。テンプレートVMを右クリックし、**イメージ > イメージの作成**を選択します。必要に応じて情報を入力し、設定を行います。**イメージの作成**をクリックします。



   - **(Nutanixの場合)** Nutanix AHVで、テンプレートVMをシャットダウンします。マスターイメージのスナップショットを作成し、名前を付けます。

> **注:**
>
> Citrix Virtual Apps™およびDesktopsで使用するために、Acropolisスナップショット名に `XD_` をプレフィックスとして付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した後、更新されたリストを取得するために、**カタログの作成**ウィザードを再起動します。

(GCPの場合) ステップ3l: RHEL 8.x/9.xおよびRocky Linux 8.x/9.xでのイーサネット接続の構成

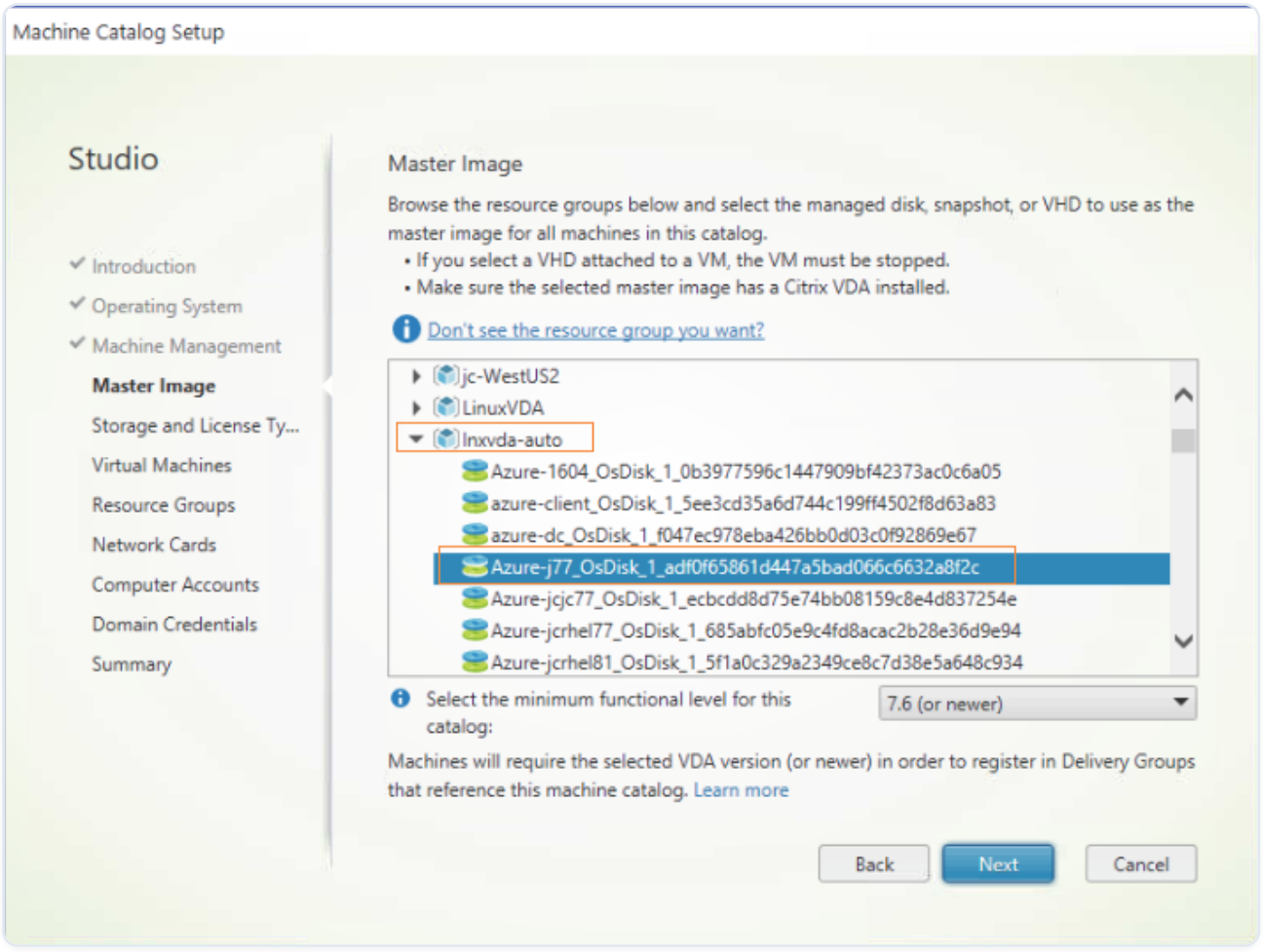
GCPでホストされているRHEL 8.x/9.xおよびRocky Linux 8.x/9.xにLinux VDAをインストールした後、VMの再起動後にイーサネット接続が失われ、Linux VDAに到達できなくなる可能性があります。この問題を回避するには、VMを再起動する前に次のコマンドを実行します。

```
nmcli dev connect eth0

service NetworkManager restart
```

ステップ4: マシンカタログを作成する

Citrix Studioで、マシンカタログを作成し、カタログに作成するVMの数を指定します。マシンカタログを作成する際に、マスターイメージを選択します。以下に例を示します。



マスターイメージの選択(/en-us/linux-virtual-delivery-agent/2303/media/choose-master-image-from-the-list.png)

Nutanix固有の**コンテナ**ページで、以前にテンプレートVMに指定したコンテナを選択します。**マスターイメージ**ページで、イメージスナップショットを選択します。**仮想マシン**ページで、仮想CPUの数とvCPUあたりのコア数を確認します。

注:

Delivery Controller™でのマシンカタログ作成プロセスにかなりの時間がかかる場合は、Nutanix Prismに移動し、**Preparation**というプレフィックスが付いたマシンを手動でパワーオンします。この方法により、作成プロセスを続行できます。

必要に応じて、その他の構成タスクを実行します。詳しくは、「Studioを使用したマシンカタログの作成」を参照してください。

ステップ5：デリバリーグループの作成

デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。詳しくは、「デリバリーグループの作成」を参照してください。

> **注:**
>
> MCSを使用して作成したVMがCitrix Cloud Connectorに登録できず、**未登録**と表示される場合があります。この問題は、AzureでVMをホストし、Samba Winbindを使用してADドメインに参加している場合に発生します。この問題を回避するには、次の手順を実行します。

1. ADSI Editコンソールに移動し、未登録のVMを選択して、そのマシンアカウントの**msDS-SupportedEncryptionTypes**属性を編集します。
2. VMで**ctxjproxy**サービスと**ctxvda**サービスを再起動します。VMのステータスが**登録済み**に変わったら、手順3〜5に進みます。
3. テンプレートVMで**/var/xdl/mcs/ad_join.sh**ファイルを開きます。
4. **/var/xdl/mcs/ad_join.sh**ファイル内で、以下の行の後に、**net ads enctypes set $NEW_HOSTNAME\\$ <Decimal value of encryption type attribute, for example, 28\ \> -U $NEW_HOSTNAME\\$ -P password**という行を追記してください。

   ```
   if [ "$AD_INTEGRATION" == "winbind" ]; then

                   join_domain_samba

                   restart_service winbind /usr/bin/systemctl
   ```

5. 新しいスナップショットを作成し、新しいテンプレートを使用してVMを作成します。

MCSを使用してLinux VDAをアップグレードする

MCSを使用してLinux VDAをアップグレードするには、次の手順を実行します。

1. Linux VDAを現在のリリースにアップグレードする前に、.NET Runtime 6.0がインストールされていることを確認してください。
2. テンプレートマシン上のLinux VDAをアップグレードします:

注:

自動ソフトウェアアップデートをスケジュールするには、Linux VDA self-update機能を使用することもできます。この目的を達成するには、テンプレートマシンのetc/xdl/mcs/mcs_local_setting.regファイルにコマンドラインを追加します。 たとえば、次のコマンドラインを追加できます:

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
-t "REG_DWORD" -v "fEnabled" -d "0x00000001" –force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
-t "REG_SZ" -v "ScheduledTime" -d "Immediately" –force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
-t "REG_SZ" -v "Url" -d "&lt;Your-Azure-Container-Url>" –force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
-t "REG_SZ" -v "CaCertificate" -d "&lt;Local-Certificate-Path-of-
PortalAzureCom>" --force
```

RHEL 7およびCentOS 7の場合:

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

RHEL 8.xおよびRocky Linux 8.xの場合:

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の場合:

注:

> RHEL 9.1/9.0およびRocky Linux 9.1/9.0でLinux VDAをアップグレードする前に、**libsepol**パッケージをバージョン3.4以降にアップデートしてください。

```
sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
```

SUSEの場合:

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Ubuntu 18.04の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Ubuntu 20.04の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

Ubuntu 22.04の場合:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

3. `/etc/xdl/mcs/mcs.conf`と`/etc/xdl/mcs/mcs_local_setting.reg`を編集します。
4. 新しいスナップショットを作成します。
5. Citrix Studioで、新しいスナップショットを選択してマシンカタログを更新します。各マシンが再起動するまで待機します。マシンを手動で再起動しないでください。

マシンアカウントのパスワード更新を自動化する

マシンアカウントのパスワードは、デフォルトでマシンカタログ作成後30日で期限切れになります。パスワードの期限切れを防ぎ、マシンアカウントのパスワード更新を自動化するには、次の手順を実行します:

1. /opt/Citrix/VDA/sbin/deploymcs.shを実行する前に、/etc/xdl/mcs/mcs.confに次のエントリを追加します。

   `UPDATE_MACHINE_PW="Y"`

2. /opt/Citrix/VDA/sbin/deploymcs.shを実行した後、/etc/cron.d/mcs_update_password_cronjobを開いて更新時間と頻度を設定します。デフォルト設定では、毎週日曜日の午前2時30分にマシンアカウントのパスワードが更新されます。

マシンアカウントのパスワードが更新されるたびに、Delivery Controller上のチケットキャッシュが無効になり、/var/log/xdl/jproxy.logに次のエラーが表示されることがあります。

```
[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred. Error: Failure unspecified at GSS-API level (Mechanism level: Checksum failed)
```

エラーを解消するには、チケットキャッシュを定期的にクリアしてください。すべてのDelivery Controllerまたはドメインコントローラーでキャッシュクリーンアップタスクをスケジュールできます。

MCSで作成されたVMでFASを有効にする

次のディストリビューションで実行されているMCSで作成されたVMでFASを有効にできます。

	ウィンバインド	SSSD	セントリファイ	PBIS
RHEL 9.1/9.0	はい	いいえ	いいえ	いいえ
RHEL 8.x	はい	いいえ	いいえ	はい
ロッキー Linux 9.1/9.0	はい	いいえ	いいえ	いいえ
ロッキー Linux 8.x	はい	いいえ	いいえ	いいえ
RHEL 7、CentOS 7	はい	はい	いいえ	はい
ウブントゥ 22.04、ウブントゥ 20.04、ウブントゥ 18.04	はい	いいえ	いいえ	いいえ
デビアン 11.3	はい	いいえ	いいえ	いいえ
SUSE 15.4	はい	いいえ	いいえ	いいえ

テンプレートVMでマスターイメージを準備する際にFASを有効にする

1. ルートCA証明書をインポートします。

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

2. ctxfascfg.shを実行します。詳しくは、ctxfascfg.shの実行 を参照してください。
3. `/etc/xdl/mcs/mcs.conf` で変数を設定します。

   注:

   これらの変数はVMの起動時に呼び出されるため、`/etc/xdl/mcs/mcs.conf` で必要なすべての変数を設定します。

   a. `Use_AD_Configuration_Files_Of_Current_VDA` の値をYに設定します。
   b. `FAS_LIST` 変数をFASサーバーアドレス、または複数のFASサーバーアドレスに設定します。複数のアドレスはセミコロンで区切り、アドレスを単一引用符で囲みます（例: `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`）。
   c. 必要に応じて、たとえば `VDI_MODE` などの他の変数を設定します。

4. スクリプト `/opt/Citrix/VDA/sbin/deploymcs.sh` を実行します。

MCSで作成されたVMでFASを有効にする

前述のようにテンプレートマシンでFASが有効になっていない場合、各MCSで作成されたVMでFASを有効にできます。

MCSで作成されたVMでFASを有効にするには、次の手順を実行します。

1. /etc/xdl/mcs/mcs.conf で変数を設定します。

   注:

   これらの変数はVMの起動時に呼び出されるため、`/etc/xdl/mcs/mcs.conf` ですべての必要な変数を設定します。

   a. `Use_AD_Configuration_Files_Of_Current_VDA` の値を Y に設定します。

b. `FAS_LIST` 変数をFASサーバーのアドレスに設定します。

c. 必要に応じて、`VDI_MODE` などの他の変数を設定します。

2. ルートCA証明書をインポートします。

```
sudo cp root.pem /etc/pki/CA/certs/
```

3. `/opt/Citrix/VDA/sbin/ctxfascfg.sh` スクリプトを実行します。詳しくは、ctxfascfg.sh の実行 を参照してください。

Citrix Provisioning™ を使用して Linux VDA を作成する

Citrix Provisioning を使用して、ドメイン参加済み VDA を作成できます。

この記事では、Linux ターゲットデバイスのストリーミングに関する情報を提供します。この機能を使用すると、Citrix Virtual Apps and Desktops™ 環境に Linux 仮想デスクトップを直接プロビジョニングできます。

以下の Linux ディストリビューションがサポートされています。

- ウブントゥ 22.04
- ウブントゥ 20.04
- ウブントゥ 18.04
- RHEL 9.1
- RHEL 9.0
- RHEL 8.6
- RHEL 8.4
- RHEL 7.9
- ロッキー リナックス 9.1
- ロッキー リナックス 9.0
- ロッキー リナックス 8.6

> **重要:**

- Citrix Provisioning の最新のインストールパッケージを使用することをお勧めします。お使いの Linux ディストリビューションに基づいたパッケージを使用してください。Linux ストリーミングエージェント 2109 以降を使用するには、Citrix Provisioning Server 2109 以降が必要です。
- Citrix Provisioning を使用して Linux ターゲットデバイスをストリーミングする場合、プロビジョニングされたデバイスが期待どおりに起動できるように、単一の共有ディスクイメージ上に個別のブートパーティションを作成します。
- **btrfs** でパーティションをフォーマットすることは避けてください。GRUB2 には、**btrfs** パーティションを見つける際に固有の問題があります。**GRUB** は **GRand Unified Bootloader** の略です。

詳細については、Citrix Provisioning のドキュメントにあるLinux ターゲットデバイスのストリーミングを参照してください。

Citrix DaaS Standard for Azure で Linux VDA を作成する

Citrix DaaS Standard for Azure (旧称 Citrix Virtual Apps and Desktops Standard for Azure) で、ドメイン参加済みおよび非ドメイン参加済みの両方の Linux VDA を作成し、Microsoft Azure から任意のデバイスに仮想アプリとデスクトップを配信できます。詳細については、Citrix DaaS Standard for Azureを参照してください。

サポートされているLinuxディストリビューション

この機能は、以下の Linux ディストリビューションでサポートされています。

- RHEL 9.1
- RHEL 9.0
- RHEL 8.7
- RHEL 8.6
- RHEL 8.4
- ロッキー リナックス 9.1
- ロッキー リナックス 9.0
- ロッキー リナックス 8.7
- ロッキー リナックス 8.6
- SUSE 15.4

- ウブントゥ 22.04
- ウブントゥ 20.04
- ウブントゥ 18.04

手順1：Azureでマスターイメージを準備する

> **注:**
>
> 自動ソフトウェアアップデートをスケジュールするために、Linux VDA セルフアップデート機能も使用できます。この目的を達成するには、マスターイメージ上のetc/xdl/mcs/mcs_local_setting.regファイルにコマンドラインを追加します。 たとえば、次のコマンドラインを追加できます。
>
> ```
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
> "REG_DWORD" -v "fEnabled" -d "0x00000001" –force
>
>
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
> "REG_SZ" -v "ScheduledTime" -d "Immediately" –force
>
>
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
> "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" –force
>
>
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
> "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-
> PortalAzureCom>" --force
> ```

1. Azureで、サポートされているディストリビューションのLinux VMを作成します。
2. 必要に応じて、Linux VMにデスクトップ環境をインストールします。
3. VMに、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>`の指示に従って.NET Runtime 6.0をインストールします。

4. (Ubuntuのみ) `source /etc/network/interfaces.d/*` 行を `/etc/network/interfaces` ファイルに追加します。
5. (Ubuntuのみ) `/etc/resolv.conf` を `/run/systemd/resolve/stub-resolv.conf` にポイントする代わりに、`/run/systemd/resolve/resolv.conf` にポイントします。

```
unlink /etc/resolv.conf



ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

6. Linux VDAパッケージをインストールします。
7. 使用するデータベースを指定します。

   実験的な機能として、PostgreSQLに加えてSQLiteを使用できます。Linux VDAパッケージのインストール後に、SQLiteとPostgreSQLを切り替えることもできます。これを行うには、次の手順を完了します。

   a. `/opt/Citrix/VDA/sbin/ctxcleanup.sh` を実行します。新規インストールの場合、この手順は省略します。
   b. `deploymcs.sh` を実行する前に `/etc/xdl/db.conf` を編集します。

   > **注:**
   >
   > - SQLiteはVDIモードでのみ使用することをお勧めします。
   > - 簡単なインストールとMCSの場合、手動でインストールすることなくSQLiteとPostgreSQLを切り替えることができます。`/etc/xdl/db.conf` で別途指定されていない限り、Linux VDAはデフォルトでPostgreSQLを使用します。
   > - PostgreSQLのポート番号を設定するために `/etc/xdl/db.conf` も使用できます。

8. MCS変数を変更します。

   MCS変数を構成する方法は2つあります。

   - `/etc/xdl/mcs/mcs.conf` ファイルを編集します。

- 簡単インストールGUIを使用します。簡単インストールGUIを開くには、Linux VDAのデスクトップ環境で`/opt/Citrix/VDA/bin/easyinstall`コマンドを実行します。

  > **注:**
  >
  > `dns`変数は指定しないでください。 マシンカタログを作成する際に**Static**または**Random**タイプを選択した場合は、`VDI_MODE=Y`を設定します。

  > `/etc/xdl/mcs/mcs.conf`を編集してMCS変数を構成する場合は、`/opt/Citrix/VDA/sbin/deploymcs.sh`を実行します。GUIを使用してMCS変数を構成する場合は、**Deploy**をクリックします。

  簡単インストールGUIの展開ボタン(/en-us/linux-virtual-delivery-agent/2303/media/deploy-button-on-easy-install-gui.png)

  GUIで**Deploy**をクリックすると、GUIで設定した変数が`/etc/xdl/mcs/mcs.conf`ファイルで設定した変数を上書きします。

9. Azureで、VMを停止（または割り当て解除）します。**ディスクのエクスポート**をクリックして、他のVMを作成するためのマスターイメージとして使用できる仮想ハードディスク（VHD）ファイルのSAS URLを生成します。

   VHDファイルのURLを生成(/en-us/linux-virtual-delivery-agent/2303/media/export-disk.png)

10. （オプション）マスターイメージでグループポリシー設定を行います。`ctxreg`ツールを使用してグループポリシー設定を行うことができます。たとえば、次のコマンドはPDF印刷用の**PDFユニバーサルプリンターの自動作成**ポリシーを有効にします。

    ```
    /opt/Citrix/VDA/bin/ctxreg create -k
    "HKLM\Software\Citrix\GroupPolicy\Defaults\PrintingPolicies" -t
    "REG_DWORD" -v "AutoCreatePDFPrinter" -d "0x00000001" –force
    ```

ステップ2：Azureからマスターイメージをインポートする

1. 管理ダッシュボードから、右側の**マスターイメージ**を展開します。Citrixが提供するマスターイメージと、作成およびインポートしたイメージが表示されます。

   > **ヒント:**

> このサービスのほとんどの管理者アクティビティは、**管理**および**監視**ダッシュボードを通じて管理されます。最初のカタログを作成すると、Citrix Cloud™にサインインして**Managed Desktops**サービスを選択した後、**管理**ダッシュボードが自動的に起動します。

> マスターイメージの画像(/en-us/linux-virtual-delivery-agent/2303/media/master-images.png)

2. **イメージのインポート**をクリックします。
3. Azure で生成した VHD ファイルの SAS URL を入力します。マスターイメージの種類には **Linux** を選択します。

   Azure からイメージをインポートする画像(/en-us/linux-virtual-delivery-agent/2303/media/import-an-image-from-azure.png)
4. ウィザードの指示に従って、マスターイメージのインポートを完了します。

ステップ 3: マシンカタログを作成する

管理 ダッシュボードにアクセスし、**カタログの作成**をクリックします。マシンカタログを作成するときは、以前に作成したマスターイメージを選択します。

> **注:**
>
> マスターイメージとして使用される VM は、SSH または RDP を介してアクセスできません。VM にアクセスするには、Azure portal のシリアルコンソールを使用します。

Linux VDA を手動でインストールする

以下の Linux ディストリビューションに Linux VDA を手動でインストールできます。

- アマゾン Linux 2、セントオーエス、RHEL、および ロッキー Linux
- SUSE
- ウブントゥ
- デビアン

Amazon Linux 2、CentOS、RHEL、Rocky Linux に Linux VDA を手動でインストールする

> **重要:**
>
> 新規インストールの場合、迅速なインストールには簡易インストールを使用することをお勧めします。簡易インストールは、時間と労力を節約し、この記事で詳述されている手動インストールよりもエラーが発生しにくいです。

ステップ 1: 構成情報とLinuxマシンを準備する

ステップ 1a: ネットワーク構成を確認する

ネットワークが正しく接続され、構成されていることを確認してください。たとえば、Linux VDAでDNSサーバーを構成する必要があります。

ステップ 1b: ホスト名を設定する

マシンのホスト名が正しく報告されるようにするには、**/etc/hostname** ファイルを、マシンのホスト名のみを含むように変更します。

```
hostname
```

ステップ 1c: ホスト名にループバックアドレスを割り当てる

マシンのDNSドメイン名と完全修飾ドメイン名（FQDN）が正しく報告されるようにするには、`/etc/hosts`ファイルの次の行を、FQDNとホスト名を最初の2つのエントリとして含むように変更します。

```
127.0.0.1 hostname-fqdn hostname localhost localhost.localdomain localhost4 localhost4.localdomain4
```

例:

```
127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4
```

ファイル内の他のエントリから、**hostname-fqdn** または **hostname** への他の参照をすべて削除します。

> **注:**

> Linux VDAは現在、NetBIOS名の切り捨てをサポートしていません。ホスト名は15文字を超えてはなりません。

> **ヒント:**

> a～z、A～Z、0～9、およびハイフン（-）文字のみを使用してください。アンダーバー（_）、スペース、その他の記号は避けてください。ホスト名を数字で始めたり、ハイフンで終わらせたりしないでください。このルールは、Delivery Controllerのホスト名にも適用されます。

ステップ 1d: ホスト名を確認する

ホスト名が正しく設定されていることを確認します。

```
hostname
```

このコマンドは、マシンのホスト名のみを返し、完全修飾ドメイン名（FQDN）は返しません。

FQDN が正しく設定されていることを確認します。

```
hostname -f
```

このコマンドは、マシンの FQDN を返します。

ステップ 1e: 名前解決とサービス到達可能性の確認

FQDN を解決し、ドメインコントローラーと Delivery Controller™ に ping できることを確認します。

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn
```

```
ping delivery-controller-fqdn
```

FQDN を解決できない場合、またはこれらのマシンのいずれかに ping できない場合は、続行する前に手順を確認してください。

ステップ 1f: クロック同期の構成

VDA、Delivery Controller、およびドメインコントローラー間で正確なクロック同期を維持することは非常に重要です。Linux VDA を仮想マシン (VM) としてホストすると、クロックスキューの問題が発生する可能性があります。このため、リモート時刻サービスとの時刻同期が推奨されます。

RHEL のデフォルト環境では、クロック同期に Chrony デーモン (`chronyd`) を使用します。

CHRONY サービスの構成

root ユーザーとして、**/etc/chrony.conf** を編集し、各リモートタイムサーバーのサーバーエントリを追加します。

```
server peer1-fqdn-or-ip-address iburst



server peer2-fqdn-or-ip-address iburst
```

通常の展開では、パブリック NTP プールサーバーから直接ではなく、ローカルのドメインコントローラーから時刻を同期します。ドメイン内の各 Active Directory ドメインコントローラーのサーバーエントリを追加します。

ループバック IP アドレス、localhost、およびパブリックサーバーの ***.pool.ntp.org** エントリを含む、リストされている他のサーバーエントリをすべて削除します。

変更を保存し、Chrony デーモンを再起動します。

```
sudo /sbin/service chronyd restart
```

ステップ 1g: PulseAudio のインストール (RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 のみ)

pulseaudio をインストールするには、次のコマンドを実行します。

```
sudo yum -y install pulseaudio --allowerasing
```

`/etc/pulse/client.conf` を開き、次のエントリを追加します。

```
autospawn = yes
```

手順 1h: OpenJDK 11 をインストールする

Linux VDA には OpenJDK 11 が必要です。

- CentOS、RHEL、または Rocky Linux を使用している場合、Linux VDA のインストール時に OpenJDK 11 は依存関係として自動的にインストールされます。
- Amazon Linux 2 を使用している場合は、次のコマンドを実行して OpenJDK 11 を有効にしてインストールします。

  ```
  amazon-linux-extras install java-openjdk11
  ```

正しいバージョンを確認します。

```
sudo yum info java-11-openjdk
```

プリパッケージされた OpenJDK は以前のバージョンである可能性があります。OpenJDK 11 に更新します。

```
sudo yum -y update java-11-openjdk
```

手順 1i: 使用するデータベースをインストールして指定する

実験的な機能として、PostgreSQL に加えて SQLite を使用できます。Linux VDA パッケージのインストール後に `/etc/xdl/db.conf` を編集することで、SQLite と PostgreSQL を切り替えることもできます。手動インストールの場合、それらを切り替える前に SQLite と PostgreSQL を手動でインストールする必要があります。

このセクションでは、PostgreSQL および SQLite データベースのインストール方法と、使用するデータベースの指定方法について説明します。

> **注:**
>
> SQLite は VDI モードでのみ使用することをお勧めします。

POSTGRESQL をインストールする

Linux VDA には PostgreSQL が必要です。

- Amazon Linux 2、RHEL 7、および CentOS 7 用の PostgreSQL 9
- RHEL 8.x および Rocky Linux 8.x 用の PostgreSQL 10
- RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 用 PostgreSQL 13

PostgreSQL をインストールするには、次のコマンドを実行します。

```
sudo yum -y install postgresql-server



sudo yum -y install postgresql-jdbc
```

RHEL 8.x および RHEL 9.1/9.0 の場合、PostgreSQL 用の `libpq` をインストールするには、次のコマンドを実行します。

```
sudo yum -y install libpq
```

データベースを初期化するには、次のコマンドを実行します。この操作により、**/var/lib/pgsql/data** の下にデータベースファイルが作成されます。

```
sudo postgresql-setup initdb
```

マシンの起動時または即座に PostgreSQL を開始するには、次のコマンドをそれぞれ実行します。

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

次の方法で PostgreSQL のバージョンを確認します。

```
psql --version
```

(RHEL 7 のみ) **psql** コマンドラインユーティリティを使用して、データディレクトリが設定されていることを確認します。

```
sudo -u postgres psql -c 'show data_directory'
```

SQLITE をインストールする

SQLite をインストールするには、次のコマンドを実行します。

```
sudo yum -y install sqlite
```

使用するデータベースを指定する

SQLite、PostgreSQL、またはその両方をインストールした後、Linux VDA パッケージのインストール後に `/etc/xdl/db.conf` を編集して、使用するデータベースを指定できます。これを行うには、次の手順を完了します。

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh` を実行します。新規インストールである場合は、この手順を省略します。
2. 使用するデータベースを指定するために `/etc/xdl/db.conf` を編集します。
3. `ctxsetup.sh` を実行します。

> **注:**
>
> PostgreSQL のポート番号を構成するには、**/etc/xdl/db.conf** を使用することもできます。

手順 2：ハイパーバイザーを準備する

サポートされているハイパーバイザー上でLinux VDAをVMとして実行する場合、いくつかの変更が必要です。使用しているハイパーバイザープラットフォームに基づいて、以下の変更を行ってください。Linuxマシンをベアメタルハードウェアで実行している場合、変更は不要です。

Citrix Hypervisor™での時刻同期の修正

Citrix Hypervisorの時刻同期機能が有効になっている場合、準仮想化された各Linux VM内でNTPとCitrix Hypervisorの両方がシステムクロックを管理しようとするため、問題が発生します。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。HVMモードでは変更は不要です。

Citrix VM Toolsがインストールされた準仮想化Linuxカーネルを実行している場合、Linux VM内からCitrix Hypervisorの時刻同期機能が存在し、有効になっているかどうかを確認できます。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは0または1を返します。

- 0 - 時刻同期機能が有効になっており、無効にする必要があります。
- 1 - 時刻同期機能は無効になっており、それ以上の操作は不要です。

/proc/sys/xen/independent_wallclock ファイルが存在しない場合、以下の手順は不要です。

有効になっている場合、ファイルに1を書き込むことで時刻同期機能を無効にします。

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

この変更を永続的にし、再起動後も維持するには、**/etc/sysctl.conf** ファイルを編集して次の行を追加します。

`xen.independent_wallclock = 1`

これらの変更を確認するには、システムを再起動します。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは値1を返します。

Microsoft Hyper-Vでの時刻同期の修正

Hyper-V Linux Integration ServicesがインストールされているLinux VMは、Hyper-Vの時刻同期機能を使用してホストオペレーティングシステムの時刻を使用できます。システムクロックの精度を維持するためには、NTPサービスと並行してこの機能を有効にする必要があります。

管理オペレーティングシステムから:

1. Hyper-V マネージャーコンソールを開きます。
2. Linux VM の設定については、**統合サービス**を選択します。
3. **時刻同期**が選択されていることを確認します。

> **注:**
>
> このアプローチは、VMware および Citrix Hypervisor とは異なります。VMware および Citrix Hypervisor では、NTP との競合を避けるためにホストの時刻同期が無効になっています。Hyper-V の時刻同期は、NTP の時刻同期と共存し、補完することができます。

ESX および ESXi での時刻同期の修正

VMware の時刻同期機能が有効になっている場合、各準仮想化 Linux VM 内で、NTP とハイパーバイザーとの間で問題が発生します。どちらもシステムクロックを同期しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各 Linux ゲスト内のシステムクロックが NTP と同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。

VMware Tools がインストールされた準仮想化 Linux カーネルを実行している場合：

1. vSphere Client を開きます。
2. Linux VM の設定を編集します。
3. **仮想マシンのプロパティ**ダイアログで、**オプション**タブを開きます。
4. **VMware Tools**を選択します。
5. **詳細設定**ボックスで、**ゲストの時刻をホストと同期**のチェックを外します。

ステップ 3：Linux VM を Windows ドメインに追加する

Active Directory (AD) ドメインに Linux マシンを追加するには、次の方法が利用可能です。

- サンバ ウィンバインド
- クエスト認証サービス
- セントリファイ ダイレクトコントロール
- SSSD
- PBIS

選択した方法に基づいて指示に従ってください。

注:

Linux VDA のローカルアカウントと AD のアカウントで同じユーザー名を使用すると、セッションの起動に失敗する可能性があります。

サンバ・ワインバインド

必要なパッケージをインストールまたは更新します。

RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x の場合:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
oddjob-mkhomedir realmd authselect
```

Amazon Linux 2、CentOS 7、および RHEL 7 の場合:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
authconfig oddjob-mkhomedir
```

マシンの起動時に WINBIND デーモンを開始する

Winbind デーモンは、マシンの起動時に開始するように構成する必要があります。

```
sudo /sbin/chkconfig winbind on
```

WINBIND 認証の構成

Winbind を使用して、Kerberos 認証用にマシンを構成します。

1. 次のコマンドを実行します。

   RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x の場合:

   ```
   sudo authselect select winbind with-mkhomedir --force
   ```

   Amazon Linux 2、CentOS 7、および RHEL 7 の場合:

   ```
   sudo authconfig --disablecache --disablesssd --disablesssdauth --
   enablewinbind --enablewinbindauth --disablewinbindoffline --
   smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --
   ```

```
krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --
winbindtemplateshell=/bin/bash --enablemkhomedir --updateall
```

REALM は大文字の Kerberos レルム名、**domain** はドメインの NetBIOS 名です。

KDC サーバーとレルム名の DNS ベースのルックアップが必要な場合は、前のコマンドに次の 2 つのオプションを追加します。

`--enablekrb5kdcdns --enablekrb5realmdns`

`authconfig` コマンドから返される、`winbind` サービスの起動失敗に関するエラーは無視してください。これらのエラーは、マシンがまだドメインに参加していない状態で `authconfig` が `winbind` サービスの起動を試みたときに発生する可能性があります。

2. **/etc/samba/smb.conf** を開き、\[Global\] セクションの下、ただし `authconfig` ツールによって生成されたセクションの後に、次のエントリを追加します。

   `kerberos method = secrets and keytab`

   `winbind refresh tickets = true` `winbind offline logon = no`

3. (RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x のみ) **/etc/krb5.conf** を開き、`[libdefaults]`、`[realms]`、および `[domain_realm]` セクションの下にエントリを追加します。

   `[libdefaults]` セクションの下:

   `default_ccache_name = FILE:/tmp/krb5cc_%{uid}`

   `default_realm = REALM` `dns_lookup_kdc = true`

   `[realms]` セクションの下:

   `REALM = {`

   `kdc = fqdn-of-domain-controller` `}`

   `[domain_realm]` セクションの下:

   `realm = REALM`

   `.realm = REALM`

Linux VDA は、Delivery Controller で認証および登録するためにシステムキータブファイル /etc/krb5.keytab を必要とします。以前の Kerberos メソッド設定により、マシンが最初にドメインに参加したときに Winbind がシステムキータブファイルを作成するよう強制されます。

WINDOWS ドメインに参加する

ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つ Active Directory ユーザーアカウントが必要です。

RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x の場合:

```
sudo realm join -U user --client-software=winbind REALM
```

Amazon Linux 2 および RHEL 7 の場合:

```
sudo net ads join REALM -U user
```

REALM は大文字の Kerberos レルム名、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

WINBIND 用に PAM を構成する

デフォルトでは、Winbind PAM モジュール (pam_winbind) の構成では、Kerberos チケットのキャッシュとホームディレクトリの作成は有効になっていません。**/etc/security/pam_winbind.conf** を開き、\[Global\] セクションの下に次のエントリを追加または変更します。

`krb5_auth = yes`

`krb5_ccache_type = FILE` `mkhomedir = yes`

各設定の先頭にあるセミコロンが削除されていることを確認してください。これらの変更を適用するには、Winbind デーモンを再起動する必要があります。

```
sudo /sbin/service winbind restart
```

ヒント:

マシンがドメインに参加している場合にのみ、`winbind` デーモンは実行され続けます。

> **/etc/krb5.conf** を開き、\[libdefaults\] セクションの下にある次の設定を KEYRING から FILE タイプに変更します。

`default_ccache_name = FILE:/tmp/krb5cc_%{uid}`

RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の場合、`pam_winbind` がルートディレクトリの所有権を変更するのを防ぎ、Winbind の SELinux の問題を解決するには、次のコマンドを実行します。

```
usermod -d /nonexistent nobody



ausearch -c 'winbindd' --raw | audit2allow -M my-winbindd -p /etc/selinux/
targeted/policy/policy.*



semodule -X 300 -i my-winbindd.pp
```

ドメインメンバーシップを確認する

Delivery Controller は、すべての VDA マシン (Windows および Linux VDA) が **Active Directory** にコンピューターオブジェクトを持っていることを要求します。

マシンがドメインに参加していることを確認するには、**Samba** の **net ads** コマンドを実行します。

```
sudo net ads testjoin
```

追加のドメインおよびコンピューターオブジェクト情報を確認するには、次のコマンドを実行します。

```
sudo net ads info
```

KERBEROS の構成を確認する

Linux VDA で使用するために Kerberos が正しく構成されていることを確認するには、システムの keytab ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してドメインコントローラーでマシンを認証するには、Kerberos `kinit` コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェルによる置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos レルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントの TGT チケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

次のコマンドを使用して、マシンのアカウント詳細を調べてください。

```
sudo net ads status
```

ユーザー認証の確認

ドメインユーザーがドメインで認証できることを確認するには、**wbinfo** ツールを使用します。

```
wbinfo --krb5auth=domain\\username%password
```

ここで指定するドメインは、Kerberosレルム名ではなく、ADドメイン名です。bashシェルでは、バックスラッシュ (\\) 文字は別のバックスラッシュでエスケープする必要があります。このコマンドは、成功または失敗を示すメッセージを返します。

Winbind PAMモジュールが正しく構成されていることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username

id -u
```

Kerberos資格情報キャッシュ内のチケットが有効で期限切れになっていないことを確認します。

```
klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の検証後、手順6：Linux VDAのインストールに進みます。

クエスト認証サービス

ドメインコントローラーでのQUESTの構成

Active Directoryドメインコントローラーにクエストソフトウェアをインストールして構成済みであり、Active Directoryでコンピューターオブジェクトを作成するための管理者権限が付与されているものとします。

ドメインユーザーがLINUX VDAマシンにログオンできるようにする

ドメインユーザーがLinux VDAマシンでHDX™セッションを確立できるようにするには：

1. Active Directoryユーザーとコンピューター管理コンソールで、そのユーザーアカウントのActive Directoryユーザープロパティを開きます。
2. **Unixアカウント**タブを選択します。
3. **Unix対応**を確認します。
4. **プライマリGID番号**を、実際のドメインユーザーグループのグループIDに設定します。

> **注:**
>
> これらの手順は、コンソール、RDP、SSH、またはその他のリモートプロトコルを使用してドメインユーザーのログオンを設定する場合に同等です。

LINUX VDAでのQUESTの構成

SELinuxポリシーの適用を回避する
デフォルトのRHEL環境では、SELinuxが完全に適用されています。この適用により、Questが使用するUnixドメインソケットIPCメカニズムが妨害され、ドメインユーザーがログオンできなくなります。

この問題を回避する便利な方法は、SELinuxを無効にすることです。ルートユーザーとして、**/etc/selinux/config**を編集し、**SELinux**の設定を変更します。

`SELINUX=permissive`

この変更にはマシンの再起動が必要です。

```
reboot
```

重要:

この設定は慎重に使用してください。無効にした後にSELinuxポリシーの適用を再度有効にすると、ルートユーザーや他のローカルユーザーであっても、完全にロックアウトされる可能性があります。

VASデーモンの構成

Kerberosチケットの自動更新を有効にし、切断する必要があります。認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

このコマンドは、更新間隔を9時間（32,400秒）に設定します。これは、デフォルトの10時間のチケット有効期間より1時間短いです。チケット有効期間が短いシステムでは、このパラメーターをより低い値に設定してください。

PAMとNSSの構成

HDXおよびsu、ssh、RDPなどの他のサービスを介したドメインユーザーのログオンを有効にするには、PAMとNSSを手動で構成するために、次のコマンドを実行します。

```
sudo /opt/quest/bin/vastool configure pam
```

```
sudo /opt/quest/bin/vastool configure nss
```

WINDOWSドメインへの参加

Questの**vastool**コマンドを使用して、LinuxマシンをActive Directoryドメインに参加させます。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

ユーザーとは、コンピューターをActive Directoryドメインに参加させる権限を持つドメインユーザーのことです。**domain-name**は、たとえばexample.comのようなドメインのDNS名です。

ドメインメンバーシップの確認

Delivery Controllerは、すべてのVDAマシン（Windows VDAおよびLinux VDA）が`Active Directory`にコンピューターオブジェクトを持つことを要求します。Questで参加したLinuxマシンがドメイン上にあることを確認するには：

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合、このコマンドはドメイン名を返します。マシンがどのドメインにも参加していない場合、次のエラーが表示されます。

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

ユーザー認証の確認

QuestがPAMを介してドメインユーザーを認証できることを確認するには、これまで使用されていないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username

id -u
```

id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

Kerberos資格情報キャッシュ内のチケットが有効で期限切れになっていないことを確認します。

```
/opt/quest/bin/vastool klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の確認後、手順6：Linux VDAのインストールに進みます。

セントリファイ ダイレクトコントロール

WINDOWSドメインへの参加

Centrify DirectControl Agentがインストールされている場合、Centrify `adjoin`コマンドを使用してLinuxマシンをActive Directoryドメインに参加させます。

```
su -

adjoin -w -V -u user domain-name
```

ユーザーパラメーターは、コンピューターをActive Directoryドメインに参加させる権限を持つActive Directoryドメインユーザーです。**domain-name**は、Linuxマシンを参加させるドメインの名前です。

ドメインメンバーシップの確認

Delivery Controllerは、すべてのVDAマシン（WindowsおよびLinux VDA）がActive Directory内にコンピューターオブジェクトを持つことを要求します。Centrifyに参加しているLinuxマシンがドメイン上にあることを確認するには、次のようにします。

```
su -

adinfo
```

「Joined to domain」の値が有効であり、CentrifyDCモードが「connected」を返すことを確認します。モードが「starting」状態のままになっている場合、Centrifyクライアントはサーバー接続または認証の問題を抱えています。

より包括的なシステムおよび診断情報は、以下を使用して利用できます。

```
adinfo --sysinfo all

adinfo –diag
```

さまざまなActive DirectoryおよびKerberosサービスへの接続をテストします。

```
adinfo --test
```

ドメイン参加の確認後、手順6：Linux VDAのインストールに進みます。

SSSD

SSSDを使用している場合は、このセクションの指示に従ってください。このセクションには、Linux VDAマシンをWindowsドメインに参加させるための手順と、Kerberos認証を構成するためのガイダンスが含まれています。

RHELおよびCentOSでSSSDをセットアップするには、次の手順を実行します。

1. ドメインに参加し、ホストキータブを作成する
2. SSSDをセットアップする
3. SSSDを有効にする
4. Kerberos構成を確認する
5. ユーザー認証を確認する

ドメインに参加し、ホストキータブを作成する

SSSD は、ドメインへの参加やシステムキータブファイルの管理のための Active Directory クライアント機能を提供しません。代わりに **adcli**、**realmd**、または **Samba** を使用できます。

このセクションでは、Amazon Linux 2 および RHEL 7 の **Samba** アプローチと、RHEL 8 の `adcli` アプローチについて説明します。**realmd** については、RHEL または CentOS のドキュメントを参照してください。これらの手順は、SSSD を構成する前に実行する必要があります。

- **Samba (Amazon Linux 2 および RHEL 7):**

  必要なパッケージをインストールまたは更新します。

  ```
  sudo yum -y install krb5-workstation authconfig oddjob-mkhomedir samba-common-tools
  ```

  適切に構成されたファイルを持つ Linux クライアントで:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Samba および Kerberos 認証用にマシンを構成します。

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --
smbrealm=REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --
update
```

ここで、**REALM** は大文字の Kerberos レルム名であり、**domain** は Active Directory ドメインの短い NetBIOS 名です。

> **注:**
>
> この記事の設定は、単一ドメイン、単一フォレストモデルを対象としています。
> Kerberos は AD インフラストラクチャに基づいて構成してください。

> KDC サーバーとレルム名の DNS ベースのルックアップが必要な場合は、前のコマンドに次の2つのオプションを追加します。

`--enablekrb5kdcdns --enablekrb5realmdns`

/etc/samba/smb.conf を開き、**authconfig** ツールによって生成されたセクションの後に、**\[Global\]** セクションの下に次のエントリを追加します。

`kerberos method = secrets and keytab`

`winbind offline logon = no`

Windows ドメインに参加します。ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つ Active Directory ユーザーアカウントがあることを確認してください。

```
sudo net ads join REALM -U user
```

REALM は大文字の Kerberos レルム名であり、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

- **Adcli (RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x):**

必要なパッケージをインストールまたは更新します。

```
sudo yum -y install samba-common samba-common-tools krb5-workstation
authconfig oddjob-mkhomedir realmd oddjob authselect
```

Samba および Kerberos 認証用にマシンを構成します。

```
sudo authselect select sssd with-mkhomedir --force
```

/etc/krb5.conf を開き、 および セクションの下にエントリを追加します。

セクションの下:

`REALM = {`

`kdc = fqdn-of-domain-controller` `}`

セクションの下:

`realm = REALM` `.realm = REALM`

Windows ドメインに参加します。ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つ Active Directory ユーザーアカウントがあることを確認してください。

```
sudo realm join REALM -U user
```

REALM は大文字の Kerberos レルム名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

SSSD をセットアップする

SSSD のセットアップは、次の手順で構成されます。

- `sudo yum -y install sssd` コマンドを実行して、Linux VDA に **sssd-ad** パッケージをインストールします。
- さまざまなファイル（例: sssd.conf）に構成変更を加えます。
- **sssd** サービスを開始します。

RHEL 7 の **sssd.conf** 構成例（必要に応じて追加オプションを追加できます）:

```
[sssd]
config_file_version = 2
domains = ad.example.com
services = nss, pam

[domain/ad.example.com]
# Uncomment if you need offline logins
# cache_credentials = true

id_provider = ad
auth_provider = ad
access_provider = ad
ldap_id_mapping = true
ldap_schema = ad

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.example.com

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

ad.example.com、**server.ad.example.com** を対応する値に置き換えます。詳細については、sssd-ad(5) - Linux man page を参照してください。

(RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x のみ) **/etc/sssd/sssd.conf** を開き、 セクションの下に次のエントリを追加します。

`ad_gpo_access_control = permissive`

`full_name_format = %2$s\%1$s` `fallback_homedir = /home/%d/%u`

`# Kerberos settings` `krb5_ccachedir = /tmp`

`krb5_ccname_template = FILE:%d/krb5cc_%U`

sssd.conf のファイル所有権とアクセス許可を設定します。

`chown root:root /etc/sssd/sssd.conf`

`chmod 0600 /etc/sssd/sssd.conf` `restorecon /etc/sssd/sssd.conf`

SSSD を有効にする

RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x の場合:

SSSD を有効にするには、次のコマンドを実行します。

```
sudo systemctl restart sssd

sudo systemctl enable sssd.service

sudo chkconfig sssd on
```

Amazon Linux 2、CentOS 7、および RHEL 7 の場合:

authconfig を使用して SSSD を有効にします。ホームディレクトリの作成が SELinux と互換性があることを確認するために、**oddjob-mkhomedir** をインストールします。

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update



sudo service sssd start



sudo chkconfig sssd on
```

KERBEROS 構成を確認する

システム **keytab** ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してマシンをドメインコントローラーで認証するには、Kerberos **kinit** コマンドを実行します。

```
sudo kinit –k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 (**$**) は、シェルによる置換を防ぐためにバックスラッシュ (****) でエスケープする必要があります。一部の環境では、DNS ドメイン名が Kerberos レルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントの TGT チケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

ユーザー認証を確認する

getent コマンドを使用して、ログオン形式がサポートされており、NSS が機能していることを確認します。

```
sudo getent passwd DOMAIN\\username
```

「**DOMAIN**」パラメーターは、短いバージョンのドメイン名を示します。別のログオン形式が必要な場合は、まず「**getent**」コマンドを使用して確認してください。

サポートされているログオン形式は次のとおりです。

- ダウンレベルログオン名: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS サフィックス形式: `username@DOMAIN`

SSSD PAM モジュールが正しく構成されていることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用して Linux VDA にログオンします。

```
sudo ssh localhost –l DOMAIN\\username



id -u
```

コマンドによって返された **uid** に対応する Kerberos 資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_{uid}
```

ユーザーの Kerberos 資格情報キャッシュ内のチケットが有効であり、期限切れになっていないことを確認します。

```
klist
```

ドメイン参加の検証後、手順 6: Linux VDA のインストールに進みます。

PBIS

必要な PBIS パッケージをダウンロードする

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

PBIS インストールスクリプトを実行可能にする

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

PBIS インストールスクリプトを実行する

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

WINDOWS ドメインに参加する

ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つ Active Directory ユーザーアカウントが必要です。

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

「**ユーザー**」は、Active Directory ドメインにコンピューターを追加する権限を持つドメインユーザーです。「**ドメイン名**」は、たとえば example.com のように、ドメインのDNS名です。

注： Bashをデフォルトシェルとして設定するには、**/opt/pbis/bin/config LoginShellTemplate/bin/bash** コマンドを実行します。

ドメインメンバーシップを確認する

Delivery Controllerは、すべてのVDAマシン（Windows VDAおよびLinux VDA）がActive Directoryにコンピューターオブジェクトを持つことを必要とします。PBISに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
/opt/pbis/bin/domainjoin-cli query
```

マシンがドメインに参加している場合、このコマンドは現在参加しているADドメインとOUに関する情報を返します。そうでない場合、ホスト名のみが表示されます。

ユーザー認証を確認する

PBISがPAMを介してドメインユーザーを認証できることを確認するには、以前に使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\user



id -u
```

id -u コマンドによって返されるUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

セッションを終了します。

```
exit
```

ドメイン参加の確認後、手順6: Linux VDAをインストールするに進みます。

手順4: .NET Runtime 6.0をインストールする

Linux VDAをインストールする前に、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>`の指示に従って.NET Runtime 6.0をインストールします。

.NET Runtime 6.0をインストールした後、**which dotnet** コマンドを実行してランタイムパスを見つけます。

コマンドの出力に基づいて、.NETランタイムバイナリパスを設定します。たとえば、コマンドの出力が /aa/bb/dotnet の場合、/aa/bb を.NETバイナリパスとして使用します。

手順5: Linux VDAパッケージをダウンロードする

1. Citrix Virtual Apps and Desktops ダウンロードページにアクセスします。
2. Citrix Virtual Apps and Desktops の適切なバージョンを展開します。
3. **Components** をクリックして、お使いの Linux ディストリビューションに一致する Linux VDA パッケージと、Linux VDA パッケージの整合性を検証するために使用できる GPG 公開キーをダウンロードします。

Linux VDA パッケージの整合性を検証するには、公開キーを RPM データベースにインポートし、次のコマンドを実行します。

```
```

rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>

```
```

ステップ 6: Linux VDA をインストールする

新規インストールを実行することも、以前の 2 つのバージョンおよび LTSR リリースから既存のインストールをアップグレードすることもできます。

ステップ 6a: 新規インストールを実行する

1. (オプション) 古いバージョンをアンインストールする

   以前の 2 つのバージョンおよび LTSR リリース以外の以前のバージョンをインストールした場合は、新しいバージョンをインストールする前にアンインストールしてください。

   a. Linux VDA サービスを停止します。

   ```
   sudo /sbin/service ctxvda stop



   sudo /sbin/service ctxhdx stop
   ```

   注:

   `ctxvda` および `ctxhdx` サービスを停止する前に、**service ctxmonitorservice stop** コマンドを実行してモニターサービスデーモンを停止します。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

   b. パッケージをアンインストールします。

```
sudo rpm -e XenDesktopVDA
```

注:

コマンドを実行するには、完全なパスが必要です。または、**/opt/Citrix/VDA/sbin** と **/opt/Citrix/VDA/bin** をシステムパスに追加することもできます。

2. Linux VDA パッケージをダウンロードする

   Citrix Virtual Apps and Desktops ダウンロードページにアクセスします。Citrix Virtual Apps and Desktops の適切なバージョンを展開し、**Components** をクリックして、お使いの Linux ディストリビューションに一致する Linux VDA パッケージをダウンロードします。

3. Linux VDA をインストールする

注:

- CentOS、RHEL、および Rocky Linux の場合、Linux VDA を正常にインストールする前に EPEL リポジトリをインストールしてください。EPEL のインストール方法については、`<https://docs.fedoraproject.org/ja-jp/epel/>` の手順を参照してください。
- RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 に Linux VDA をインストールする前に、**libsepol** パッケージをバージョン 3.4 以降に更新してください。

- `Yum` を使用して Linux VDA ソフトウェアをインストールします。

  Amazon Linux 2 の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
  ```

  RHEL 8.x および Rocky Linux 8.x の場合:

```
sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

CentOS 7 および RHEL 7 の場合:

```
sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

- RPM パッケージマネージャーを使用して Linux VDA ソフトウェアをインストールします。これを行う前に、以下の依存関係を解決する必要があります。

Amazon Linux 2 の場合:

```
sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
```

RHEL 9.1/9.0 および Rocky Linux 9.1/9.0:

```
sudo rpm -i XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

RHEL 8.x および Rocky Linux 8.x の場合:

```
sudo rpm -i XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

CentOS 7 および RHEL 7 の場合:

```
sudo rpm -i XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の RPM 依存関係リスト:

```
java-11-openjdk >= 11


 icoutils >= 0.32


 firewalld >= 0.6.3
```

```
policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12
```

```
libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0
```

```
foomatic-filters >= 4.0.9


cups-filters >= 1.20.0


ghostscript >= 9.25


libxml2 >= 2.9


libmspack >= 0.7


krb5-workstation >= 1.13


ibus >= 1.5


nss-tools >= 3.44.0


gperftools-libs >= 2.4


cyrus-sasl-gssapi >= 2.1


python3 >= 3.6~
```

```
qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

RHEL 8.x および Rocky Linux 8.x の RPM 依存関係リスト:

```
java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8
```

```
dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1
```

```
util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9
```

```
libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4
```

```
imlib2 >= 1.4.9
```

CentOS 7 および RHEL 7 の RPM 依存関係リスト:

```
java-11-openjdk >= 11


ImageMagick >= 6.7.8.9


firewalld >= 0.3.9


policycoreutils-python >= 2.0.83


dbus >= 1.6.12


dbus-x11 >= 1.6.12


xorg-x11-server-utils >= 7.7


xorg-x11-xinit >= 1.3.2


xorg-x11-server-Xorg >= 1.20.4


libXpm >= 3.5.10
```

```
libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9
```

```
libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qt5-qtbase >= 5.5~

imlib2 >= 1.4.5
```

Amazon Linux 2 の RPM 依存関係リスト:

```
java-11-openjdk >= 11

ImageMagick >= 6.7.8.9
```

```
firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8
```

```
util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1
```

```
gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qrencode-libs >= 3.4.1

imlib2 >= 1.4.5
```

注:

このバージョンの Linux VDA がサポートする Linux ディストリビューションと Xorg バージョンのマトリックスについては、「システム要件」を参照してください。

RHEL 7.x に Linux VDA をインストールした後、`sudo yum install -y python-websockify x11vnc` コマンドを実行します。これは、セッションシャドウ機能を使用するために `python-websockify` と `x11vnc` を手動でインストールすることを目的としています。詳細については、「セッションのシャドウ」を参照してください。

手順 6b: 既存のインストールをアップグレードする (オプション)

既存のインストールは、以前の2つのバージョンおよびLTSRリリースからアップグレードできます。

注:

- 既存のインストールをアップグレードすると、/etc/xdl の下の構成ファイルが上書きされます。アップグレードを実行する前に、ファイルをバックアップしてください。
- RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 で Linux VDA をアップグレードする前に、**libsepol** パッケージをバージョン 3.4 以降に更新してください。

- `Yum` を使用してソフトウェアをアップグレードするには:

  Amazon Linux 2 の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  RHEL 9.1/9.0 および Rocky Linux 9.1/9.0 の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
  ```

  RHEL 8.x および Rocky Linux 8.x の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
  ```

  CentOS 7 および RHEL 7 の場合:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  ```

- RPM パッケージマネージャーを使用してソフトウェアをアップグレードするには:

  Amazon Linux 2 の場合:

  ```
  sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  RHEL 9.1/9.0およびロッキーリナックス 9.1/9.0の場合：

  ```
  sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
  ```

  RHEL 8.xおよびRocky Linux 8.xの場合：

  ```
  sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
  ```

CentOS 7およびRHEL 7の場合：

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

注:

RHEL 7を使用している場合は、前述のアップグレードコマンドを実行した後、以下の手順を完了してください。

1. 正しい.NETランタイムパスを設定するために`/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "DotNetRuntimePath" -d "/opt/rh/rh-dotnet31/root/usr/bin/" --force`を実行します。
2. `ctxvda`サービスを再起動します。

重要:

ソフトウェアのアップグレード後、Linux VDAマシンを再起動します。

手順7：NVIDIA GRIDドライバーをインストールする

HDX 3D Proを有効にするには、ハイパーバイザーとVDAマシンにNVIDIA GRIDドライバーをインストールする必要があります。

注:

Amazon Linux 2でHDX 3D Proを使用するには、NVIDIAドライバー470をインストールすることをお勧めします。詳しくは、「システム要件」を参照してください。

特定のハイパーバイザーにNVIDIA GRID Virtual GPU Manager（ホストドライバー）をインストールして構成するには、以下のガイドを参照してください。

- シトリックス ハイパーバイザー
- ヴイエムウェア ESX

- ニュータニックス AHV

NVIDIA GRIDゲストVMドライバーをインストールして構成するには、次の手順を実行します。

1. ゲストVMがシャットダウンされていることを確認します。
2. XenCenter®で、VMにGPUを割り当てます。
3. VMを起動します。
4. NVIDIA GRIDドライバー用にVMを準備します。

```
yum install gcc



yum install "kernel-devel-$(uname -r)"



systemctl set-default multi-user.target
```

5. Red Hat Enterprise Linuxドキュメントの手順に従って、NVIDIA GRIDドライバーをインストールします。

注:

GPUドライバーのインストール中に、各質問に対してデフォルト（「いいえ」）を選択します。

重要:

GPUパススルーが有効になると、Linux VMはXenCenter経由でアクセスできなくなります。SSHを使用して接続してください。

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

カードの正しい構成を設定します。

`etc/X11/ctx-nvidia.sh`

高解像度およびマルチモニター機能を利用するには、有効なNVIDIAライセンスが必要です。ライセンスを申請するには、「GRID Licensing Guide.pdf - DU-07757-001 September 2015」の製品ドキュメントに従ってください。

ステップ8：Linux VDAを構成する

> **注:**
>
> ランタイム環境をセットアップする前に、OSに **en_US.UTF-8** ロケールがインストールされていることを確認してください。ロケールがOSで利用できない場合は、**sudo locale-gen en_US.UTF-8** コマンドを実行してください。Debianの場合、**/etc/locale.gen** ファイルを編集して **# en_US.UTF-8 UTF-8** の行のコメントを解除し、**sudo locale-gen** コマンドを実行してください。

> パッケージのインストール後、ctxsetup.shスクリプトを実行してLinux VDAを構成する必要があります。変更を加える前に、スクリプトは環境を検証し、すべての依存関係がインストールされていることを確認します。必要に応じて、いつでもスクリプトを再実行して設定を変更できます。

スクリプトは、プロンプトに従って手動で実行することも、事前設定された応答で自動的に実行することもできます。続行する前に、スクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

プロンプトによる構成

プロンプトによる質問で手動構成を実行します。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

自動構成

自動インストールの場合、セットアップスクリプトで必要なオプションを環境変数で指定します。必要な変数がすべて存在する場合、スクリプトは情報を要求しません。

サポートされている環境変数には、次のものがあります。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Linux VDAは、DNS CNAMEレコードを使用してDelivery Controller名を指定することをサポートしています。デフォルトではNに設定されています。
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Linux VDAは、Delivery Controllerへの登録に使用するDelivery Controllerの完全修飾ドメイン名（FQDN）のスペース区切りリストを必要とします。少なくとも1つのFQDNまたはCNAMEエイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT=port-number** – Linux VDAは、TCP/IPポート（デフォルトはポート80）を介してDelivery Controllerと通信します。
- **CTX_XDL_REGISTER_SERVICE=Y \| N** - Linux VDAサービスは、マシンの起動後に開始されます。デフォルトではYに設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Linux VDAサービスでは、システムファイアウォールを介した受信ネットワーク接続が許可されている必要があります。Linux Virtual Desktopの場合、必要なポート（デフォルトではポート80と1494）をシステムファイアウォールで自動的に開くことができます。デフォルトではYに設定されています。
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Linux VDAは、Delivery Controllerで認証するためにKerberos構成設定を必要とします。Kerberos構成は、システムにインストールおよび構成されているActive Directory統合ツールから決定されます。
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Linux VDAは、グラフィックを多用するアプリケーションの仮想化を最適化するために設計されたGPUアクセラレーションテクノロジーのセットであるHDX 3D Proをサポートしています。HDX 3D Proが選択されている場合、VDAはVDIデスクトップ（シングルセッション）モード（つまり、CTX_XDL_VDI_MODE=Y）用に構成されます。

- **CTX_XDL_VDI_MODE=Y \| N** – マシンを専用デスクトップ配信モデル（VDI）として構成するか、ホスト型共有デスクトップ配信モデルとして構成するかを決定します。HDX 3D Pro環境では、この変数をYに設定します。この変数はデフォルトでNに設定されています。
- **CTX_XDL_SITE_NAME=dns-name** – Linux VDAはDNSを介してLDAPサーバーを検出します。DNS検索結果をローカルサイトに限定するには、DNSサイト名を指定します。この変数はデフォルトで**\<none\>**に設定されています。
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Linux VDAはDNSにクエリを実行してLDAPサーバーを検出します。DNSがLDAPサービスレコードを提供できない場合、LDAPポートを含むLDAP FQDNのスペース区切りリストを提供できます。たとえば、ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268。LDAPポート番号を389として指定すると、Linux VDAは指定されたドメイン内の各LDAPサーバーをポーリングモードでクエリします。ポリシーの数がx、LDAPサーバーの数がyの場合、Linux VDAは合計XかけるYのクエリを実行します。ポーリング時間がしきい値を超えると、セッションログオンが失敗する可能性があります。より高速なLDAPクエリを有効にするには、ドメインコントローラーで**Global Catalog**を有効にし、関連するLDAPポート番号を3268として指定します。この変数はデフォルトで**\<none\>**に設定されています。
- **CTX_XDL_SEARCH_BASE=search-base-set** – Linux VDAは、Active Directoryドメインのルート（例: DC=mycompany,DC=com）に設定された検索ベースを介してLDAPにクエリを実行します。検索パフォーマンスを向上させるには、検索ベース（例: OU=VDI,DC=mycompany,DC=com）を指定できます。この変数はデフォルトで**\<none\>**に設定されています。
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Federated Authentication Service (FAS) サーバーは、ADグループポリシーを介して構成されます。Linux VDAはADグループポリシーをサポートしていませんが、代わりにFASサーバーのセミコロン区切りリストを提供できます。シーケンスはADグループポリシーで構成されているものと同じである必要があります。サーバーアドレスが削除された場合は、その空白を**\<none\>**テキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。FASサーバーと適切に通信するには、FASサーバーで指定されたポート番号と一致するポート番号を追加してください。例: CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – 新しいブローカーエージェントサービス（`ctxvda`）をサポートするための.NET Runtime 6.0のインストールパス。デフォルトのパスは/usr/binです。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – セッションで使用するGNOME、GNOME Classic、またはMATEデスクトップ環境を指定します。変数を指定しない場合、VDAに現在インストールされているデスクトップが使用されます。ただし、現在イン

ストールされているデスクトップがMATEである場合は、変数の値を**mate**に設定する必要があります。

ターゲットセッションユーザーのデスクトップ環境は、次の手順で変更することもできます。

a. VDA上の**$HOME/<username\>**ディレクトリの下に`.xsession`または`.Xclients`ファイルを作成します。Amazon Linux 2を使用している場合は、`.Xclients`ファイルを作成します。その他のディストリビューションを使用している場合は、`.xsession`ファイルを作成します。

   2\. `.xsession`または`.Xclients`ファイルを編集して、デスクトップ環境を指定します。

   - **MATEデスクトップの場合**

     ```
     MSESSION="$(type -p mate-session)"



     if [ -n "$MSESSION" ]; then

       exec mate-session



     fi
     ```

   - **GNOME Classicデスクトップの場合**

     ```
     GSESSION="$(type -p gnome-session)"



     if [ -n "$GSESSION" ]; then

     export GNOME_SHELL_SESSION_MODE=classic



     exec gnome-session --session=gnome-classic
     ```

```
fi
```

- **GNOMEデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

exec gnome-session



fi
```

b. ターゲットセッションユーザーと700ファイル権限を共有します。

バージョン2209以降、セッションユーザーはデスクトップ環境をカスタマイズできます。この機能を有効にするには、VDAに切り替え可能なデスクトップ環境を事前にインストールする必要があります。詳しくは、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

- **CTX_XDL_START_SERVICE=Y \| N** – Linux VDAの構成が完了したときにLinux VDAサービスを開始するかどうかを決定します。デフォルト値はYです。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scoutのリッスン用ソケットポート。デフォルトポートは7503です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scoutとの通信用ポート。デフォルトポートは7502です。

環境変数を設定し、構成スクリプトを実行します。

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N



export CTX_XDL_DDC_LIST='list-ddc-fqdns'
```

```
export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
```

```
export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate |
'<none>'


export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number


export CTX_XDL_TELEMETRY_PORT=port-number


export CTX_XDL_START_SERVICE=Y|N


sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

sudoコマンドを実行するときは、**-E**オプションを入力して、既存の環境変数を新しく作成されるシェルに渡します。上記のコマンドから、最初の行に**#\!/bin/bash**を含むシェルスクリプトファイルを作成することをお勧めします。

または、単一のコマンドを使用してすべてのパラメーターを指定することもできます。

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \
```

```
CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \
```

```
CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

構成の変更を削除する

シナリオによっては、Linux VDAパッケージをアンインストールせずに、**ctxsetup.sh**スクリプトによって行われた構成の変更を削除する必要がある場合があります。

続行する前に、このスクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

構成の変更を削除するには：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

重要:

このスクリプトは、データベースからすべての構成データを削除し、Linux VDAを動作不能にします。

構成ログ

ctxsetup.shおよび**ctxcleanup.sh**スクリプトは、コンソールにエラーを表示し、追加情報は構成ログファイル **/tmp/xdl.configure.log**に書き込まれます。

変更を有効にするには、Linux VDAサービスを再起動してください。

ステップ9：XDPingを実行する

Linux VDA環境における一般的な構成の問題を確認するには、`sudo /opt/Citrix/VDA/bin/xdping`を実行します。詳細については、「XDPing」を参照してください。

ステップ10：Linux VDAを実行する

ctxsetup.shスクリプトを使用してLinux VDAを構成した後、次のコマンドを実行してLinux VDAを制御できます。

Linux VDAを開始する：

Linux VDAサービスを開始するには：

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDAを停止する：

Linux VDAサービスを停止するには：

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **注:**
>
> `ctxvda`および`ctxhdx`サービスを停止する前に、`service ctxmonitorservice stop`コマンドを実行してモニターサービスデーモンを停止してください。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

> **Linux VDAを再起動する：**

Linux VDAサービスを再起動するには：

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

Linux VDAのステータスを確認する：

Linux VDAサービスの実行ステータスを確認するには：

```
sudo /sbin/service ctxvda status


sudo /sbin/service ctxhdx status
```

ステップ11：マシンカタログを作成する

マシンカタログを作成し、Linux VDAマシンを追加するプロセスは、従来のWindows VDAのアプローチと似ています。これらのタスクを完了する方法の詳細については、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

Linux VDAマシンを含むマシンカタログを作成する場合、Windows VDAマシン用のマシンカタログを作成するプロセスとは異なるいくつかの制限があります。

- オペレーティングシステムには、以下を選択します。
  - ホストされた共有デスクトップ配信モデルの場合は、**Multi-session OS**オプション。
  - VDI専用デスクトップ配信モデルの場合は、**Single-session OS**オプション。
- 同じマシンカタログ内でLinux VDAマシンとWindows VDAマシンを混在させないでください。

注:

Citrix Studioの初期バージョンでは、「Linux OS」という概念はサポートされていませんでした。ただし、**Windows Server OS**または**Server OS**オプションを選択すると、同等のホストされた共有デスクトップ配信モデルが意味されます。**Windows Desktop OS**または**Desktop OS**オプションを選択すると、マシンごとに1人のユーザーという配信モデルが意味されます。

ヒント:

削除したマシンをActive Directoryドメインに再参加させる場合は、そのマシンをマシンカタログから削除し、再度追加してください。

ステップ12：デリバリーグループを作成する

デリバリーグループを作成し、Linux VDAマシンを含むマシンカタログを追加するプロセスは、Windows VDAマシンとほぼ同じです。これらのタスクを完了する方法の詳細については、「デリバリーグループの作成」を参照してください。

Linux VDAマシンカタログを含むデリバリーグループを作成する場合、以下の制限が適用されます。

- 選択したADユーザーとグループが、Linux VDAマシンにログオンできるように適切に構成されていることを確認してください。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- デリバリーグループをWindowsマシンを含むマシンカタログと混在させないでください。

重要:

アプリケーションの公開は、Linux VDAバージョン1.4以降でサポートされています。ただし、Linux VDAは、デスクトップとアプリを同じマシンに配信することをサポートしていません。

マシンカタログとデリバリーグループの作成方法については、「Citrix Virtual Apps and Desktops 7 2303」を参照してください。

SUSE に Linux VDA を手動でインストールする

重要:

新規インストールの場合、迅速なインストールには簡易インストールを使用することをお勧めします。簡易インストールは、時間と労力を節約し、この記事で詳述されている手動インストールよりもエラーが発生しにくいです。

ステップ 1: 構成情報と Linux マシンを準備する

ステップ 1a: YaST ツールを起動する

SUSE Linux Enterprise YaST ツールは、オペレーティングシステムのあらゆる側面を構成するために使用されます。

テキストベースの YaST ツールを起動するには:

```
su -



yast
```

UI ベースの YaST ツールを起動するには:

```
su -



yast2 &
```

ステップ 1b: ネットワークを構成する

以下のセクションでは、Linux VDA で使用されるさまざまなネットワーク設定とサービスの構成に関する情報を提供します。ネットワークの構成は、Network Manager などの他の方法ではなく、YaST ツールを介して実行されます。これらの手順は、UI ベースの YaST ツールを使用することを前提としています。テキストベースの YaST ツールも使用できますが、ここでは文書化されていない異なるナビゲーション方法があります。

ホスト名とドメインネームシステム (DNS) を構成する

1. UI ベースの YaST ツールを起動します。
2. **System** を選択し、次に **Network Settings** を選択します。
3. **Hostname/DNS** タブを開きます。
4. **Set Hostname via DHCP** で **no** オプションを選択します。
5. **Modify DNS Configuration** で **Use Custom Policy** オプションを選択します。
6. ネットワーク設定を反映するように以下を編集します。

    - **静的ホスト名** – マシンのDNSホスト名を追加します。

- **ネームサーバー** – DNSサーバーのIPアドレスを追加します。通常、これはADドメインコントローラーのIPアドレスです。
- **ドメイン検索リスト** – DNSドメイン名を追加します。

7. `/etc/hosts` ファイルの次の行を変更して、FQDNとホスト名を最初の2つのエントリとして含めます。

   `127.0.0.1 <FQDN of the VDA> <hostname of the VDA> localhost`

> **注:**
>
> Linux VDAは現在、NetBIOS名の切り捨てをサポートしていません。したがって、ホスト名は15文字を超えてはなりません。 **ヒント:**
>
> a～z、A～Z、0～9、およびハイフン (-) の文字のみを使用してください。アンダースコア (_)、スペース、その他の記号は避けてください。ホスト名を数字で始めたり、ハイフンで終わらせたりしないでください。この規則は、Delivery Controllerのホスト名にも適用されます。

ホスト名の確認

ホスト名が正しく設定されていることを確認します。

```
hostname
```

このコマンドは、マシンのホスト名のみを返し、完全修飾ドメイン名 (FQDN) は返しません。

FQDNが正しく設定されていることを確認します。

```
hostname -f
```

このコマンドは、マシンのFQDNを返します。

名前解決とサービスの到達可能性の確認

FQDNを解決し、ドメインコントローラーとDelivery Controller™にpingできることを確認します。

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

FQDNを解決できない場合、またはこれらのマシンのいずれかにpingできない場合は、続行する前に手順を確認してください。

ステップ 1c: NTPサービスを構成する

VDA、Delivery Controller、およびドメインコントローラー間で正確なクロック同期を維持することが重要です。Linux VDAを仮想マシン（VM）としてホストすると、クロックスキューの問題が発生する可能性があります。このため、リモートNTPサービスを使用して時刻を維持することが推奨されます。デフォルトのNTP設定にいくつかの変更が必要になる場合があります。

SUSE 15.4の場合:

1. UIベースのYaSTツールを起動します。
2. **ネットワークサービス**を選択し、次に**NTP構成**を選択します。
3. **NTPデーモンの開始**セクションで、**今すぐ起動してブート時にも起動**を選択します。
4. **構成ソース**に**動的**を選択します。
5. 必要に応じてNTPサーバーを追加します。NTPサービスは通常、Active Directoryドメインコントローラーでホストされます。
6. /etc/chrony.confに以下の行が存在する場合は、削除またはコメントアウトします。

   `include /etc/chrony.d/*.conf`

   chrony.confを編集した後、`chronyd`サービスを再起動します。

   ```
   sudo systemctl restart chronyd.service
   ```

ステップ 1d: Linux VDAの依存パッケージをインストールする

SUSE Linux Enterprise用Linux VDAソフトウェアは、以下のパッケージに依存しています。

- OpenJDK 11
- オープンモティーフ実行環境 2.3.1 以降
- Cups 1.6.0以降
- ImageMagick 6.8以降

リポジトリの追加

ImageMagickを除くほとんどの必須パッケージは、公式リポジトリから入手できます。ImageMagickパッケージを入手するには、YaSTまたは次のコマンドを使用して、`sle-module-desktop-applications`リポジトリを有効にします。

`SUSEConnect -p sle-module-desktop-applications/<version number>/x86_64`

KERBEROSクライアントのインストール

Linux VDAとDelivery Controller間の相互認証のために、Kerberosクライアントをインストールします。

```
sudo zypper install krb5-client
```

Kerberosクライアントの構成は、使用されるActive Directory統合アプローチによって異なります。以下の説明を参照してください。

OPENJDK 11のインストール

Linux VDAにはOpenJDK 11が必要です。

OpenJDK 11をインストールするには、次のコマンドを実行します。

```
sudo zypper install java-11-openjdk
```

使用するデータベースをインストールして指定する

実験的な機能として、PostgreSQLに加えてSQLiteを使用できます。Linux VDAパッケージのインストール後、`/etc/xdl/db.conf`を編集することでSQLiteとPostgreSQLを切り替えることもできます。手動インストールの場合、それらを切り替える前にSQLiteとPostgreSQLを手動でインストールする必要があります。

このセクションでは、PostgreSQLおよびSQLiteデータベースをインストールする方法と、使用するデータベースを指定する方法について説明します。

> **注:**
>
> VDIモードでのみSQLiteを使用することをお勧めします。

PostgreSQLのインストール
`Postgresql`をインストールするには、次のコマンドを実行します。

```
sudo zypper install postgresql-server



sudo zypper install postgresql-jdbc
```

PostgreSQLをマシンの起動時または即座に開始するには、次のコマンドを実行します。

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

SQLiteをインストールする
SUSEの場合、SQLiteをインストールするには次のコマンドを実行します。

```
sudo zypper install sqlite3
```

使用するデータベースを指定する
SQLite、PostgreSQL、またはその両方をインストールした後、Linux VDAパッケージのインストール後に`/etc/xdl/db.conf`を編集して、使用するデータベースを指定できます。これを行うには、次の手順を完了します。

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh`を実行します。新規インストールの場合、この手順は省略してください。
2. 使用するデータベースを指定するには、`/etc/xdl/db.conf`を編集します。
3. `ctxsetup.sh`を実行します。

注:

PostgreSQLのポート番号を構成するには、`/etc/xdl/db.conf`を使用することもできます。

ステップ2：ハイパーバイザーを準備する

サポートされているハイパーバイザー上でLinux VDAをVMとして実行する場合、いくつかの変更が必要です。使用しているハイパーバイザープラットフォームに基づいて、次の変更を行います。Linuxマシンをベアメタルハードウェアで実行している場合、変更は不要です。

Citrix Hypervisor™での時刻同期を修正する

Citrix Hypervisorの時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとCitrix Hypervisorに関する問題が発生します。どちらもシステムクロックを管理しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックをNTPと同期させます。この場合、ホストの時刻同期を無効にする必要があります。HVMモードでは変更は不要です。

Citrix VM Toolsがインストールされた準仮想化Linuxカーネルを実行している場合、Linux VM内からCitrix Hypervisorの時刻同期機能が存在し、有効になっているかどうかを確認できます。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは0または1を返します。

- 0 - 時刻同期機能が有効になっており、無効にする必要があります。
- 1 - 時刻同期機能は無効になっており、それ以上の操作は必要ありません。

/proc/sys/xen/independent_wallclock ファイルが存在しない場合、以下の手順は必要ありません。

有効になっている場合は、ファイルに **1** を書き込むことで時刻同期機能を無効にします。

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

この変更を永続化し、再起動後も維持するには、**/etc/sysctl.conf** ファイルを編集して次の行を追加します。

```
xen.independent_wallclock = 1
```

これらの変更を確認するには、システムを再起動します。

```
reboot
```

再起動後、設定が正しいことを確認します。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは値 1 を返します。

Microsoft Hyper-V での時刻同期の修正

Hyper-V Linux Integration Services がインストールされている Linux VM は、Hyper-V の時刻同期機能を使用してホストオペレーティングシステムの時刻を使用できます。システムクロックの精度を維持するために、NTP サービスと並行してこの機能を有効にしてください。

管理オペレーティングシステムから：

1. Hyper-V マネージャーコンソールを開きます。
2. Linux VM の設定で、**Integration Services** を選択します。
3. **Time synchronization** が選択されていることを確認します。

> **注:**
>
> このアプローチは、NTP との競合を避けるためにホストの時刻同期が無効になっている VMware や Citrix Hypervisor とは異なります。Hyper-V の時刻同期は、NTP の時刻同期と共存し、補完することができます。

ESX および ESXi での時刻同期の修正

VMware Time Synchronization機能が有効になっている場合、各準仮想化Linux VM内でNTPとハイパーバイザーに関する問題が発生します。両方ともシステムクロックを同期しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックをNTPと同期させてください。この場合、ホストの時刻同期を無効にする必要があります。

VMware Toolsがインストールされた準仮想化Linuxカーネルを実行している場合：

1. vSphere Clientを開きます。
2. Linux VMの設定を編集します。
3. **Virtual Machine Properties**ダイアログで、**Options**タブを開きます。
4. **VMware Tools**を選択します。
5. **Advanced**ボックスで、**Synchronize guest time with host**のチェックを外します。

ステップ3：Linux VMをWindowsドメインに追加する

LinuxマシンをActive Directory (AD) ドメインに追加するには、以下の方法があります：

- サンバ Winbind
- セントリファイ ダイレクトコントロール
- SSSD
- PBIS

選択した方法に基づいて指示に従ってください。

> **注:**
>
> Linux VDAのローカルアカウントとADのアカウントで同じユーザー名を使用すると、セッションの起動に失敗する可能性があります。

サンバ Winbind

WINDOWSドメインへの参加

ドメインコントローラーに到達可能である必要があり、マシンをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

1. YaSTを起動し、［**Network Services**］、次に**［Windows Domain Membership］**を選択します。

2. 次の変更を行います。
    - **［Domain or Workgroup］**をActive Directoryドメインの名前またはドメインコントローラーのIPアドレスに設定します。ドメイン名が大文字であることを確認してください。
    - **［Use SMB information for Linux Authentication］**をオンにします。
        - **［Create Home Directory on Login］**をオンにします。
        - **［Single Sign-on for SSH］**をオンにします。
        - **［Offline Authentication］**がオフになっていることを確認します。このオプションはLinux VDAと互換性がありません。
3. **［OK］をクリックします。一部のパッケージのインストールを求められた場合は、**［Install］**をクリックします。
4. ドメインコントローラーが見つかると、ドメインに参加するかどうかを尋ねられます。**［Yes］**をクリックします。
5. プロンプトが表示されたら、マシンをドメインに追加する権限を持つドメインユーザーの資格情報を入力し、**［OK］**をクリックします。
6. サービスを手動で再起動するか、マシンを再起動します。マシンの再起動をお勧めします。

```
su -

reboot
```

ドメインメンバーシップの確認

Delivery Controller は、すべての VDA マシン (Windows および Linux VDA) が Active Directory にコンピューターオブジェクトを持つことを要求します。

マシンがドメインに参加していることを確認するには、**Samba** の **net ads** コマンドを実行します。

```
sudo net ads testjoin
```

追加のドメインおよびコンピューターオブジェクト情報を確認するには、次のコマンドを実行します。

```
sudo net ads info
```

KERBEROS 構成を確認する

システムの keytab ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist –ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してドメインコントローラーでマシンを認証するには、Kerberos `kinit` コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェル置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNS ドメイン名が Kerberos レルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントの TGT チケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

マシンアカウントの詳細を確認するには、次を使用します。

```
sudo net ads status
```

ユーザー認証を確認する

ドメインユーザーがドメインで認証できることを確認するには、**wbinfo** ツールを使用します。

```
wbinfo --krb5auth=domain\\username%password
```

ここで指定するドメインは AD ドメイン名であり、Kerberos レルム名ではありません。bash シェルの場合、バックスラッシュ (\\) 文字は別のバックスラッシュでエスケープする必要があります。このコマンドは、成功または失敗を示すメッセージを返します。

Winbind PAM モジュールが正しく構成されていることを確認します。これを行うには、以前に使用したことのないドメインユーザーアカウントを使用して Linux VDA にログオンします。

```
ssh localhost -l domain\\username

id -u
```

id -u コマンドによって返された uid に対応する Kerberos 資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

ユーザーの Kerberos 資格情報キャッシュ内のチケットが有効で、期限切れになっていないことを確認します。

```
klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/2303/installation-overview/manual-installation-overview/suse.html#step-6-install-the-linux-vda)に進みます。

Quest認証サービス

ドメインコントローラーでQUESTを構成する

ドメインコントローラーにQuestソフトウェアをインストールして構成済みであり、`Active Directory`でコンピューターオブジェクトを作成するための管理者権限が付与されていると仮定します。

ドメインユーザーがLINUX VDAマシンにログオンできるようにする

ドメインユーザーがLinux VDAマシンでHDX™セッションを確立できるようにするには：

1. Active Directoryユーザーとコンピューター管理コンソールで、そのユーザーアカウントのActive Directoryユーザープロパティを開きます。
2. **Unixアカウント**タブを選択します。
3. **Unix対応**をオンにします。
4. **プライマリGID番号**を実際のドメインユーザーグループのグループIDに設定します。

> **注:**
>
> これらの手順は、コンソール、RDP、SSH、またはその他のリモートプロトコルを使用してログオンするドメインユーザーを設定する場合にも同様に適用されます。

LINUX VDAでQUESTを構成する

VASデーモンを構成する
Kerberosチケットの自動更新は有効にして切断する必要があります。認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

このコマンドは、更新間隔を9時間（32,400秒）に設定します。これは、デフォルトの10時間のチケット有効期間より1時間短いです。チケット有効期間が短いシステムでは、このパラメーターをより低い値に設定してください。
PAMとNSSを構成する
HDXおよびsu、ssh、RDPなどの他のサービスを介したドメインユーザーログオンを有効にするには、PAMとNSSを手動で構成します。

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

WINDOWSドメインに参加する

Quest `vastool` コマンドを使用して、LinuxマシンをActive Directoryドメインに参加させます。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

userは、マシンをActive Directoryドメインに参加させる権限を持つ任意のドメインユーザーです。**domain-name**は、ドメインのDNS名です（例：example.com）。

ドメインメンバーシップを確認する

Delivery Controllerは、すべてのVDAマシン（WindowsおよびLinux VDA）が`Active Directory`にコンピューターオブジェクトを持つことを要求します。Questに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合、このコマンドはドメイン名を返します。マシンがどのドメインにも参加していない場合、次のエラーが表示されます。

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

ユーザー認証を確認する

QuestがPAMを介してドメインユーザーを認証できることを確認します。これを行うには、以前使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username

id -u
```

id -uコマンドによって返されたuidに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

Kerberos資格情報キャッシュ内のチケットが有効で期限切れになっていないことを確認します。

```
/opt/quest/bin/vastool klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の確認後、手順6：Linux VDAをインストールするに進みます。

セントリファイ ダイレクトコントロール

WINDOWS ドメインに参加する

Centrify DirectControl Agent がインストールされている場合、Centrify の **adjoin** コマンドを使用して Linux マシンを Active Directory ドメインに参加させます。

```
sudo adjoin -w -V -u user domain-name
```

user は、マシンを Active Directory ドメインに参加させる権限を持つ Active Directory ドメインユーザーです。**domain-name** は、Linux マシンを参加させるドメインの名前です。

ドメインメンバーシップを確認する

Delivery Controller は、すべての VDA マシン (Windows および Linux VDA) が Active Directory にコンピューターオブジェクトを持つことを要求します。Centrify に参加している Linux マシンがドメイン上にあることを確認するには:

```
sudo adinfo
```

Joined to domain の値が有効であり、**CentrifyDC** の **mode** が **connected** を返すことを確認します。モードが開始状態のままになっている場合、Centrify クライアントはサーバー接続または認証の問題を抱えています。

より包括的なシステムおよび診断情報は、以下を使用して利用できます。

```
adinfo --sysinfo all



adinfo –diag
```

さまざまな Active Directory および Kerberos サービスへの接続をテストします。

```
adinfo --test
```

ドメイン参加の検証後、手順 6: Linux VDA をインストールする に進みます。

SSSD

SUSE で SSSD を使用している場合は、このセクションの指示に従ってください。このセクションには、Linux VDA マシンを Windows ドメインに参加させるための手順と、Kerberos 認証を構成するためのガイダンスが含まれています。

SUSE で SSSD をセットアップするには、次の手順を実行します。

1. ドメインに参加し、ホストキータブを作成する
2. SSSD 用に PAM を構成する
3. SSSDをセットアップする
4. SSSDを有効にする
5. ドメインメンバーシップを確認する
6. Kerberos構成を確認する
7. ユーザー認証を確認する

ドメインに参加し、ホストキータブを作成する

SSSDは、ドメインへの参加やシステムキータブファイルの管理のためのActive Directoryクライアント機能を提供しません。代わりに**Samba**アプローチを使用できます。SSSDを構成する前に、以下の手順を完了してください。

1. ネームサービスキャッシュデーモン（NSCD）デーモンを停止して無効にします。

```
sudo systemctl stop nscd

sudo systemctl disable nscd
```

2. ホスト名とChrony時刻同期を確認します。

```
hostname

hostname -f

chronyc traking
```

3. 必要なパッケージをインストールまたは更新します。

```
sudo zypper install samba-client sssd-ad
```

4. ルートユーザーとして`/etc/krb5.conf`ファイルを編集し、**kinit**ユーティリティがターゲットドメインと通信できるようにします。、、および****セクションの下に次のエントリを追加します。

> **注:**
>
> ADインフラストラクチャに基づいてKerberosを構成します。以下の設定は、単一ドメイン、単一フォレストモデルを対象としています。

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {

        kdc = fqdn-of-domain-controller
```

```
        default_domain = realm



        admin_server = fqdn-of-domain-controller
    }
[domain_realm]



    .realm = REALM
```

realmは、example.comのようなKerberosレルム名です。**REALM**は、EXAMPLE.COMのような大文字のKerberosレルム名です。

5. ルートユーザーとして`/etc/samba/smb.conf`を編集し、**net**ユーティリティがターゲットドメインと通信できるようにします。****セクションの下に次のエントリを追加します。

```
[global]
    workgroup = domain



    client signing = yes



    client use spnego = yes



    kerberos method = secrets and keytab



    realm = REALM
```

```
    security = ADS
```

domainは、EXAMPLEのようなActive Directoryドメインの短いNetBIOS名です。

6. ユーザーとグループを解決する際にSSSDを参照するように、`/etc/nsswitch.conf` ファイル内の **passwd** および **group** エントリを変更します。

```
passwd: compat sss



group: compat sss
```

7. 構成済みのKerberosクライアントを使用して、ターゲットドメインに管理者として認証します。

```
kinit administrator
```

8. **net** ユーティリティを使用して、システムをドメインに参加させ、システムキーファイルを作成します。

```
net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
administrator
```

SSSD 用にPAMを構成する

SSSD 用にPAMを構成する前に、必要なパッケージをインストールまたは更新します。

```
sudo zypper install sssd sssd-ad
```

SSSDを介したユーザー認証のためにPAMモジュールを構成し、ユーザーログオン用のホームディレクトリを作成します。

```
sudo pam-config --add  --sss

sudo pam-config --add --mkhomedir
```

SSSDをセットアップする

1. rootユーザーとして`/etc/sssd/sssd.conf`を編集し、SSSDデーモンがターゲットドメインと通信できるようにします。`sssd.conf`の構成例（必要に応じて追加オプションを追加できます）：

```
[sssd]

    config_file_version = 2

    services = nss,pam

    domains = domain-dns-name



[domain/domain-dns-name]

    id_provider = ad

    auth_provider = ad

    access_provider = ad

    ad_domain = domain-dns-name

    ad_server = fqdn-of-domain-controller

    ldap_id_mapping = true

    ldap_schema = ad



# Kerberos settings

    krb5_ccachedir = /tmp

    krb5_ccname_template = FILE:%d/krb5cc_%U



# Comment out if the users have the shell and home dir set on the AD
```

```
side



    fallback_homedir = /home/%d/%u

    default_shell = /bin/bash



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available



# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM



    ad_gpo_access_control = permissive
```

domain-dns-name はDNSドメイン名です（例：example.com）。

> **注:**
>
> **ldap_id_mapping** はtrueに設定されており、SSSD自体がWindows SIDをUnix UIDにマッピングします。そうでない場合、Active DirectoryはPOSIX拡張機能を提供できる必要があります。**ad_gpo_access_control** は、Linuxセッションでの無効なログオンエラーを防ぐために **permissive** に設定されています。`sssd.conf` および `sssd-ad` のmanページを参照してください。

2. `sssd.conf` のファイルの所有権と権限を設定します。

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

SSSDを有効にする

次のコマンドを実行して、システム起動時にSSSDデーモンを有効にして開始します。

```
sudo systemctl enable sssd

sudo systemctl start sssd
```

ドメインメンバーシップを確認する

1. **Samba** の `net ads` コマンドを実行して、マシンがドメインに参加していることを確認します。

   ```
   sudo net ads testjoin
   ```

2. 追加のドメインおよびコンピューターオブジェクト情報を検証するには、次のコマンドを実行します。

   ```
   sudo net ads info
   ```

KERBEROS構成を検証する

システムkeytabファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。

これらのキーを使用してマシンをドメインコントローラーで認証するには、Kerberos**kinit**コマンドを実行します。

```
sudo kinit –k MACHINE\$@REALM
```

マシン名とレルム名はすべて大文字で指定する必要があります。ドル記号（**$**）は、シェル置換を防ぐためにバックスラッシュ（****）でエスケープする必要があります。一部の環境では、DNSドメイン名がKerberosレルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントのTGTチケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

ユーザー認証を検証する

SSSDは、デーモンと直接認証をテストするためのコマンドラインツールを提供しておらず、PAMを介してのみ実行できます。

SSSD PAMモジュールが正しく構成されていることを確認するには、以前に使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u



klist



exit
```

`klist`コマンドによって返されたKerberosチケットがそのユーザーに対して正しく、期限切れになっていないことを確認します。

rootユーザーとして、以前の`id -u`コマンドによって返されたuidに対応するチケットキャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の検証後、手順6：Linux VDAをインストールするに進みます。

PBIS

必要なPBISパッケージをダウンロードする

例:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

PBISインストールスクリプトを実行可能にする

例:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

PBISインストールスクリプトを実行する

例:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

WINDOWSドメインに参加する

ドメインコントローラーに到達可能である必要があり、マシンをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

userは、Active Directoryドメインにマシンを追加する権限を持つドメインユーザーです。**domain-name**は、ドメインのDNS名です（例: example.com）。

注： Bashをデフォルトシェルとして設定するには、**/opt/pbis/bin/config LoginShellTemplate/bin/bash**コマンドを実行します。

ドメインメンバーシップを確認する

Delivery Controllerは、すべてのVDAマシン（WindowsおよびLinux VDA）が`Active Directory`にコンピューターオブジェクトを持つことを要求します。PBISに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
/opt/pbis/bin/domainjoin-cli query
```

マシンがドメインに参加している場合、このコマンドは現在参加しているADドメインとOUに関する情報を返します。そうでない場合は、ホスト名のみが表示されます。

ユーザー認証を確認する

PBISがPAMを介してドメインユーザーを認証できることを確認します。これを行うには、以前使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\user



id -u
```

id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

セッションを終了します。

```
exit
```

ドメイン参加の検証後、手順6：Linux VDAをインストールするに進みます。

手順4：.NET Runtime 6.0をインストールする

Linux VDA をインストールする前に、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>` の指示に従って .NET Runtime 6.0 をインストールします。

.NET Runtime 6.0 をインストールした後、**which dotnet** コマンドを実行してランタイムパスを見つけます。

コマンドの出力に基づいて、.NET ランタイムバイナリパスを設定します。たとえば、コマンドの出力が /aa/bb/dotnet の場合、/aa/bb を .NET バイナリパスとして使用します。

ステップ 5: Linux VDA パッケージをダウンロードする

1. Citrix Virtual Apps and Desktops ダウンロードページ にアクセスします。
2. 適切なバージョンの Citrix Virtual Apps and Desktops を展開します。
3. **Components** をクリックして、お使いの Linux ディストリビューションに一致する Linux VDA パッケージと、Linux VDA パッケージの整合性を検証するために使用できる GPG 公開キーをダウンロードします。

   公開キーを使用して Linux VDA パッケージの整合性を検証するには、公開キーを RPM データベースにインポートし、次のコマンドを実行します。

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

ステップ 6: Linux VDA をインストールする

ステップ 6a: 古いバージョンをアンインストールする

以前の2つのバージョンとLTSRリリース以外の古いバージョンをインストールしている場合は、新しいバージョンをインストールする前にアンインストールしてください。

1. Linux VDA サービスを停止します。

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **注:**
>
> `ctxvda` および `ctxhdx` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止します。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

2. パッケージをアンインストールします。

```
sudo rpm -e XenDesktopVDA
```

> **重要:**
>
> 最新の2つのバージョンからのアップグレードがサポートされています。

> **注:**
>
> インストールされたコンポーネントは **/opt/Citrix/VDA/** にあります。

> コマンドを実行するには、フルパスが必要です。または、**/opt/Citrix/VDA/sbin** と **/opt/Citrix/VDA/bin** をシステムパスに追加することもできます。

ステップ 6b: Linux VDA をインストールする

Zypper を使用して Linux VDA ソフトウェアをインストールします。

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

RPM パッケージマネージャーを使用して Linux VDA ソフトウェアをインストールします。

```
sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

ステップ 6c: Linux VDA をアップグレードする (オプション)

既存のインストールを、以前の2つのバージョンおよびLTSRリリースからアップグレードできます。

> **注:**
>
> 既存のインストールをアップグレードすると、/etc/xdl の下の構成ファイルが上書きされます。アップグレードを実行する前に、ファイルをバックアップしてください。

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

SUSE 15 の RPM 依存関係リスト:

```
java-11-openjdk >= 11



ImageMagick >= 7.0



dbus-1 >= 1.12.2
```

```
dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2
```

```
cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0
```

```
libImlib2-1 >= 1.4.10
```

重要:

アップグレード後、Linux VDA マシンを再起動します。

ステップ 7: NVIDIA GRID ドライバーをインストールする

HDX 3D Pro を有効にするには、ハイパーバイザーと VDA マシンに NVIDIA GRID ドライバーをインストールする必要があります。

特定のハイパーバイザーに NVIDIA GRID Virtual GPU Manager (ホストドライバー) をインストールして構成するには、以下のガイドを参照してください。

- シトリックス ハイパーバイザー
- ヴイエムウェア ESX
- ニュータニックス AHV

NVIDIA GRID ゲスト VM ドライバーをインストールして構成するには、以下の一般的な手順を実行します。

1. ゲストVMがシャットダウンされていることを確認します。
2. ハイパーバイザーのコントロールパネルで、VMにGPUを割り当てます。
3. VMを起動します。
4. VMにゲストVMドライバーをインストールします。

ステップ8：Linux VDAを構成する

注:

ランタイム環境をセットアップする前に、**en_US.UTF-8**ロケールがOSにインストールされていることを確認してください。ロケールがOSで利用できない場合は、**sudo locale-gen en_US.UTF-8**コマンドを実行します。Debianの場合、**/etc/locale.gen**ファイルを編集し、**# en_US.UTF-8 UTF-8**行のコメントを解除してから、**sudo locale-gen**コマンドを実行します。

> パッケージのインストール後、`ctxsetup.sh`スクリプトを実行してLinux VDAを構成する必要があります。スクリプトは変更を加える前に、環境を検証し、すべての依存関係がインストールされていることを確認します。必要に応じて、いつでもスクリプトを再実行して設定を変更できます。

スクリプトは、プロンプトに従って手動で実行することも、事前設定された応答で自動的に実行することもできます。続行する前に、スクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

プロンプトによる構成

プロンプトによる質問で手動構成を実行します。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

自動構成

自動インストールの場合、セットアップスクリプトで必要なオプションを環境変数で指定します。必要なすべての変数が存在する場合、スクリプトは情報を要求しません。

サポートされている環境変数には、次のものがあります。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Linux VDAは、DNS CNAMEレコードを使用してDelivery Controller名を指定することをサポートしています。デフォルトではNに設定されています。
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Linux VDAは、Delivery Controllerに登録するために使用する、スペース区切りのDelivery Controllerの完全修飾ドメイン名（FQDN）のリストを必要とします。少なくとも1つのFQDNまたはCNAMEエイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT=port-number** – Linux VDA は、TCP/IP ポートを介して Delivery Controller と通信します。デフォルトではポート 80 です。
- **CTX_XDL_REGISTER_SERVICE=Y \| N** - Linux VDA サービスは、マシンの起動後に開始されます。デフォルトでは値は Y に設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Linux VDA サービスでは、システムファイアウォールを介した受信ネットワーク接続が許可されている必要があります。Linux VDA のシステムファイアウォールで、必要なポート（デフォルトではポート 80 および 1494）を自動的に開くことができます。デフォルトでは Y に設定されています。

- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd** – Linux VDA は、Delivery Controller で認証するために Kerberos 構成設定を必要とします。Kerberos 構成は、システムにインストールおよび構成されている Active Directory 統合ツールから決定されます。
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Linux VDA は、リッチグラフィックアプリケーションの仮想化を最適化するために設計された GPU アクセラレーションテクノロジーのセットである HDX 3D Pro をサポートしています。HDX 3D Pro が選択されている場合、VDA は VDI デスクトップ（シングルセッション）モード（つまり、CTX_XDL_VDI_MODE=Y）用に構成されます。
- **CTX_XDL_VDI_MODE=Y \| N** – マシンを専用デスクトップ配信モデル（VDI）として構成するか、ホスト型共有デスクトップ配信モデルとして構成するか。HDX 3D Pro 環境の場合は、この変数を Y に設定します。この変数はデフォルトで N に設定されています。
- **CTX_XDL_SITE_NAME=dns-name** – Linux VDA は DNS を介して LDAP サーバーを検出します。DNS 検索結果をローカルサイトに限定するには、DNS サイト名を指定します。この変数はデフォルトで **\<none\>** に設定されています。
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Linux VDA は、LDAP サーバーを検出するために DNS を照会します。DNS が LDAP サービスレコードを提供できない場合は、LDAP ポートを含む LDAP FQDN のスペース区切りリストを指定できます。たとえば、ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 のように指定します。LDAP ポート番号を 389 と指定した場合、Linux VDA は指定されたドメイン内の各 LDAP サーバーをポーリングモードで照会します。ポリシーの数が x で LDAP サーバーの数が y の場合、Linux VDA は合計で X かける Y のクエリを実行します。ポーリング時間がしきい値を超えると、セッションログオンが失敗する可能性があります。より高速な LDAP クエリを有効にするには、ドメインコントローラーで **Global Catalog** を有効にし、関連する LDAP ポート番号を 3268 と指定します。この変数はデフォルトで **\<none\>** に設定されています。
- **CTX_XDL_SEARCH_BASE=search-base-set** – Linux VDA は、Active Directory ドメインのルートに設定された検索ベース（例: DC=mycompany,DC=com）を介して LDAP を照会します。検索パフォーマンスを向上させるには、検索ベース（例: OU=VDI,DC=mycompany,DC=com）を指定できます。この変数はデフォルトで **\<none\>** に設定されています。
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Federated Authentication Service (FAS) サーバーは、AD グループポリシーを介して構成されます。Linux VDA は AD グループポリシーをサポートしていませんが、代わりにセミコロン区切りの FAS サーバーのリストを提供できます。シーケンスは AD グループポリシーで構成されているものと同じである必要があります。サーバーアドレスが削除された場合は、その空白を **\<none\>** テキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。FAS サーバーと適切に通信するには、FAS

サーバーで指定されているポート番号と一致するポート番号を追加してください。例: CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。

- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – 新しいブローカーエージェントサービス (`ctxvda`) をサポートするために .NET Runtime 6.0 をインストールするパス。デフォルトのパスは /usr/bin です。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – セッションで使用する GNOME、GNOME Classic、または MATE デスクトップ環境を指定します。この変数を指定しない場合、VDA に現在インストールされているデスクトップが使用されます。ただし、現在インストールされているデスクトップが MATE の場合は、変数の値を **mate** に設定する必要があります。

  ターゲットセッションユーザーのデスクトップ環境は、次の手順で変更することもできます。

  a. VDA 上の **$HOME/<username\>** ディレクトリの下に `.xsession` ファイルを作成します。

  2\. `.xsession` ファイルを編集して、デスクトップ環境を指定します。

  - **SUSE 15 の MATE デスクトップの場合**

```
MSESSION="$(type -p mate-session)"



if [ -n "$MSESSION" ]; then

  exec mate-session



fi
```

  - **SUSE 15 の GNOME Classic デスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then
```

```
export GNOME_SHELL_SESSION_MODE=classic



exec gnome-session --session=gnome-classic

fi
```

◦ **SUSE 15 の GNOME デスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

exec gnome-session



fi
```

b. ターゲットセッションユーザーと 700 ファイル権限を共有します。

バージョン 2209 以降、セッションユーザーはデスクトップ環境をカスタマイズできます。この機能を有効にするには、VDA に切り替え可能なデスクトップ環境を事前にインストールする必要があります。詳細については、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

- **CTX_XDL_START_SERVICE=Y \| N** – Linux VDA の構成が完了したときに Linux VDA サービスを開始するかどうか。デフォルトでは Y に設定されています。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scout のリッスン用ソケットポート。デフォルトポートは 7503 です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scout と通信するためのポート。デフォルトポートは 7502 です。

環境変数を設定し、構成スクリプトを実行します。

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
```

```
export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'


export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime


export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate |
'<none>'


export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number


export CTX_XDL_TELEMETRY_PORT=port-number


export CTX_XDL_START_SERVICE=Y|N


sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

sudo コマンドを実行するときは、**-E** オプションを入力して、既存の環境変数を新しく作成されるシェルに渡します。前述のコマンドから、最初の行に **#\!/bin/bash** を含むシェルスクリプトファイルを作成することをお勧めします。

または、単一のコマンドを使用してすべてのパラメーターを指定することもできます。

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \
```

```
CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
```

```
CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

構成の変更を削除する

シナリオによっては、Linux VDA パッケージをアンインストールせずに、**ctxsetup.sh** スクリプトによって行われた構成の変更を削除する必要がある場合があります。

続行する前に、このスクリプトに関するヘルプを確認してください。

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

構成の変更を削除するには：

```
sudo /usr/local/sbin/ctxcleanup.sh
```

> **重要:**
>
> このスクリプトは、データベースからすべての構成データを削除し、Linux VDA を動作不能にします。

構成ログ

ctxsetup.sh および **ctxcleanup.sh** スクリプトは、コンソールにエラーを表示し、追加情報は構成ログファイルに書き込まれます。

`/tmp/xdl.configure.log`

変更を有効にするには、Linux VDA サービスを再起動します。

ステップ 9: XDPing を実行する

Linux VDA 環境における一般的な構成の問題を確認するには、`sudo /opt/Citrix/VDA/bin/xdping` を実行します。詳細については、「XDPing」を参照してください。

ステップ 10: Linux VDA を実行する

ctxsetup.sh スクリプトを使用して Linux VDA を構成した後、次のコマンドを実行して Linux VDA を制御できます。

Linux VDA を開始する:

Linux VDA サービスを開始するには:

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDA を停止する:

Linux VDA サービスを停止するには:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

注:

`ctxvda` および `ctxhdx` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止します。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

Linux VDA を再起動する:

Linux VDA サービスを再起動するには:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Linux VDA のステータスを確認する:

Linux VDA サービスの稼働状況を確認するには:

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

ステップ 11: マシンカタログを作成する

マシンカタログを作成し、Linux VDA マシンを追加するプロセスは、従来の Windows VDA のアプローチと似ています。これらのタスクを完了する方法の詳細については、「マシンカタログを作成する」および「マシンカタログを管理する」を参照してください。

Linux VDA マシンを含むマシンカタログを作成する場合、Windows VDA マシン用のマシンカタログを作成するプロセスとは異なるいくつかの制限があります。

- オペレーティングシステムについては、以下を選択します:
  - ホストされた共有デスクトップの配信モデルの場合は、**Multi-session OS** オプション。
  - VDI 専用デスクトップの配信モデルの場合は、**Single-session OS** オプション。
- 同じマシンカタログ内で Linux VDA マシンと Windows VDA マシンを混在させないでください。

注:

Citrix Studio の初期バージョンでは、「Linux OS」という概念はサポートされていませんでした。ただし、**Windows Server OS** または **Server OS** オプションを選択すると、同等のホストされた共有デスクトップ配信モデルが示唆されます。**Windows Desktop OS** または **Desktop OS** オプションを選択すると、マシンごとに単一ユーザーの配信モデルが示唆されます。

ヒント:

マシンを Active Directory ドメインから削除して再参加させる場合、そのマシンをマシンカタログから削除し、再度追加する必要があります。

ステップ 12: デリバリーグループを作成する

デリバリーグループを作成し、Linux VDA マシンを含むマシンカタログを追加するプロセスは、Windows VDA マシンの場合とほぼ同じです。これらのタスクを完了する方法の詳細については、「デリバリーグループを作成する」を参照してください。

Linux VDA マシンカタログを含むデリバリーグループを作成する場合、以下の制限が適用されます:

- 選択した AD ユーザーとグループが、Linux VDA マシンにログオンできるように適切に構成されていることを確認してください。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- デリバリーグループと、Windowsマシンを含むマシンカタログを混在させないでください。

重要:

アプリケーションの公開は、Linux VDAバージョン1.4以降でサポートされています。ただし、Linux VDAは、デスクトップとアプリを同じマシンに配信することをサポートしていません。

マシンカタログとデリバリーグループの作成方法については、Citrix Virtual Apps and Desktops 7 2303を参照してください。

Ubuntu に Linux VDA を手動でインストールする

> **重要:**
>
> 新規インストールの場合、迅速なインストールには easy install (/ja-jp/linux-virtual-delivery-agent/current-release/installation-overview/create-domain-joined-vdas-using-easy-install.html) を使用することをお勧めします。easy install は時間と労力を節約し、この記事で詳述されている手動インストールよりもエラーが発生しにくいです。

ステップ 1: 構成情報と Linux マシンを準備する

ステップ 1a: ネットワーク構成を確認する

ネットワークが正しく接続され、構成されていることを確認してください。たとえば、Linux VDA で DNS サーバーを構成する必要があります。

Ubuntu 18.04 Live Server を使用している場合は、ホスト名を設定する前に **/etc/cloud/cloud.cfg** 構成ファイルで次の変更を行ってください。

```
preserve_hostname: true
```

ステップ 1b: ホスト名を設定する

マシンのホスト名が正しく報告されるように、**/etc/hostname** ファイルをマシンのホスト名のみを含むように変更します。

```
hostname
```

ステップ 1c: ホスト名にループバックアドレスを割り当てる

マシンの DNS ドメイン名と完全修飾ドメイン名 (FQDN) が正しく報告されることを確認してください。そのためには、**/etc/hosts** ファイルの次の行を変更して、FQDN とホスト名を最初の 2 つのエントリとして含めます。

```
127.0.0.1 hostname-fqdn hostname localhost
```

例:

```
127.0.0.1 vda01.example.com vda01 localhost
```

ファイル内の他のエントリから `hostname-fqdn` または `hostname` への他の参照を削除します。

> **注:**
>
> Linux VDA は現在、NetBIOS 名の切り捨てをサポートしていません。したがって、ホスト名は 15 文字を超えてはなりません。

> **ヒント:**
>
> a–z、A–Z、0–9、およびハイフン (-) の文字のみを使用してください。アンダースコア (_)、スペース、その他の記号は避けてください。ホスト名を数字で始めたり、ハイフンで終わらせたりしないでください。この規則は Delivery Controller のホスト名にも適用されます。

ステップ 1d: ホスト名を確認する

ホスト名が正しく設定されていることを確認してください。

```
hostname
```

このコマンドは、マシンのホスト名のみを返し、FQDNは返しません。

FQDNが正しく設定されていることを確認します。

```
hostname -f
```

このコマンドは、マシンのFQDNを返します。

ステップ1e: マルチキャストDNSを無効にする

デフォルト設定ではマルチキャストDNS (**mDNS**) が有効になっており、名前解決の結果が不安定になる可能性があります。

mDNSを無効にするには、**/etc/nsswitch.conf**を編集し、次の行を変更します。

`hosts: files mdns_minimal [NOTFOUND=return] dns`

次のように変更します。

`hosts: files dns`

ステップ1f: 名前解決とサービスの到達可能性を確認する

FQDNを解決し、ドメインコントローラーとDelivery Controller™にpingできることを確認します。

```
nslookup domain-controller-fqdn



ping domain-controller-fqdn



nslookup delivery-controller-fqdn



ping delivery-controller-fqdn
```

FQDNを解決できない場合、またはこれらのマシンのいずれかにpingできない場合は、続行する前に手順を確認してください。

ステップ1g: クロック同期を構成する (chrony)

VDA、Delivery Controller、およびドメインコントローラー間で正確なクロック同期を維持することは非常に重要です。Linux VDAを仮想マシン (VM) としてホストすると、クロックスキューの問題が発生する可能性があります。このため、リモート時刻サービスとの時刻同期が推奨されます。

chronyをインストールします。

```
apt-get install chrony
```

rootユーザーとして、**/etc/chrony/chrony.conf**を編集し、各リモートタイムサーバーのサーバーエントリを追加します。

`server peer1-fqdn-or-ip-address iburst`

`server peer2-fqdn-or-ip-address iburst`

通常の展開では、パブリックNTPプールサーバーから直接ではなく、ローカルのドメインコントローラーから時刻を同期します。ドメイン内の各Active Directoryドメインコントローラーのサーバーエントリを追加します。

ループバックIPアドレス、localhost、およびパブリックサーバーの ***.pool.ntp.org** エントリを含む、リストされている他のすべての **server** または **pool** エントリを削除します。

変更を保存し、Chronyデーモンを再起動します。

```
sudo systemctl restart chrony
```

ステップ1h: OpenJDK 11をインストールする

Linux VDAにはOpenJDK 11が必要です。

Ubuntu 20.04およびUbuntu 18.04では、以下を使用してOpenJDK 11をインストールします。

```
sudo apt-get install -y openjdk-11-jdk
```

ステップ1i: 使用するデータベースをインストールして指定する

実験的機能として、PostgreSQLに加えてSQLiteを使用できます。Linux VDAパッケージのインストール後に`/etc/xdl/db.conf`を編集することで、SQLiteとPostgreSQLを切り替えることもできます。手動インストールの場合、それらを切り替える前にSQLiteとPostgreSQLを手動でインストールする必要があります。

このセクションでは、PostgreSQLおよびSQLiteデータベースのインストール方法と、使用するデータベースの指定方法について説明します。

> **注:**
>
> SQLiteはVDIモードでのみ使用することをお勧めします。

POSTGRESQLをインストールする

PostgreSQLをインストールするには、次のコマンドを実行します。

```
sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

マシンの起動時または即座にPostgreSQLを開始するには、それぞれ次のコマンドを実行します。

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

SQLITEをインストールする

Ubuntuの場合、SQLiteをインストールするには次のコマンドを実行します。

```
sudo apt-get install -y sqlite3
```

使用するデータベースを指定する

SQLite、PostgreSQL、またはその両方をインストールした後、Linux VDAパッケージのインストール後に`/etc/xdl/db.conf`を編集して、使用するデータベースを指定できます。これを行うには、次の手順を完了します。

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh`を実行します。新規インストールの場合、この手順は省略してください。
2. 使用するデータベースを指定するために`/etc/xdl/db.conf`を編集します。
3. `ctxsetup.sh`を実行します。

> **注:**
>
> PostgreSQLのポート番号を構成するには、**/etc/xdl/db.conf**を使用することもできます。

ステップ1j：Motifをインストールする

```
sudo apt-get install -y libxm4
```

ステップ1k：その他のパッケージをインストールする

Ubuntu 22.04の場合：

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit

sudo apt-get install -y libldap-2.5-0
```

```
sudo apt-get install -y krb5-user

sudo apt-get install -y libgtk2.0-0
```

Ubuntu 20.04、Ubuntu 18.04の場合：

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit

sudo apt-get install -y libldap-2.4-2

sudo apt-get install -y krb5-user

sudo apt-get install -y libgtk2.0-0
```

ステップ2：ハイパーバイザーを準備する

サポートされているハイパーバイザー上でLinux VDAをVMとして実行する場合、いくつかの変更が必要です。使用しているハイパーバイザープラットフォームに基づいて、以下の変更を行ってください。Linuxマシンをベアメタルハードウェアで実行している場合、変更は不要です。

Citrix Hypervisor™での時刻同期の修正

Citrix Hypervisorの時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとCitrix Hypervisorに関する問題が発生します。両方ともシステムクロックを管理しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。HVMモードでは変更は不要です。

Citrix VM Toolsがインストールされた準仮想化Linuxカーネルを実行している場合、Linux VM内からCitrix Hypervisorの時刻同期機能が存在し、有効になっているかを確認できます。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは0または1を返します。

- 0 - 時刻同期機能が有効になっており、無効にする必要があります。
- 1 - タイム同期機能は無効になっており、それ以上の操作は不要です。

/proc/sys/xen/independent_wallclock ファイルが存在しない場合、以下の手順は不要です。

有効になっている場合は、ファイルに 1 を書き込むことでタイム同期機能を無効にします。

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

この変更を永続化し、再起動後も維持するには、**/etc/sysctl.conf ファイル**を編集して次の行を追加します。

`xen.independent_wallclock = 1`

これらの変更を確認するには、システムを再起動します。

```
su -



cat /proc/sys/xen/independent_wallclock
```

このコマンドは値 1 を返します。

Microsoft Hyper-V での時刻同期の修正

Hyper-V Linux Integration Services がインストールされている Linux VM は、Hyper-V の時刻同期機能を使用してホストオペレーティングシステムの時刻を使用できます。システムクロックが正確に保たれるように、NTP サービスと並行してこの機能を有効にしてください。

管理オペレーティングシステムから:

1. Hyper-V マネージャーコンソールを開きます。
2. Linux VM の設定で、**統合サービス**を選択します。
3. **時刻同期**が選択されていることを確認します。

> **注:**

> このアプローチは、NTP との競合を避けるためにホストの時刻同期が無効になっている VMware や Citrix Hypervisor とは異なります。Hyper-V の時刻同期は、NTP の時刻同期と共存し、補完することができます。

ESX および ESXi での時刻同期の修正

VMware の時刻同期機能が有効になっている場合、各準仮想化 Linux VM 内で NTP とハイパーバイザーとの間で問題が発生します。両方ともシステムクロックを同期しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各 Linux ゲスト内のシステムクロックが NTP と同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。

VMware Toolsがインストールされた準仮想化Linuxカーネルを実行している場合：

1. vSphere Clientを開きます。
2. Linux VMの設定を編集します。
3. **Virtual Machine Properties**ダイアログで、**Options**タブを開きます。
4. **VMware Tools**を選択します。
5. **Advanced**ボックスで、**Synchronize guest time with host**のチェックを外します。

ステップ3：Linux VMをWindowsドメインに追加する

LinuxマシンをActive Directory（AD）ドメインに追加するには、次の方法があります。

- サンバ Winbind
- セントリファイ ダイレクトコントロール
- SSSD
- PBIS

選択した方法に基づいて指示に従ってください。

> **注:**

> Linux VDAのローカルアカウントとADのアカウントで同じユーザー名を使用すると、セッションの起動に失敗する可能性があります。

サンバ Winbind

必要なパッケージをインストールまたは更新する

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

マシン起動時にWINBINDデーモンが開始するように有効にする

Winbindデーモンは、マシンの起動時に開始するように構成する必要があります。

```
sudo systemctl enable winbind
```

> **注:**
>
> `winbind` スクリプトが `/etc/init.d` の下にあることを確認してください。

KERBEROSを構成する

ルートユーザーとして **/etc/krb5.conf** を開き、次の設定を行います。

> **注:**
>
> ADインフラストラクチャに基づいてKerberosを構成します。以下の設定は、単一ドメイン、単一フォレストモデルを対象としています。

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` `REALM`

`.domain-dns-name` `=` `REALM`

このコンテキストにおける **domain-dns-name** パラメーターは、**example.com** のようなDNSドメイン名です。**REALM** は、**EXAMPLE.COM** のような大文字のKerberosレルム名です。

WINBIND認証を構成する

UbuntuにはRHELの**authconfig**やSUSEのyast2のようなツールがないため、Winbindを手動で構成します。

/etc/samba/smb.confを開き、次の設定を行います。

`[global]`

`workgroup =` `WORKGROUP`

`security = ADS`

`realm =` `REALM`

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`winbind trusted domains only = no`

`kerberos method = secrets and keytab`

`winbind refresh tickets = yes`

`template shell = /bin/bash`

WORKGROUPは**REALM**の最初のフィールドであり、**REALM**はKerberosレルム名の大文字表記です。

NSSWITCHを構成する

/etc/nsswitch.confを開き、次の行に**winbind**を追加します。

`passwd: compat winbind`

`group: compat winbind`

WINDOWSドメインに参加する

ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
sudo net ads join REALM -U user
```

ここで、**REALM**はKerberosレルム名の大文字表記であり、**user**はコンピューターをドメインに追加する権限を持つドメインユーザーです。

`WINBIND`を再起動する

```
sudo systemctl restart winbind
```

WINBIND用にPAMを構成する

次のコマンドを実行し、**Winbind NT/Active Directory authentication**と**Create home directory on login**オプションが選択されていることを確認します。

```
sudo pam-auth-update
```

> **ヒント:**
>
> **winbind**デーモンは、マシンがドメインに参加している場合にのみ実行され続けます。

ドメインメンバーシップを確認する

Delivery Controller は、Windows または Linux のいずれであっても、すべての VDA マシンが Active Directory にコンピューターオブジェクトを持つことを要求します。

マシンがドメインに参加していることを確認するには、**Samba** の **net ads** コマンドを実行します。

```
sudo net ads testjoin
```

追加のドメインおよびコンピューターオブジェクト情報を確認するには、次のコマンドを実行します。

```
sudo net ads info
```

KERBEROS構成の確認

Kerberos が Linux VDA で使用するために正しく構成されていることを確認するには、システム **keytab** ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してドメインコントローラーでマシンを認証するには、Kerberos の **kinit** コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェル置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNS ドメイン名が Kerberos レルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントの TGT チケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

次を使用して、マシンのアカウントの詳細を調べます。

```
sudo net ads status
```

ユーザー認証の確認

ドメインユーザーがドメインで認証できることを確認するには、**wbinfo** ツールを使用します。

```
wbinfo --krb5auth=domain\\username%password
```

ここで指定するドメインは AD ドメイン名であり、Kerberos レルム名ではありません。bash シェルの場合、バックスラッシュ (\\) 文字は別のバックスラッシュでエスケープする必要があります。このコマンドは、成功または失敗を示すメッセージを返します。

Winbind PAM モジュールが正しく構成されていることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用して Linux VDA にログオンします。

```
ssh localhost -l domain\\username



id -u
```

注:

SSH コマンドを正常に実行するには、SSH が有効になっており、正しく動作していることを確認してください。

id -u コマンドによって返された uid に対応する Kerberos 資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

ユーザーのKerberos認証情報キャッシュ内のチケットが有効で期限切れでないことを確認します。

```
klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/2303/installation-overview/manual-installation-overview/ubuntu.html#step-6-install-the-linux-vda)に進みます。

ヒント:

ユーザー認証に成功しても、ドメインアカウントでログオンしたときにデスクトップが表示されない場合は、マシンを再起動してからもう一度試してください。

Quest認証サービス

ドメインコントローラーでのQUESTの構成

Active Directoryドメインコントローラーにインストールして構成済みであり、`Active Directory`でコンピューターオブジェクトを作成するための管理者権限が付与されていると仮定します。

ドメインユーザーがLINUX VDAマシンにログオンできるようにする

ドメインユーザーがLinux VDAマシンでHDX™セッションを確立できるようにするには：

1. Active Directoryユーザーとコンピューター管理コンソールで、そのユーザーアカウントのActive Directoryユーザープロパティを開きます。
2. **Unixアカウント**タブを選択します。
3. **Unix対応**をオンにします。
4. **プライマリGID番号**を実際のドメインユーザーグループのグループIDに設定します。

> **注:**
>
> これらの手順は、コンソール、RDP、SSH、またはその他のリモートプロトコルを使用してログオンするドメインユーザーを設定する場合にも同様に適用されます。

LINUX VDAでのQUESTの構成

SELinuxポリシーの適用を回避する
デフォルトのRHEL環境では、SELinuxが完全に適用されています。この適用により、Questが使用するUnixドメインソケットIPCメカニズムが妨げられ、ドメインユーザーがログオンできなくなります。

この問題を回避する便利な方法は、SELinuxを無効にすることです。rootユーザーとして、**/etc/selinux/config** を編集し、**SELinux** の設定を変更します。

`SELINUX=disabled`

この変更にはマシンの再起動が必要です。

```
reboot
```

> **重要:**

> この設定は慎重に使用してください。無効にした後にSELinuxポリシーの適用を再度有効にすると、rootユーザーや他のローカルユーザーであっても、完全にロックアウトされる可能性があります。

VASデーモンを構成する
Kerberosチケットの自動更新は有効にして切断する必要があります。認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

このコマンドは、更新間隔を9時間（32,400秒）に設定します。これは、デフォルトの10時間のチケット有効期間より1時間短いです。チケット有効期間が短いシステムでは、このパラメーターをより低い値に設定してください。
PAMとNSSを構成する
HDXおよびsu、ssh、RDPなどの他のサービスを介したドメインユーザーのログオンを有効にするには、次のコマンドを実行してPAMとNSSを手動で構成します。

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

WINDOWSドメインに参加する

Questの**vastool**コマンドを使用して、LinuxマシンをActive Directoryドメインに参加させます。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

ユーザーは、コンピューターをActive Directoryドメインに参加させる権限を持つ任意のドメインユーザーです。**domain-name** はドメインのDNS名です（例: example.com）。

ドメインメンバーシップを確認する

Delivery Controllerは、WindowsまたはLinuxのすべてのVDAマシンがActive Directoryにコンピューターオブジェクトを持つことを要求します。Questに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合、このコマンドはドメイン名を返します。マシンがどのドメインにも参加していない場合、次のエラーが表示されます。

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

ユーザー認証の確認

QuestがPAMを介してドメインユーザーを認証できることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u
```

id -u コマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

Kerberos資格情報キャッシュ内のチケットが有効で期限切れになっていないことを確認します。

```
/opt/quest/bin/vastool klist
```

セッションを終了します。

```
exit
```

ドメイン参加の検証後、手順6：Linux VDAのインストールに進みます。

セントリファイ ダイレクトコントロール

WINDOWSドメインへの参加

Centrify DirectControl Agentがインストールされたら、Centrifyの**adjoin**コマンドを使用してLinuxマシンをActive Directoryドメインに参加させます。

```
su –

adjoin -w -V -u user domain-name
```

userパラメーターは、コンピューターを**Active Directory**ドメインに参加させる権限を持つActive Directoryドメインユーザーです。**domain-name**パラメーターは、Linuxマシンを参加させるドメインの名前です。

ドメインメンバーシップの確認

Delivery Controllerは、WindowsまたはLinuxにかかわらず、すべてのVDAマシンが**Active Directory**にコンピューターオブジェクトを持つことを要求します。Centrifyに参加しているLinuxマシンがドメイン上にあることを確認するには、次の手順を実行します。

```
su –


adinfo
```

Joined to domainの値が有効であり、**CentrifyDC mode**が**connected**を返すことを確認します。モードが開始状態のままになっている場合、Centrifyクライアントはサーバー接続または認証の問題を抱えています。

より包括的なシステムおよび診断情報は、以下を使用して利用できます。

```
adinfo --sysinfo all


adinfo --diag
```

さまざまなActive DirectoryおよびKerberosサービスへの接続をテストします。

```
adinfo --test
```

ドメイン参加の検証後、手順6: Linux VDAのインストールに進みます。

SSSD

KERBEROSの構成

Kerberosをインストールするには、次のコマンドを実行します。

```
sudo apt-get install krb5-user
```

Kerberosを構成するには、rootとして **/etc/krb5.conf** を開き、パラメーターを設定します。

> **注:**
>
> ADインフラストラクチャに基づいてKerberosを構成します。以下の設定は、単一ドメイン、単一フォレストモデルを対象としています。

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` *`REALM`*

`.domain-dns-name` `=` *`REALM`*

このコンテキストでの `domain-dns-name` パラメーターは、example.comなどのDNSドメイン名です。*REALM* は、EXAMPLE.COMなどの大文字のKerberosレルム名です。

ドメインへの参加

SSSDは、Active DirectoryをIDプロバイダーとして、Kerberosを認証に使用するように構成する必要があります。ただし、SSSDはドメインへの参加やシステムキータブファイルの管理のためのADクライアント機能を提供しません。代わりに、**adcli**、**realmd**、または**Samba**を使用できます。

> **注:**
>
> このセクションでは、**adcli**と**Samba**に関する情報のみを提供します。

- **adcliを使用してドメインに参加する場合は、次の手順を完了してください。**

1. **adcli**をインストールします。

   ```
   sudo apt-get install adcli
   ```

2. **adcli**でドメインに参加します。

   古いシステムキータブファイルを削除し、以下を使用してドメインに参加します。

   ```
   su -


   rm -rf /etc/krb5.keytab


   adcli join domain-dns-name -U user -H hostname-fqdn
   ```

   userは、マシンをドメインに追加する権限を持つドメインユーザーです。**hostname-fqdn**は、マシンのFQDN形式のホスト名です。

   -Hオプションは、Linux VDAが必要とするhost/hostname-fqdn@REALM形式のSPNを**adcli**が生成するために必要です。

3. ドメインメンバーシップを確認します。

Ubuntu 22.04およびUbuntu 20.04マシンでは、`adcli testjoin`コマンドを実行して、マシンがドメインに参加しているかどうかをテストします。

Ubuntu 18.04マシンでは、`sudo klist -ket`コマンドを実行します。**adcli**ツールの機能は限られています。このツールは、マシンがドメインに参加しているかどうかをテストする方法を提供しません。最善の代替策は、システムキータブファイルが作成されていることを確認することです。各キーのタイムスタンプが、マシンがドメインに参加した時刻と一致することを確認してください。

- **Sambaを使用してドメインに参加する場合は、次の手順を完了してください。**

1. パッケージをインストールします。

```
sudo apt-get install samba krb5-user
```

2. **Samba**を構成します。

   /etc/samba/smb.confを開き、次の設定を行います。

   `[global]`

   `workgroup =` *`WORKGROUP`*

   `security = ADS`

   `realm =` *`REALM`*

   `client signing = yes`

   `client use spnego = yes`

   `kerberos method = secrets and keytab`

   WORKGROUP は **REALM** の最初のフィールドであり、**REALM** は大文字の Kerberos レルム名です。

3. **Samba** を使用してドメインに参加します。

   ドメインコントローラーに到達可能である必要があり、ドメインにコンピューターを追加する権限を持つ Windows アカウントが必要です。

```
sudo net ads join REALM -U user
```

ここで、**REALM** は大文字の Kerberos レルム名であり、**user** はドメインにコンピューターを追加する権限を持つドメインユーザーです。

SSSD のセットアップ

必要なパッケージのインストールまたは更新:

必要な SSSD および構成パッケージがまだインストールされていない場合は、インストールします。

```
sudo apt-get install sssd
```

パッケージがすでにインストールされている場合は、更新をお勧めします。

```
sudo apt-get install --only-upgrade sssd
```

注:

デフォルトでは、Ubuntu のインストールプロセスは **nsswitch.conf** と PAM ログインモジュールを自動的に構成します。

SSSD の構成

SSSD デーモンを開始する前に、SSSD 構成の変更が必要です。SSSD の一部のバージョンでは、**/etc/sssd/sssd.conf** 構成ファイルはデフォルトでインストールされておらず、手動で作成する必要があります。root として、**/etc/sssd/sssd.conf** を作成または開き、次の設定を行います。

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/` *`domain-dns-name`* `]`

`id_provider = ad`

`access_provider = ad`

`auth_provider = krb5`

```
krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

注:

ldap_id_mapping は **true** に設定されており、SSSD 自体が Windows SID を Unix UID にマッピングする処理を行います。そうでない場合、Active Directory は POSIX 拡張機能を提供できる必要があります。PAM サービス `ctxhdx` は ad_gpo_map_remote_interactive に追加されます。

このコンテキストにおける **domain-dns-name** パラメータは、example.com のような DNS ドメイン名です。**REALM** は、EXAMPLE.COM のような大文字の Kerberos レルム名です。NetBIOS ドメイン名を設定する必要はありません。

構成設定の詳細については、sssd.conf および `sssd-ad` の man ページを参照してください。

> SSSD デーモンは、構成ファイルが所有者による読み取り権限のみを持つことを要求します。

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

SSSD デーモンの開始

SSSD デーモンを今すぐ開始し、マシンの起動時にデーモンが開始されるようにするには、次のコマンドを実行します。

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM 構成

次のコマンドを実行し、**SSS 認証**と**ログイン時にホームディレクトリを作成**オプションが選択されていることを確認します。

```
sudo pam-auth-update
```

ドメインメンバーシップの確認

Delivery Controller は、すべての VDA マシン（Windows および Linux VDA）が `Active Directory` にコンピューターオブジェクトを持つことを要求します。

- **adcli** を使用してドメインメンバーシップを確認する場合は、`sudo adcli info domain-dns-name` コマンドを実行してドメイン情報を表示します。
- **Samba** を使用してドメインメンバーシップを確認する場合は、`sudo net ads testjoin` コマンドを実行してマシンがドメインに参加していることを確認し、`sudo net ads info` コマンドを実行して追加のドメインおよびコンピューターオブジェクト情報を確認します。

KERBEROS 構成の確認

Linux VDA で使用するために Kerberos が正しく構成されていることを確認するには、システム keytab ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用して、ドメインコントローラーでマシンを認証するには、Kerberos `kinit` コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェルによる置換を防ぐために、バックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNSドメイン名がKerberosレルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントのTGTがキャッシュされていることを、以下を使用して確認します。

```
sudo klist
```

ユーザー認証の確認

SSSDは、デーモンで認証を直接テストするためのコマンドラインツールを提供しておらず、PAMを介してのみ実行できます。

SSSD PAMモジュールが正しく構成されていることを確認するには、以前使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u



klist



exit
```

klist コマンドによって返されたKerberosチケットがそのユーザーに対して正しく、期限切れになっていないことを確認します。

rootユーザーとして、以前の **id -u** コマンドによって返されたuidに対応するチケットキャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

同様のテストは、KDEまたはGnome Display Managerにログオンすることで実行できます。ドメイン参加の検証後、手順6：Linux VDAのインストールに進みます。

PBIS

必要なPBISパッケージをダウンロードする

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBISインストールスクリプトを実行可能にする

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBISインストールスクリプトを実行する

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

WINDOWSドメインに参加する

ドメインコントローラーに到達可能である必要があり、ドメインにコンピューターを追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

「**ユーザー**」は、Active Directoryドメインにコンピューターを追加する権限を持つドメインユーザーです。「**ドメイン名**」は、たとえばexample.comのようなドメインのDNS名です。

注：Bashをデフォルトシェルとして設定するには、**sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**コマンドを実行します。

ドメインメンバーシップを確認する

Delivery Controllerは、すべてのVDAマシン（WindowsおよびLinux VDA）が`Active Directory`にコンピューターオブジェクトを持つことを必要とします。PBISに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
/opt/pbis/bin/domainjoin-cli query
```

マシンがドメインに参加している場合、このコマンドは現在参加しているADドメインとOUに関する情報を返します。そうでない場合、ホスト名のみが表示されます。

ユーザー認証を確認する

PBISがPAMを介してドメインユーザーを認証できることを確認するには、以前に使用されていないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
sudo ssh localhost -l domain\\user



id -u
```

id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

セッションを終了します。

```
exit
```

ドメイン参加の確認後、手順6：Linux VDAをインストールするに進みます。

手順4：.NET Runtime 6.0をインストールする

Linux VDAをインストールする前に、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>`の指示に従って.NET Runtime 6.0をインストールします。

.NET Runtime 6.0をインストールした後、**which dotnet**コマンドを実行してランタイムパスを見つけます。

コマンドの出力に基づいて、.NETランタイムバイナリパスを設定します。たとえば、コマンドの出力が/aa/bb/dotnetの場合、/aa/bbを.NETバイナリパスとして使用します。

手順5：Linux VDAパッケージをダウンロードする

1. 「Citrix Virtual Apps and Desktops ダウンロードページ」にアクセスします。

2. 適切なバージョンのCitrix Virtual Apps and Desktopsを展開します。
3. をクリックして、お使いのLinuxディストリビューションに一致するLinux VDAパッケージと、Linux VDAパッケージの整合性を検証するために使用できるGPG公開キーをダウンロードします。

   公開キーを使用してLinux VDAパッケージの整合性を検証するには、公開キーをDEBデータベースにインポートし、次のコマンドを実行します。

   ```
   ```

   ```
   sudo apt-get install dpkg-sig

   gpg --import <path to the public key>

   dpkg-sig --verify <path to the Linux VDA package>
   ```

   ```

### 手順6：Linux VDAのインストール

#### 手順6a：Linux VDAのインストール

Debianパッケージマネージャーを使用してLinux VDAソフトウェアをインストールします。

**Ubuntu 22.04の場合：**

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

**Ubuntu 20.04の場合：**

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

> **注:**
>
> GCP上のUbuntu 20.04では、RDNSを無効にします。これを行うには、/etc/krb5.confの**の下にrdns = false**の行を追加します。

> **Ubuntu 18.04の場合：**
```

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Ubuntu 22.04のDebian依存関係リスト：

```
openjdk-11-jdk >= 11


imagemagick >= 8:6.9.11


libgtkmm-3.0-1v5 >= 3.24.5


ufw >= 0.36


ubuntu-desktop >= 1.481


libxrandr2 >= 2:1.5.2


libxtst6 >= 2:1.2.3


libxm4 >= 2.3.8


util-linux >= 2.37


gtk3-nocsd >= 3
```

```
bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~
```

```
libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4
```

Ubuntu 20.04のDebian依存関係リスト：

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34
```

```
gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.49
```

```
libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

libimlib2 >= 1.6.1
```

Ubuntu 18.04のDebian依存関係リスト：

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.8.9.9

ufw >= 0.35

libgtkmm-3.0-1v5 >= 3.22.2

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2
```

```
libxm4 >= 2.3.4

util-linux >= 2.27.1

gtk3-nocsd >= 3

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libmspack0 >= 0.6

ibus >= 1.5

libsasl2-modules-gssapi-mit >= 2.1.~

libgoogle-perftools4 >= 2.4~
```

```
libpython3.6 >= 3.6~


libnss3-tools >= 2:3.35


libqt5widgets5 >= 5.7~


libqrencode3 >= 3.4.4


libimlib2 >= 1.4.10
```

注:

このバージョンのLinux VDAがサポートするLinuxディストリビューションとXorgバージョンのマトリックスについては、「システム要件」を参照してください。

ステップ 6b: Linux VDA をアップグレードする (オプション)

既存のインストールを、以前の2つのバージョンおよびLTSRリリースからアップグレードできます。

```
sudo dpkg -i <PATH>/<Linux VDA deb>
```

注:

既存のインストールをアップグレードすると、/etc/xdl の下の構成ファイルが上書きされます。アップグレードを実行する前に、ファイルをバックアップしてください。

ステップ 7: NVIDIA GRID ドライバーをインストールする

HDX 3D Pro を有効にするには、ハイパーバイザーとVDAマシンにNVIDIA GRIDドライバーをインストールする必要があります。

特定のハイパーバイザーにNVIDIA GRID Virtual GPU Manager（ホストドライバー）をインストールして構成するには、次のガイドを参照してください。

- シトリックス ハイパーバイザー
- ヴイエムウェア ESX
- ニュータニックス AHV

NVIDIA GRIDゲストVMドライバーをインストールして構成するには、次の一般的な手順を実行します。

1. ゲストVMがシャットダウンされていることを確認します。
2. ハイパーバイザーのコントロールパネルで、VMにGPUを割り当てます。
3. VMを起動します。
4. VMにゲストVMドライバーをインストールします。

ステップ 8: Linux VDA を構成する

> **注:**

> ランタイム環境をセットアップする前に、OSに **en_US.UTF-8** ロケールがインストールされていることを確認してください。OSでロケールが利用できない場合は、**sudo locale-gen en_US.UTF-8** コマンドを実行します。Debianの場合、**/etc/locale.gen** ファイルを編集して **# en_US.UTF-8 UTF-8** の行のコメントを解除し、**sudo locale-gen** コマンドを実行します。

> パッケージのインストール後、ctxsetup.sh スクリプトを実行してLinux VDAを構成する必要があります。変更を加える前に、スクリプトは環境を検証し、すべての依存関係がインストールされていることを確認します。必要に応じて、いつでもスクリプトを再実行して設定を変更できます。

スクリプトは、プロンプトに従って手動で実行することも、事前設定された応答で自動的に実行することもできます。続行する前に、スクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

プロンプトによる構成

プロンプトによる質問で手動構成を実行します。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

自動構成

自動インストールの場合、セットアップスクリプトで必要なオプションは環境変数で指定できます。必要なすべての変数が存在する場合、スクリプトはユーザーに情報を要求せず、スクリプトによるインストールプロセスが可能になります。

サポートされている環境変数には、次のものがあります。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Linux VDAは、DNS CNAMEレコードを使用してDelivery Controller名を指定することをサポートしています。デフォルトではNに設定されています。
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Linux VDAは、Delivery Controllerに登録するために、スペース区切りのDelivery Controllerの完全修飾ドメイン名（FQDN）のリストを必要とします。少なくとも1つのFQDNまたはCNAMEエイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT=port-number** – Linux VDAは、TCP/IPポートを介してDelivery Controllerと通信します。デフォルトではポート80です。
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Linux VDAサービスは、マシンの起動後に開始されます。デフォルトではYに設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Linux VDAサービスは、システムファイアウォールを介して受信ネットワーク接続が許可される必要があります。Linux VDAのシステムファイアウォールで、必要なポート（デフォルトではポート80と1494）を自動的に開くことができます。デフォルトではYに設定されています。
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Linux VDAは、Delivery Controllerで認証するためにKerberos構成設定を必要とします。Kerberos構成は、システムにインストールおよび構成されているActive Directory統合ツールから決定されます。
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Linux VDAは、リッチグラフィックアプリケーションの仮想化を最適化するために設計されたGPUアクセラレーションテクノロジーのセットであるHDX 3D Proをサポートしています。HDX 3D Proが選択されている場合、VDAはVDIデスクトップ（シングルセッション）モード（つまり、CTX_XDL_VDI_MODE=Y）用に構成されます。

- **CTX_XDL_VDI_MODE=Y \| N** – マシンを専用デスクトップ配信モデル（VDI）として構成するか、ホスト型共有デスクトップ配信モデルとして構成するか。HDX 3D Pro環境では、この変数をYに設定します。この変数はデフォルトでNに設定されています。
- **CTX_XDL_SITE_NAME=dns-name** – Linux VDAは、DNSを介してLDAPサーバーを検出します。DNS検索結果をローカルサイトに制限するには、DNSサイト名を指定します。この変数はデフォルトで**\<none\>**に設定されています。
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Linux VDAはDNSを照会してLDAPサーバーを検出します。DNSがLDAPサービスレコードを提供できない場合は、LDAPポートを持つLDAP FQDNのスペース区切りリストを指定できます。例：ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268。LDAPポート番号を389として指定した場合、Linux VDAは指定されたドメイン内の各LDAPサーバーをポーリングモードで照会します。ポリシーがx個、LDAPサーバーがy個ある場合、Linux VDAはXにYを乗じた合計数のクエリを実行します。ポーリング時間がしきい値を超えると、セッションログオンが失敗する可能性があります。より高速なLDAPクエリを有効にするには、ドメインコントローラーで**グローバルカタログ**を有効にし、関連するLDAPポート番号を3268として指定します。この変数は、デフォルトで**\<none\>**に設定されています。
- **CTX_XDL_SEARCH_BASE=search-base-set** – Linux VDAは、Active Directoryドメインのルートに設定された検索ベースを介してLDAPを照会します（例：DC=mycompany,DC=com）。ただし、検索パフォーマンスを向上させるために、検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。この変数は、デフォルトで**\<none\>**に設定されています。
- **CTX_XDL_FAS_LIST='list-fas-servers'** – フェデレーション認証サービス（FAS）サーバーは、ADグループポリシーを介して構成されます。Linux VDAはADグループポリシーをサポートしていませんが、代わりにFASサーバーのセミコロン区切りリストを提供できます。シーケンスは、ADグループポリシーで構成されているものと同じである必要があります。サーバーアドレスが削除された場合は、その空白を**\<none\>**というテキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。FASサーバーと適切に通信するには、FASサーバーで指定されているものと一致するポート番号を追加してください。例：CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – 新しいブローカーエージェントサービス (`ctxvda`) をサポートするための.NET Runtime 6.0のインストールパス。デフォルトのパスは/usr/binです。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – セッションで使用するGNOME、GNOME Classic、またはMATEデスクトップ環境を指定します。変数を指定しない場合、VDAに現在インストールされているデスクトップが使用されます。ただし、現在イン

ストールされているデスクトップがMATEである場合は、変数の値を**mate**に設定する必要があります。

ターゲットセッションユーザーのデスクトップ環境は、次の手順で変更することもできます。

a. VDA上の**$HOME/<username\>**ディレクトリの下に`.xsession`ファイルを作成します。

   2\. ディストリビューションに基づいてデスクトップ環境を指定するように、`.xsession`ファイルを編集します。

   - **MATEデスクトップの場合**

```
MSESSION="$(type -p mate-session)"



if [ -n "$MSESSION" ]; then

  exec mate-session



fi
```

   - **GNOME Classicデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

export GNOME_SHELL_SESSION_MODE=classic



exec gnome-session --session=gnome-classic

fi
```

   - **GNOMEデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

exec gnome-session



fi
```

b. ターゲットセッションユーザーと700のファイル権限を共有します。

バージョン2209以降、セッションユーザーはデスクトップ環境をカスタマイズできます。この機能を有効にするには、VDAに切り替え可能なデスクトップ環境を事前にインストールする必要があります。詳しくは、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

- **CTX_XDL_START_SERVICE=Y \| N** – Linux VDAの構成が完了したときにLinux VDAサービスが開始されるかどうか。デフォルトではYに設定されています。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scoutをリッスンするためのソケットポート。デフォルトのポートは7503です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scout と通信するためのポート。デフォルトのポートは7502です。

環境変数を設定し、構成スクリプトを実行します。

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N



export CTX_XDL_DDC_LIST='list-ddc-fqdns'



export CTX_XDL_VDA_PORT=port-number



export CTX_XDL_REGISTER_SERVICE=Y|N
```

```
export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate |
'<none>'
```

```
export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number


export CTX_XDL_TELEMETRY_PORT=port-number


export CTX_XDL_START_SERVICE=Y|N


sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

sudoコマンドを実行するときは、既存の環境変数を新しく作成するシェルに渡すために、**-E**オプションを入力します。最初の行に**#\!/bin/bash**を記述して、上記のコマンドからシェルスクリプトファイルを作成することをお勧めします。

または、単一のコマンドを使用してすべてのパラメーターを指定することもできます。

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \


CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \
```

```
CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \
```

```
/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

構成の変更を削除する

シナリオによっては、Linux VDAパッケージをアンインストールせずに、**ctxsetup.sh**スクリプトによって行われた構成の変更を削除する必要がある場合があります。

続行する前に、このスクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

構成の変更を削除するには：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

重要:

このスクリプトは、データベースからすべての構成データを削除し、Linux VDAを動作不能にします。

構成ログ

ctxsetup.shおよび**ctxcleanup.sh**スクリプトは、コンソールにエラーを表示し、追加情報は構成ログファイル**/tmp/xdl.configure.log**に書き込まれます。

変更を有効にするには、Linux VDAサービスを再起動します。

Linux VDAソフトウェアをアンインストールする

Linux VDAがインストールされているかどうかを確認し、インストールされているパッケージのバージョンを表示するには：

```
dpkg -l xendesktopvda
```

詳細情報を表示するには：

```
apt-cache show xendesktopvda
```

Linux VDAソフトウェアをアンインストールするには：

```
dpkg -r xendesktopvda
```

注:

Linux VDAソフトウェアをアンインストールすると、関連するPostgreSQLおよびその他の構成データが削除されます。ただし、Linux VDAのインストール前に設定されたPostgreSQLパッケージおよびその他の依存パッケージは削除されません。

ヒント:

このセクションの情報には、PostgreSQLを含む依存パッケージの削除は含まれていません。

ステップ9：XDPingを実行する

Linux VDA環境で一般的な構成の問題を確認するには、`sudo /opt/Citrix/VDA/bin/xdping`を実行します。詳細については、XDPingを参照してください。

ステップ10：Linux VDAを実行する

ctxsetup.shスクリプトを使用してLinux VDAを構成したら、以下のコマンドを使用してLinux VDAを制御します。

Linux VDAを開始する：

Linux VDAサービスを開始するには：

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDAを停止する：

Linux VDAサービスを停止するには：

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

注:

`ctxvda` および `ctxhdx` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止してください。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

Linux VDAを再起動する：

Linux VDAサービスを再起動するには：

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Linux VDAのステータスを確認する：

Linux VDA サービスの実行状態を確認するには:

```
sudo systemctl status ctxvda



sudo systemctl status ctxhdx
```

ステップ 11: マシンカタログを作成する

マシンカタログを作成し、Linux VDA マシンを追加するプロセスは、従来の Windows VDA のアプローチと似ています。これらのタスクを完了する方法の詳細については、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

Linux VDA マシンを含むマシンカタログを作成する場合、Windows VDA マシン用のマシンカタログを作成するプロセスとは異なるいくつかの制限があります。

- オペレーティングシステムには、以下を選択します。
  - ホストされた共有デスクトップ配信モデルの場合は、**マルチセッション OS** オプション。
  - VDI 専用デスクトップ配信モデルの場合は、**シングルセッション OS** オプション。
- 同じマシンカタログ内で Linux VDA マシンと Windows VDA マシンを混在させないでください。

> **注:**
>
> Citrix Studio の初期バージョンでは、「Linux OS」という概念はサポートされていませんでした。ただし、**Windows Server OS** または **Server OS** オプションを選択すると、同等のホストされた共有デスクトップ配信モデルが意味されます。**Windows Desktop OS** または **Desktop OS** オプションを選択すると、マシンあたり単一ユーザーの配信モデルが意味されます。

> **ヒント:**
>
> マシンを Active Directory ドメインから削除して再参加させる場合は、そのマシンをマシンカタログから削除し、再度追加する必要があります。

ステップ 12: デリバリーグループを作成する

デリバリーグループを作成し、Linux VDA マシンを含むマシンカタログを追加するプロセスは、Windows VDA マシンの場合とほぼ同じです。これらのタスクを完了する方法の詳細については、「デリバリーグループの作成」を参照してください。

Linux VDA マシンカタログを含むデリバリーグループを作成する場合、以下の制限が適用されます。

- 選択した AD ユーザーとグループが、Linux VDA マシンにログオンできるように適切に構成されていることを確認してください。
- 認証されていない（匿名）ユーザーのログオンは許可しないでください。
- デリバリーグループとWindowsマシンを含むマシンカタログを混在させないでください。

マシンカタログとデリバリーグループの作成方法については、「Citrix Virtual Apps and Desktops 7 2303」を参照してください。

Debian に Linux VDA を手動でインストールする

> **重要:**

> 新規インストールの場合、迅速なインストールには 簡易インストール を使用することをお勧めします。簡易インストールは、この記事で詳述されている手動インストールよりも時間と労力を節約でき、エラーが発生しにくいです。

ステップ 1：構成情報と Linux マシンを準備する

ステップ 1a：ネットワーク構成を確認する

ネットワークが接続され、正しく構成されていることを確認します。たとえば、Linux VDA で DNS サーバーを構成するには、次のコマンドを実行します。

```
echo "nameserver <dns ip address>" > "/etc/resolv.conf.custom"

echo "#!/bin/bash

    #

    # Description: script to override default resolv.conf file

    # with customized file.

    cp -f /etc/resolv.conf.custom /etc/resolv.conf">"/etc/NetworkManager/
dispatcher.d/15-resolv"



chmod +x /etc/NetworkManager/dispatcher.d/15-resolv
```

ステップ 1b：ホスト名を設定する

マシンのホスト名が正しく報告されるように、**/etc/hostname** ファイルをマシンのホスト名のみを含むように変更します。

`hostname`

ステップ 1c：ホスト名にループバックアドレスを割り当てる

マシンの DNS ドメイン名と完全修飾ドメイン名 (FQDN) が正しく報告されることを確認します。その方法は、**/etc/hosts** ファイルの次の行を、FQDN とホスト名を最初の 2 つのエントリとして含むように変更することです。

`127.0.0.1 hostname-fqdn hostname localhost`

例:

`127.0.0.1 vda01.example.com vda01 localhost`

ファイル内の他のエントリから `hostname-fqdn` または `hostname` への他の参照を削除します。

> **注:**
>
> Linux VDA は現在、NetBIOS 名の切り捨てをサポートしていません。ホスト名は 15 文字を超えてはなりません。

> **ヒント:**
>
> 使用できる文字はa～z、A～Z、0～9、ハイフン(-)のみです。アンダーバー(_)、スペース、その他の記号は避けてください。ホスト名を数字で始めたり、ハイフンで終わらせたりしないでください。このルールはDelivery Controllerのホスト名にも適用されます。

ステップ 1d：ホスト名を確認する

マシンを再起動し、ホスト名が正しく設定されていることを確認します。

```
hostname
```

このコマンドは、マシンのホスト名のみを返し、FQDN は返しません。

FQDNが正しく設定されていることを確認します。

```
hostname -f
```

このコマンドは、マシンのFQDNを返します。

手順1e：マルチキャストDNSを無効にする

デフォルト設定ではマルチキャストDNS（**mDNS**）が有効になっており、名前解決の結果が一貫しない場合があります。

mDNSを無効にするには、**/etc/nsswitch.conf**を編集し、次の行を変更します。

`hosts: files mdns_minimal [NOTFOUND=return] dns`

変更後：

`hosts: files dns`

手順1f：名前解決とサービス到達可能性を確認する

FQDNを解決し、ドメインコントローラーとDelivery Controller™にpingできることを確認します。

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

FQDNを解決できない場合、またはこれらのマシンのいずれかにpingできない場合は、続行する前に手順を確認してください。

手順1g：クロック同期を構成する（chrony）

VDA、Delivery Controller、およびドメインコントローラー間で正確なクロック同期を維持することは非常に重要です。Linux VDAを仮想マシン（VM）としてホストすると、クロックスキューの

問題が発生する可能性があります。このため、リモート時刻サービスとの時刻同期が推奨されます。

chronyをインストールします。

```
apt-get install chrony
```

rootユーザーとして、**/etc/chrony/chrony.conf**を編集し、各リモートタイムサーバーのサーバーエントリを追加します。

`server peer1-fqdn-or-ip-address iburst`

`server peer2-fqdn-or-ip-address iburst`

一般的な展開では、パブリックNTPプールサーバーから直接ではなく、ローカルのドメインコントローラーから時刻を同期します。ドメイン内の各Active Directoryドメインコントローラーのサーバーエントリを追加します。

ループバックIPアドレス、localhost、およびパブリックサーバーの***.pool.ntp.org**エントリを含む、リストされている他の**server**または**pool**エントリをすべて削除します。

変更を保存し、Chronyデーモンを再起動します:

```
sudo systemctl restart chrony
```

ステップ1h: パッケージをインストールする

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libgtk2.0-0
```

ステップ1i: 必要な依存関係をインストールするためのリポジトリを追加する

Debian 11.3の場合、/etc/apt/sources.list ファイルに `deb http://deb.debian.org/debian/ bullseye main` の行を追加します。

ステップ1j: 使用するデータベースをインストールして指定する

実験的な機能として、PostgreSQLに加えてSQLiteを使用できます。Linux VDAパッケージのインストール後、`/etc/xdl/db.conf` を編集することでSQLiteとPostgreSQLを切り替えることもで

きます。手動インストールの場合、それらを切り替える前にSQLiteとPostgreSQLを手動でインストールする必要があります。

このセクションでは、PostgreSQLおよびSQLiteデータベースのインストール方法と、使用するデータベースの指定方法について説明します。

> **注:**
>
> VDIモードでのみSQLiteを使用することをお勧めします。

POSTGRESQLをインストールする

PostgreSQLをインストールするには、次のコマンドを実行します:

```
sudo apt-get update



sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

マシンの起動時または即座にPostgreSQLを開始するには、それぞれ次のコマンドを実行します:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

SQLITEをインストールする

Debianの場合、SQLiteをインストールするには次のコマンドを実行します:

```
sudo apt-get install -y sqlite3
```

使用するデータベースを指定する

Linux VDAパッケージのインストール後、 `/etc/xdl/db.conf` を編集して使用するデータベースを指定できます。これを行うには、次の手順を完了します:

1. `/opt/Citrix/VDA/sbin/ctxcleanup.sh`を実行します。新規インストールの場合、この手順は省略してください。
2. 使用するデータベースを指定するために、`/etc/xdl/db.conf`を編集します。
3. `ctxsetup.sh`を実行します。

> **注:**
>
> PostgreSQLのポート番号を構成するには、**/etc/xdl/db.conf**を使用することもできます。

ステップ2：ハイパーバイザーの準備

サポートされているハイパーバイザー上でLinux VDAをVMとして実行する場合、いくつかの変更が必要です。使用しているハイパーバイザープラットフォームに基づいて、以下の変更を行ってください。Linuxマシンをベアメタルハードウェアで実行している場合、変更は不要です。

Citrix Hypervisor™での時刻同期の修正

Citrix Hypervisorの時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとCitrix Hypervisorの両方で問題が発生します。両方ともシステムクロックを管理しようとします。クロックが他のサーバーと同期しなくなるのを避けるため、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホストの時刻同期を無効にする必要があります。HVMモードでは変更は不要です。

Citrix VM Toolsがインストールされた準仮想化Linuxカーネルを実行している場合、Linux VM内からCitrix Hypervisorの時刻同期機能が存在し、有効になっているかどうかを確認できます。

```
su -

cat /proc/sys/xen/independent_wallclock
```

このコマンドは0または1を返します。

- 0 - 時刻同期機能が有効になっており、無効にする必要があります。
- 1 - 時刻同期機能は無効になっており、それ以上の操作は不要です。

/proc/sys/xen/independent_wallclockファイルが存在しない場合、以下の手順は不要です。

有効になっている場合、ファイルに1を書き込むことで時刻同期機能を無効にします。

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

この変更を永続的にし、再起動後も維持するには、**/etc/sysctl.confファイル**を編集して次の行を追加します。

```
xen.independent_wallclock = 1
```

これらの変更を確認するには、システムを再起動します。

```
su -

cat /proc/sys/xen/independent_wallclock
```

このコマンドは値1を返します。

Microsoft Hyper-Vでの時刻同期の修正

Hyper-V Linux Integration Servicesがインストールされ ているLinux VMは、Hyper-Vの時刻同期機能を使用してホストオペレーティングシステムの時刻を使用できます。システムクロックが正確に保たれるように、NTPサービスと並行してこの機能を有効にしてください。

管理オペレーティングシステムから：

1. Hyper-Vマネージャーコンソールを開きます。
2. Linux VMの設定で、**統合サービス**を選択します。
3. **時刻同期**が選択されていることを確認します。

> **注:**
>
> このアプローチは、NTPとの競合を避けるためにホスト時刻同期が無効になっているVMwareおよびCitrix Hypervisorとは異なります。Hyper-Vの時刻同期は、NTP時刻同期と共存し、それを補完することができます。

ESXおよびESXiでの時刻同期の修正

VMwareの時刻同期機能が有効になっている場合、各準仮想化Linux VM内でNTPとハイパーバイザーとの間で問題が発生します。両方ともシステムクロックを同期しようとします。クロックが他のサーバーと同期しなくなるのを避けるために、各Linuxゲスト内のシステムクロックがNTPと同期していることを確認してください。この場合、ホスト時刻同期を無効にする必要があります。

VMware Toolsがインストールされた準仮想化Linuxカーネルを実行している場合：

1. vSphere Clientを開きます。
2. Linux VMの設定を編集します。
3. **仮想マシンのプロパティ**ダイアログで、**オプション**タブを開きます。
4. **VMware Tools**を選択します。
5. 「**詳細設定**」ボックスで、「**ゲストの時刻をホストと同期する**」のチェックを外します。

ステップ3: Linux VMをWindowsドメインに追加する

LinuxマシンをActive Directory (AD) ドメインに追加するには、以下の方法が利用可能です:

- サンバ Winbind
- セントリファイ DirectControl
- SSSD
- PBIS

選択した方法に基づいて手順に従ってください。

> **注:**
>
> Linux VDAのローカルアカウントとADのアカウントで同じユーザー名が使用されている場合、セッションの起動に失敗する可能性があります。

サンバ Winbind

必要なパッケージをインストールまたは更新する

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

マシンの起動時にWINBINDデーモンが起動するように有効にする

Winbindデーモンは、マシンの起動時に開始するように構成する必要があります:

```
sudo systemctl enable winbind
```

> **注:**
>
> `/etc/init.d` の下に `winbind` スクリプトがあることを確認してください。

KERBEROSを構成する

ルートユーザーとして **/etc/krb5.conf** を開き、次の設定を行います。

> **注:**
>
> ADインフラストラクチャに基づいてKerberosを構成します。以下の設定は、単一ドメイン、単一フォレストモデルを対象としています。

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` *`REALM`*

`.domain-dns-name` `=` *`REALM`*

このコンテキストでの **domain-dns-name** パラメーターは、**example.com** のようなDNSドメイン名です。**REALM** は、**EXAMPLE.COM** のような大文字のKerberosレルム名です。

WINBIND認証を構成する

vim /etc/samba/smb.conf コマンドを実行して **/etc/samba/smb.conf** を開き、次の設定を行います。

`[global]`

`workgroup =` *`WORKGROUP`*

`security = ADS`

`realm =` *`REALM`*

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`winbind trusted domains only = no`

`kerberos method = secrets and keytab`

`winbind refresh tickets = yes`

`template shell = /bin/bash`

WORKGROUP は *REALM* の最初のフィールドであり、*REALM* は大文字のKerberosレルム名です。

NSSWITCH を構成する

「**/etc/nsswitch.conf**」を開き、次の行に`winbind`を追加します。

`passwd: systemd winbind`

`group: systemd winbind`

WINDOWSドメインへの参加

ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
sudo net ads join <Kerberos realm name in uppercase> -U <domain user with
permission to add computers to the domain>
```

WINBINDの再起動

```
sudo systemctl restart winbind
```

WINBINDのPAMを構成する

次のコマンドを実行し、**Winbind NT/Active Directory認証**と**ログイン時にホームディレクトリを作成**オプションが選択されていることを確認します。

```
sudo pam-auth-update
```

ヒント:

winbindデーモンは、マシンがドメインに参加している場合にのみ実行され続けます。

ドメインメンバーシップの確認

Delivery Controllerは、WindowsまたはLinuxのすべてのVDAマシンが`Active Directory`にコンピューターオブジェクトを持っていることを要求します。

Sambaの**net ads**コマンドを実行して、マシンがドメインに参加していることを確認します。

```
sudo net ads testjoin
```

追加のドメインおよびコンピューターオブジェクト情報を確認するには、次のコマンドを実行します。

```
sudo net ads info
```

KERBEROS構成の確認

KerberosがLinux VDAで使用するために正しく構成されていることを確認するには、システム**keytab**ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してドメインコントローラーでマシンを認証するには、Kerberos **kinit**コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェル置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNSドメイン名がKerberosレルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントのTGTチケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist
```

次を使用して、マシンのアカウントの詳細を調べます。

```
sudo net ads status
```

ユーザー認証の確認

wbinfo ツールを使用して、ドメインユーザーがドメインで認証できることを確認します。

```
wbinfo --krb5auth=domain\\username%password
```

ここで指定するドメインはADドメイン名であり、Kerberosレルム名ではありません。bashシェルでは、バックスラッシュ (\\) 文字は別のバックスラッシュでエスケープする必要があります。このコマンドは、成功または失敗を示すメッセージを返します。

Winbind PAMモジュールが正しく構成されていることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u
```

注:

> SSHコマンドを正常に実行するには、SSHが有効になっており、正しく機能していることを確認してください。

> **id -u** コマンドによって返されたuidに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

ユーザーのKerberos資格情報キャッシュ内のチケットが有効であり、期限切れになっていないことを確認します。

```
klist
```

セッションを終了します。

```
exit
```

同様のテストは、GnomeまたはKDEコンソールに直接ログオンすることで実行できます。ドメイン参加の確認後、(/ja-jp/linux-virtual-delivery-agent/2303/installation-overview/manual-installation-overview/debian.html#step-6-install-the-linux-vda)に進みます。

> **ヒント:**

> ユーザー認証に成功しても、ドメインアカウントでログオンしたときにデスクトップが表示されない場合は、マシンを再起動してもう一度試してください。

Quest認証サービス

ドメインコントローラーでのQUESTの構成

Active Directoryドメインコントローラーにソフトウェアをインストールして構成し、`Active Directory`でコンピューターオブジェクトを作成するための管理者権限が付与されていることを前提とします。

ドメインユーザーがLINUX VDAマシンにログオンできるようにする

ドメインユーザーがLinux VDAマシンでHDX™セッションを確立できるようにするには、次の手順を実行します。

1. Active Directoryユーザーとコンピューター管理コンソールで、そのユーザーアカウントのActive Directoryユーザープロパティを開きます。
2. **Unixアカウント**タブを選択します。
3. **Unix-enabled**をオンにします。
4. **Primary GID Number**を実際のドメインユーザーグループのグループIDに設定します。

> **注:**
>
> これらの手順は、コンソール、RDP、SSH、またはその他のリモートプロトコルを使用してログオンするドメインユーザーを設定する場合にも同様に適用されます。

LINUX VDAでQUESTを構成する

SELinuxポリシーの適用を回避する
デフォルトのRHEL環境では、SELinuxが完全に適用されています。この適用により、Questが使用するUnixドメインソケットIPCメカニズムが妨害され、ドメインユーザーがログオンできなくなります。

この問題を回避する便利な方法は、SELinuxを無効にすることです。rootユーザーとして、***/etc/selinux/config***を編集し、**SELinux**設定を変更します。

```
SELINUX=disabled
```

この変更にはマシンの再起動が必要です。

```
reboot
```

> **重要:**
>
> この設定は慎重に使用してください。無効にした後にSELinuxポリシーの適用を再度有効にすると、rootユーザーや他のローカルユーザーであっても完全にロックアウトされる可能性があります。

VASデーモンを構成する
Kerberosチケットの自動更新は有効にして切断する必要があります。認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

このコマンドは、更新間隔を9時間（32,400秒）に設定します。これは、デフォルトの10時間のチケット有効期間より1時間短いです。チケット有効期間が短いシステムでは、このパラメーターをより低い値に設定してください。

PAMとNSSを構成する

HDXおよびsu、ssh、RDPなどの他のサービスを介したドメインユーザーログオンを有効にするには、次のコマンドを実行してPAMとNSSを手動で構成します。

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
```

WINDOWSドメインに参加する

Quest `vastool` コマンドを使用して、LinuxマシンをActive Directoryドメインに参加させます。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

ユーザーは、コンピューターをActive Directoryドメインに参加させる権限を持つドメインユーザーです。`domain-name` はドメインのDNS名です（例: example.com）。

ドメインメンバーシップを確認する

Delivery Controllerは、WindowsまたはLinuxにかかわらず、すべてのVDAマシンが `Active Directory` にコンピューターオブジェクトを持つことを要求します。Questで参加したLinuxマシンがドメイン上にあることを確認するには、次の手順を実行します。

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合、このコマンドはドメイン名を返します。マシンがどのドメインにも参加していない場合、次のエラーが表示されます。

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

ユーザー認証を確認する

QuestがPAMを介してドメインユーザーを認証できることを確認するには、これまで使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u
```

id -u コマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

Kerberos資格情報キャッシュ内のチケットが有効で、期限切れになっていないことを確認します。

```
/opt/quest/bin/vastool klist
```

セッションを終了します。

```
exit
```

ドメイン参加の確認後、手順6: Linux VDAをインストールする に進みます。

セントリファイ ダイレクトコントロール

WINDOWSドメインへの参加

Centrify DirectControl Agentがインストールされたら、Centrify `adjoin` コマンドを使用してLinuxマシンをActive Directoryドメインに参加させます。

```
su -

adjoin -w -V -u user domain-name
```

userパラメーターは、コンピューターをActive Directoryドメインに参加させる権限を持つActive Directoryドメインユーザーです。**domain-name**パラメーターは、Linuxマシンを参加させるドメインの名前です。

ドメインメンバーシップの確認

Delivery Controllerは、WindowsまたはLinuxにかかわらず、すべてのVDAマシンがActive Directoryにコンピューターオブジェクトを持つことを要求します。Centrifyに参加したLinuxマシンがドメイン上にあることを確認するには、次の手順を実行します。

```
su –



adinfo
```

Joined to domainの値が有効であり、**CentrifyDC mode**が**connected**を返すことを確認します。モードが開始状態のままになっている場合、Centrifyクライアントはサーバー接続または認証の問題を抱えています。

より包括的なシステムおよび診断情報は、以下を使用して利用できます。

```
adinfo --sysinfo all



adinfo --diag
```

さまざまなActive DirectoryおよびKerberosサービスへの接続をテストします。

```
adinfo --test
```

ドメイン参加の確認後、(/ja-jp/linux-virtual-delivery-agent/2303/installation-overview/manual-installation-overview/debian.html#step-6-install-the-linux-vda)に進みます。

SSSD

KERBEROSの構成

Kerberosをインストールするには、次のコマンドを実行します。

```
sudo apt-get install krb5-user
```

Kerberosを構成するには、rootとして**/etc/krb5.conf**を開き、パラメーターを設定します。

> **注:**
>
> ADインフラストラクチャに基づいてKerberosを構成します。以下の設定は、単一ドメイン、単一フォレストモデルを対象としています。

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`rdns = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` *`REALM`*

`.domain-dns-name` `=` *`REALM`*

このコンテキストでの`domain-dns-name`パラメーターは、example.comのようなDNSドメイン名です。*REALM*は、EXAMPLE.COMのような大文字のKerberosレルム名です。

ドメインに参加する

SSSDは、IDプロバイダーとしてActive Directoryを、認証にKerberosを使用するように構成する必要があります。ただし、SSSDはドメインへの参加やシステムキータブファイルの管理のための

ADクライアント機能を提供しません。代わりに、**adcli**、**realmd**、または**Samba**を使用できます。

> **注:**
>
> このセクションでは、**adcli**と**Samba**に関する情報のみを提供します。

- **adcliを使用してドメインに参加する場合は、次の手順を実行します。**

1. **adcli**をインストールします。

   ```
   sudo apt-get install adcli
   ```

2. **adcli**を使用してドメインに参加します。

   古いシステムキータブファイルを削除し、以下を使用してドメインに参加します。

   ```
   su -



   rm -rf /etc/krb5.keytab



   adcli join domain-dns-name -U user -H hostname-fqdn
   ```

   userは、マシンをドメインに追加する権限を持つドメインユーザーです。**hostname-fqdn**は、マシンのFQDN形式のホスト名です。

   「**-H** オプションは、Linux VDA が必要とする host/hostname-fqdn@REALM 形式で SPN を生成するために **adcli** に必要です。」.

3. 「システムキータブを確認します。」.

   「システムキータブファイルが作成されていることを確認するために、`sudo klist -ket` コマンドを実行します。」.

   「各キーのタイムスタンプが、マシンがドメインに参加した時刻と一致することを確認します。」.

- 「**Samba を使用してドメインに参加する場合は、次の手順を完了します。**」:

1. 「パッケージをインストールします。」.

```
sudo apt-get install samba krb5-user
```

2. 「**Samba** を構成します。」.

   「**/etc/samba/smb.conf** を開き、次の設定を行います。」:

   `[global]`

   「`workgroup =` *`WORKGROUP`*」

   `security = ADS`

   「`realm =` *`REALM`*」

   `client signing = yes`

   `client use spnego = yes`

   `kerberos method = secrets and keytab`

   「*WORKGROUP* は *REALM* の最初のフィールドであり、*REALM* は大文字の Kerberos レルム名です。」.

3. 「**Samba** を使用してドメインに参加します。」.

   「ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つ Windows アカウントが必要です。」.

```
sudo net ads join <the Kerberos realm name in uppercase> -U <domain
user with permission to add computers to the domain>
```

「SSSD をセットアップする」

「**必要なパッケージをインストールまたは更新します。**」:

必要なSSSDと構成パッケージがまだインストールされていない場合は、インストールします。

```
sudo apt-get install sssd
```

パッケージがすでにインストールされている場合は、更新することをお勧めします。

```
sudo apt-get install --only-upgrade sssd
```

SSSDを構成する

SSSDデーモンを開始する前に、SSSD構成の変更が必要です。SSSDの一部のバージョンでは、**/etc/sssd/sssd.conf** 構成ファイルはデフォルトでインストールされていないため、手動で作成する必要があります。rootとして、**/etc/sssd/sssd.conf** を作成または開き、次の設定を行います。

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/` *`domain-dns-name`* `]`

`id_provider = ad`

`access_provider = ad`

`auth_provider = krb5`

`krb5_realm =` *`REALM`*

`# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days`

`krb5_renewable_lifetime = 14d`

`# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours`

`krb5_renew_interval = 1h`

`krb5_ccachedir = /tmp`

`krb5_ccname_template = FILE:%d/krb5cc_%U`

`# This ldap_id_mapping setting is also the default value`

`ldap_id_mapping = true`

`override_homedir = /home/%d/%u`

`default_shell = /bin/bash`

`ad_gpo_map_remote_interactive = +ctxhdx`

> **注:**
>
> ldap_id_mapping は **true** に設定されており、SSSD自体がWindows SIDをUnix UIDにマッピングする処理を行います。そうでない場合、`Active Directory` はPOSIX拡張機能を提供できる必要があります。PAMサービス `ctxhdx` は ad_gpo_map_remote_interactive に追加されます。

> このコンテキストでの **domain-dns-name** パラメーターは、example.com のようなDNSドメイン名です。*REALM* は、EXAMPLE.COM のような大文字のKerberosレルム名です。NetBIOSドメイン名を構成する必要はありません。

> 構成設定の詳細については、sssd.conf および `sssd-ad` のmanページを参照してください。

> SSSDデーモンは、構成ファイルが所有者による読み取り権限のみを持つことを要求します。

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

SSSDデーモンを開始する

SSSDデーモンを今すぐ開始し、マシンの起動時にデーモンが開始されるようにするには、次のコマンドを実行します。

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM構成

次のコマンドを実行し、**SSS authentication** および **Create home directory on login** オプションが選択されていることを確認します。

```
sudo pam-auth-update
```

ドメインメンバーシップの確認

デリバリーコントローラーは、すべてのVDAマシン (WindowsおよびLinux VDA) が `Active Directory` にコンピューターオブジェクトを持っていることを必要とします。

- ドメインメンバーシップを確認するために**adcli**を使用する場合は、`sudo adcli info domain-dns-name` コマンドを実行してドメイン情報を表示します。
- ドメインメンバーシップを確認するために**Samba**を使用する場合は、`sudo net ads testjoin` コマンドを実行してマシンがドメインに参加していることを確認し、`sudo net ads info` コマンドを実行して追加のドメインおよびコンピューターオブジェクト情報を確認します。

KERBEROS構成の確認

Linux VDAで使用するためにKerberosが正しく構成されていることを確認するには、システムのkeytabファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。これらのキーを使用してドメインコントローラーでマシンを認証するには、Kerberos `kinit` コマンドを実行します。

```
sudo kinit -k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェル置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNSドメイン名がKerberosレルム名と異なる場合があります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントのTGTがキャッシュされていることを確認するには、以下を使用します。

```
sudo klist
```

ユーザー認証の確認

SSSDは、デーモンと直接認証をテストするためのコマンドラインツールを提供しておらず、PAMを介してのみ実行できます。

SSSD PAMモジュールが正しく構成されていることを確認するには、これまで使用されていないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
ssh localhost -l domain\\username



id -u



klist



exit
```

klistコマンドによって返されるKerberosチケットがそのユーザーに対して正しく、期限切れになっていないことを確認します。

rootユーザーとして、以前の**id -u**コマンドによって返されたuidに対応するチケットキャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

同様のテストは、KDEまたはGnome Display Managerにログオンすることで実行できます。ドメイン参加の確認後、手順6: Linux VDAをインストールするに進みます。

PBIS

必要なPBISパッケージをダウンロードする

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBISインストールスクリプトを実行可能にする

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBISインストールスクリプトを実行する

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

WINDOWSドメインに参加する

ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

userは、コンピューターをActive Directoryドメインに追加する権限を持つドメインユーザーです。**domain-name**は、ドメインのDNS名です（例：example.com）。

注：Bashをデフォルトシェルとして設定するには、**sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**コマンドを実行します。

ドメインメンバーシップを確認する

Delivery Controllerは、すべてのVDAマシン（WindowsおよびLinux VDA）が`Active Directory`にコンピューターオブジェクトを持つことを要求します。PBISに参加しているLinuxマシンがドメイン上にあることを確認するには：

```
/opt/pbis/bin/domainjoin-cli query
```

マシンがドメインに参加している場合、このコマンドは現在参加しているADドメインとOUに関する情報を返します。そうでない場合は、ホスト名のみが表示されます。

ユーザー認証を確認する

PBISがPAMを介してドメインユーザーを認証できることを確認するには、以前に使用したことのないドメインユーザーアカウントを使用してLinux VDAにログオンします。

```
sudo ssh localhost -l domain\\user



id -u
```

id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

セッションを終了します。

```
exit
```

ドメイン参加の検証後、手順 6: Linux VDA のインストール に進みます。

手順 4: .NET Runtime 6.0 をインストールする

Linux VDA をインストールする前に、`<https://docs.microsoft.com/ja-jp/dotnet/core/install/linux-package-managers>` の指示に従って .NET Runtime 6.0 をインストールします。

.NET Runtime 6.0 のインストール後、**which dotnet** コマンドを実行してランタイムパスを見つけます。

コマンドの出力に基づいて、.NET ランタイムバイナリパスを設定します。たとえば、コマンドの出力が /aa/bb/dotnet の場合、/aa/bb を .NET バイナリパスとして使用します。

手順 5: Linux VDA パッケージをダウンロードする

1. Citrix Virtual Apps and Desktops ダウンロードページ にアクセスします。
2. 適切なバージョンの Citrix Virtual Apps and Desktops を展開します。
3. **Components** をクリックして、お使いの Linux ディストリビューションに一致する Linux VDA パッケージと、Linux VDA パッケージの整合性を検証するために使用できる GPG 公開キーをダウンロードします。

   Linux VDA パッケージの整合性を検証するには、公開キーを DEB データベースにインポートし、次のコマンドを実行します。

   ```
   ```

   sudo apt-get install dpkg-sig

   gpg --import <path to the public key>

   dpkg-sig --verify <path to the Linux VDA package>

   ```
   ```

手順 6: Linux VDA をインストールする

手順 6a: Linux VDA をインストールする

Debian パッケージマネージャーを使用して Linux VDA ソフトウェアをインストールします。

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
```

Debian 11.3 の依存関係リスト:

```
openjdk-11-jdk >= 11


imagemagick >= 8:6.9.10


ufw >= 0.36


desktop-base >= 10.0.2


libxrandr2 >= 2:1.5.1


libxtst6 >= 2:1.2.3


libxm4 >= 2.3.8


util-linux >= 2.33


gtk3-nocsd >= 3
```

```
bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.9 >= 3.9~

libsasl2-modules-gssapi-mit >= 2.1.~

libqt5widgets5 >= 5.5~
```

```
mutter >= 3.38.6~

libqrencode4 >= 4.0.0

libimlib2 >= 1.5.1
```

注:

このバージョンの Linux VDA がサポートする Linux ディストリビューションと Xorg バージョンのマトリックスについては、システム要件 を参照してください。

ステップ 6b: Linux VDA のアップグレード (オプション)

既存のインストールを、以前の2つのバージョンおよびLTSRリリースからアップグレードできます。

```
sudo dpkg -i <PATH>/<Linux VDA deb>
```

注:

既存のインストールをアップグレードすると、/etc/xdl の下の構成ファイルが上書きされます。アップグレードを実行する前に、ファイルをバックアップしてください。

ステップ 7: NVIDIA GRID ドライバーのインストール

HDX 3D Pro を有効にするには、ハイパーバイザーとVDAマシンにNVIDIA GRID ドライバーをインストールする必要があります。

特定のハイパーバイザーにNVIDIA GRID Virtual GPU Manager (ホストドライバー) をインストールして構成するには、次のガイドを参照してください。

- シトリックス ハイパーバイザー

- ヴイエムウェア イーエスエックス
- ニュータニックス AHV

NVIDIA GRID ゲストVMドライバーをインストールして構成するには、次の一般的な手順を実行します。

1. ゲストVMがシャットダウンされていることを確認します。
2. ハイパーバイザーのコントロールパネルで、VMにGPUを割り当てます。
3. VMを起動します。
4. VMにゲストVMドライバーをインストールします。

ステップ 8: Linux VDA の構成

> **注:**

> ランタイム環境をセットアップする前に、**en_US.UTF-8** ロケールがOSにインストールされていることを確認してください。ロケールがOSで利用できない場合は、**sudo locale-gen en_US.UTF-8** コマンドを実行します。Debianの場合、**/etc/locale.gen** ファイルを編集し、**# en_US.UTF-8 UTF-8** の行のコメントを解除してから、**sudo locale-gen** コマンドを実行します。

> パッケージのインストール後、ctxsetup.sh スクリプトを実行してLinux VDAを構成する必要があります。変更を行う前に、スクリプトは環境を検証し、すべての依存関係がインストールされていることを確認します。必要に応じて、いつでもスクリプトを再実行して設定を変更できます。

スクリプトをプロンプトに従って手動で実行することも、事前設定された応答で自動的に実行することもできます。続行する前に、スクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

プロンプトによる構成

プロンプトによる質問で手動構成を実行します。

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

自動構成

自動インストールの場合、セットアップスクリプトで必要なオプションは環境変数で指定できます。必要なすべての変数が存在する場合、スクリプトはユーザーに情報を要求しないため、スクリプトによるインストールプロセスが可能になります。

サポートされている環境変数には、次のものがあります。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Linux VDAは、DNS CNAMEレコードを使用してDelivery Controller名を指定することをサポートしています。デフォルトではNに設定されています。
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Linux VDAは、Delivery Controllerに登録するために、スペースで区切られたDelivery Controllerの完全修飾ドメイン名（FQDN）のリストを必要とします。少なくとも1つのFQDNまたはCNAMEエイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT=port-number** – Linux VDAは、TCP/IPポートを介してDelivery Controllerと通信します。デフォルトではポート80です。
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Linux VDAサービスは、マシンの起動後に開始されます。デフォルトではYに設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Linux VDAサービスは、システムファイアウォールを介した受信ネットワーク接続を許可する必要があります。Linux VDAに必要なポート（デフォルトではポート80と1494）をシステムファイアウォールで自動的に開くことができます。デフォルトではYに設定されています。
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Linux VDAは、Delivery Controllerとの認証のためにKerberos構成設定を必要とします。Kerberos構成は、システムにインストールおよび構成されているActive Directory統合ツールから決定されます。
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Linux VDAは、リッチグラフィックアプリケーションの仮想化を最適化するために設計されたGPUアクセラレーションテクノロジーのセットであるHDX 3D Proをサポートしています。HDX 3D Proが選択されている場合、VDAはVDIデスクトップ（シングルセッション）モード（つまり、CTX_XDL_VDI_MODE=Y）用に構成されます。
- **CTX_XDL_VDI_MODE=Y \| N** – マシンを専用デスクトップ配信モデル（VDI）として構成するか、ホスト型共有デスクトップ配信モデルとして構成するか。HDX 3D Pro環境では、この変数をYに設定します。この変数はデフォルトでNに設定されています。
- **CTX_XDL_SITE_NAME=dns-name** – Linux VDAは、DNSを介してLDAPサーバーを検出します。DNS検索結果をローカルサイトに制限するには、DNSサイト名を指定します。この変数はデフォルトで**\<none\>**に設定されています。

- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Linux VDAはDNSにクエリを実行してLDAPサーバーを検出します。DNSがLDAPサービスレコードを提供できない場合、LDAPポートを含むLDAP FQDNのスペース区切りリストを指定できます。例：ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268。LDAPポート番号を389と指定した場合、Linux VDAは指定されたドメイン内の各LDAPサーバーにポーリングモードでクエリを実行します。ポリシーの数がx、LDAPサーバーの数がyの場合、Linux VDAはXにYを乗じた合計数のクエリを実行します。ポーリング時間がしきい値を超えると、セッションログオンが失敗する可能性があります。LDAPクエリを高速化するには、ドメインコントローラーで**グローバルカタログ**を有効にし、関連するLDAPポート番号を3268と指定します。この変数は、デフォルトで**\<none\>**に設定されています。
- **CTX_XDL_SEARCH_BASE=search-base-set** – Linux VDAは、Active Directoryドメインのルートに設定された検索ベース（例：DC=mycompany,DC=com）を介してLDAPにクエリを実行します。ただし、検索パフォーマンスを向上させるために、検索ベース（例：OU=VDI,DC=mycompany,DC=com）を指定できます。この変数は、デフォルトで**\<none\>**に設定されています。
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Federated Authentication Service (FAS) サーバーは、ADグループポリシーを介して構成されます。Linux VDAはADグループポリシーをサポートしていませんが、代わりにセミコロン区切りのFASサーバーのリストを提供できます。シーケンスはADグループポリシーで構成されているものと同じである必要があります。サーバーアドレスが削除された場合は、その空白を**\<none\>**というテキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。FASサーバーと適切に通信するには、FASサーバーで指定されているポート番号と一致するポート番号を追加してください。例：CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – 新しいブローカーエージェントサービス（`ctxvda`）をサポートするための.NET Runtime 6.0のインストールパス。デフォルトのパスは/usr/binです。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – セッションで使用するGNOME、GNOME Classic、またはMATEデスクトップ環境を指定します。この変数を指定しない場合、VDAに現在インストールされているデスクトップが使用されます。ただし、現在インストールされているデスクトップがMATEである場合は、変数の値を**mate**に設定する必要があります。

  ターゲットセッションユーザーのデスクトップ環境は、次の手順で変更することもできます。

  a. VDA上の**$HOME/<username\>**ディレクトリの下に`.xsession`ファイルを作成します。

2\. `.xsession` ファイルを編集して、ディストリビューションに基づいてデスクトップ環境を指定します。

- **MATEデスクトップの場合**

```
MSESSION="$(type -p mate-session)"



if [ -n "$MSESSION" ]; then

  exec mate-session



fi
```

- **GNOME Classicデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

export GNOME_SHELL_SESSION_MODE=classic



exec gnome-session --session=gnome-classic

fi
```

- **GNOMEデスクトップの場合**

```
GSESSION="$(type -p gnome-session)"



if [ -n "$GSESSION" ]; then

exec gnome-session
```

```
fi
```

b. ターゲットセッションユーザーと700ファイル権限を共有します。

バージョン2209以降、セッションユーザーはデスクトップ環境をカスタマイズできます。この機能を有効にするには、VDAに切り替え可能なデスクトップ環境を事前にインストールする必要があります。詳しくは、「セッションユーザーによるカスタムデスクトップ環境」を参照してください。

- **CTX_XDL_START_SERVICE=Y \| N** – Linux VDAの構成が完了したときにLinux VDAサービスを開始するかどうか。デフォルトではYに設定されています。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scoutをリッスンするためのソケットポート。デフォルトのポートは7503です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scout と通信するためのポート。デフォルトポートは 7502 です。

環境変数を設定し、構成スクリプトを実行します。

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N


export CTX_XDL_DDC_LIST='list-ddc-fqdns'


export CTX_XDL_VDA_PORT=port-number


export CTX_XDL_REGISTER_SERVICE=Y|N


export CTX_XDL_ADD_FIREWALL_RULES=Y|N


export CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis
```

```
export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate |
'<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number
```

```
export CTX_XDL_START_SERVICE=Y|N


sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

sudo コマンドを実行するときは、既存の環境変数を新しく作成されるシェルに渡すために、**-E** オプションを入力します。前述のコマンドから、最初の行に **#\!/bin/bash** を含むシェルスクリプトファイルを作成することをお勧めします。

または、単一のコマンドを使用してすべてのパラメーターを指定することもできます。

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \


CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \


CTX_XDL_HDX_3D_PRO=Y|N \


CTX_XDL_VDI_MODE=Y|N \
```

```
CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

構成の変更を削除する

シナリオによっては、Linux VDA パッケージをアンインストールせずに、**ctxsetup.sh** スクリプトによって行われた構成の変更を削除する必要がある場合があります。

続行する前に、このスクリプトに関するヘルプを確認してください。

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

構成の変更を削除するには：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

> **重要:**
>
> このスクリプトは、データベースからすべての構成データを削除し、Linux VDA を動作不能にします。

構成ログ

ctxsetup.sh および **ctxcleanup.sh** スクリプトは、コンソールにエラーを表示し、追加情報は構成ログファイル **/tmp/xdl.configure.log** に書き込まれます。

変更を有効にするには、Linux VDA サービスを再起動します。

Linux VDA ソフトウェアをアンインストールする

Linux VDA がインストールされているかどうかを確認し、インストールされているパッケージのバージョンを表示するには：

```
dpkg -l xendesktopvda
```

詳細情報を表示するには：

```
apt-cache show xendesktopvda
```

Linux VDAソフトウェアをアンインストールするには：

```
dpkg -r xendesktopvda
```

> **注:**

Linux VDAソフトウェアをアンインストールすると、関連するPostgreSQLおよびその他の構成データが削除されます。ただし、Linux VDAのインストール前に設定されたPostgreSQLパッケージおよびその他の依存パッケージは削除されません。

ヒント:

このセクションの情報には、PostgreSQLを含む依存パッケージの削除は含まれていません。

ステップ9：XDPingを実行する

Linux VDA環境で一般的な構成の問題を確認するには、`sudo /opt/Citrix/VDA/bin/xdping`を実行します。詳細については、XDPingを参照してください。

ステップ10：Linux VDAを実行する

ctxsetup.shスクリプトを使用してLinux VDAを構成したら、次のコマンドを使用してLinux VDAを制御します。

Linux VDAを開始する：

Linux VDAサービスを開始するには：

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDAを停止する：

Linux VDAサービスを停止するには：

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **注:**
>
> `ctxvda` および `ctxhdx` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止します。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

> **Linux VDAを再起動する：**

Linux VDAサービスを再起動するには：

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Linux VDAのステータスを確認する：

Linux VDAサービスの稼働状況を確認するには：

```
sudo systemctl status ctxvda



sudo systemctl status ctxhdx
```

ステップ11：マシンカタログを作成する

マシンカタログを作成し、Linux VDAマシンを追加するプロセスは、従来のWindows VDAのアプローチと似ています。これらのタスクを完了する方法の詳細については、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

Linux VDAマシンを含むマシンカタログを作成する場合、Windows VDAマシン用のマシンカタログを作成するプロセスとは異なるいくつかの制限があります。

- オペレーティングシステムについては、以下を選択します。

  - ホストされた共有デスクトップ配信モデルの場合は、**Multi-session OS**オプション。
  - VDI専用デスクトップ配信モデルの場合は、**Single-session OS**オプション。
- 同じマシンカタログ内でLinux VDAマシンとWindows VDAマシンを混在させないでください。

注:

Citrix Studioの初期バージョンでは、「Linux OS」という概念をサポートしていませんでした。ただし、**Windows Server OS**または**Server OS**オプションを選択すると、同等のホストされた共有デスクトップ配信モデルが意味されます。**Windows Desktop OS**または**Desktop OS**オプションを選択すると、マシンごとに1人のユーザーという配信モデルが意味されます。

ヒント:

マシンをActive Directoryドメインから削除して再参加させる場合は、そのマシンをマシンカタログから削除して再度追加する必要があります。

ステップ12：デリバリーグループを作成する

デリバリーグループを作成し、Linux VDAマシンを含むマシンカタログを追加するプロセスは、Windows VDAマシンとほぼ同じです。これらのタスクを完了する方法の詳細については、「デリバリーグループの作成」を参照してください。

Linux VDAマシンカタログを含むデリバリーグループを作成する場合、以下の制限が適用されます。

- 選択したADユーザーとグループが、Linux VDAマシンにログオンできるように適切に構成されていることを確認してください。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- デリバリーグループと、Windowsマシンを含むマシンカタログを混在させないでください。

マシンカタログとデリバリーグループの作成方法については、Citrix Virtual Apps and Desktops 7 2303を参照してください。

設定

このセクションでは、Linux VDA の機能について、機能の説明、構成、トラブルシューティングを含めて詳しく説明します。

管理

このセクションには、次のトピックが含まれています。

- CEIP
- HDX インサイト
- Citrix Telemetry Serviceとの統合
- Citrix DaaS Standard for Azure向けLinux VDAの自己更新
- Linux VMおよびLinuxセッションメトリック
- ログ収集
- セッションシャドウイング
- モニターサービスデーモン
- ツールとユーティリティ
- その他
    - Citrix Workspaceアプリ for HTML5のサポート
    - Python3仮想環境の作成
    - NISとActive Directoryの統合
    - IPv6
    - LDAPS
    - **Xオーソリティ**

Citrixカスタマーエクスペリエンス向上プログラム (CEIP)

CEIPに参加すると、Citrix製品の品質とパフォーマンスを向上させるために、匿名の統計情報と使用状況情報がCitrixに送信されます。さらに、匿名データのコピーは、迅速かつ効率的な分析のためにGoogle Analytics (GA) に送信されます。GAはデフォルトで無効になっています。

レジストリ設定

デフォルトでは、Linux VDAをインストールするとCEIPに自動的に参加します。データの初回アップロードは、Linux VDAのインストール後約7日で行われます。このデフォルト設定はレジストリで変更できます。

- **CEIPスイッチ**

CEIPを有効または無効にするレジストリ設定 (デフォルト = 0):

場所: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

名前: **CEIPSwitch**

値: 1 = 無効、0 = 有効

指定されていない場合、CEIPは有効になります。

クライアントで次のコマンドを実行してCEIPを無効にできます。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **GAスイッチ**

GAを有効または無効にするレジストリ設定 (デフォルト = 1):

場所: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

名前: **GASwitch**

値: 1 = 無効, 0 = 有効

指定しない場合、GAは無効になります。

クライアントで次のコマンドを実行してGAを有効にできます:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "GASwitch" -d "0"
```

- **DataPersistPath**

データ永続化パスを制御するレジストリ設定 (デフォルト = /var/xdl/ceip):

場所: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

名前: DataPersistPath

値: 文字列

このパスを設定するには、次のコマンドを実行します:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "DataPersistPath" -d
"your_path"
```

構成されたパスが存在しないかアクセスできない場合、データはデフォルトパスに保存されます。

Linux VDAから収集されたCEIPデータ

次の表は、収集される匿名情報の種類の例を示しています。このデータには、お客様を特定するような詳細は含まれていません。

データポイント	キー名	説明
マシンGUID	**machine_guid**	データの発信元となるマシンを識別します
ADソリューション	**ad_solution**	マシンのドメイン参加方法を示すテキスト文字列
Linuxカーネルバージョン	**kernel_version**	マシンのカーネルバージョンを示すテキスト文字列
LVDAバージョン	**vda_version**	インストールされているLinux VDAのバージョンを示すテキスト文字列。
LVDAの更新または新規インストール	**update_or_fresh_install**	現在のLinux VDAパッケージが新規インストールされているか、更新されているかを示すテキスト文字列
LVDAのインストール方法	install_method	現在のLinux VDAパッケージがMCS、PVS、簡易インストール、または手動インストールを使用してインストー

データポイント	キー名	説明
		ルされていることを示すテキスト文字列。
HDX™ 3D Proが有効かどうか	**hdx_3d_pro**	HDX 3D Proがマシンで有効になっているかどうかを示すテキスト文字列
VDIモードが有効かどうか	**vdi_mode**	VDIモードが有効になっているかどうかを示すテキスト文字列
システムロケール	**system_locale**	このマシンのロケールを示すテキスト文字列
LVDAキーサービスの最終再起動時刻	**ctxhdx ctxvda**	`ctxhdx`および`ctxvda`サービスの最終再起動時刻。形式はdd-hh:mm:ss（例：10-17:22:19）
GPUの種類	**gpu_type**	マシンのGPUタイプを示す
CPUコア数	**cpu_cores**	マシンのCPUコア数を示す整数
CPU周波数	**cpu_frequency**	MHz単位のCPU周波数を示す浮動小数点数
物理メモリサイズ	**memory_size**	KB単位の物理メモリサイズを示す整数
起動されたセッション数	**session_launch**	このデータポイントを収集した時点でマシン上で起動された（ログオンまたは再接続された）セッション数を示す整数
Linux OS名とバージョン	**os_name_version**	マシンのLinux OS名とバージョンを示すテキスト文字列
セッションキー	**session_key**	データの発信元となるセッションを識別します

データポイント	キー名	説明
リソースの種類	**resource_type**	起動されたセッションのリソースタイプを示すテキスト文字列: デスクトップまたは `<appname>`
アクティブセッション時間	**active_session_time**	セッションのアクティブ時間を保存するために使用されます。セッションは切断/再接続できるため、1つのセッションに複数のアクティブ時間を持つことができます。
セッション継続時間	**session_duration_time**	ログオンからログオフまでのセッションの継続時間を保存するために使用されます。
Receiverクライアントタイプ	**receiver_type**	セッションの起動に使用されたCitrix Workspace™アプリのタイプを示す整数
Receiverクライアントバージョン	**receiver_version**	セッションの起動に使用されたCitrix Workspaceアプリのバージョンを示すテキスト文字列
印刷回数	**printing_count**	セッションが印刷機能を使用した回数を示す整数
USBリダイレクト回数	**usb_redirecting_count**	セッションがUSBデバイスを使用した回数を示す整数
Gfxプロバイダータイプ	**gfx_provider_type**	セッションのグラフィックプロバイダータイプを示すテキスト文字列
シャドウイング回数	**shadow_count**	セッションがシャドウされた回数を示す整数
ユーザーが選択した言語	**ctxism_select**	ユーザーが選択したすべての言語を含む長い文字列

データポイント	キー名	説明
スマートカードリダイレクト回数	**scard_redirecting_count**	セッションログオンおよびセッション内アプリのユーザー認証にスマートカードリダイレクトが使用された回数を示す整数

HDX™ インサイト

概要

Linux VDA は HDX Insight 機能を部分的にサポートしています。

インストール

依存パッケージをインストールする必要はありません。

使用方法

HDX Insight は、Citrix Workspace™ アプリと Linux VDA の間で Citrix ADC を介して渡される ICA® メッセージを分析します。すべての HDX Insight データは NSAP 仮想チャネルから取得され、非圧縮で送信されます。NSAP 仮想チャネルはデフォルトで有効になっています。

次のコマンドは、NSAP 仮想チャネルをそれぞれ無効化および有効化します。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000000" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000001" --force
```

トラブルシューティング

データポイントが表示されない

原因は2つ考えられます。

- HDX Insight が正しく構成されていません。

たとえば、Citrix ADC で AppFlow® が有効になっていないか、Citrix ADM で誤った Citrix ADC インスタンスが構成されています。

- Linux VDA で ICA Control Virtual Channel が開始されていません。

  `ps aux | grep -i ctxctl`

  `ctxctl` が実行されていない場合は、管理者に連絡して Citrix にバグを報告してください。

アプリケーションのデータポイントが表示されない

シームレス仮想チャネルが有効になっており、シームレスアプリケーションが実行されていることを確認してください。

Citrix Telemetry Serviceとの統合

Linux VDAソフトウェアにCitrix Telemetry Service (`ctxtelemetry`) を統合することで、Citrix Scoutを実行し、/opt/Citrix/VDA/bin/xdlcollect.shスクリプトを使用してLinux VDAに関するログを収集できます。

シトリックス スカウト(/en-us/linux-virtual-delivery-agent/2303/media/citrix-scout.png)

> **注:**

> Linux VDA 1912以前のバージョンからアップグレードした後、Citrix Telemetry Service (`ctxtelemetry`) の変数を構成するには、/opt/Citrix/VDA/sbin/ctxsetup.shを再実行する必要があります。変数について詳しくは、「Easy install」を参照してください。

Citrix Telemetry Serviceの有効化と無効化

- サービスを有効にするには、**sudo systemctl enable ctxtelemetry.socket**コマンドを実行します。
- サービスを無効にするには、**sudo systemctl disable ctxtelemetry.socket**を実行します。

ポート

Citrix Telemetry Service (`ctxtelemetry`) は、デフォルトでTCP/IPポート7503を使用してCitrix Scoutをリッスンします。Delivery ControllerではTCP/IPポート7502を使用してCitrix Scoutと通信します。

Linux VDAのインストール時に、デフォルトのポートを使用するか、以下の変数を通じてポートを変更できます。

- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Citrix Scoutをリッスンするためのソケットポート。デフォルトポートは7503です。
- **CTX_XDL_TELEMETRY_PORT** – Citrix Scoutと通信するためのポート。デフォルトポートは7502です。

VDAのインストール後にポートを変更するには、次の手順を実行します。

1. Scoutと通信するためのポートを変更するには、次のコマンドを実行します。

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\Software\Citrix\VirtualDesktopAgent" -v "TelemetryServicePort" -d
   <port number> -t REG_DWORD
   ```

2. Scoutをリッスンするためのソケットポートを変更するには、次のコマンドを実行してctxtelemetry.socketファイルを開き、編集します。

   ```
   sudo vi /etc/systemd/system/ctxtelemetry.socket
   ```

   ソケットポートの画像(/en-us/linux-virtual-delivery-agent/2303/media/socket-port.png)

3. ソケットポートを再起動するには、次のコマンドを実行します。

   ```
   sudo systemctl daemon-reload

   sudo systemctl stop ctxtelemetry.socket

   sudo systemctl start ctxtelemetry.socket
   ```

4. ファイアウォール構成で新しいポートを有効にします。

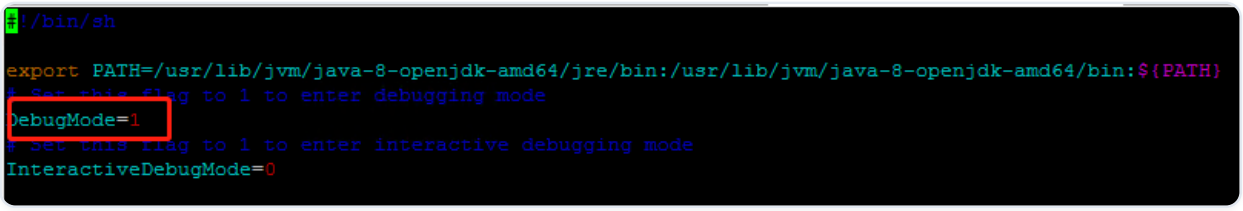
   たとえば、Ubuntuを使用している場合は、**sudo ufw allow 7503**コマンドを実行してポート7503を有効にします。

デバッグモード

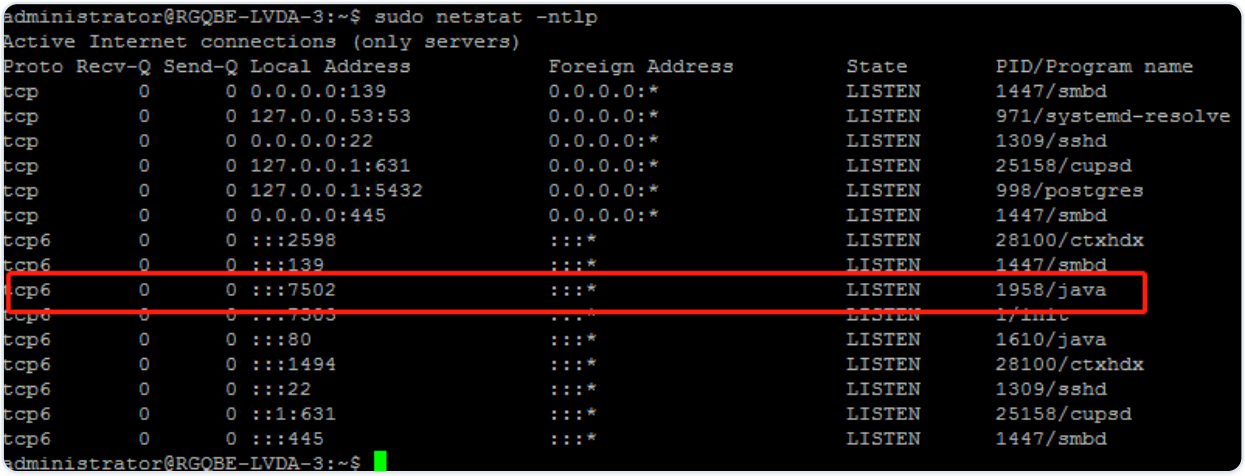
Citrix Telemetry Serviceが期待どおりに動作しない場合は、デバッグモードを有効にして原因を特定できます。

1. デバッグモードを有効にするには、次のコマンドを実行して`ctxtelemetry`ファイルを開き、DebugModeの値を1に変更します。

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
```



2. Citrix Telemetry Serviceを手動で停止するか、サービスが自動的に停止するまで15分間待ちます。



この例では、次のコマンドを実行してCitrix Telemetry Serviceを停止できます。

```
sudo netstat -ntlp

Kill -9 1958
```

3. Citrix Telemetry Serviceを再起動するには、ScoutでLinux VDAを選択し、/var/log/xdl/にあるtelemetry-debug.logを見つけます。

サービス待機時間

ソケットポートを開く`systemd`デーモンは、デフォルトで起動し、使用するリソースはごくわずかです。Citrix Telemetry Serviceはデフォルトで停止しており、Delivery Controllerからのログ収集要求がある場合にのみ起動します。ログ収集が完了すると、サービスは15分間新しい収集要求を待ち、要求がない場合は再び停止します。待機時間は、次のコマンドで構成できます。最小値は10分です。10分未満の値を設定した場合、最小値である10分が適用されます。待機時間を設定したら、サービスを停止して再起動します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"TelemetryServiceIdleTimeoutInMinutes" -d <number> -t REG_DWORD
```

検証テスト

収集が開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scout は推奨される修正措置とともにメッセージを表示します。検証テストの詳細については、Citrix Scoutドキュメントの検証テストセクションを参照してください。

Azure を介した Linux VDA のセルフアップデート

この機能は、Linux VDA ソフトウェアを即時またはスケジュールされた時間に自動的に更新するのに役立ちます。Citrix DaaS Standard for Azure (旧称 Citrix Virtual Apps and Desktops Standard for Azure) で Linux VDA を作成する場合に便利です。Azure の VM の管理者権限は必要ありません。詳細については、「Citrix DaaS Standard for Azure で Linux VDA を作成する」を参照してください。

構成

この機能を使用するには、次の手順を完了します。

ステップ 1: 更新情報と新しい VDA パッケージを Azure コンテナーにアップロードする

ステップ 1a: Azure ストレージアカウントの下にコンテナーを作成し、コンテナーのアクセスレベルを **Blob (匿名読み取りアクセスのみ)** に設定します。

> **注:**
>
> Azure コンテナーと BLOB は、お客様が排他的に保持および管理します。Citrix® は、それらに関するセキュリティ問題について責任を負いません。データセキュリティとコスト効率を確保するため、**セルフアップデート**のたびにコンテナーのアクセスレベルを **Private (匿名アクセスなし)** に設定してください。

ステップ 1b: VDA 更新情報を UpdateInfo.json という名前の JSON ファイルに組み込みます。ファイル形式の例については、次のブロックを参照してください。

```
{

 "Version": "21.04.200.4",

"Distributions":[

{

"TargetOS": "RHEL7_9",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "UBUNTU18_04",

"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",

"PackageHash":
"4148cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"

},

{

"TargetOS": "UBUNTU20_04",

"PackageName": "",

"PackageHash": ""

}

]

}
```

ここで、**"Version"** は新しい VDA バージョンを示し、**"Distributions"** は更新オブジェクトの配列です。各オブジェクトには次の 3 つの項目が含まれます。

- **"TargetOS"**: 「RHEL7_9」（RHEL 7、CentOS 7、Amazon Linux 2 の場合）、「UBUNTU18_04」、または「UBUNTU20_04」である必要があります。`ctxmonitorservice` は他のディストリビューションを認識しません。
- **"PackageName"**: 指定されたバージョンの VDA パッケージの完全な名前。
- **"PackageHash"**: `shasum -a 256 <pkgname>` コマンドを使用して計算する SHA-256 値。

ステップ 1c: JSON ファイルと新しいバージョンの Linux VDA パッケージを Azure コンテナーにアップロードします。

ステップ 2: マスターイメージまたは各 VDA でセルフアップデート機能を有効にする

デフォルトでは、**セルフアップデート**は無効になっています。Citrix DaaS Standard for Azure で Linux VDA を作成する場合、機能の有効化はマスターイメージで実行する必要があります。それ以外の場合は、各ターゲット VDA で直接機能を有効にします。

セルフアップデートを有効にするには、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate のレジストリキーを編集するために、次のようなコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD"
-v "fEnabled" -d "0x00000001" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"ScheduledTime" -d "Immediately" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"Url" -d "<Your-Azure-Container-Url>" --force



/opt/Citrix/VDA/bin/ctxreg create -k
```

```
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
```

以下の表はレジストリ設定について説明しています。

レジストリ設定	説明
fEnabled	この設定は必須です。デフォルトでは値は0で、**セルフアップデート**が無効であることを意味します。1に設定すると、**セルフアップデート**を有効にできます。
Url	この設定は必須です。更新情報と新しいVDAパッケージを取得するためのAzureコンテナのURLを設定します。
ScheduledTime	この設定は必須です。**Immediately**または**NextStart**に設定できます。**Immediately**は、VDAパッケージのダウンロード後すぐにアップデートを実行することを意味します。このオプションは、ダウンロード速度が速く、アップデートが緊急である場合に適しています。ただし、パッケージのダウンロード中にライブセッションがある場合、ユーザーエクスペリエンスを妨げる可能性があります。**NextStart**は、`ctxmonitorservice`の次回の起動時にアップデートを実行することを意味します。このオプションは、ダウンロード速度が速くなく、アップデートが緊急でない場合に適しています。
CaCertificate	この設定はオプションです。Azureコンテナの URLを検証するためのPEM証明書のフルパスを設定します。Azure BLOBの場合、portal.azure.comの証明書をブラウザから取得し、PEMに変換したものを使用できます。セキュリティのため、このレジストリ設定を追加することをお勧めしますが、Ubuntuでのみサポートされています。RHELでは、`curl`コマンド用のNSSライブラリの一部がリンクされていません。証明書の最小限の特権を設定するようにしてください。

`ctxmonitorservice`が再起動すると、まず**Url**を照会してUpdateInfo.jsonファイルを取得し、JSONファイルから更新バージョンを取得します。次に、`ctxmonitorservice`は更新バージョンを現在のバージョンと比較します。現在のバージョンが古い場合、サービスはAzureからVDAパッケージの新しいバージョンをダウンロードし、ローカルに保存します。その後、**ScheduledTime**の設定に従ってアップデートを実行します。オンプレミス展開の場合、`ctxmonitorservice`を直接再起動してアップデートをトリガーできます。ただし、VMに対する管理者権限がないCitrix DaaS Standard for Azureでは、`ctxmonitorservice`はVDAマシンが再起動された後にのみ再起動できます。アップデートが失敗した場合、VDAは既存のバージョンにロールバックされます。

注:

- マスターイメージで構成したレジストリ設定は変更できません。
- 環境内のすべてのVMが同時にパッケージをダウンロードすると、ローカルネットワークが混雑する可能性があります。
- アップデートとロールバックの両方が失敗した場合、ユーザーデータは失われます。
- アップデートが失敗してもロールバックが成功した場合、同じネットワーク上のユーザーは異なるバージョンのLinux VDAを使用している可能性があります。このケースは最適ではありません。
- 更新には通常、数分かかります。Citrix Studioにはステータスインジケーターはありません。

Linux VMおよびLinuxセッションのメトリック

次の表は、Linux VMおよびLinuxセッションで利用可能なメトリックの一部を示しています。

メトリック	必要なVDAの最小バージョン	説明	備考
ログオン期間	2109	これは、ユーザーがCitrix Workspaceアプリから接続してからセッションが使用可能になるまでのログオンプロセスを測定するものです。セッションのメトリックを表示するに	Monitorでのみ利用可能です。

メトリック	必要なVDAの最小バージョン	説明	備考
		は、Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）のMonitorタブに移動します。Monitorは、Citrix Virtual Apps and DesktopsのCurrent ReleaseおよびLTSR展開を監視およびトラブルシューティングするためのDirectorコンソールとして利用できます。Monitorタブで、**Average Logon Duration**セクションの**View Historical Trend**をクリックします。**Logon Performance**ページで、フィルター条件を設定し、**Apply**をクリックしてメトリックを視覚化します。	
セッションの自動再接続回数	2109	セッションでの自動再接続の回数を表示するには、**Trends**ビューにアクセスします。条件を設定し、**Apply**をクリックして検索結果を絞り込みます。**Session Auto Reconnect Count**列には、セッションでの自動再接続の回数が表示されます。自動再接続は、	Citrix DirectorとMonitorの両方で利用可能です。

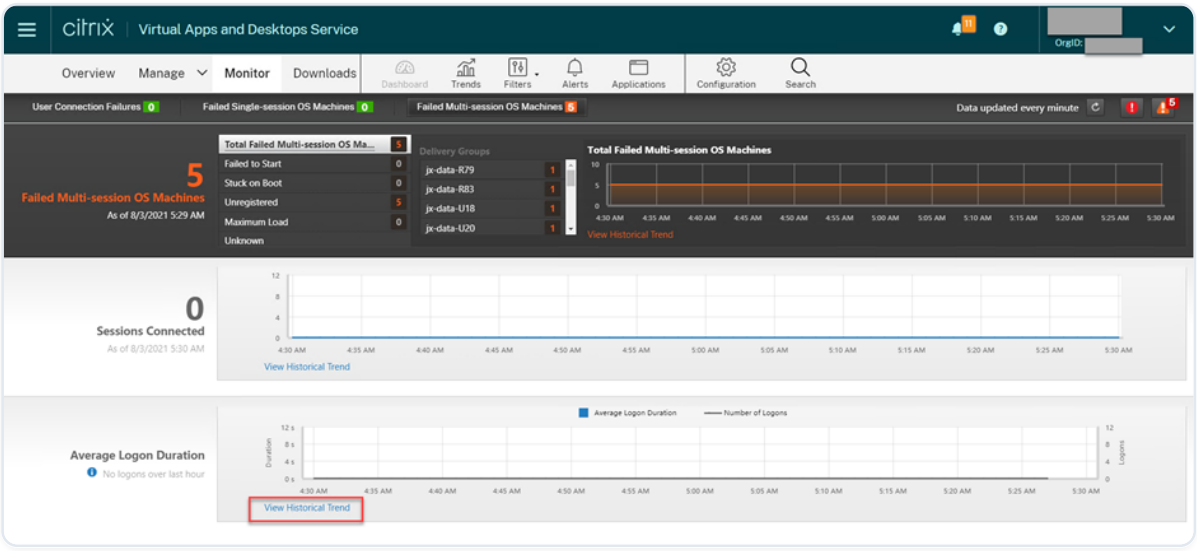
メトリック	必要なVDAの最小バージョン	説明	備考
		Session Reliabilityまたは**Auto Client Reconnect**ポリシーが有効な場合に有効になります。セッションの再接続について詳しくは、「Sessions」を参照してください。ポリシーについて詳しくは、「Auto client reconnect policy settings」および「Session reliability policy settings」を参照してください。	
アイドル時間	2103	このメトリックにアクセスするには、**Filters > Sessions > All Sessions**を選択して**All Sessions**ページを開きます。	Citrix DirectorとMonitorの両方で利用可能です。
Linux VMのメトリック	2103	Linux VMで利用可能なメトリックは、CPUコア数、メモリサイズ、ハードディスク容量、現在のCPUおよびメモリ使用率、履歴のCPUおよびメモリ使用率です。	Citrix DirectorとMonitorの両方で利用可能です。
プロトコル	1909	Linuxセッションのトランスポートプロトコルは、**セッションの詳細**パネルにUDPまたはTCPとして表示されます。	Citrix DirectorとMonitorの両方で利用可能です。

メトリック	必要なVDAの最小バージョン	説明	備考
ICA® RTT	1903	ICAラウンドトリップタイム (RTT) は、キーを押してからエンドポイントに応答が表示されるまでの経過時間です。ICA RTTメトリックを取得するには、Citrix Studioで**ICAラウンドトリップ計算**および**ICAラウンドトリップ計算間隔**ポリシーを作成します。	Citrix DirectorとMonitorの両方で利用可能です。

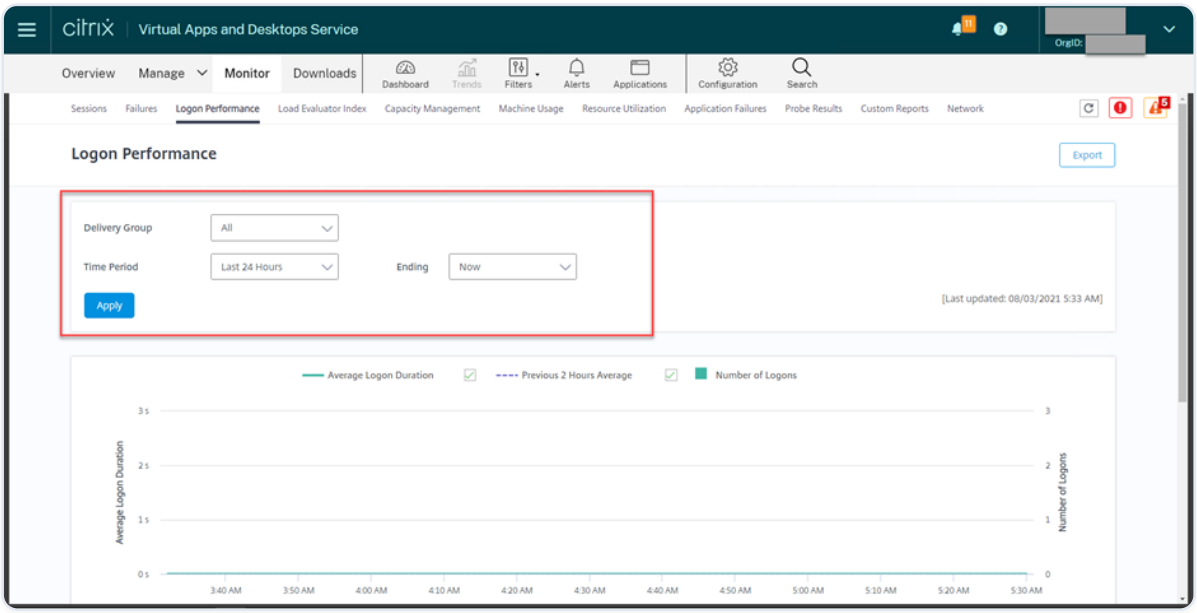
Citrix DirectorおよびMonitorでさまざまなメトリックにアクセスする方法の例

- ログオン期間

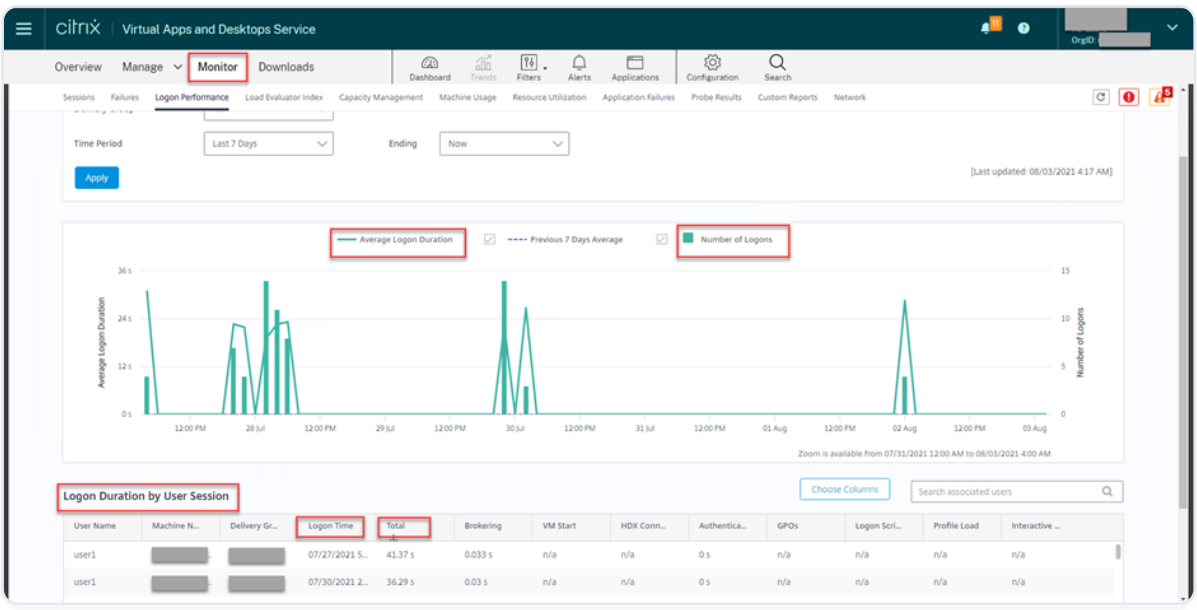
  a. Citrix DaaSのMonitorタブで、**平均ログオン期間**セクションの**履歴トレンドの表示**をクリックします。



  b. **ログオンパフォーマンス**ページで、フィルター条件を設定します。

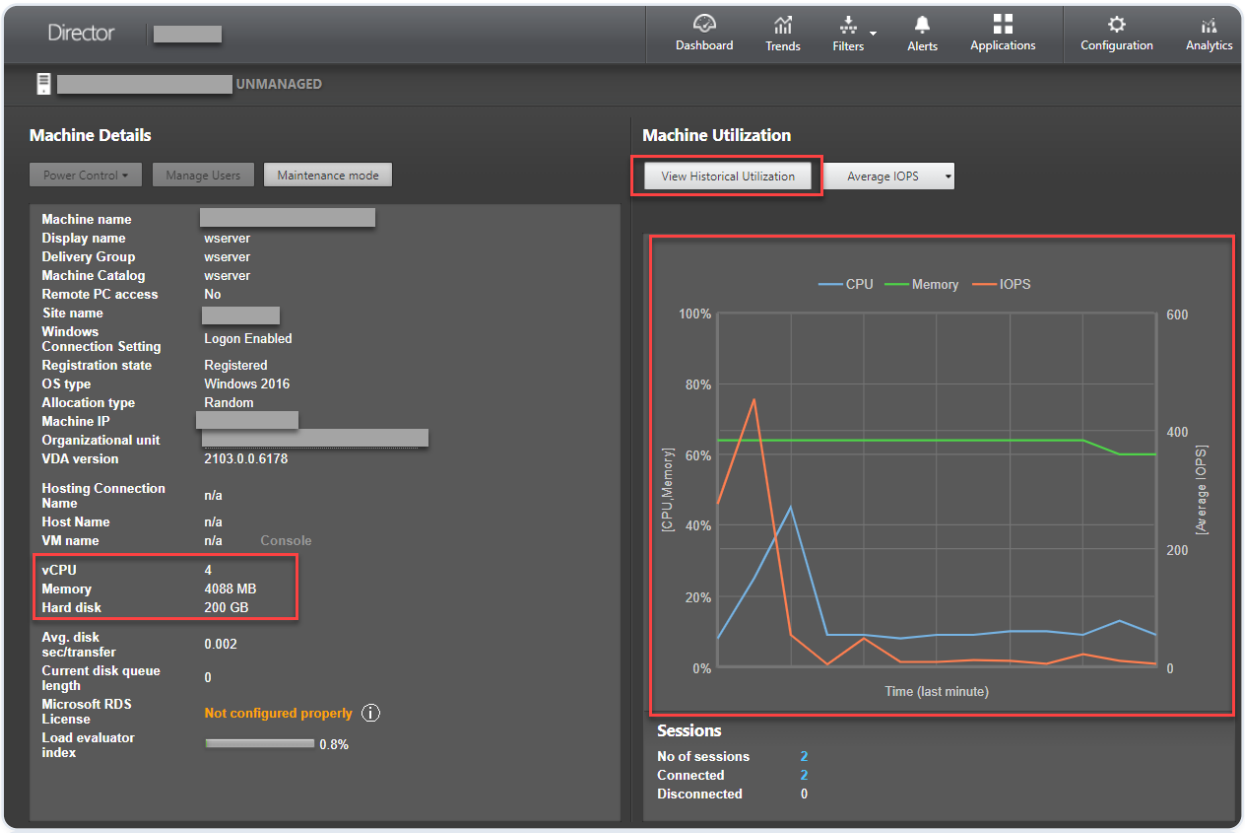


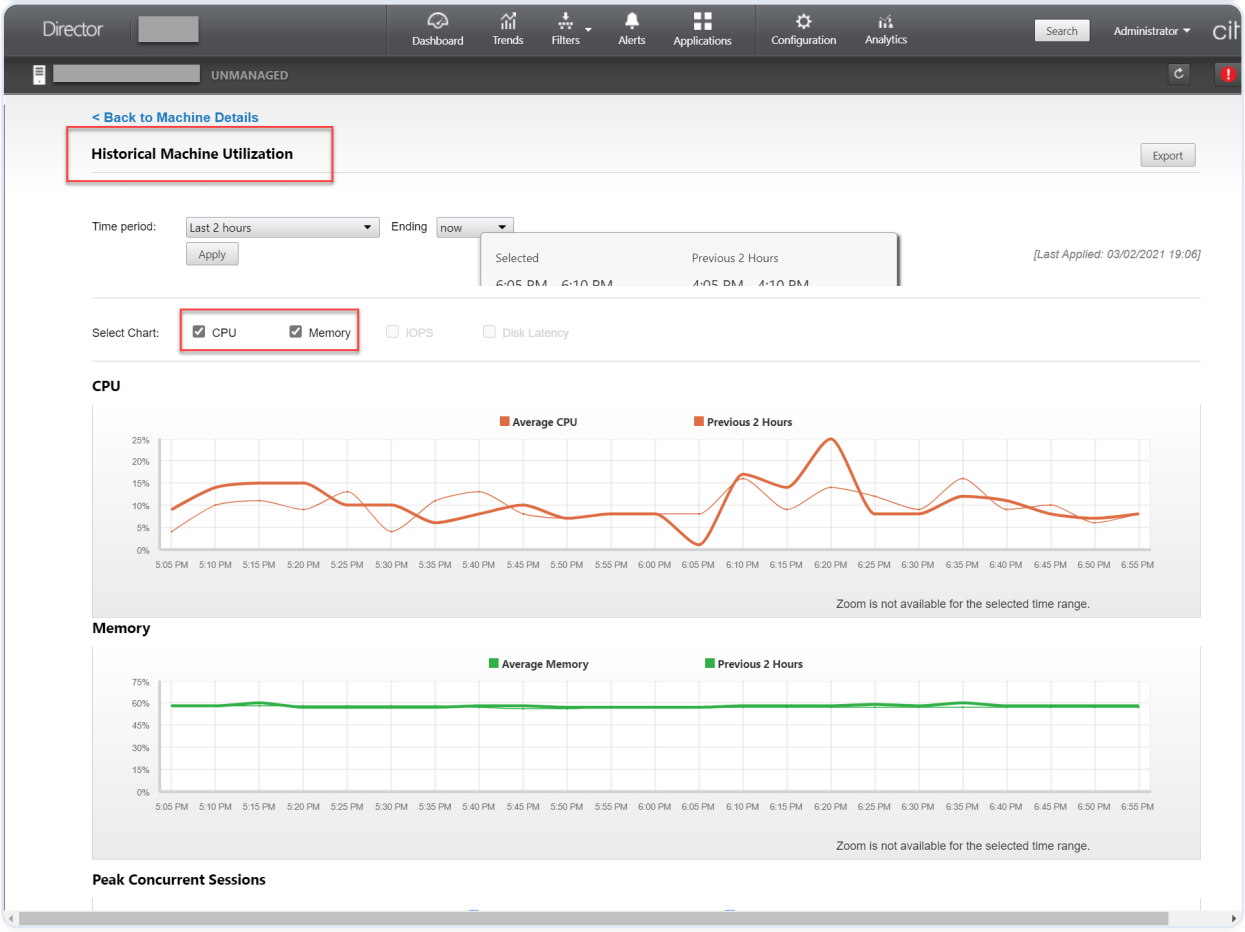
c. **適用**をクリックして、ログオン期間メトリックを視覚化します。



- Linux VMのCPUコア数、メモリサイズ、ハードディスク容量、および現在と過去のCPUとメモリ使用率

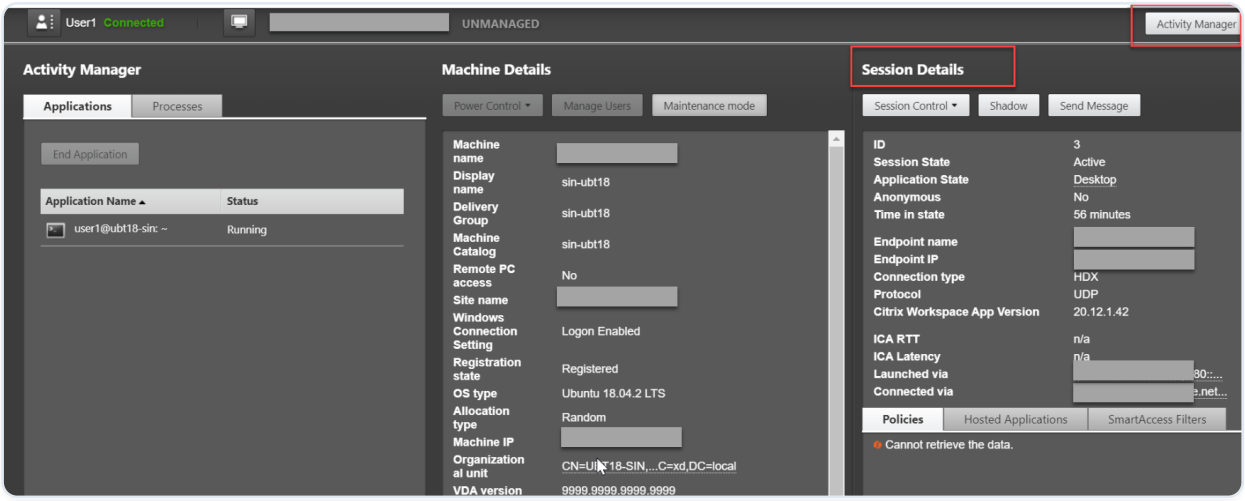
  Linux VMのこれらのメトリックにアクセスするには、Citrix DirectorまたはMonitorでVMを見つけ、**マシンの詳細**パネルを確認します。例：





- ICA RTT、プロトコル

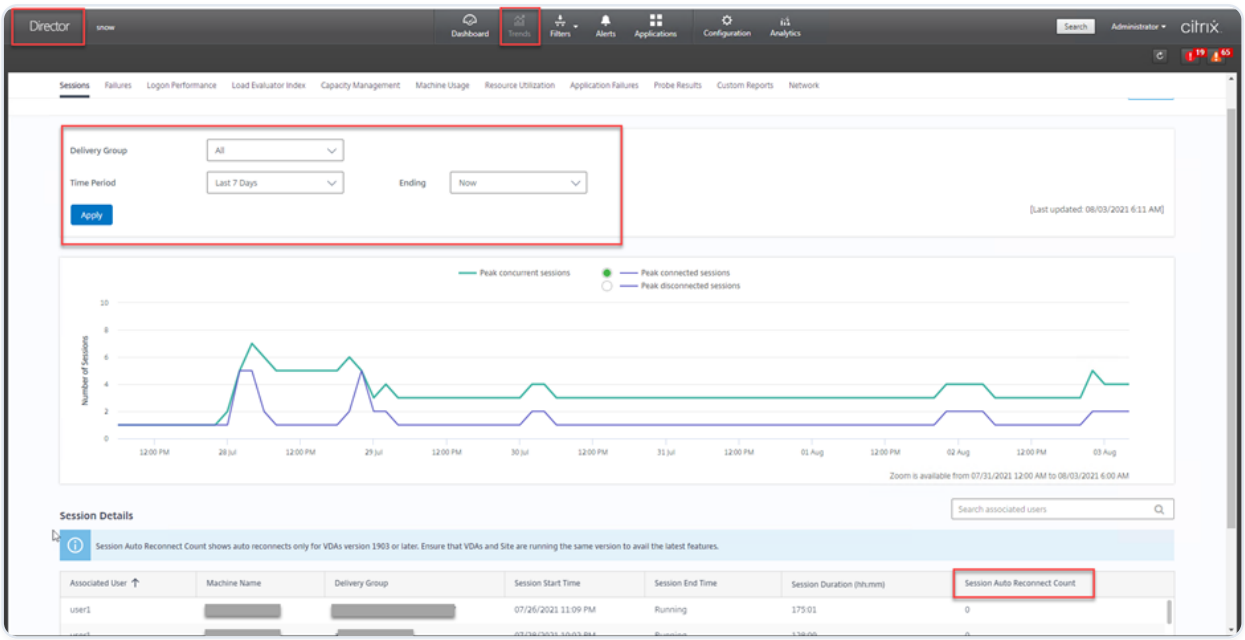
Linuxセッションのメトリックを表示するには、**フィルター > セッション > すべてのセッション**を選択して**すべてのセッション**ページを開くか、**セッションの詳細**パネルにアクセスします。**セッションの詳細**パネルにアクセスするには、**すべてのセッション**ページを開き、目的のセッションをクリックして**アクティビティマネージャー**ビューにアクセスします。例:



- セッションの自動再接続数

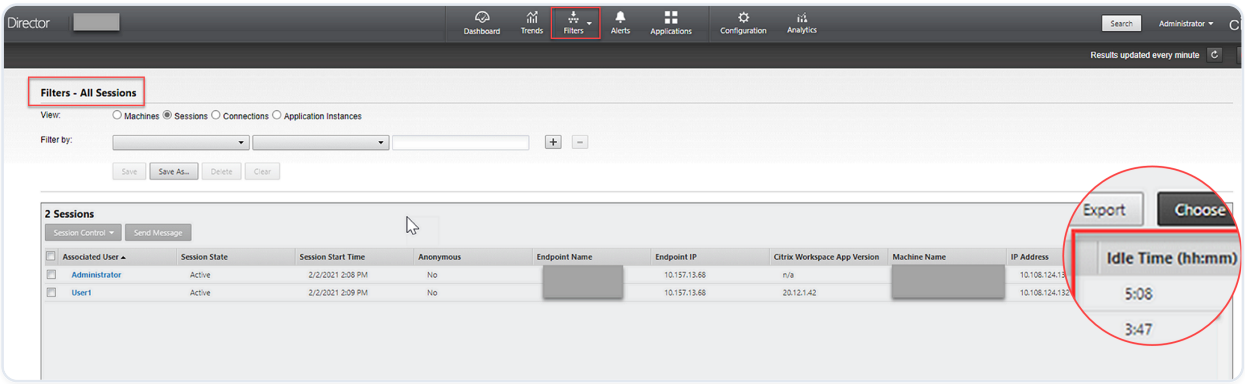
  セッション内の自動再接続数を表示するには、**トレンド**ビューにアクセスします。条件を設定し、**適用**をクリックして検索結果を絞り込みます。

  セッションの自動再接続数列には、セッション内の自動再接続数が表示されます。例:



- アイドル時間

  例:



ログ収集

概要

ログ収集は、デフォルトでLinux VDAに対して有効になっています。

構成

`ctxlogd`デーモンと`setlog`ユーティリティは、Linux VDAリリースパッケージに含まれています。デフォルトでは、Linux VDAのインストールと構成後に`ctxlogd`デーモンが起動します。

ctxlogdデーモン

トレースされる他のすべてのサービスは、`ctxlogd`デーモンに依存します。Linux VDAのトレースを継続したくない場合は、`ctxlogd`デーモンを停止できます。

setlogユーティリティ

ログ収集は、**/opt/Citrix/VDA/bin/**パスにある`setlog`ユーティリティを使用して構成されます。rootユーザーのみが実行する権限を持っています。GUIを使用するか、コマンドを実行して構成を表示および変更できます。`setlog`ユーティリティに関するヘルプについては、次のコマンドを実行してください。

```
setlog help
```

値

デフォルトでは、**ログ出力パス**は**/var/log/xdl/hdx.log**に設定され、**最大ログサイズ**は200 MBに設定されており、**ログ出力パス**の下に最大2つの古いログファイルを保存できます。

現在の`setlog`値を表示します。

```
setlog values
```

```
log_path (Log Output Path) = /var/log/xdl/hdx.log


log_size (Max Log Size (MiB)) = 200


log_count (Max Old Log Files) = 2
```

単一の`setlog`値を表示または設定します。

```
setlog value <name> [<value>]
```

例:

```
setlog value log_size 100
```

レベル

デフォルトでは、ログレベルは**warning**（大文字と小文字を区別しない）に設定されています。

さまざまなコンポーネントに設定されているログレベルを表示するには、次のコマンドを実行します。

```
setlog levels
```

ログレベル（Disabled、Inherited、Verbose、Information、Warnings、Errors、Fatal Errorsを含む）を設定するには、次のコマンドを実行します。

```
setlog level <class> [<level>]
```

ログレベル	コマンドパラメーター（大文字と小文字を区別しない）
無効	なし
継承	継承

ログレベル	コマンドパラメーター（大文字と小文字を区別しない）
詳細	詳細
情報	情報
警告	警告
エラー	エラー
致命的なエラー	致命的

「`<class>`」変数は、Linux VDA の 1 つのコンポーネントを指定します。すべてのコンポーネントを対象とするには、「all」に設定します。例：

```
setlog level all error
```

フラグ

デフォルトでは、フラグは次のように設定されています。

```
setlog flags


DATE = true


TIME = true


NAME = true


PID = true


TID = false
```

```
SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
```

現在のフラグを表示する：

```
setlog flags
```

単一のログフラグを表示または設定する：

```
setlog flag <flag> [<state>]
```

デフォルトに戻す

すべてのレベル、フラグ、および値をデフォルト設定に戻します。

```
setlog default
```

重要:

`ctxlogd`サービスは、ルートユーザーのみが作成できる**/var/xdl/.ctxlog**ファイルを使用して構成されます。他のユーザーはこのファイルへの書き込み権限を持っていません。ルートユーザーは他のユーザーに書き込み権限を与えないことをお勧めします。これに従わない場合、任意のまたは悪意のある構成が`ctxlogd`を引き起こし、サーバーのパフォーマンス、ひいてはユーザーエクスペリエンスに影響を与える可能性があります。

トラブルシューティング

/var/xdl/.ctxlogファイルが見つからない場合（たとえば、誤って削除された場合）、`ctxlogd`デーモンが失敗し、`ctxlogd`サービスを再起動できません。

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
configuration file.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited,
code=exited, status=1/FAILURE



Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

この問題を解決するには、ルートユーザーとして`setlog`を実行して、**/var/xdl/.ctxlog**ファイルを再作成します。その後、他のサービスが依存している`ctxlogd`サービスを再起動します。

セッションシャドウイング

セッションシャドウイングにより、ドメイン管理者はイントラネット内でユーザーのICA®セッションを表示できます。この機能は、noVNCを使用してICAセッションに接続します。

> **注:**
>
> この機能を使用するには、`Citrix Director` 7.16以降を使用してください。

インストールと構成

依存関係

セッションシャドウイングには、`python-websockify`と`x11vnc`の2つの新しい依存関係が必要です。Linux VDAのインストール後に、`python-websockify`と`x11vnc`を手動でインストールしてください。

RHEL 7.xおよびAmazon Linux2の場合:

`python-websockify`と`x11vnc` (`x11vnc`バージョン0.9.13以降) をインストールするには、次のコマンドを実行します。

```
sudo pip3 install websockify

sudo yum install x11vnc
```

(RHEL 7.xの場合) Extra Packages for Enterprise Linux (EPEL) およびオプションのRPMリポジトリを有効にして、`python-websockify`と`x11vnc`を解決します。

- EPEL

  EPELリポジトリは`x11vnc`に必要です。EPELリポジトリを有効にするには、次のコマンドを実行します。

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  ```

- オプションのRPM

`x11vnc`の一部の依存パッケージをインストールするために、オプションの`RPMs`リポジトリを有効にするには、次のコマンドを実行します。

```
subscription-manager repos --enable rhel-7-server-optional-rpms --
enable rhel-7-server-extras-rpms
```

RHEL 9.1/9.0/8.x および Rocky Linux 9.1/9.0/8.x の場合:

`python-websockify`と`x11vnc` (`x11vnc`バージョン0.9.13以降) をインストールするには、次のコマンドを実行します。

```
sudo pip3 install websockify

sudo yum install x11vnc
```

EPELおよびCodeReady Linux Builderリポジトリを有効にして、`x11vnc`を解決します。

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-
release-latest-8.noarch.rpm



subscription-manager repos --enable "codeready-builder  -for-rhel-8-
x86_64-rpms"
```

Ubuntuの場合:

`python-websockify` と `x11vnc` (`x11vnc` バージョン 0.9.13 以降) をインストールするには、次のコマンドを実行します。

```
sudo pip3 install websockify

sudo apt-get install x11vnc
```

SUSEの場合:

`python-websockify` と `x11vnc` (`x11vnc` バージョン 0.9.13 以降) をインストールするには、次のコマンドを実行します。

```
sudo pip3 install websockify

sudo zypper install x11vnc
```

Debianの場合:

`python-websockify` と `x11vnc` (`x11vnc` バージョン 0.9.13 以降) をインストールするには、次のコマンドを実行します。

```
sudo pip3 install websockify

sudo apt-get install x11vnc
```

ポート

セッションシャドウイング機能は、Linux VDA から `Citrix Director` への接続を確立するために、6001～6099 の範囲内で利用可能なポートを自動的に選択します。したがって、同時にシャドウできる ICA セッションの数は 99 に制限されます。特にマルチセッションシャドウイングの場合、要件を満たすのに十分なポートが利用可能であることを確認してください。

レジストリ

次の表に、関連するレジストリを示します。

レジストリ	説明	デフォルト値
EnableSessionShadowing	セッションシャドウイング機能を有効または無効にします	1 (有効)
ShadowingUseSSL	Linux VDA と Citrix Director 間の接続を暗号化するかどうかを決定します	0 (無効)

レジストリ値を変更するには、Linux VDA で `ctxreg` コマンドを実行します。たとえば、セッションシャドウイングを無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "EnableSessionShadowing" -d
"0x00000000"
```

SSL

Linux VDAとCitrix Director間のnoVNC接続はWebSocketプロトコルを使用します。セッションシャドウイングの場合、`ws://`と`wss://`のどちらが選択されるかは、前述の「ShadowingUseSSL」レジストリによって異なります。デフォルトでは、`ws://`が選択されます。ただし、セキュリティ上の理由から、`wss://`を使用し、各Citrix Directorクライアントと各Linux VDAサーバーに証明書をインストールすることをお勧めします。Citrixは、`ws://`を使用してLinux VDAセッションシャドウイングを行う場合のセキュリティ上の責任を負いません。

SSLを有効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "ShadowingUseSSL" -d
"0x00000001"
```

サーバーおよびルートSSL証明書を取得する

証明書は、信頼された認証局（CA）によって署名されている必要があります。

SSLを構成する各Linux VDAサーバーには、個別のサーバー証明書（キーを含む）が必要です。サーバー証明書は特定のコンピューターを識別するため、各サーバーの完全修飾ドメイン名（FQDN）を知っている必要があります。便宜上、ドメイン全体にワイルドカード証明書を使用することを検討してください。

Linux VDAと通信する各Citrix Directorクライアントにもルート証明書が必要です。ルート証明書は、サーバー証明書を発行するのと同じCAから入手できます。

以下のCAからサーバーおよびクライアント証明書をインストールできます。

- オペレーティングシステムにバンドルされているCA
- エンタープライズCA（組織がアクセスを許可しているCA）
- オペレーティングシステムにバンドルされていないCA

証明書を取得するために組織のセキュリティチームがどの方法を要求しているかを確認してください。

重要:

- サーバー証明書の共通名は、Linux VDAの正確なFQDNであるか、少なくとも正しいワイルドカードとドメイン文字である必要があります。例: vda1.basedomain.com または *.basedomain.com。

- SHA1やMD5を含むハッシュアルゴリズムは、一部のブラウザがサポートするデジタル証明書の署名には弱すぎます。そのため、SHA-256が最小標準として指定されています。
- Chromeは自己署名SSL証明書を安全でないとみなし、受け入れなくなりました。`NET::ERR_CERT_COMMON_NAME_INVALID`エラーは、生成された証明書にSAN (subjectAltName) フィールドがないために発生します。この問題を解決するには、SANフィールドを含む拡張属性 (X509 v3拡張) を持つ証明書を提供してください。

各CITRIX DIRECTORクライアントにルート証明書をインストールする

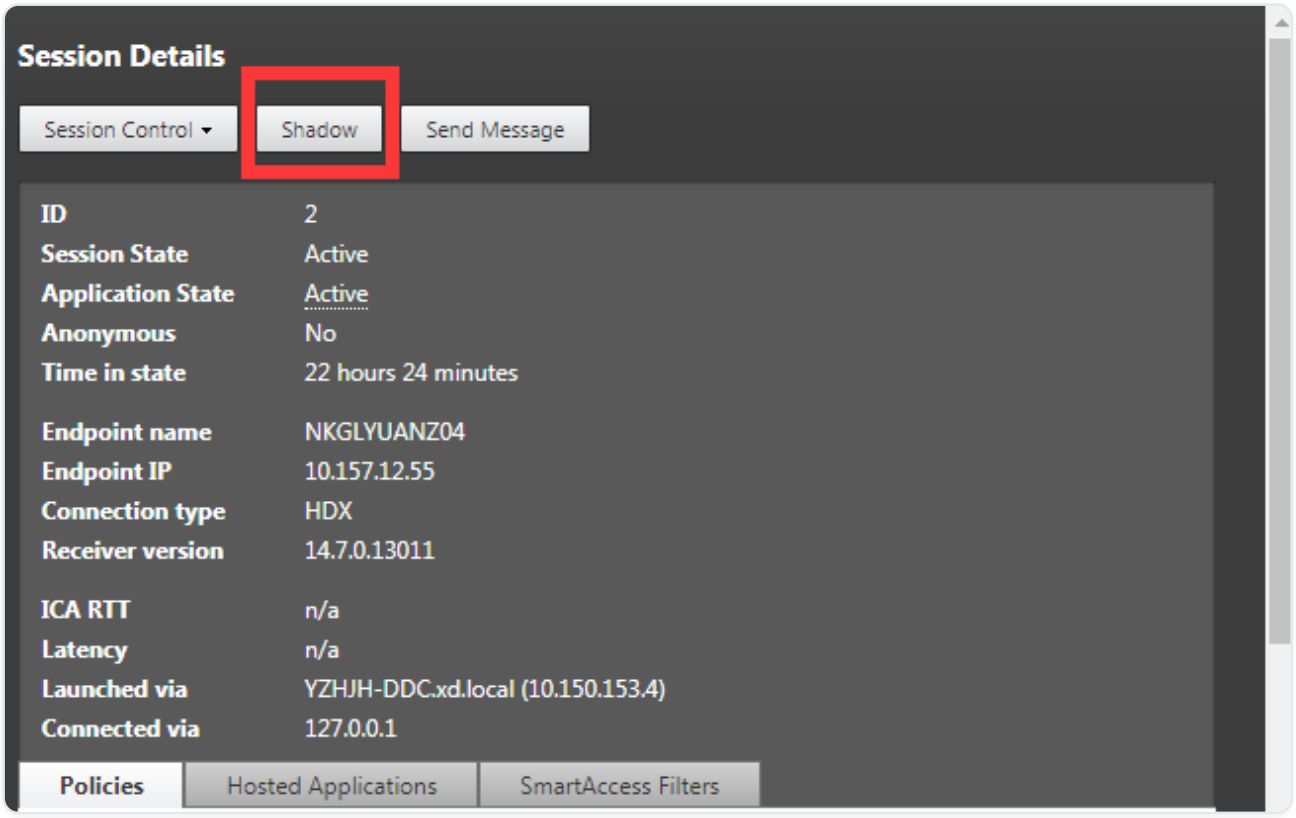
セッションシャドウイングはIISと同じレジストリベースの証明書ストアを使用するため、IISまたはMicrosoft管理コンソール (MMC) の証明書スナップインを使用してルート証明書をインストールできます。CAから証明書を受け取ったら、IISでWebサーバー証明書ウィザードを再起動すると、ウィザードが証明書をインストールします。または、MMCを使用してコンピューター上の証明書を表示およびインポートし、スタンドアロンスナップインとして証明書を追加することもできます。Internet ExplorerとGoogle Chromeは、オペレーティングシステムにインストールされている証明書をデフォルトでインポートします。Mozilla Firefoxの場合は、証明書マネージャーの**認証局**タブでルートSSL証明書をインポートする必要があります。

各LINUX VDAサーバーにサーバー証明書とそのキーをインストールする

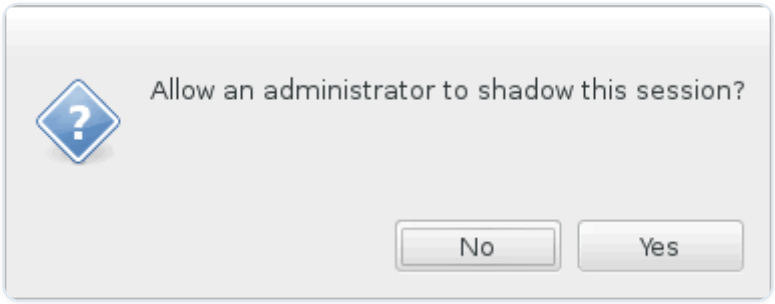
サーバー証明書には「shadowingcert.*」、キーファイルには「shadowingkey.*」という名前を付けます（*は形式を示します。例：shadowingcert.pem、shadowingkey.key）。サーバー証明書とキーファイルをパス **/etc/xdl/shadowingssl** の下に置き、制限された権限で適切に保護してください。名前またはパスが正しくないと、Linux VDAは特定の証明書またはキーファイルを見つけることができず、`Citrix Director`との接続障害が発生します。

使用方法

`Citrix Director`から、ターゲットセッションを見つけ、**セッションの詳細**ビューで**シャドウ**をクリックして、Linux VDAにシャドウイング要求を送信します。



接続が初期化されると、ICAセッションクライアント（`Citrix Director`クライアントではない）に確認が表示され、ユーザーにセッションをシャドウする許可を求めます。



ユーザーが**はい**をクリックすると、`Citrix Director`側にウィンドウが表示され、ICAセッションがシャドウされていることを示します。

使用方法の詳細については、Citrix Directorのドキュメントを参照してください。

制限事項

- セッションシャドウイングはイントラネット内でのみ使用するように設計されています。Citrix Gateway経由で接続する場合でも、外部ネットワークでは機能しません。Citrixは、外部ネットワークでのLinux VDAセッションシャドウイングについて一切の責任を負いません。
- セッションシャドウイングが有効になっている場合、ドメイン管理者はICAセッションを表示することしかできず、書き込みや制御の権限はありません。

- 管理者が`Citrix Director`から**シャドウ**をクリックすると、ユーザーにセッションをシャドウする許可を求める確認が表示されます。セッションは、セッションユーザーが許可を与えた場合にのみシャドウできます。
- 前述の確認には20秒のタイムアウト制限があります。時間が経過すると、シャドウイング要求は失敗します。
- 1つのセッションは、1人の管理者のみがシャドウできます。たとえば、管理者Bが管理者Aがシャドウしているセッションに対してシャドウ要求を送信した場合、ユーザーデバイスにユーザー権限取得の確認が再表示されます。ユーザーが同意すると、管理者Aのシャドウ接続は停止し、管理者Bのために新しいシャドウ接続が構築されます。管理者が同じセッションに対して別のシャドウ要求を送信した場合でも、新しいシャドウ接続を構築できます。
- セッションシャドウを使用するには、`Citrix Director` 7.16以降をインストールします。
- `Citrix Director`クライアントは、ターゲットのLinux VDAサーバーに接続するために、IPアドレスではなくFQDNを使用します。したがって、`Citrix Director`クライアントはLinux VDAサーバーのFQDNを解決できる必要があります。

トラブルシューティング

セッションシャドウが失敗した場合は、`Citrix Director`クライアントとLinux VDAの両方でデバッグを行います。

Citrix Directorクライアントで

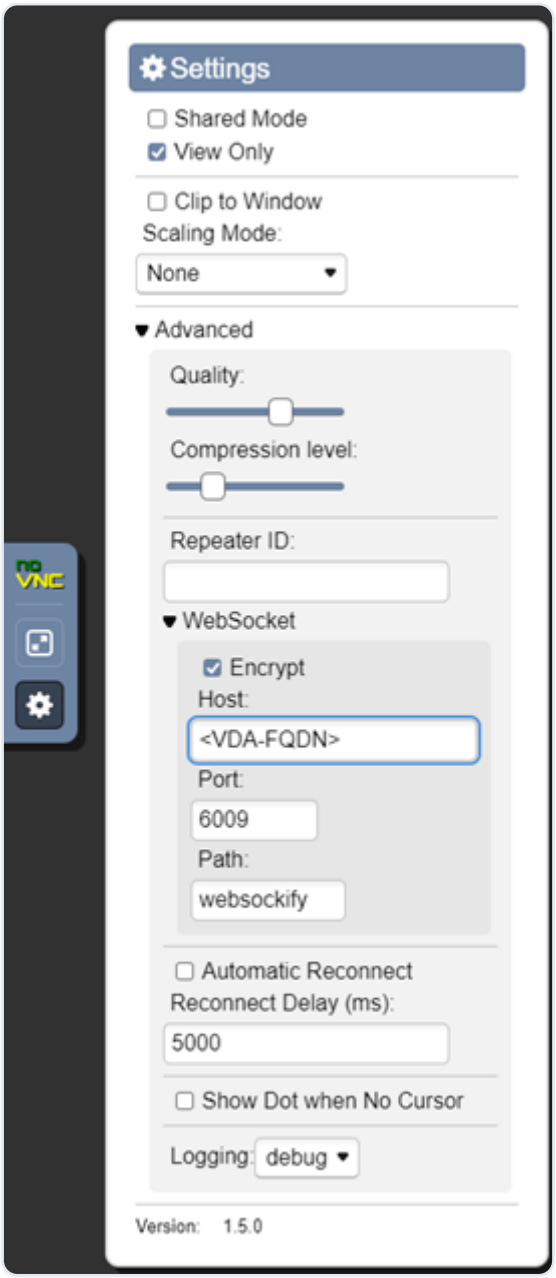
ブラウザの開発者ツールを使用して、**コンソール**タブで出力ログを確認します。または、**ネットワーク**タブでShadowLinuxSession APIの応答を確認します。ユーザー権限取得の確認が表示されても接続の確立に失敗する場合は、VDAのFQDNを手動でpingして、`Citrix Director`がFQDNを解決できることを確認します。`wss://`接続に問題がある場合は、証明書を確認してください。

Linux VDA において

1. `/var/log/xdl/vda.log`ファイルで手がかりを確認します。
2. `/var/xdl/sessionshadowing.sh`ファイルを編集し、「logFile」変数を変更して、Directorからのセッションシャドウ中に手がかりを追跡できるログファイルを指定します。
3. また、noVNC接続で証明書が正しく機能するかどうかを手動で確認できます。
    a. **ps aux \| grep xorg**を実行して、現在のセッションのXorgディスプレイ番号`<display-num>`（例: `:3`）を見つけます。
    b. 次のコマンドを実行して、x11vncサーバーを起動し、受信接続を待ちます。

```
runuser -l "ctxsrvr" -s /bin/bash -c "websockify <port> -v --cert  /
etc/xdl/shadowingssl/shadowingcert.pem --key  /etc/xdl/shadowingssl/
shadowingkey.key -- x11vnc  -viewonly  -shared -passwd <passwd>
-rfbport <port> -display <display-num> -many -o /var/log/xdl/
x11vnc.log"
```

c. noVNCを使用してSSLモードを確認するために、次のように接続を試行します。VDAのFQDNとポート番号を入力します。この例では、ポート番号は6009です。



d. VDA上のWebsockifyによって出力されたエラー、またはクライアント上のブラウザによって報告されたエラーを解決します。

接続確立中の主要なチェックポイント:

i. セッションシャドウイングがポートを開くのを妨げるファイアウォール制限がないか確認します。

ii. SSLシナリオの場合、証明書とキーファイルが適切に命名され、正しいパスに配置されていることを確認します。

iii. 新しいシャドウイング要求のために、6001～6099の間に十分なポートが残っていることを確認します。

iv. `/var/xdl/sessionshadowing.sh`で必要となるため、「netstat」がインストールされていることを確認します。

v. 証明書が正しく構成されていることを確認するために`openssl x509 -in shadowingcert.pem -text -noout`を実行し、特にCNフィールドとSANフィールドに注意してください。

vi. RHEL 8では、`rebind.so`が見つからないという問題が発生する可能性があります。この問題を解決するには、次のコマンドを実行します:

```
ln -s /usr/bin/rebind.so /usr/local/bin/rebind.so
```

監視サービスデーモン

監視サービスデーモンは、定期的なスキャンを実行することで主要なサービスを監視します。例外を検出すると、デーモンはサービスプロセスを再起動または停止し、リソースを解放するためにプロセスの残骸をクリーンアップします。検出された例外は、**/var/log/xdl/ms.log** ファイルに記録されます。

構成

監視サービスデーモンは、VDAを起動すると自動的に起動します。

管理者権限で、**/opt/Citrix/VDA/sbin** の下にある **scanningpolicy.conf**、**rulesets.conf**、および **whitelist.conf** ファイルを通じてこの機能を構成できます。

scanningpolicy.conf、**rulesets.conf**、および **whitelist.conf** ファイルでの変更を有効にするには、次のコマンドを実行して監視サービスデーモンを再起動します。

```
service ctxmonitorservice restart
```

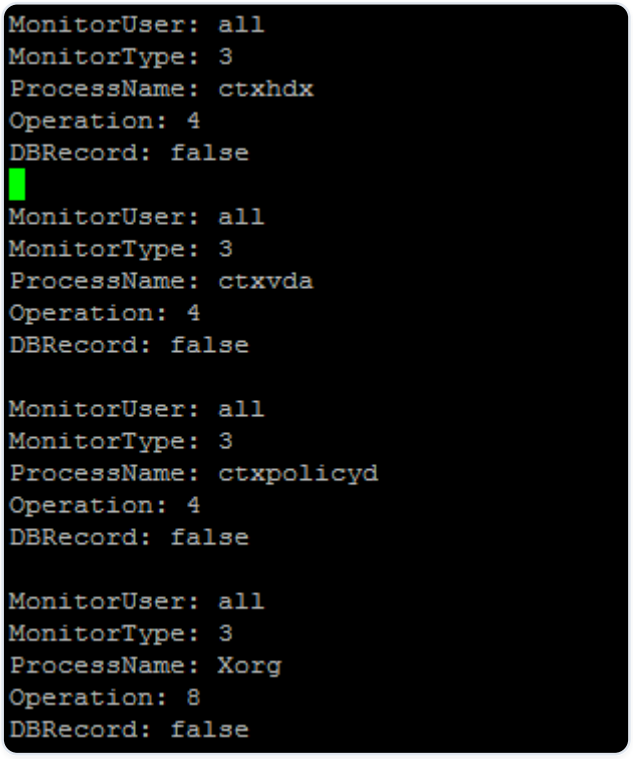
- **scanningpolicy.conf**

この構成ファイルは、監視サービスデーモンを有効または無効にします。サービス検出間隔を設定し、検出された例外を修復するかどうかを指定します。

- MonitorEnable: true/false (既定ではtrue)
- DetectTime: 20 (単位: 秒、既定値: 20、最小値: 5)
- AutoRepair: true/false (既定ではtrue)
- MultBalance: 無効
- ReportAlarm: 無効

- **rulesets.conf**

この構成ファイルは、監視するターゲットサービスを指定します。次のスクリーンショットに示すように、既定では4つの監視対象サービスがあります。



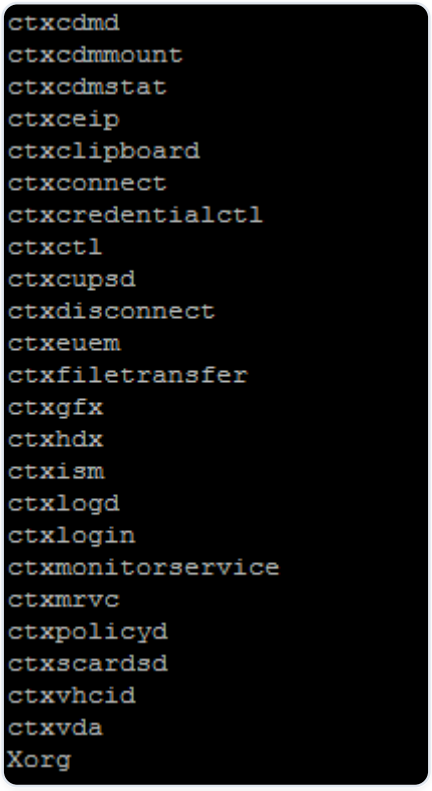
監視する各サービスを設定するには、次のフィールドを設定します。

- **MonitorUser**: すべて
- **MonitorType**: 3
- **ProcessName**: <> (プロセス名は空白にできず、完全に一致している必要があります。)
- **Operation**: 1/2/4/8 (1 = 例外が検出されたときにサービスを停止します。2 = 例外が検出されたときにサービスを強制終了します。4 = サービスを再起動します。8 = Xorg プロセス残存をクリアします。)
- **DBRecord**: 無効

- **whitelist.conf**

  rulesets.conf ファイルで指定されたターゲットサービスは、**whitelist.conf** ファイルでも構成する必要があります。ホワイトリスト構成は、セキュリティのためのセカンダリフィルターです。

  ホワイトリストを構成するには、**whitelist.conf** ファイルにプロセス名のみを含めます（完全に一致している必要があります）。例については、次のスクリーンキャプチャを参照してください。



注:

`ctxvda`、`ctxhdx`、および `ctxpolicyd` サービスを停止する前に、`service ctxmonitorservice stop` コマンドを実行してモニターサービスデーモンを停止します。そうしないと、モニターサービスデーモンが停止したサービスを再起動します。

ツールとユーティリティ

セッションデータクエリユーティリティ

各Linux VDAでセッションデータを照会するために使用できるユーティリティ（**ctxsdcutil**）を提供しています。VDAでホストされているすべてのセッションまたは特定のセッションの以下のデー

タを照会するには、`/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]`コマンドを実行します。`[-c]`引数は、1秒ごとにデータを照会することを意味します。

- **入力セッション帯域幅**
- **出力セッション帯域幅**
- **出力セッション回線速度**
- **遅延 - 最終記録**
- **ラウンドトリップタイム**
- **出力ThinWire帯域幅**
- **出力オーディオ帯域幅**
- **出力プリンター帯域幅**
- **入力ドライブ帯域幅**
- **出力ドライブ帯域幅**

xdlcollect Bashスクリプト

ログ収集に使用される**xdlcollect** Bashスクリプトは、Linux VDAソフトウェアに統合されており、**/opt/Citrix/VDA/bin**にあります。Linux VDAをインストールした後、bash **/opt/Citrix/VDA/bin/xdlcollect.sh**コマンドを実行してログを収集できます。ログ収集が完了すると、スクリプトと同じフォルダーに圧縮ログファイルが生成されます。**xdlcollect** Bashスクリプトは、圧縮ログファイルをCitrix Insight Services (CIS)にアップロードするかどうかを尋ねることができます。同意すると、アップロード完了後に**xdlcollect**はupload_IDを返します。アップロードによって、ローカルマシンから圧縮ログファイルが削除されることはありません。他のユーザーは、upload_IDを使用してCIS内のログファイルにアクセスできます。

エックスディーピング

Linux **XDPing** ツールはコマンドラインアプリケーションです。これは、Linux VDA 環境における一般的な構成の問題をチェックするプロセスを自動化します。

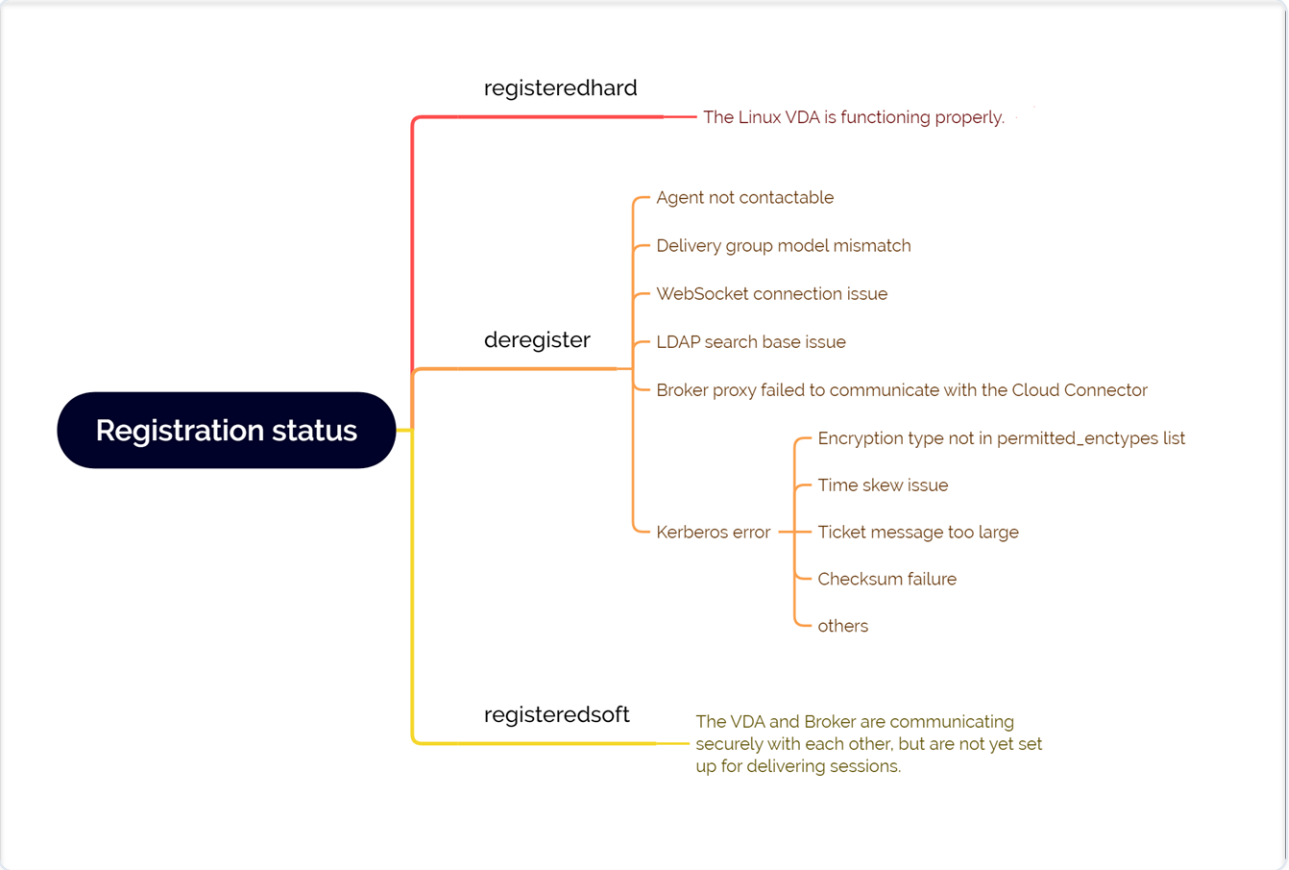
Linux **XDPing** ツールは、システム上で150以上の個別のテストを実行します。これらは大まかに次のように分類されます。

- Linux VDA のシステム要件が満たされているかを確認します
- Linux ディストリビューションを含むマシン情報を特定して表示します
- Linux カーネルの互換性を確認します

- Linux VDA の動作に影響を与える可能性のある既知の Linux ディストリビューションの問題を確認します
- Security-Enhanced Linux (SELinux) のモードと互換性を確認します
- ネットワークインターフェイスを特定し、ネットワーク設定を確認します
- ストレージのパーティション分割と利用可能なディスク容量を確認します
- マシンのホスト名とドメイン名の構成を確認します
- DNS 構成を確認し、ルックアップテストを実行します
- 基盤となるハイパーバイザーを特定し、仮想マシンの構成を確認します。サポート対象:
  - シトリックス ハイパーバイザー™
  - マイクロソフト ハイパーV
  - ヴイエムウェア ブイスフィア
- 時刻設定を確認し、ネットワーク時刻同期が動作しているかを確認します
- PostgreSQLサービスが適切に構成され、動作しているかを確認します。
- ファイアウォールが有効になっており、必要なポートが開いているかを確認します。
- Kerberosの構成を確認し、認証テストを実行します。
- グループポリシーサービスエンジン用のLDAP検索環境を確認します。
- Active Directory統合が適切に設定されており、現在のマシンがドメインに参加しているかを確認します。サポート対象:
  - サンバ・ウィンバインド
  - デル クエスト 認証サービス
  - セントリファイ・ダイレクトコントロール
  - SSSD
- Active Directory内のLinuxコンピューターオブジェクトの整合性を確認します。
- Pluggable Authentication Module (PAM) の構成を確認します。
- コアダンプパターンを確認します。
- Linux VDAに必要なパッケージがインストールされているかを確認します。
- Linux VDAパッケージを特定し、インストールの整合性を確認します。
- PostgreSQLレジストリデータベースの整合性を確認します。
- Linux VDAサービスが適切に構成され、動作しているかを確認します。

- VDAおよびHDX™構成の整合性を確認します。
- 各構成済みDelivery Controller™をプローブして、Broker Serviceが到達可能で、動作しており、応答性があることをテストします。
- マシンがDelivery Controllerファームに登録されているかを確認します。
- 各アクティブまたは切断されたHDXセッションの状態を確認します。
- Linux VDA関連のエラーと警告についてログファイルをスキャンします。
- Xorgのバージョンが適切であるかを確認します。
- 必要な依存関係がインストールされているかを確認します。

Linux XDPingツールは、VDA登録ステータスを確認および分析するのに役立つ分析モジュールも提供します。登録ステータスチェックの範囲については、次のスクリーンショットを参照してください。



Linux XDPingツールのインストール

ctxsetup.shを実行しても**XDPing**はインストールされません。**XDPing**をインストールするには、`sudo /opt/Citrix/VDA/bin/xdping`を実行します。 このコマンドは、**XDPing**に必要なPython3仮想環境も作成します。このコマンドでPython3仮想環境の作成に失敗した場合は、Python3仮想環境の作成の手順に従って手動で作成してください。

pipツールを使用する際に発生する可能性のあるSSL接続エラーに対処するには、次の信頼済みホストを/etc/pip.confファイルに追加することを検討してください。

`[global]`

`trusted-host =` `pypi.org`

`files.pythonhosted.org`

Linux XDPingツールの使用

XDPingには、コマンドシェルから実行される**xdping**という単一の実行可能ファイルが付属しています。

コマンドラインオプションを表示するには、**-h**オプションを使用します。

```
sudo /opt/Citrix/VDA/bin/xdping -h
```

テストの全スイートを実行するには、コマンドラインオプションなしで**xdping**を実行します。

```
sudo /opt/Citrix/VDA/bin/xdping
```

VDA登録ステータスチェックを実行するには、**-a**オプションを使用します。

```
sudo /opt/Citrix/VDA/bin/xdping -a
```

Linux VDAパッケージをインストールする前に環境を確認するには、**pre-flight**テストを実行します。

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
```

特定のテストカテゴリのみを実行するには、たとえば、時間テストとKerberosテストなど、**-T**オプションを使用します。

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
```

特定のXenDesktop® Controllerをプローブするには:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
```

出力例

以下は、Kerberosテストを実行したときの出力例です。

Kerberosテスト出力例の最初の部分(/en-us/linux-virtual-delivery-agent/2303/media/kerberos-test-sample-output-1.png)

Kerberosテスト出力例の2番目の部分(/en-us/linux-virtual-delivery-agent/2303/media/kerberos-test-sample-output-2.png)

Kerberosテスト出力例の3番目の部分(/en-us/linux-virtual-delivery-agent/2303/media/kerberos-test-sample-output-3.png)

その他

このセクションには、次のトピックが含まれています。

- HTML5向けCitrix Workspaceアプリのサポート
- Python3仮想環境の作成
- NISとActive Directoryの統合
- IPv6
- LDAPS
- **エックスオーソリティ**

Citrix Workspace™ app for HTML5 のサポート

Citrix Workspace app for HTML5 を使用すると、クライアントを Citrix Gateway に接続せずに、Linux 仮想アプリおよびデスクトップに直接アクセスできます。Citrix Workspace app for HTML5 の詳細については、Citrix ドキュメントを参照してください。

この機能を有効にする

この機能はデフォルトで無効になっています。有効にするには、次の手順を実行します。

1. Citrix StoreFront™ で、Citrix Workspace app for HTML5 を有効にします。

   詳細な手順については、Knowledge Center の記事 CTX208163のステップ1を参照してください。

2. WebSocket接続を有効にします。

   a. Citrix Studio で、**WebSockets connections**ポリシーを**Allowed**に設定します。

その他のWebSocketポリシーも設定できます。WebSocketポリシーの完全なリストについては、WebSockets policy settingsを参照してください。

b. 設定を有効にするには、VDAで`ctxvda`サービスと`ctxhdx`サービスをこの順序で再起動します。

c. VDAで、WebSocketリスナーが実行されているかどうかを確認するために、次のコマンドを実行します。

```
netstat -an | grep 8008
```

WebSocketリスナーが実行されている場合、コマンド出力は次のようになります。

```
tcp 0 0 :::8008 :::* LISTEN
```

注： WebSocket接続を保護するためにTLS暗号化を有効にすることもできます。TLS暗号化の有効化については、Secure user sessions using TLSを参照してください。

Python3仮想環境を作成する

ネットワークに接続している場合、`sudo /opt/Citrix/VDA/bin/xdping`または`/opt/Citrix/VDA/sbin/enable_ldaps.sh`コマンドを実行すると、Python3仮想環境を作成できます。ただし、コマンドでPython3仮想環境を作成できない場合は、ネットワーク接続がなくても手動で作成できます。この記事では、ネットワーク接続なしでPython3仮想環境を作成するための前提条件と手順について詳しく説明します。

前提条件

- `/opt/Citrix/VDA/sbin/ctxpython3`ディレクトリにアクセスするための管理者権限が必要です。
- `Python3`パッケージのwheelファイルが配置されていること。wheelファイルは`<https://pypi.org/>`からダウンロードできます。

Python3仮想環境を作成する

Python3仮想環境を作成するには、次の手順を実行します。

1. Python3の依存関係をインストールします。

   Amazon Linux 2の場合：

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   ```

   RHELおよびRocky Linuxの場合：

```
yum -y install python3-devel krb5-devel gcc
```

注:

一部の依存関係をインストールするには、特定のレポジトリを有効にする必要がある場合があります。RHEL 7の場合は、`subscription-manager repos --enable rhel-7-server-optional-rpms`コマンドを実行します。RHEL 8の場合は、`subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms`コマンドを実行します。

Debian、Ubuntuの場合：

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

SUSEの場合：

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
```

2. Python3仮想環境を作成します。

注:

pipツールを使用する際に発生する可能性のあるSSL接続エラーに対処するには、次の信頼済みホストを/etc/pip.confファイルに追加することを検討してください。

\>`[global]`

`trusted-host =`

\>`pypi.org`

`files.pythonhosted.org`

アマゾン Linux 2、デビアン、RHEL、ロッキー Linux、ウブントゥの場合:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

SUSE の場合:

```
sudo ln -s /usr/lib/mit/bin/krb5-config /usr/bin/krb5-config



export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin



sudo mkdir -p /usr/lib/mit/include/gssapi/



sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/gssapi/
gssapi_ext.h



sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

3. LDAPS の依存関係をインストールします。

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
upgrade pip==21.3.1



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi==1.7.3
ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
```

4. **XDPing** の依存関係をインストールします。

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
upgrade pip==21.3.1



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1
gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging==21.3
pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser==2.21
pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor==1.1.0



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

NISとActive Directoryの統合

この記事では、SSSDを使用してLinux VDAでNISとWindows Active Directory (AD) を統合する方法について説明します。Linux VDAはCitrix Virtual Apps and Desktopsのコンポーネントと見なされます。その結果、Windows AD環境にしっかりと適合します。

UIDおよびGIDプロバイダーとしてADの代わりにNISを使用する場合、アカウント情報（ユーザー名とパスワードの組み合わせ）がADとNISで同じである必要があります。

注:

認証は引き続きADサーバーによって実行されます。NIS+はサポートされていません。NISをUIDおよびGIDプロバイダーとして使用する場合、WindowsサーバーからのPOSIX属性は使用されなくなります。

ヒント:

この方法は、Linux VDAを展開する非推奨の方法であり、特別なユースケースでのみ使用されます。RHEL/CentOSディストリビューションの場合は、Amazon Linux 2、CentOS、RHEL、およびRocky LinuxにLinux VDAを手動でインストールするの手順に従ってください。Ubuntuディストリビューションの場合は、UbuntuにLinux VDAを手動でインストールするの手順に従ってください。

> SSSDとは？

SSSDはシステムデーモンです。その主な機能は、システムのキャッシュとオフラインサポートを提供できる共通のフレームワークを通じて、リモートリソースを識別および認証するためのアクセスを提供することです。PAMモジュールとNSSモジュールの両方を提供し、将来的には拡張ユーザー情報のためのD-BUSベースのインターフェイスをサポートできます。また、ローカルユーザーアカウントと拡張ユーザーデータを保存するためのより優れたデータベースも提供します。

NISとADの統合

NISをADと統合するには、次の手順を実行します。

ステップ1：LINUX VDAをNISクライアントとして追加する

NISクライアントを構成します。

```
yum –y install ypbind rpcbind oddjob-mkhomedir
```

NISドメインを設定します。

```
ypdomainname nis.domain

echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

NISサーバーとクライアントのIPアドレスを **/etc/hosts** に追加します。

```
{NIS server IP address}   server.nis.domain nis.domain
```

`authconfig` でNISを構成します。

```
sudo authconfig --enablenis --nisdomain=nis.domain --
nisserver=server.nis.domain --enablemkhomedir --update
```

nis.domain はNISサーバーのドメイン名を表します。**server.nis.domain** はNISサーバーのホスト名であり、NISサーバーのIPアドレスでもかまいません。

NISサービスを設定します:

```
sudo systemctl start rpcbind ypbind
```

```
sudo systemctl enable rpcbind ypbind
```

NIS構成が正しいことを確認します:

```
ypwhich
```

アカウント情報がNISサーバーから利用可能であることを検証します:

```
getent passwd nisaccount
```

> **注:**
>
> **nisaccount** は、NISサーバー上の実際のNISアカウントを表します。UID、GID、ホームディレクトリ、およびログインシェルが正しく構成されていることを確認してください。

ステップ2：SAMBAを使用してドメインに参加し、ホストキータブを作成する

SSSDは、ドメインへの参加やシステムキータブファイルの管理のためのADクライアント機能を提供しません。これらの機能を実現するにはいくつかの方法があり、以下が含まれます:

- `adcli`
- `realmd`
- `Winbind`
- `Samba`

このセクションの情報は、Sambaのアプローチのみを説明しています。`realmd`については、RHELまたはCentOSベンダーのドキュメントを参照してください。これらの手順は、SSSDを構成する前に実行する必要があります。

Sambaを使用してドメインに参加し、ホストキータブを作成する:

適切に構成されたファイルを持つLinuxクライアントで:

- /etc/krb5.conf
- /etc/samba/smb.conf:

SambaおよびKerberos認証用にマシンを構成します:

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM
--krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
```

ここで、**REALM** は大文字のKerberosレルム名であり、**domain** はドメインのNetBIOS名です。

KDCサーバーとレルム名のDNSベースのルックアップが必要な場合は、前のコマンドに次の2つのオプションを追加します:

`--enablekrb5kdcdns --enablekrb5realmdns`

/etc/samba/smb.conf を開き、**authconfig** ツールによって生成されたセクションの後に、**\[Global\]** セクションの下に次のエントリを追加します:

`kerberos method = secrets and keytab`

`winbind offline logon = no`

Windowsドメインに参加するには、ドメインコントローラーに到達可能であり、コンピューターをドメインに追加する権限を持つADユーザーアカウントが必要です。

```
sudo net ads join REALM -U user
```

REALM は大文字のKerberosレルム名であり、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

ステップ3：SSSDのセットアップ

SSSDのセットアップは、次の手順で構成されます。

- Linuxクライアントマシンに **sssd-ad** および **sssd-proxy** パッケージをインストールします。
- さまざまなファイル（例：**sssd.conf**）に構成変更を加えます。
- **sssdサービス** を開始します。

/etc/sssd/sssd.conf
sssd.conf 構成の例（必要に応じてオプションを追加できます）：

```
[sssd]

config_file_version = 2

domains = EXAMPLE
```

```
services = nss, pam



[domain/EXAMPLE]

# Uncomment if you need offline logins

# cache_credentials = true

re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?
P<domain>.+$))|(^(?P<name>[^@\\]+)$))

id_provider = proxy

proxy_lib_name = nis

auth_provider = ad

access_provider = ad



# Should be specified as the long version of the Active Directory domain.

ad_domain = EXAMPLE.COM



# Kerberos settings

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U



# Uncomment if service discovery is not working

# ad_server = server.ad.example.com
```

```
# Comment out if the users have the shell and home dir set on the AD side

default_shell = /bin/bash

fallback_homedir = /home/%d/%u



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

ad.domain.com、**server.ad.example.com** を対応する値に置き換えます。詳細については、**sssd-ad**(5) - Linux man page を参照してください。

sssd.conf のファイルの所有権と権限を設定します。

`chown root:root /etc/sssd/sssd.conf`

`chmod 0600 /etc/sssd/sssd.conf` `restorecon /etc/sssd/sssd.conf`

ステップ4：NSS/PAMの構成

RHEL/CentOS:

authconfig を使用してSSSDを有効にします。ホームディレクトリの作成がSELinuxと互換性があることを確認するために **oddjob-mkhomedir** をインストールします。

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update



sudo systemctl start sssd



sudo systemctl enable sssd
```

ヒント:

> Linux VDA設定を構成する際、SSSDにはLinux VDAクライアント用の特別な設定がないことに注意してください。**ctxsetup.sh** スクリプトの追加ソリューションについては、デフォルト値を使用してください。

ステップ5：KERBEROS構成を確認する

KerberosがLinux VDAで使用するために正しく構成されていることを確認するには、システム**keytab**ファイルが作成され、有効なキーが含まれていることを確認します。

```
sudo klist -ke
```

このコマンドは、プリンシパル名と暗号スイートのさまざまな組み合わせで利用可能なキーのリストを表示します。Kerberos **kinit**コマンドを実行して、これらのキーを使用してマシンをドメインコントローラーで認証します。

```
sudo kinit –k MACHINE\$@REALM
```

マシン名とレルム名は大文字で指定する必要があります。ドル記号 ($) は、シェル置換を防ぐためにバックスラッシュ (\\) でエスケープする必要があります。一部の環境では、DNSドメイン名がKerberosレルム名と異なります。レルム名が使用されていることを確認してください。このコマンドが成功した場合、出力は表示されません。

マシンアカウントのTGTチケットがキャッシュされていることを確認するには、次を使用します。

```
sudo klist -ke
```

ステップ6：ユーザー認証を確認する

getentコマンドを使用して、ログオン形式がサポートされているか、NSSが機能しているかを確認します。

```
sudo getent passwd DOMAIN\\username
```

DOMAINパラメーターは、短いバージョンのドメイン名を示します。別のログオン形式が必要な場合は、まず**getent**コマンドを使用して確認してください。

サポートされているログオン形式は次のとおりです。

- ダウンレベルログオン名：`DOMAIN\username`

- UPN：`username@domain.com`
- NetBIOSサフィックス形式：`username@DOMAIN`

SSSD PAMモジュールが正しく構成されていることを確認するには、ドメインユーザーアカウントを使用してLinux VDAにログオンします。このドメインユーザーアカウントは以前使用されたことがありません。

```
sudo ssh localhost –l DOMAIN\\username



id -u
```

コマンドによって返された**uid**に対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_{uid}
```

ユーザーのKerberos資格情報キャッシュ内のチケットが有効で期限切れになっていないことを確認します。

```
klist
```

IPv6

Linux VDAは、Citrix Virtual Apps and Desktopsと連携するためにIPv6をサポートしています。この機能を使用する際は、次の点を考慮してください。

- デュアルスタック環境では、IPv6が明示的に有効になっていない限り、IPv4が使用されます。
- IPv4環境でIPv6が有効になっている場合、Linux VDAは機能しません。

> **重要:**
>
> - ネットワーク環境全体がIPv6である必要があり、Linux VDAだけでなく全体がIPv6である必要があります。
> - Centrifyは純粋なIPv6をサポートしていません。

> Linux VDAをインストールする際に、IPv6に関する特別なセットアップタスクは必要ありません。

Linux VDAのIPv6を構成する

Linux VDAの構成を変更する前に、Linux仮想マシンが以前にIPv6ネットワークで動作していたことを確認してください。IPv6構成に関連するレジストリキーは2つあります。

```
“HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD” -v
“OnlyUseIPv6ControllerRegistration”

“HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD” -v
“ControllerRegistrationIPv6Netmask”
```

Linux VDAでIPv6を有効にするには、**OnlyUseIPv6ControllerRegistration**を1に設定する必要があります。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

Linux VDAに複数のネットワークインターフェイスがある場合、**ControllerRegistrationIPv6Netmask**を使用して、Linux VDAの登録に使用するインターフェイスを指定できます。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ControllerRegistrationIPv6Netmask " -d "{IPv6 netmask}" --force
```

{IPv6 ネットマスク} を実際のネットマスク（例：2000::/64）に置き換えてください。

Citrix Virtual Apps and DesktopsでのIPv6展開の詳細については、「IPv4/IPv6のサポート」を参照してください。

トラブルシューティング

基本的なIPv6ネットワーク環境を確認し、ping6を使用してADおよびDelivery Controller™に到達可能かどうかを確認します。

LDAPS

LDAPS は、TLS/SSL を使用して LDAP 通信が暗号化される、Lightweight Directory Access Protocol (LDAP) のセキュアバージョンです。

デフォルトでは、クライアントアプリケーションとサーバーアプリケーション間の LDAP 通信は暗号化されません。LDAPS を使用すると、Linux VDA と LDAP サーバー間の LDAP クエリコンテンツを保護できます。

以下の Linux VDA コンポーネントは LDAPS に依存しています。

- ブローカーエージェント: Delivery Controller™ への Linux VDA 登録
- ポリシーサービス: ポリシー評価

LDAPS の構成には以下が含まれます。

- Active Directory (AD)/LDAP サーバーで LDAPS を有効にする
- クライアントで使用するためにルート CA をエクスポートする
- Linux VDA で LDAPS を有効/無効にする
- サードパーティプラットフォーム向けに LDAPS を構成する
- SSSD を構成する
- Winbind を構成する
- Centrify を構成する
- Quest を構成する

注:

LDAP サーバーの監視サイクルを設定するには、次のコマンドを実行します。デフォルト値は 15 分です。少なくとも 10 分に設定してください。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"ListOfLDAPServersMonitorPeroid" -t "REG_DWORD" -d "0x0000000f" --
force
```

AD/LDAPサーバーでLDAPSを有効にする

Microsoft 認証局 (CA) または Microsoft 以外の CA のいずれかから、適切な形式の証明書をインストールすることで、LDAP over SSL (LDAPS) を有効にできます。

> **ヒント:**
>
> ドメインコントローラーにエンタープライズルート CA をインストールすると、LDAPS は自動的に有効になります。

> 証明書のインストール方法と LDAPS 接続の確認方法の詳細については、サードパーティの認証局で LDAP over SSL を有効にする方法を参照してください。

多層認証局階層を使用している場合、ドメインコントローラーでの LDAPS 認証のために適切な証明書が自動的に提供されるわけではありません。

多層認証局階層を使用してドメインコントローラーで LDAPS を有効にする方法については、LDAP over SSL (LDAPS) 証明書の記事を参照してください。

クライアントでの使用のためにルート認証局を有効にする

クライアントは、LDAP サーバーが信頼する CA からの証明書を使用する必要があります。クライアントの LDAPS 認証を有効にするには、ルート CA 証明書を信頼されたキーストアにインポートします。

ルート CA のエクスポート方法の詳細については、Microsoft サポート Web サイトのルート認証局証明書をエクスポートする方法を参照してください。

Linux VDA での LDAPS の有効化または無効化

Linux VDA で LDAPS を有効または無効にするには、（管理者としてログオンした状態で）次のスクリプトを実行します。

このコマンドの構文には、以下が含まれます。

- 提供されたルート CA 証明書を使用して LDAP over SSL/TLS を有効にする:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- チャネルバインディングを使用して LDAP over SSL/TLS を有効にする:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
```

注:

チャネルバインディング用のルート CA 証明書は PEM 形式である必要があります。
LDAPS を有効にしても Python3 仮想環境が正常に作成されない場合は、Python3 仮想環境を作成するの手順に従って手動で作成してください。

pipツールを使用する際に発生する可能性のあるSSL接続エラーに対処するには、次の信頼できるホストを/etc/pip.confファイルに追加することを検討してください。

\>`[global]`

`trusted-host =`

\>`pypi.org`

`files.pythonhosted.org`

- SSL/TLSなしでLDAPにフォールバックする

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

LDAPS専用のJavaキーストアは **/etc/xdl/.keystore** にあります。影響を受けるレジストリキーは次のとおりです。

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers



HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
```

```
HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS


HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore


HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
```

サードパーティプラットフォーム向けLDAPSの構成

Linux VDAコンポーネントの他に、VDAに準拠するSSSD、Winbind、Centrify、QuestなどのいくつかのサードパーティソフトウェアコンポーネントもセキュアLDAPを必要とする場合があります。以下のセクションでは、LDAPS、STARTTLS、またはSASLサインアンドシールを使用してセキュアLDAPを構成する方法について説明します。

ヒント:

これらのソフトウェアコンポーネントのすべてが、セキュアLDAPを確保するためにSSLポート636を使用することを好むわけではありません。そしてほとんどの場合、LDAPS（ポート636上のSSL経由のLDAP）はポート389上のSTARTTLSと共存できません。

SSSD

オプションに従って、ポート636またはポート389でSSSDセキュアLDAPトラフィックを構成します。詳細については、SSSD LDAP Linux manページを参照してください。

ウィンバインド

Winbind LDAPクエリはADSメソッドを使用します。Winbindはポート389でのStartTLSメソッドのみをサポートします。影響を受ける構成ファイルは **/etc/samba/smb.conf** および **/etc/openldap/ldap.conf** (RHELの場合) または **/etc/ldap/ldap.conf** (Ubuntuの場合) です。ファイルを次のように変更します。

- smb.conf

  `ldap ssl = start tls`

  `ldap ssl ads = yes` `client ldap sasl wrapping = plain`

- ldap.conf

`TLS_REQCERT never`

あるいは、SASL GSSAPIサインアンドシールによってセキュアLDAPを構成することもできますが、TLS/SSLとは共存できません。SASL暗号化を使用するには、**smb.conf**構成を変更します。

`ldap ssl = off`

`ldap ssl ads = no` `client ldap sasl wrapping = seal`

セントリファイ

Centrifyはポート636でのLDAPSをサポートしていません。ただし、ポート389ではセキュアな暗号化を提供します。詳細については、Centrifyサイトを参照してください。

クエスト

Quest Authentication Service はポート 636 での LDAPS をサポートしていませんが、別の方法を使用してポート 389 で安全な暗号化を提供します。

トラブルシューティング

この機能を使用すると、以下の問題が発生する可能性があります。

- **LDAPS サービスの可用性**

  AD/LDAP サーバーで LDAPS 接続が利用可能であることを確認します。ポートはデフォルトで 636 です。

- **LDAPS が有効な場合に Linux VDA の登録に失敗しました**

  LDAP サーバーとポートが正しく構成されていることを確認します。まずルート CA 証明書を確認し、AD/LDAP サーバーと一致していることを確認します。

- **誤ってレジストリが変更された**

  enable_ldaps.sh を使用せずに誤って LDAPS 関連のキーを更新した場合、LDAPS コンポーネントの依存関係が壊れる可能性があります。

- **Wireshark またはその他のネットワーク監視ツールから SSL/TLS 経由で LDAP トラフィックが暗号化されていない**

  デフォルトでは、LDAPS は無効になっています。強制的に有効にするには、**/opt/Citrix/VDA/sbin/enable_ldaps.sh** を実行します。

- **Wireshark またはその他のネットワーク監視ツールから LDAPS トラフィックがない**

  LDAP/LDAPS トラフィックは、Linux VDA の登録とグループポリシーの評価が行われるときに発生します。

- **AD サーバーで ldp connect を実行して LDAPS の可用性を確認できませんでした**

  IP アドレスの代わりに AD FQDN を使用します。

- **/opt/Citrix/VDA/sbin/enable_ldaps.sh スクリプトの実行時にルートCA証明書のインポートに失敗しました**

  CA証明書のフルパスを指定し、ルートCA証明書が正しいタイプであることを確認してください。これは、サポートされているほとんどのJava Keytoolタイプと互換性があるはずです。サポートリストにない場合は、まずタイプを変換できます。証明書形式の問題が発生した場合は、base64エンコードされたPEM形式をお勧めします。

- **Keytool -list でルートCA証明書を表示できませんでした**

  `/opt/Citrix/VDA/sbin/enable_ldaps.sh` を実行してLDAPSを有効にすると、証明書は /etc/xdl/.keystore にインポートされ、キーストアを保護するためにパスワードが設定されます。パスワードを忘れた場合は、スクリプトを再実行してキーストアを作成できます。

Xオーソリティ

Linux VDAは、インタラクティブなリモートアクセスにX11ディスプレイ機能（`xterm`や`gvim`を含む）を使用する環境をサポートしています。この機能は、XClientとXServer間の安全な通信を確保するために必要なセキュリティメカニズムを提供します。

この安全な通信のアクセス許可を保護するには、2つの方法があります。

- **Xhost**。デフォルトでは、Xhostはローカルホストの XClientのみがXServerと通信することを許可します。リモートのXClientがXServerにアクセスすることを許可する場合は、特定のコンピューターでXhostコマンドを実行してアクセス許可を付与する必要があります。または、**xhost +** を使用して、任意のXClientがXServerに接続できるようにすることもできます。
- **Xauthority**。`.Xauthority`ファイルは各ユーザーのホームディレクトリにあります。これは、XServerの認証のためにxauthが使用するクッキーに認証情報を保存するために使用されます。XServerインスタンス（Xorg）が起動すると、その特定のディスプレイへの接続を認証するためにクッキーが使用されます。

仕組み

Xorgが起動すると、`.Xauthority`ファイルがXorgに渡されます。この`.Xauthority`ファイルには、以下の要素が含まれています。

- ディスプレイ番号
- リモート要求プロトコル
- クッキー番号

`xauth`コマンドを使用してこのファイルを参照できます。例：

```
# xauth -f ~/.Xauthority



# > list



# > us01msip06:107  MIT-MAGIC-COOKIE-1  fb228d1b695729242616c5908f11624b
```

XClientがXorgにリモートで接続する場合、2つの前提条件を満たす必要があります。

- **DISPLAY**環境変数をリモートXServerに設定する。
- Xorg内のクッキー番号のいずれかを含む`.Xauthority`ファイルを取得する。

Xauthorityの構成

リモートX11ディスプレイのためにLinux VDAで**Xauthority**を有効にするには、以下の2つのレジストリキーを作成する必要があります。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"XauthEnabled" -d "0x00000001" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"ListenTCP" -d "0x00000001" --force
```

Xauthority を有効にした後、`.Xauthority` ファイルを **XClient** に手動で渡すか、共有ホームディレクトリをマウントして渡します。

- `.Xauthority` ファイルを XClient に手動で渡す

  ICA® セッションを起動すると、Linux VDA は XClient 用の `.Xauthority` ファイルを生成し、ログオンユーザーのホームディレクトリに保存します。この `.Xauthority` ファイルをリモートの XClient マシンにコピーし、**DISPLAY** および **XAUTHORITY** 環境変数を設定できます。`DISPLAY` は `.Xauthority` ファイルに保存されているディスプレイ番号であり、

`XAUTHORITY` は **Xauthority** のファイルパスです。例については、次のコマンドを参照してください。

```
export DISPLAY={Display number stored in the Xauthority file}



export XAUTHORITY={the file path of .Xauthority}
```

> **注:**
>
> **XAUTHORITY** 環境変数が設定されていない場合、デフォルトで `~/.Xauthority` ファイルが使用されます。

- 共有ホームディレクトリをマウントして `.Xauthority` ファイルを XClient に渡す

  便利な方法は、ログオンユーザー用に共有ホームディレクトリをマウントすることです。Linux VDA が ICA セッションを開始すると、`.Xauthority` ファイルがログオンユーザーのホームディレクトリに作成されます。このホームディレクトリが XClient と共有されている場合、ユーザーはこの `.Xauthority` ファイルを XClient に手動で転送する必要はありません。**DISPLAY** および **XAUTHORITY** 環境変数が正しく設定されると、GUI は XServer デスクトップに自動的に表示されます。

トラブルシューティング

Xauthority が機能しない場合は、以下のトラブルシューティング手順に従ってください。

1. root 権限を持つ管理者として、すべての Xorg クッキーを取得します。

   ```
   ps aux | grep -i xorg
   ```

   このコマンドは、Xorg プロセスと、起動時に Xorg に渡されたパラメーターを表示します。別のパラメーターは、どの `.Xauthority` ファイルが使用されているかを表示します。例：

   ```
   /var/xdl/xauth/.Xauthority110
   ```

   Xauth コマンドを使用してクッキーを表示します。

```
Xauth -f /var/xdl/xauth/.Xauthority110
```

2. `Xauth` コマンドを使用して、`~/.Xauthority` に含まれるクッキーを表示します。同じディスプレイ番号の場合、表示されるクッキーは Xorg と XClient の `.Xauthority` ファイルで同じである必要があります。
3. クッキーが同じである場合は、Linux VDA の IP アドレスと公開デスクトップのディスプレイ番号を使用して、リモートディスプレイポートのアクセシビリティを確認します。

   たとえば、XClient マシンで次のコマンドを実行します。

   ```
   telnet 10.158.11.11 6160
   ```

   ポート番号は 6000 + \<display number\> の合計です。

   この telnet 操作が失敗した場合、ファイアウォールが要求をブロックしている可能性があります。

認証

このセクションには、次のトピックが含まれています。

- Azure Active Directory を使用した認証
- ダブルホップシングルサインオン認証
- フェデレーション認証サービス
- SSO 以外の認証
- スマートカード
- 匿名ユーザーによる非認証セッション

Azure Active Directory を使用した認証

注:

この機能は、Azure でホストされている VDA でのみ利用できます。

必要に応じて、Azure には2種類のLinux VDAを展開できます。

- Azure AD DS に参加しているVM。VMはAzure Active Directory (AAD) Domain Services (DS) マネージド ドメインに参加しています。ユーザーはドメイン資格情報を使用してVMにログオンします。
- ドメインに参加していないVM。VMはAAD IDサービスと統合してユーザー認証を提供します。ユーザーはAAD資格情報を使用してVMにログオンします。

AAD DSとAADの詳細については、このMicrosoft記事を参照してください。

この記事では、ドメインに参加していないVDAでAAD IDサービスを有効にして構成する方法について説明します。

サポートされているディストリビューション

- Ubuntu 22.04版、20.04版、18.04版
- RHEL 8.7、8.6、8.4、7.9
- SUSE 15.4

詳細については、このMicrosoftの記事を参照してください。

既知の問題と回避策

RHEL 7.9では、AADユーザー認証後にPAM (Pluggable Authentication Module) `pam_loginuid.so` が `loginuid` の設定に失敗します。この問題により、AADユーザーはVDAセッションにアクセスできません。

この問題を回避するには、`/etc/pam.d/remote` で、行 `Session required pam_loginuid.so` をコメントアウトします。例については、次のスクリーンショットを参照してください。

```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

ステップ1：Azureポータルでテンプレートvmを作成する

テンプレートVMを作成し、そのVMにAzure CLIをインストールします。

1. Azure portalでテンプレートVMを作成します。「**Review + create**」をクリックする前に、「**Management**」タブで「**Login with Azure AD**」を必ず選択してください。

   AADでのログインを有効にする設定(/en-us/linux-virtual-delivery-agent/2303/media/aad-auth-create-vm.png)

2. テンプレートVMにAzure CLIをインストールします。 詳細については、このMicrosoft記事を参照してください。

ステップ2：テンプレートVMでマスターイメージを準備する

マスターイメージを準備するには、Use MCS to create Linux VMs on Azureの「**ステップ3：マスターイメージを準備する**」に従ってください。

ステップ3：テンプレートVMを非ドメイン参加モードに設定する

マスターイメージを作成したら、以下の手順に従ってVMを非ドメイン参加モードに設定します。

1. コマンドプロンプトから次のスクリプトを実行します。

   ```
   Modify /var/xdl/mcs/mcs_util.sh
   ```

2. `function read_non_domain_joined_info()`を見つけて、`NonDomainJoined`の値を`2`に変更します。例については、次のコードブロックを参照してください。

   ```
   function read_non_domain_joined_info()

   {

   log "Debug: Enter read_non_domain_joined_info"

   # check if websocket enabled

   TrustIdentity=`cat ${id_disk_mnt_point}${ad_info_file_path} | grep '\
   [TrustIdentity\]' | sed 's/\s//g'`

   if [ "$TrustIdentity" == "[TrustIdentity]" ]; then

   NonDomainJoined=2

   fi

   ...
   ```

```
}
```

3. 変更を保存します。
4. テンプレートVMをシャットダウンします。

ステップ4：テンプレートVMからLinux VMを作成する

非ドメイン参加のテンプレートVMの準備ができたら、以下の手順に従ってVMを作成します。

1. Citrix Cloudにサインインします。
2. Citrix DaaS™をダブルクリックし、Full Configuration管理コンソールにアクセスします。
3. 「**マシンカタログ**」で、テンプレートVMからLinux VMを作成するためにMachine Creation Servicesを使用することを選択します。詳しくは、Citrix DaaSの記事「ドメインに参加していない」を参照してください。

ステップ5：Linux VMにAADユーザーアカウントを割り当てる

ドメインに参加していないVMを作成したら、それらにAADユーザーアカウントを割り当てます。

VMにAADユーザーアカウントを割り当てるには、次の手順に従います。

1. 管理者アカウントを使用してVMにアクセスします。
2. 「**ID > システム割り当て済み**」タブで、「**システムID**」を有効にします。

   AADでのログインを有効にする設定(/en-us/linux-virtual-delivery-agent/2303/media/aad-auth-identity-setting.png)
3. 「**アクセス制御 (IAM) > ロールの割り当て**」タブで、「**仮想マシンユーザーログイン**」領域を見つけ、必要に応じてAADユーザーアカウントを追加します。

   AADでのログインを有効にする設定(/en-us/linux-virtual-delivery-agent/2303/media/aad-auth-assign-aad-account.png)

ドメインに参加していないVDAへのログオン

組織のエンドユーザーは、ドメインに参加していないVDAに2つの方法でログオンできます。詳細な手順は次のとおりです。

1. Workspaceアプリを起動し、AADユーザー名とパスワードを入力してワークスペースにログオンします。Workspaceページが表示されます。

2. ドメインに参加していないデスクトップをダブルクリックします。AADログインページが表示されます。

   ページは、VDAに設定されているログインモード（デバイスコードまたはAADアカウント/パスワード）によって異なります。デフォルトでは、Linux VDAは次のようにデバイスコードログインモードを使用してAADユーザーを認証します。管理者は、必要に応じてログインモードをAADアカウント/パスワードに変更できます。詳細な手順については、次のセクションを参照してください。

   AADでのログインを有効にする設定(/en-us/linux-virtual-delivery-agent/2303/media/aad-auth-device-code.png)

3. 画面の指示に従って、次のいずれかの方法でデスクトップセッションにログオンします。

   - QRコードをスキャンし、コードを入力します。
   - AADユーザー名とパスワードを入力します。

AADアカウント/パスワードログインモードへの変更

デフォルトでは、Linux VDAはデバイスコードを使用してAADユーザーを認証します。詳細については、このMicrosoft記事を参照してください。ログインモードを*AADアカウント/パスワード*に変更するには、次の手順に従います。

VDAで次のコマンドを実行し、キー`AADAcctPwdAuthEnable`を見つけ、その値を`0x00000001`に変更します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket" -t
"REG_DWORD" -v "AADAcctPwdAuthEnable" -d "0x00000001" --force
```

注:

この方法は、Microsoftアカウントまたは2要素認証が有効になっているアカウントでは機能しません。

ダブルホップシングルサインオン認証

StoreFrontストアにアクセスするためのユーザー資格情報は、Citrix Workspaceアプリ for LinuxおよびCitrix Receiver for Linux 13.10のAuthManagerモジュールに挿入できます。挿入後、クライア

ントを使用して、Linux仮想デスクトップセッション内から仮想デスクトップおよびアプリケーションに、ユーザー資格情報を再度入力することなくアクセスできます。

注:

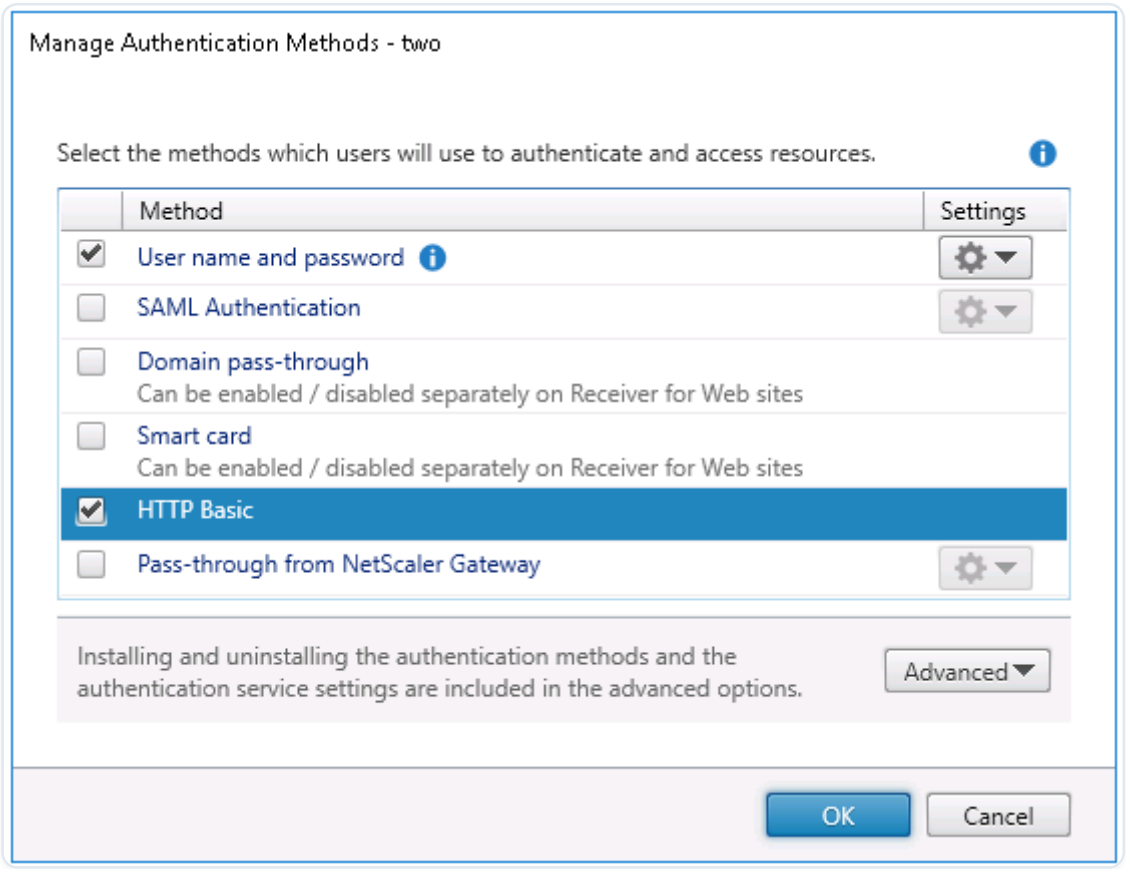
この機能は、Citrix Workspaceアプリ for LinuxおよびCitrix Receiver for Linux 13.10でサポートされています。

この機能を有効にするには：

1. Linux VDAに、Citrix Workspaceアプリ for LinuxまたはCitrix Receiver for Linux 13.10をインストールします。

   Citrix WorkspaceアプリまたはCitrix Receiver向けに、Citrixダウンロードページからアプリをダウンロードします。

   デフォルトのインストールパスは/opt/Citrix/ICAClient/です。アプリを別のパスにインストールする場合は、ICAROOT環境変数を実際のインストールパスを指すように設定します。
2. Citrix StoreFront™管理コンソールで、ターゲットストアに**HTTP Basic**認証方法を追加します。



3. HTTP Basic認証を許可するために、AuthManager構成ファイル（$ICAROOT/config/AuthManConfig.xml）に次のキーを追加します。

```
<Protocols>

     <HTTPBasic>

         <Enabled>True</Enabled>

    </HTTPBasic>

</Protocols>
```

4. 指定されたディレクトリにルート証明書をインストールするには、次のコマンドを実行します。

```
cp rootcert.pem $ICAROOT/keystore/cacerts/

$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

5. この機能を有効にするには、次のコマンドを実行します。

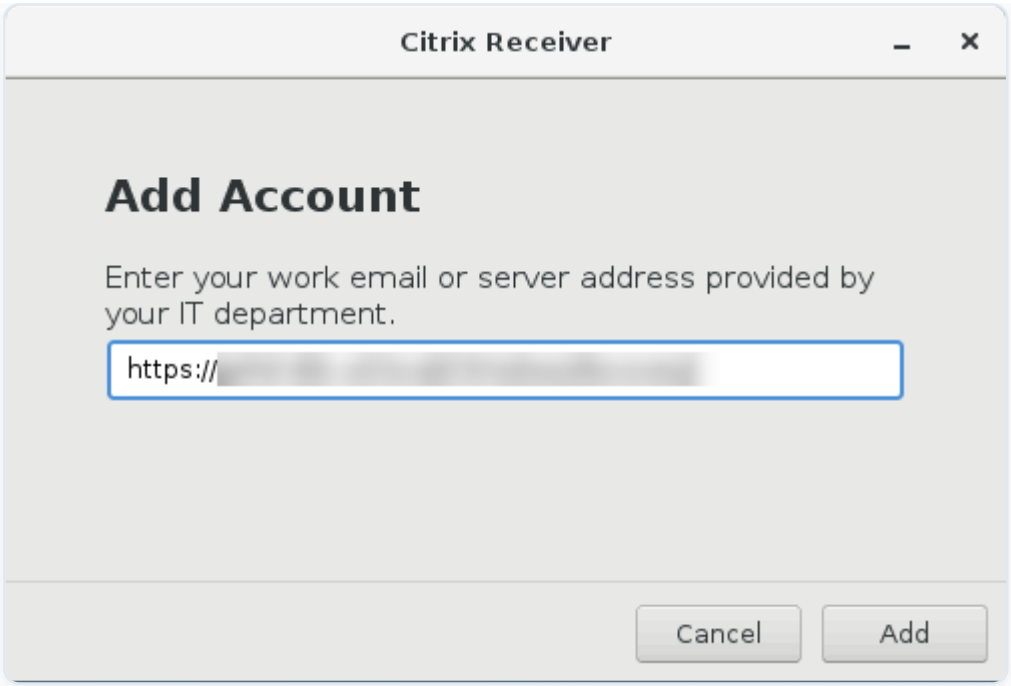
```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d
"0x00000001"
```

6. Linux仮想デスクトップセッションを起動し、そのセッション内でCitrix Workspaceアプリ for LinuxまたはCitrix Receiver for Linux 13.10を開始します。

   Citrix Workspace™アプリを初めて起動すると、ストアアカウントの入力を求められます。その後は、以前に指定したストアに自動的にログオンされます。

   注:

   ストアアカウントとしてHTTPS URLを入力します。



フェデレーション認証サービス

フェデレーション認証サービス (FAS) を使用して、Linux VDAにログオンするユーザーを認証できます。Linux VDAは、FASログオン機能にWindows VDAと同じWindows環境を使用します。FASのWindows環境の構成については、フェデレーション認証サービスを参照してください。この記事では、Linux VDAに特化した追加情報を提供します。

注:

- Linux VDAは、**セッション内動作**ポリシーをサポートしていません。
- Linux VDAは、FASサーバーとデータを送信するために短い接続を使用します。
- 2206リリース以降、ctxsetup.shのCTX_XDL_FAS_LISTを介して、Linux VDA側でFASポートをカスタマイズできます。詳しくは、お使いのディストリビューションに基づいたLinux VDAのインストールに関する記事を参照してください。

Linux VDAでFASを構成する

RHEL 8.xおよびRocky Linux 8.xでのFASのサポート

FASはpam_krb5モジュールに依存しますが、これはRHEL 8.xおよびRocky Linux 8.xでは非推奨です。マルチセッションOSモードで提供されるRHEL 8.xおよびRocky Linux 8.xマシンでFASを使用

する場合は、次の手順が必要です。シングルセッションOS（VDI）モードで提供されるRHEL 8.xおよびRocky Linux 8.xマシンでのFASについては、次の手順をスキップできます。

1. 次のWebサイトからpam_krb5-2.4.8-6ソースコードをダウンロードします:

   `<https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html>`。

2. RHEL 8.xおよびRocky Linux 8.xにpam_krb5モジュールをビルドしてインストールします。

   ```
   yum install make gcc krb5-devel pam-devel autoconf libtool

   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div

   tar xvzf pam_krb5-2.4.8.tar.gz

   cd pam_krb5-2.4.8

   ./configure --prefix=/usr

   make

   make install
   ```

3. /usr/lib64/security/の下にpam_krb5.soが存在することを確認します。

   ```
   ls -l /usr/lib64/security | grep pam_krb5
   ```

FASサーバーを設定する

新規のLinux VDAインストールでFASを使用するには、ctxinstall.shまたはctxsetup.shを実行するときに、各FASサーバーのFQDNを入力します。Linux VDAはADグループポリシーをサポートしていないため、代わりにセミコロン区切りのFASサーバーのリストを指定できます。サーバーアドレスが削除された場合は、その空白を**\<none\>**というテキスト文字列で埋め、サーバーアドレスの順序を変更しないでください。

既存のLinux VDAインストールをアップグレードするには、`ctxsetup.sh`を再実行してFASサーバーを設定できます。または、次のコマンドを実行してFASサーバーを設定し、`ctxvda`サービスを再起動して設定を有効にすることもできます。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force



service ctxjproxy restart



service ctxvda restart
```

`ctxreg`を介してFASサーバーを更新するには、次のコマンドを実行します:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -v "Addresses" -d "<Your-FAS-Server-List>"



service ctxjproxy restart



service ctxvda restart
```

証明書をインストールする

ユーザーの証明書を検証するには、ルートCA証明書とすべての中間証明書をVDAにインストールします。たとえば、ルートCA証明書をインストールするには、前の「**Microsoft CA (AD上) からCA証明書を取得する**」の手順からADルート証明書を取得するか、ルートCAサーバーからそのDER形式をダウンロードします`http://CA-SERVER/certsrv`。

> **注:**

> 次のコマンドは、中間証明書の設定にも適用されます。

> 次のようなコマンドを実行して、DERファイル（.crt、.cer、.der）をPEMに変換します。

```
sudo openssl x509 -inform der -in root.cer -out root.pem
```

次に、次のようなコマンドを実行して、ルートCA証明書を`openssl`ディレクトリにインストールします。

```
sudo cp root.pem /etc/pki/CA/certs/
```

注:

ルートCA証明書を **/root** パスに配置しないでください。そうしないと、FASはルートCA証明書への読み取り権限を持ちません。

ctxfascfg.shを実行する

FASを構成するには、ctxfascfg.shスクリプトを実行します。

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
```

`ctxfascfg.sh`をサイレントモードで実行できるように、環境変数が追加されます。

- **CTX_FAS_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis**: Active Directory統合方法を示します。これは、`CTX_EASYINSTALL_ADINTEGRATIONWAY`が指定されている場合に`CTX_EASYINSTALL_ADINTEGRATIONWAY`と等しくなります。
  `CTX_EASYINSTALL_ADINTEGRATIONWAY`が指定されていない場合、
  `CTX_FAS_ADINTEGRATIONWAY`は独自の値を設定します。
- **CTX_FAS_CERT_PATH \=\<certificate path\>**: ルート証明書とすべての中間証明書を格納する完全なパスを指定します。
- **CTX_FAS_KDC_HOSTNAME**: PBISを選択した場合のキー配布センター（KDC）のホスト名を指定します。
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: PKINIT KDCホスト名を指定します。特に指定がない限り、CTX_FAS_KDC_HOSTNAMEと同じです。複数のDelivery Controllerがある場合は、ドメインのすべてのKDCのホスト名を **/etc/krb5.conf** ファイルのpkinit_kdc_hostnameに追加します。詳細については、Knowledge Centerの記事CTX322129を参照してください。

正しいActive Directory統合方法を選択し、証明書の正しいパス（例: `/etc/pki/CA/certs/`）を入力します。

その後、スクリプトはkrb5-pkinitおよびpam_krb5パッケージをインストールし、関連する構成ファイルを設定します。

FASを無効にする

Linux VDA で FAS を無効にするには、次のコマンドを使用して ConfDB からすべての FAS サーバーを削除します。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "" --force



service ctxjproxy restart



service ctxvda restart
```

制限事項

- FAS は、限られた Linux プラットフォームと AD 統合方法をサポートしています。次のマトリックスを参照してください。

	ウィンバインド	SSSD	セントリファイ	PBIS
アマゾン リナックス 2	はい	はい	はい	はい
デビアン 11.3	はい	はい	はい	はい
RHEL 9.1/9.0	はい	はい	いいえ	いいえ
RHEL 8.7/8.6/8.4	はい	はい	はい	はい
RHEL 7.9、CentOS 7.9	はい	はい	はい	はい
ロッキー Linux 9.1/9.0	はい	はい	いいえ	いいえ

	ウィンバインド	SSSD	セントリファイ	PBIS
ロッキー Linux 8.7/8.6	はい	はい	いいえ	いいえ
SUSE 15.4	はい	はい	はい	いいえ
ウブントゥ 22.04/20.04/18.04	はい	はい	はい	はい

- FASはまだロック画面をサポートしていません。セッション内でロックボタンをクリックすると、FASを使用してセッションに再度ログオンすることはできません。
- このリリースは、フェデレーション認証サービスアーキテクチャの概要記事にまとめられている一般的なFAS展開のみをサポートしており、**Windows 10 Azure AD Join**は含まれていません。

トラブルシューティング

FASのトラブルシューティングを行う前に、Linux VDAが正しくインストールおよび構成されていること、およびパスワード認証を使用して共通ストアで非FASセッションが正常に起動できることを確認してください。

非FASセッションが正常に動作する場合は、**Login**クラスのHDXログレベルをVERBOSEに、VDAログレベルをTRACEに設定します。Linux VDAのトレースログを有効にする方法については、Knowledge Centerの記事CTX220130を参照してください。

Linux VDA環境に存在する可能性のある一般的な構成の問題を確認するには、Linuxの**XDPing**ツールを使用することもできます。詳細については、XDPingを参照してください。

FASサーバー構成エラー

FASストアからのセッション起動に失敗します。

/var/log/xdl/hdx.logを確認し、次のようなエラーログを見つけてください。

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon
Type] Federated Authentication Logon.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry
```

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
connect to server 0


2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed
to connect: Connection refused.


2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed
to connect to server [0], please confirm if fas service list is well
configurated in condb


2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit,
43


2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed
to validate fas credential


2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
```

解決策

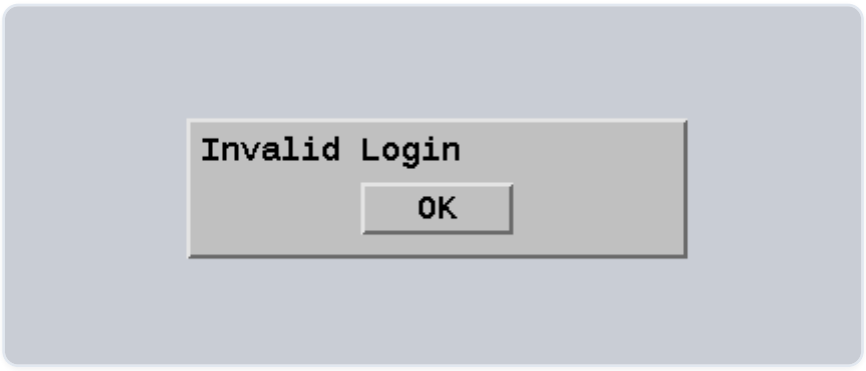
次のコマンドを実行して、Citrixレジストリ値「HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\VirtualDesktopAgent\\Authentication\\UserCredentialService」が「\<Your-FAS-Server-List\>」に設定されていることを確認します。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

既存の設定が正しくない場合は、前述のFASサーバーの設定手順に従って再度設定してください。

CA証明書構成が正しくありません

FASストアからのセッション起動に失敗します。数秒後に灰色のウィンドウが表示され、消えます。



/var/log/xdl/hdx.logを確認し、次のようなエラーログを見つけてください。

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: entry



2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller: current
process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]



2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_public_certificate: entry



2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
for response...



2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query to
server success



2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
get_public_certificate: exit
```

```
2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
input size 1888



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
output size 1415



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: get logon certificate success



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
cache certificate success



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: exit, 0



2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

解決策

ルートCA証明書とすべての中間証明書を格納する完全なパスが`/etc/krb5.conf`に正しく設定されていることを確認してください。完全なパスは次のようになります。

```
 [realms]



EXAMPLE.COM = {
```

```
    ......


    pkinit_anchors = DIR:/etc/pki/CA/certs/


    ......

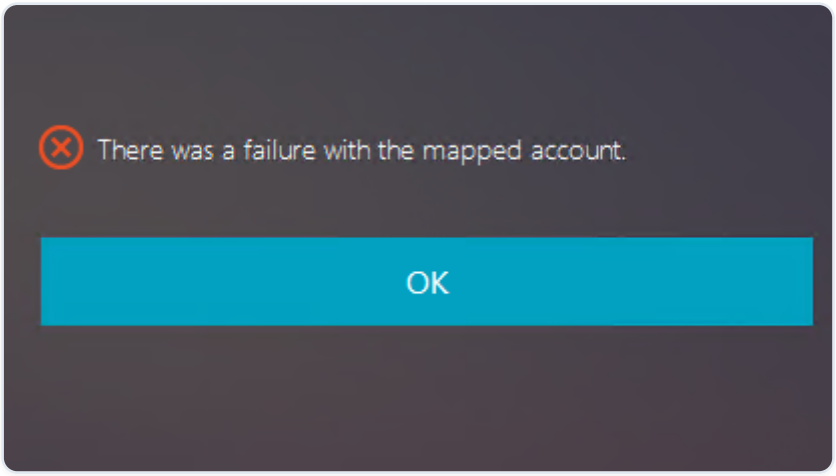

}
```

既存の設定が正しくない場合は、前の証明書のインストールの手順に従って再度設定してください。

または、ルートCA証明書が有効であるか確認してください。

シャドウアカウントマッピングエラー

FASはSAML認証によって構成されます。ADFSユーザーがADFSログオンページでユーザー名とパスワードを入力した後、次のエラーが発生する可能性があります。



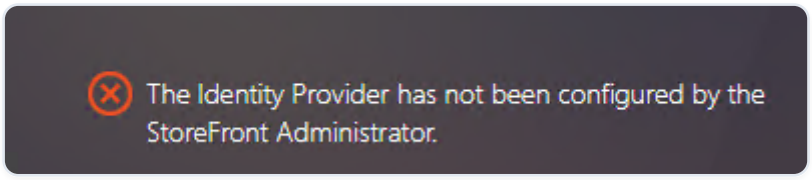
このエラーは、ADFSユーザーが正常に検証されたものの、AD上にシャドウユーザーが構成されていないことを示しています。

解決策

ADでシャドウアカウントを設定します。

ADFSが構成されていません

FASストアへのログオン試行中に次のエラーが発生します。



この問題は、FASストアがSAML認証を使用するように構成されているにもかかわらず、ADFS展開が不足している場合に発生します。

解決策

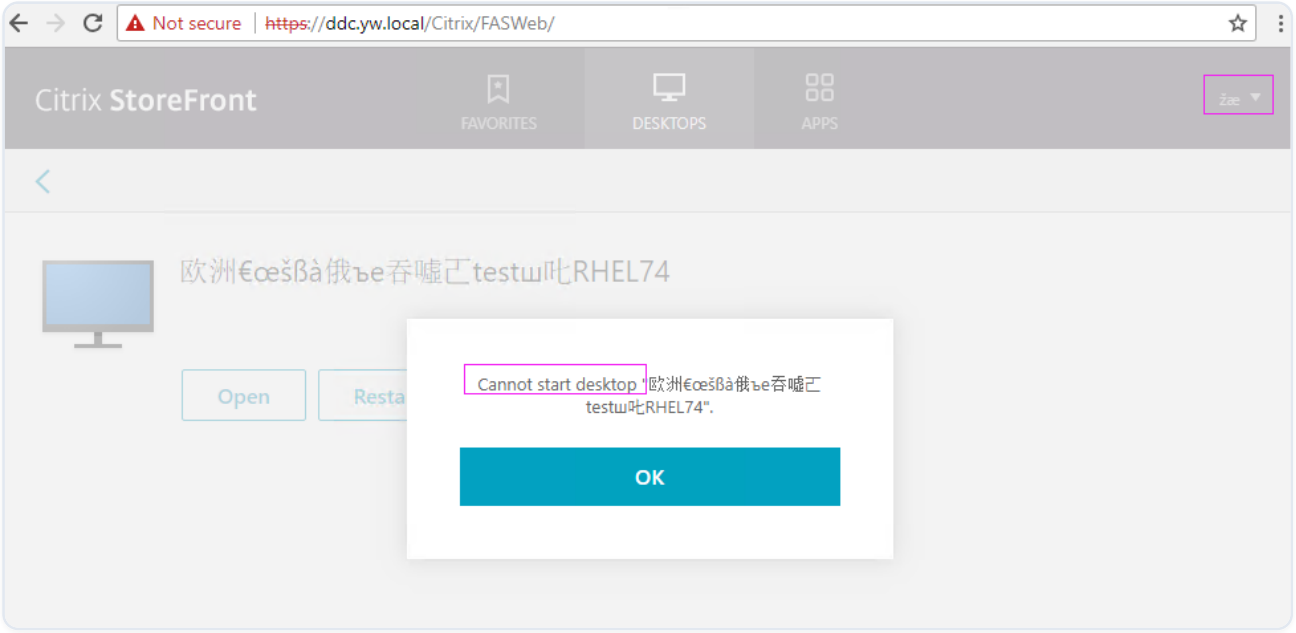
フェデレーション認証サービス用にADFS IdPを展開します。詳細については、フェデレーション認証サービス ADFS展開を参照してください。

関連情報

- 一般的なFAS展開については、フェデレーション認証サービスのアーキテクチャの概要の記事にまとめられています。
- 「ハウツー」記事は、フェデレーション認証サービスの高度な構成の章で紹介されています。

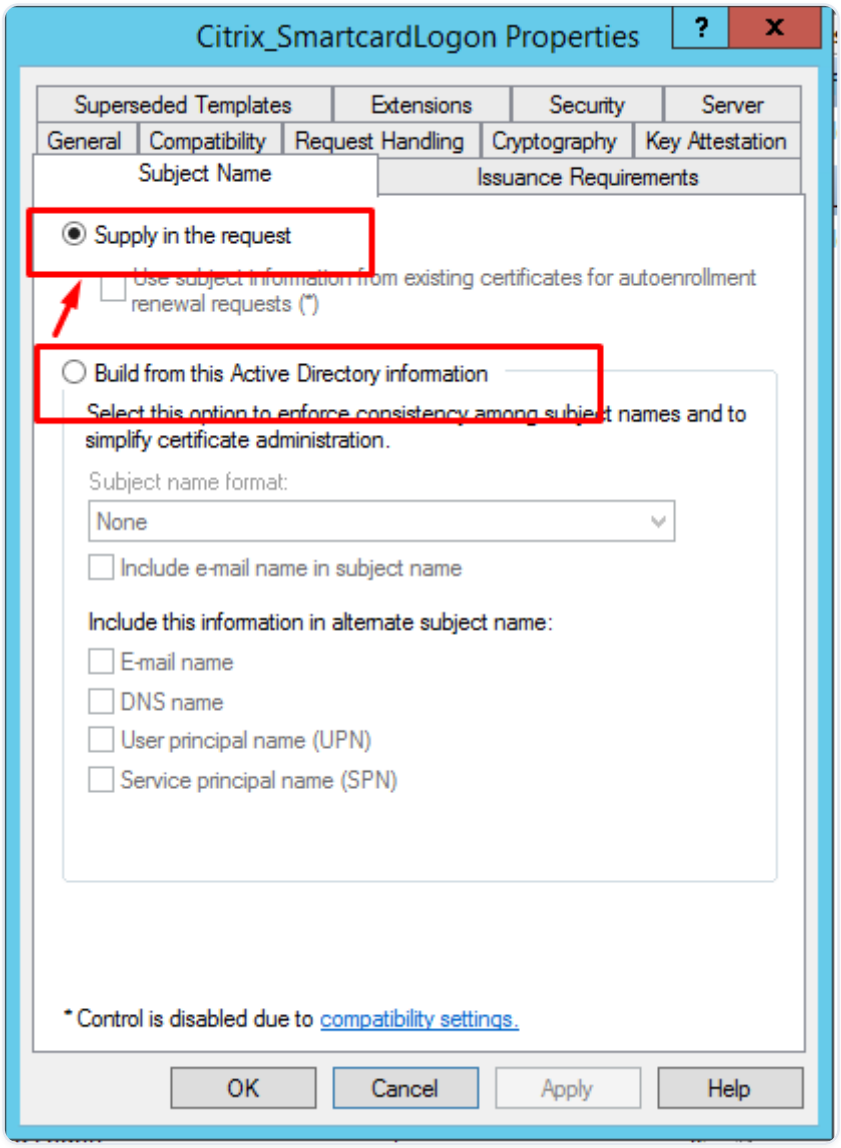
既知の問題

FASを使用している場合、英語以外の文字を含む公開デスクトップまたはアプリセッションを起動しようとすると失敗する可能性があります。



回避策

CAツールで**テンプレートの管理**を右クリックし、**Citrix_SmartcardLogon**テンプレートを**この Active Directory情報から構築**から**要求で提供**に変更します。



非SSO認証

この記事では、Linux VDAで非SSO認証を有効にする方法について説明します。

概要

デフォルトでは、Linux VDAではシングルサインオン (SSO) が有効になっています。ユーザーは、1組の資格情報を使用してCitrix Workspace™アプリとVDAセッションにログオンします。

ユーザーが異なる資格情報を使用してVDAセッションにログオンするようにするには、Linux VDAでSSOを無効にします。次の表に、非SSOシナリオでサポートされているユーザー認証方法の組み合わせを示します。

CITRIX WORKSPACEアプリ	VDAセッション
ユーザー名	ユーザー名

CITRIX WORKSPACEアプリ	VDAセッション
スマートカード	ユーザー名
ユーザー名	スマートカード

SSOを無効にする

Linux VDAで次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

スマートカード

クライアントデバイスに接続されたスマートカードを使用して、Linux仮想デスクトップセッションにログオンする際の認証を行うことができます。この機能は、ICA®スマートカード仮想チャネルを介したスマートカードリダイレクトによって実装されます。セッション内でスマートカードを使用することもできます。使用例は次のとおりです。

- ドキュメントへのデジタル署名の追加
- メールを暗号化または復号化する
- Webサイトへの認証

この機能について、Linux VDAはWindows VDAと同じ構成を使用します。詳細については、この記事のスマートカード環境の構成セクションを参照してください。

注:

Linux VDAセッション内でマップされたスマートカードを使用してCitrix Gatewayにサインオンすることはサポートされていません。

前提条件

スマートカードパススルー認証の可用性は、次の条件に依存します。

- お使いのLinux VDAは、次のいずれかのディストリビューションにインストールされています。

- RHEL 9.1/9.0
- RHEL 8.7/8.6/8.4
- RHEL 7、CentOS 7
- ロッキー リナックス 9.1/9.0
- ロッキー リナックス 8.7/8.6
- ウブントゥ 22.04
- ウブントゥ 20.04
- ウブントゥ 18.04
- デビアン 11.3

VDA のインストールが完了したら、VDA が Delivery Controller™ に登録できること、および Windows 資格情報を使用して公開された Linux デスクトップセッションを開けることを確認します。

- OpenSC でサポートされているスマートカードが使用されます。詳細については、「OpenSC がスマートカードをサポートしていることを確認する」を参照してください。
- Citrix Workspace™ app for Windows が使用されます。

OpenSC がスマートカードをサポートしていることを確認する

OpenSC は、RHEL 7.4 以降で広く使用されているスマートカードドライバーです。CoolKey の完全互換の代替として、OpenSC は多くの種類のスマートカードをサポートしています（「Red Hat Enterprise Linux でのスマートカードのサポート」を参照）。

この記事では、構成を説明するための例として YubiKey スマートカードを使用します。YubiKey は、Amazon やその他の小売業者から簡単に購入できるオールインワンの USB CCID PIV デバイスです。OpenSC ドライバーは YubiKey をサポートしています。

組織でさらに高度なスマートカードが必要な場合は、サポートされている Linux ディストリビューションと OpenSC パッケージがインストールされた物理マシンを準備してください。OpenSC のインストールについては、「スマートカードドライバーをインストールする」を参照してください。スマートカードを挿入し、次のコマンドを実行して、OpenSC がスマートカードをサポートしていることを確認します。

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
```

構成

ルート証明書を準備する

ルート証明書は、スマートカード上の証明書を検証するために使用されます。ルート証明書をダウンロードしてインストールするには、次の手順を完了します。

1. 通常、CA サーバーから PEM 形式のルート証明書を取得します。

   DER ファイル（*.crt、*.cer、*.der）を PEM に変換するには、次のようなコマンドを実行します。次のコマンド例では、**certnew.cer** が DER ファイルです。

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   ```

2. ルート証明書を `openssl` ディレクトリにインストールします。**certnew.pem** ファイルは例として使用されます。

   ```
   cp certnew.pem <path where you install the root certificate>
   ```

   ルート証明書をインストールするためのパスを作成するには、`sudo mdkir -p <path where you install the root certificate>` を実行します。

RHEL 8.x および Rocky Linux 8.x で pam_krb5 モジュールをビルドする

スマートカード認証は pam_krb5 モジュールに依存しますが、このモジュールは RHEL 8.x および Rocky Linux 8.x では非推奨です。マルチセッション OS モードで提供される RHEL 8.x および Rocky Linux 8.x マシンでスマートカード認証を使用する場合は、以下の手順が必要です。シングルセッション OS (VDI) モードで提供される RHEL 8.x および Rocky Linux 8.x マシンでのスマートカード認証の場合、以下の手順はスキップできます。

1. `<https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html>` から pam_krb5-2.4.8-6 ソースコードをダウンロードします。
2. RHEL 8.x および Rocky Linux 8.x に pam_krb5 モジュールをビルドしてインストールします。

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools

   yum install gcc krb5-devel pam-devel autoconf libtool

   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio –div
   ```

```
tar xvzf pam_krb5-2.4.8.tar.gz

cd pam_krb5-2.4.8

./configure --prefix=/usr

make

make install
```

3. /usr/lib64/security/ に pam_krb5.so が存在することを確認します。

```
ls -l /usr/lib64/security | grep pam_krb5
```

スマートカード環境を構成する

ctxsmartlogon.sh スクリプトを使用してスマートカード環境を構成するか、手動で構成を完了できます。

(オプション 1) CTXSMARTLOGON.SH スクリプトを使用してスマートカード環境を構成する

注:

ctxsmartlogon.sh スクリプトは、デフォルトのレルムに PKINIT 情報を追加します。この設定は、**/etc/krb5.conf** 構成ファイルを通じて変更できます。

スマートカードを初めて使用する前に、ctxsmartlogon.sh スクリプトを実行してスマートカード環境を構成します。

ヒント:

ドメイン参加に SSSD を使用している場合は、ctxsmartlogon.sh を実行した後、SSSD サービスを再起動してください。

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

結果は次のようになります。

```
#************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

ctxsmartlogon.sh スクリプトを実行してスマートカードを無効にすることもできます。

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

結果は次のようになります。

ctxsmartlogon.shスクリプトを実行し、「いいえ」を選択する(/en-us/linux-virtual-delivery-agent/2303/media/smart-card-logon-script2.png)

(オプション2) スマートカード環境を手動で構成する

Linux VDAはWindows VDAと同じスマートカード環境を使用します。この環境では、ドメインコントローラー、Microsoft証明機関 (CA)、インターネットインフォメーションサービス、Citrix StoreFront、Citrix Workspaceアプリなど、複数のコンポーネントを構成する必要があります。YubiKeyスマートカードに基づいた構成については、Knowledge Centerの記事CTX206156を参照してください。

次のステップに進む前に、以下を確認してください。

- すべてのコンポーネントが正しく構成されていること。
- 秘密キーとユーザー証明書をスマートカードにダウンロードしていること。
- スマートカードを使用してVDAに正常にログオンできること。

PC/SC Liteパッケージをインストールする
PCSC Liteは、LinuxにおけるPersonal Computer/Smart Card (PC/SC) 仕様の実装です。これは、スマートカードおよびリーダーと通信するためのWindowsスマートカードインターフェイスを提

供します。Linux VDAにおけるスマートカードリダイレクトは、PC/SCレベルで実装されています。

PC/SC Liteパッケージをインストールするには、次のコマンドを実行します。

RHEL 9.1/9.0/8.x、Rocky Linux 9.1/9.0/8.x、RHEL 7/CentOS 7:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04、Debian 11.3:

```
apt-get install -y libpcsclite1 libccid
```

スマートカードドライバーをインストールする
OpenSCは広く使用されているスマートカードドライバーです。OpenSCがインストールされていない場合は、次のコマンドを実行してインストールします。

RHEL 9.1/9.0/8.x、Rocky リナックス 9.1/9.0/8.x、RHEL 7/CentOS 7：

```
yum install opensc
```

ウブントゥ 22.04、ウブントゥ 20.04、ウブントゥ 18.04、Debian 11.3：

```
apt-get install -y opensc
```

スマートカード認証用のPAMモジュールをインストールする
pam_krb5およびkrb5-pkinitモジュールをインストールするには、次のコマンドを実行します。

RHEL 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
```

RHEL 9.1/9.0/8.x、ロッキー・リナックス 9.1/9.0/8.x：

```
yum install krb5-pkinit
```

ウブントゥ 22.04、ウブントゥ 20.04、ウブントゥ 18.04：

```
apt-get install libpam-krb5 krb5-pkinit
```

デビアン 11.3:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

pam_krb5モジュールは、プラガブル認証モジュールです。PAM対応アプリケーションは、pam_krb5を使用してパスワードをチェックし、Key Distribution Center (KDC) からチケット許可チケットを取得できます。krb5-pkinitモジュールには、クライアントが秘密鍵と証明書を使用してKDCから初期資格情報を取得できるようにするPKINITプラグインが含まれています。
pam_krb5モジュールを構成する
pam_krb5モジュールは、スマートカード内の証明書を使用してKerberosチケットを取得するためにKDCと対話します。PAMでpam_krb5認証を有効にするには、次のコマンドを実行します。

```
authconfig --enablekrb5 --update
```

/etc/krb5.conf 構成ファイルに、実際のレルムに従ってPKINIT情報を追加します。

> **注:**

> **pkinit_cert_match** オプションは、PKINIT認証を試行する前にクライアント証明書が一致する必要がある照合ルールを指定します。照合ルールの構文は次のとおりです。

> **コンポーネントルール ...**

> ここで、**relation-operator** は、すべてのコンポーネントルールが一致する必要があることを意味する **&&**、または1つのコンポーネントルールのみが一致する必要があることを意味する **\|\|** のいずれかです。

> 以下は、一般的なkrb5.confファイルの例です。

```
EXAMPLE.COM = {
```

```
    kdc = KDC.EXAMPLE.COM



    auth_to_local = RULE:[1:$1@$0]



    pkinit_anchors = FILE:<path where you install the root certificate>/
certnew.pem



    pkinit_kdc_hostname = KDC.EXAMPLE.COM



    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature



    pkinit_eku_checking = kpServerAuth



 }
```

PKINIT情報を追加すると、構成ファイルは次のようになります。

PKINIT情報が追加されました(/en-us/linux-virtual-delivery-agent/2303/media/pkinit-information-new2.png)
PAM認証を構成する
PAM構成ファイルは、PAM認証にどのモジュールが使用されるかを示します。pam_krb5を認証モジュールとして追加するには、**/etc/pam.d/smartcard-auth** ファイルに次の行を追加します。

`auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.so`

SSSDを使用する場合、変更後の構成ファイルは次のようになります。

SSSDを使用する場合の変更された構成ファイル(/en-us/linux-virtual-delivery-agent/2303/media/smartcard-authentication-file.png)

(オプション) スマートカードを使用したシングルサインオン

シングルサインオン (SSO) は、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能により、ユーザーがPINを入力する回数が減ります。Linux VDAでSSOを使用するには、Citrix Workspaceアプリを構成します。構成はWindows VDAと同じです。詳細については、Knowledge Centerの記事CTX133982を参照してください。

Citrix Workspaceアプリでグループポリシーを構成する際に、スマートカード認証を次のように有効にします。

Workspaceアプリでスマートカード認証を有効にする(/en-us/linux-virtual-delivery-agent/2303/media/enable-smart-card-auth-in-receiver.jpg)

高速スマートカードログオン

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。これにより、高遅延WAN環境でスマートカードを使用する際のパフォーマンスが向上します。詳細については、スマートカードを参照してください。

Linux VDAは、Citrix Workspaceアプリの次のバージョンで高速スマートカードをサポートしています。

- シトリックス レシーバー フォー ウィンドウズ 4.12
- Windows向けCitrix Workspaceアプリ1808以降

クライアントで高速スマートカードログオンを有効にする

高速スマートカードログオンは、VDAではデフォルトで有効になっており、クライアントではデフォルトで無効になっています。クライアントで高速スマートカードログオンを有効にするには、関連付けられたStoreFrontサイトのdefault.icaファイルに次のパラメータを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

クライアントで高速スマートカードログオンを無効にする

クライアントで高速スマートカードログオンを無効にするには、関連付けられたStoreFrontサイトのdefault.icaファイルから**SmartCardCryptographicRedirection**パラメータを削除します。

XDPingを実行する

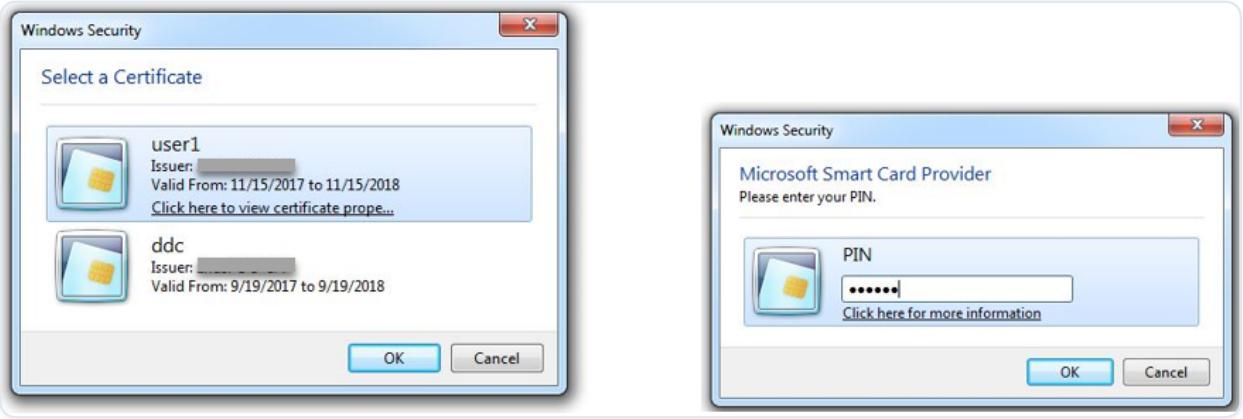
上記のステップを完了した後、Linux **XDPing**ツールを使用して、Linux VDA環境に存在する可能性のある一般的な構成の問題を確認できます。詳細については、XDPingを参照してください。

使用方法

スマートカードを使用してLinux VDAにログオンする

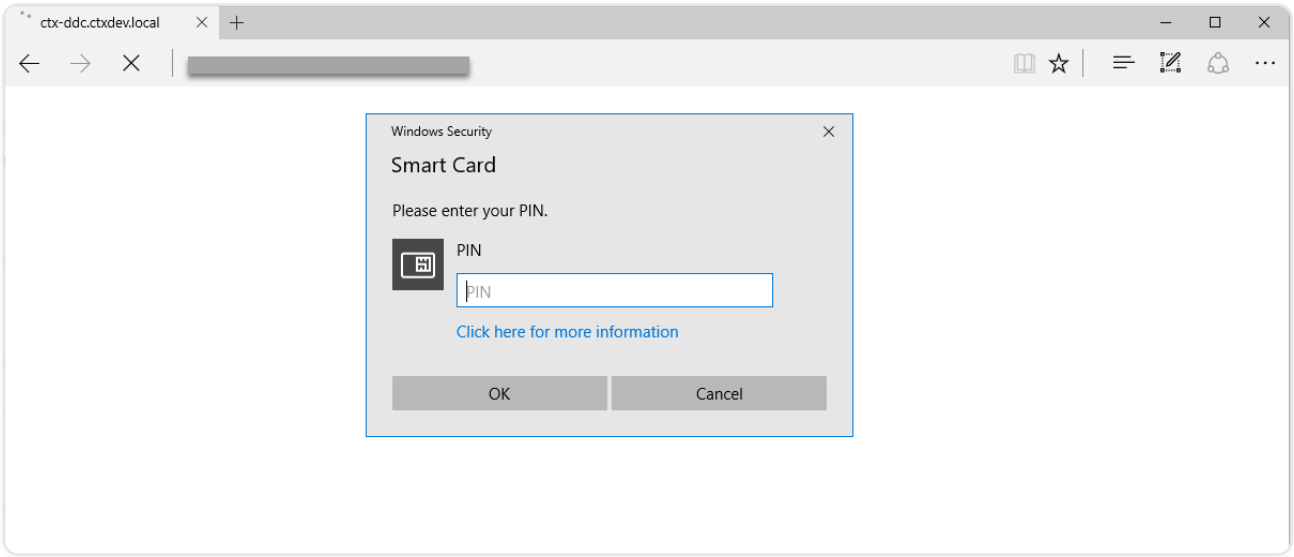
SSOシナリオと非SSOシナリオの両方で、スマートカードを使用してLinux VDAにログオンできます。

- SSOシナリオでは、キャッシュされたスマートカード証明書とPINを使用して、StoreFront™に自動的にログオンします。StoreFrontでLinux仮想デスクトップセッションを起動すると、PINがスマートカード認証のためにLinux VDAに渡されます。
- 非SSOシナリオでは、証明書を選択し、PINを入力してStoreFrontにログオンするよう求められます。



StoreFrontでLinux仮想デスクトップセッションを起動すると、Linux VDAへのログオンダイアログボックスが次のように表示されます。ユーザー名はスマートカードの証明書から抽出され、ログオン認証のためにPINを再度入力する必要があります。

この動作はWindows VDAと同じです。



スマートカードを使用してセッションに再接続する

セッションに再接続するには、スマートカードがクライアントデバイスに接続されていることを確認してください。そうしないと、Linux VDA側で灰色のキャッシュウィンドウが表示され、スマートカードが接続されていないため再認証が失敗し、すぐに終了します。この場合、スマートカードを接続するように促す他のプロンプトは表示されません。

ただし、StoreFront側では、セッションに再接続するときにスマートカードが接続されていない場合、StoreFront Webは次のようなアラートを表示する可能性があります。

スマートカードを挿入するイメージ(/en-us/linux-virtual-delivery-agent/2303/media/please-insert-smart-card.png)

制限事項

制限されたLinuxディストリビューションとAD統合方法のサポート

- スマートカードパススルー認証は、制限されたLinuxディストリビューションとAD統合方法をサポートしています。次のマトリックスを参照してください。

	ウィンバインド	SSSD	セントリファイ
デビアン 11.3	はい	はい	はい
RHEL 9.1/9.0	はい	はい	いいえ
RHEL 8.7/8.6/8.4	はい	はい	はい
RHEL 7.9, CentOS 7.9	はい	はい	はい

	ウィンバインド	SSSD	セントリファイ
ロッキー Linux 9.1/9.0	はい	はい	いいえ
ロッキー Linux 8.7/8.6	はい	はい	いいえ
ウブントゥ 22.04/20.04/18.04	はい	はい	はい

スマートカード取り外しポリシー

現在、Linux VDAはスマートカードの取り外しに対してデフォルトの動作のみを使用します。Linux VDAに正常にログオンした後でスマートカードを取り外しても、セッションは接続されたままで、セッション画面はロックされません。

他のスマートカードとPKCS#11ライブラリのサポート

Citrixは汎用スマートカードリダイレクトソリューションを提供しています。サポートリストにはOpenSCスマートカードのみが記載されていますが、他のスマートカードやPKCS#11ライブラリを試すことができます。特定のスマートカードまたはPKCS#11ライブラリに切り替えるには、次の手順を実行します。

1. すべての`opensc-pkcs11.so`インスタンスを、お使いのPKCS#11ライブラリに置き換えます。
2. PKCS#11ライブラリのパスをレジストリに設定するには、次のコマンドを実行します。

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v
   "PKCS11LibPath" -d "PATH"
   ```

   ここで、**PATH**は、/usr/lib64/pkcs11/opensc-pkcs11.soのようなPKCS#11ライブラリを指します。
3. クライアントで高速スマートカードログオンを無効にします。

匿名ユーザーによる非認証セッション

この記事の情報を使用して、非認証セッションを構成します。この機能を使用するためにLinux VDAをインストールする際に、特別な設定は必要ありません。

注:

非認証セッションを構成する際は、セッションの事前起動がサポートされていないことに注意してください。セッションの事前起動は、Android版Citrix Workspace™アプリでもサポートされていません。

非認証ストアを作成する

Linux VDAで非認証セッションをサポートするには、StoreFrontを使用して非認証ストアを作成します。

デリバリーグループで非認証ユーザーを有効にする

非認証ストアを作成したら、デリバリーグループで非認証ユーザーを有効にして、非認証セッションをサポートします。デリバリーグループで非認証ユーザーを有効にするには、Citrix Virtual Apps and Desktopsのドキュメントの手順に従ってください。

非認証セッションのアイドル時間を設定する

非認証セッションのデフォルトのアイドルタイムアウトは10分です。この値は、レジストリ設定 **AnonymousUserIdleTime** を介して構成されます。この値を変更するには、**ctxreg** ツールを使用します。たとえば、このレジストリ設定を5分に設定するには、次のようにします。

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime
 -d 0x00000005
```

非認証ユーザーの最大数を設定する

非認証ユーザーの最大数を設定するには、レジストリキー **MaxAnonymousUserNumber** を使用します。この設定は、単一のLinux VDAで同時に実行される非認証セッションの数を制限します。このレジストリ設定を構成するには、**ctxreg** ツールを使用します。たとえば、値を32に設定するには、次のようにします。

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber
 -d  0x00000020
```

重要:

> 非認証セッションの数を制限してください。同時に起動されるセッションが多すぎると、利用可能なメモリが不足するなど、VDAで問題が発生する可能性があります。

トラブルシューティング

非認証セッションを構成する際は、次の点を考慮してください。

- **非認証セッションへのログオンに失敗しました。**

レジストリが次のように更新されていることを確認してください（0に設定）。

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k
"HKLM\System\CurrentControlSet\Control\Citrix" –v MaxAnonymousUserNumber
```

ncsd サービスが実行されており、**passwd** キャッシュを有効にするように構成されていることを確認します。

```
ps  uax | grep nscd

cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

passwd キャッシュ変数が有効になっている場合は、**no** に設定してから、**ncsd** サービスを再起動します。この構成を変更した後、Linux VDA を再インストールする必要がある場合があります。

- **KDE を使用した非認証セッションでロック画面ボタンが表示される。**

ロック画面ボタンとメニューは、非認証セッションではデフォルトで無効になっています。ただし、KDE では引き続き表示されることがあります。KDE で特定のユーザーのロック画面ボタンとメニューを無効にするには、構成ファイル **$Home/.kde/share/config/kdeglobals** に次の行を追加します。例：

```
[KDE Action Restrictions]

action/lock_screen=false
```

ただし、`KDE Action Restrictions` パラメーターが `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals` のようなグローバルな `kdeglobals` ファイルで不変として構成されている場合、ユーザー構成は無効になります。

この問題を解決するには、システム全体の `kdeglobals` ファイルを変更して、`[KDE Action Restrictions]` セクションの `[$i]` タグを削除するか、システム全体の構成を直接使用してロック画面ボタンとメニューを無効にします。KDE 構成の詳細については、KDE System Administration/Kiosk/Keys ページ を参照してください。

ファイル

このセクションには、次のトピックが含まれています。

- ファイルのコピーと貼り付け
- ファイル転送

ファイルのコピーと貼り付け

ユーザーは、右クリックメニューまたはキーボードショートカットを使用して、セッションとローカルクライアント間でファイルをコピー＆ペーストできます。この機能には、Citrix Virtual Apps and Desktops™ 2006以降、およびWindows用Citrix Workspace™アプリ1903以降が必要です。

ファイルを正常にコピー＆ペーストするには、以下を確認してください。

- ファイルの最大数が20を超えないこと。
- ファイルの最大サイズが200 MBを超えないこと。
- Linux VDAをインストールしたマシンで Nautilus ファイルマネージャーが利用可能であること。

サポートされているLinuxディストリビューション

ファイルコピー＆ペースト機能は、Linux VDAがサポートするすべてのLinuxディストリビューションで利用できます。

関連するポリシー

以下のクリップボードポリシーは、この機能の設定に関連しています。クリップボードポリシーの詳細については、「ポリシーサポートリスト」を参照してください。

- クライアントクリップボードリダイレクト
- クリップボード選択更新モード
- プライマリ選択更新モード

> **注:**
>
> ファイルコピー＆ペースト機能を無効にするには、Citrix Studioで**クライアントクリップボードリダイレクト**ポリシーを**禁止**に設定します。

制限事項

- 切り取りはサポートされていません。ファイルを切り取る要求はコピーとして扱われます。
- ドラッグ＆ドロップはサポートされていません。
- ディレクトリのコピーはサポートされていません。
- ファイルのコピーとペーストは順次実行する必要があります。前のファイルが正常にコピーおよびペーストされてからでないと、次のファイルをコピーできません。

ファイル転送

ファイル転送は、Linux VDAとクライアントデバイス間でサポートされています。この機能は、クライアントデバイスがHTML5サンドボックス属性をサポートするWebブラウザを実行している場合に利用できます。HTML5サンドボックス属性により、ユーザーはCitrix Workspace™ app for HTML5およびfor Chromeを使用して仮想デスクトップとアプリにアクセスできます。

> **注:**
>
> ファイル転送は、Citrix Workspace app for HTML5およびfor Chromeで利用できます。

> 公開されたアプリおよびデスクトップセッション内では、ファイル転送によりLinux VDAとクライアントデバイス間でファイルのアップロードとダウンロードが可能です。クライアントデバイスからLinux VDAにファイルをアップロードするには、Citrix Workspaceアプリのツールバーにある**アップロード**アイコンをクリックし、ファイルダイアログから目的のファイルを選択します。Linux VDAからクライアントデバイスにファイルをダウンロードするには、**ダウンロード**アイコンをクリックします。アップロードまたはダウンロード中にファイルを追加できます。一度に最大100個のファイルを転送できます。

ツールバーのアップロードアイコンの画像(/en-us/linux-virtual-delivery-agent/2303/media/upload-icon-on-toolbar.png)

> **注:**

Linux VDAとクライアントデバイス間でファイルをアップロードおよびダウンロードするには、Citrix Workspaceアプリのツールバーを有効にします。

ファイルをドラッグアンドドロップできるバージョンのCitrix Workspaceアプリを使用できます。

自動ダウンロードは、ファイル転送の機能強化です。VDA上の**Save to My Device**ディレクトリにダウンロードまたは移動したファイルは、自動的にクライアントデバイスに転送されます。

注:

自動ダウンロードには、**デスクトップとクライアント間のファイル転送を許可する**および**デスクトップからファイルをダウンロードする**ポリシーが**許可**に設定されている必要があります。

自動ダウンロードのユースケースをいくつか示します。

- **Save to My Device**にファイルをダウンロードする

  公開されたデスクトップおよびWebブラウザアプリセッション内では、Webサイトからダウンロードしたファイルを VDA上の**Save to My Device**ディレクトリに保存して、クライアントデバイスに自動転送できます。自動ダウンロードを実現するには、セッション内Webブラウザのデフォルトのダウンロードディレクトリを**Save to My Device**に設定し、Citrix Workspace app for HTML5またはfor Chromeを実行するWebブラウザでローカルダウンロードディレクトリを設定します。

- **Save to My Device**にファイルを移動またはコピーする

  公開されたデスクトップセッション内では、ターゲットファイルを選択し、それらを**Save to My Device**ディレクトリに移動またはコピーして、クライアントデバイスで利用できるようにします。

ファイル転送ポリシー

Citrix Studioを使用してファイル転送ポリシーを設定できます。デフォルトでは、ファイル転送は有効になっています。

ファイル転送ポリシーの画像(/en-us/linux-virtual-delivery-agent/2303/media/file-transfer-policies.png)

ポリシーの説明：

- **デスクトップとクライアント間のファイル転送を許可する。** ユーザーがCitrix Virtual Apps and Desktops™セッションとデバイス間でファイルを転送することを許可または禁止します。
- **デスクトップからファイルをダウンロードする。** ユーザーがCitrix Virtual Apps™ and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。
- **デスクトップにファイルをアップロードする。** ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。

> **注:**
>
> 「**デスクトップからファイルをダウンロードする**」および「**デスクトップにファイルをアップロードする**」ポリシーが有効になるように、「**デスクトップとクライアント間のファイル転送を許可する**」ポリシーを「**許可**」に設定します。

使用方法

Citrix Workspace app for HTML5を介してファイル転送機能を使用するには：

1. Citrix Studioで、**WebSockets接続**ポリシーを**許可**に設定します。

   WebSockets接続ポリシーの設定を示す画像(/en-us/linux-virtual-delivery-agent/2303/media/websockets-connection.png)
2. Citrix Studioで、前述のファイル転送ポリシーを介してファイル転送を有効にします。
3. Citrix StoreFront管理コンソールで、**Stores**をクリックし、**Manage Receiver for Web Sites**ノードを選択して、**Always use Receiver for HTML5**オプションを選択してCitrix Receiver™ for HTML5を有効にします。

   Always use Receiver for HTML5オプションを選択する画像(/en-us/linux-virtual-delivery-agent/2303/media/always-use-receiver-for-html5.png)
4. 仮想デスクトップまたはWebブラウザアプリセッションを起動します。Linux VDAとクライアントデバイス間で1つ以上のファイル転送を実行します。

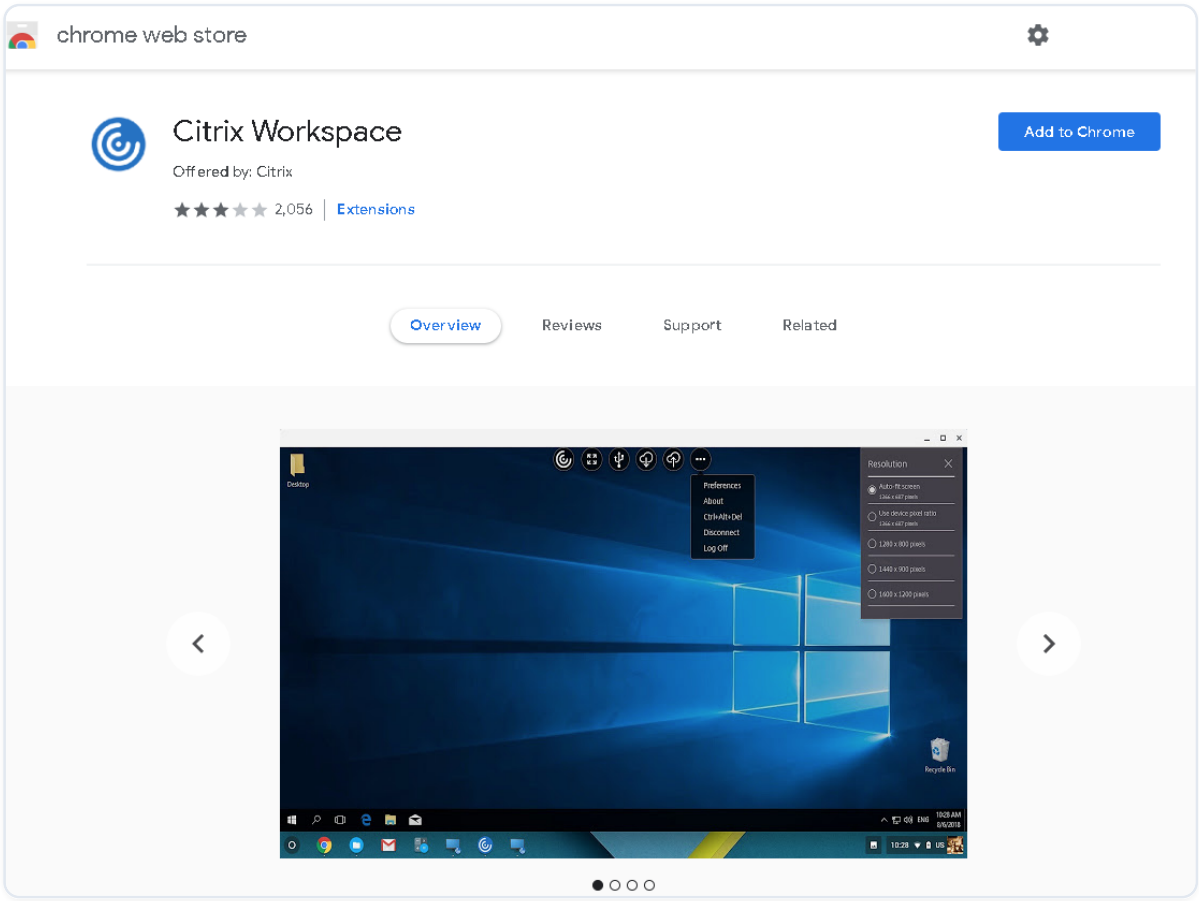
Citrix Workspace app for Chromeを介してファイル転送機能を使用するには：

1. 前述のファイル転送ポリシーを介してファイル転送を有効にします。
2. Chrome Web StoreからCitrix Workspaceアプリを入手します。

   Citrix Workspace app for ChromeをChrome Appsページにすでに追加している場合は、この手順をスキップしてください。

   a. Google Chrome の検索ボックスに「**Citrix Workspace for Chrome**」と入力します。検索アイコンをクリックします。

   b. 検索結果の中から、Citrix Workspace アプリが利用可能な Chrome ウェブストアへの URL をクリックします。



   c. 「**Chrome に追加**」をクリックして、Citrix Workspace アプリを Google Chrome に追加します。

3. Chrome アプリページで Citrix Workspace app for Chrome をクリックします。
4. 接続する StoreFront™ ストアの URL を入力します。

   以前に URL を入力したことがある場合は、この手順はスキップしてください。

5. 仮想デスクトップまたはアプリセッションを起動します。Linux VDA とクライアントデバイスの間で1つ以上のファイル転送を実行します。

グラフィックス

このセクションには、次のトピックが含まれています。

- DPIの自動スケーリング
- クライアントのバッテリー状態表示
- グラフィックの構成と微調整
- HDX画面共有
- 非仮想化GPU
- セッションの透かし
- Thinwireプログレッシブ表示

自動DPIスケーリング

Linux VDAは自動DPIスケーリングをサポートしています。ユーザーが仮想デスクトップまたはアプリケーションセッションを開くと、セッション内のDPI値はクライアント側のDPI設定に合わせて自動的に変更されます。

この機能に関する考慮事項は次のとおりです。

- この機能を使用するには、Citrix WorkspaceでDPIマッチングを有効にする必要があります。Windows向けCitrix Workspaceアプリの場合、**いいえ、ネイティブ解像度を使用します**オプションが選択されていることを確認してください。Windows向けCitrix WorkspaceアプリのDPIスケーリングの構成について詳しくは、「DPIスケーリング」を参照してください。
- マルチモニター環境でこの機能を使用するには、各モニターが同じDPI設定で構成されている必要があります。DPI設定が混在するシナリオはサポートされていません。モニターが異なるDPI設定で構成されている場合、Linux VDAはすべての画面に最小のDPI値を適用します。
- この機能は、MATE、GNOME、GNOME Classic、およびKDEで有効です。KDEまたはMATEを使用する場合は、次の点を考慮してください。
    - KDEデスクトップ環境で実行されているLinux仮想デスクトップの場合：
        - KDE Plasma 5以降を使用することをお勧めします。
        - セッションの実行中にクライアント側でDPI設定を変更するには、ユーザーがログオフして再度ログオンする必要があります。
    - MATEデスクトップ環境で実行されているLinux仮想デスクトップの場合：
        - スケールファクター1および2のみがサポートされています。

    - セッションの実行中にクライアント側でDPI設定を変更するには、ユーザーがログオフして再度ログオンする必要があります。

- 仮想セッションのDPI値は、クライアント側のDPI設定に従って自動的に変更されます。現在、この機能は、100%や200%などの整数型のスケールファクターのみをサポートしています。クライアント側で構成されているスケールファクターが分数型の場合、仮想セッションのDPIは次の表に従って整数型のスケールファクターに変更されます。例：スケールファクターが125%の場合、DPI値は100%に変更されます。

クライアント側のスケールファクター	リモートセッションのDPI
174%以下	96 (1 x 96)
175%～274%	192 (2 x 96)
275%～399%	288 (3 x 96)
400%以上	384 (4 x 96)

クライアントのバッテリーステータス表示

Linux VDAは、仮想デスクトップ内のクライアントデバイスのバッテリーステータスをリダイレクトして表示できます。この機能はデフォルトで有効になっており、Citrix Workspace™アプリの以下のバージョンで利用できます。

- iOS向けCitrix Workspaceアプリ
- Linux向けCitrix Workspaceアプリ
- Mac版Citrix Workspaceアプリ（バージョン2204.1はサポートされていません）
- Windows版Citrix Workspaceアプリ（バージョン2204.1はサポートされていません）

概要

ユーザーが仮想デスクトップを開くと、Linuxシステムトレイにバッテリーアイコンが表示されます。バッテリーアイコンは、クライアントデバイスのバッテリーステータスを示します。バッテリー残量の割合を確認するには、バッテリーアイコンをクリックします。たとえば、次のスクリーンショットを参照してください。

バッテリーステータスアイコン(/en-us/linux-virtual-delivery-agent/2303/media/battery-status-icon.png)

異なるバッテリーアイコンは、異なるバッテリーステータスを示します。概要については、次の表を参照してください。

バッテリーアイコン	充電ステータス	バッテリー残量レベル	バッテリー残量パーセンテージ
充電中でバッテリー残量が多いバッテリー(/en-us/linux-virtual-delivery-agent/2303/media/battery-charging-high.png)	充電中（「+」記号で表示）	高（緑色で表示）	>=80%
充電中で、バッテリー残量が中程度のバッテリー(/en-us/linux-virtual-delivery-agent/2303/media/battery-charging-medium.png)	充電中、「+」記号で表示	中程度、琥珀色で表示	>=20% かつ <80%
充電中で、バッテリー残量が低いバッテリー(/en-us/linux-virtual-delivery-agent/2303/media/battery-charging-low.png)	充電中、「+」記号で表示	低、赤色で表示	< 20%
充電中でなく、バッテリー残量が高いバッテリー(/en-us/linux-virtual-delivery-agent/2303/media/battery-not-charging-high.png)	充電中でない、「-」記号で表示	高、緑色で表示	>=80%
充電中でなく、バッテリー残量が中程度のバッテリー(/en-us/linux-virtual-delivery-agent/2303/media/	充電中でない、「-」記号で表示	中程度、琥珀色で表示	20%以上80%未満

バッテリーアイコン	充電ステータス	バッテリー残量レベル	バッテリー残量パーセンテージ
battery-not-charging-medium.png)			
	充電中ではない（「-」記号で示される）	低い（赤色で示される）	20%未満
	不明	不明	不明

構成

クライアントのバッテリー状態表示は、デフォルトで有効になっています。

この機能を無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

この機能を有効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000001"
```

注:

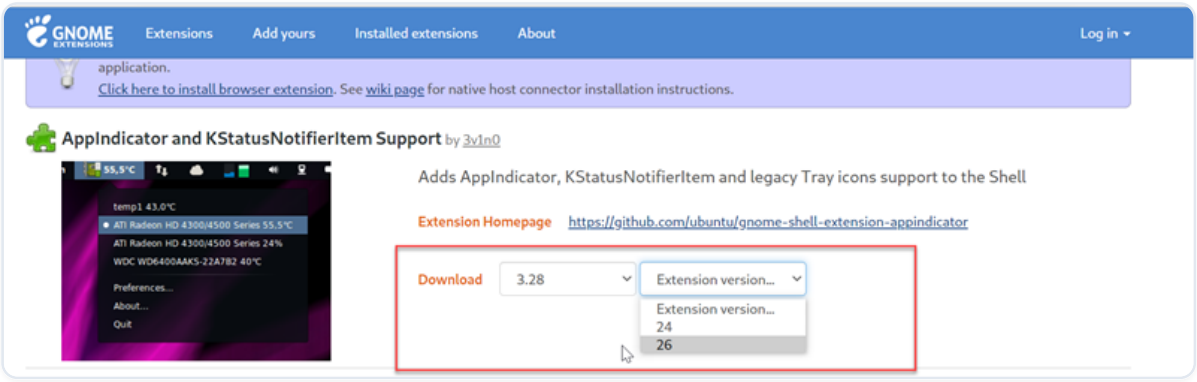
前述のコマンドは、クライアントのバッテリー状態表示とモバイルレシーバー仮想チャネル（MRVC）を共有するソフトキーボード機能に影響します。

お使いのディストリビューションに応じて、次の追加手順を実行します。

1. GNOMEがインストールされたRHEL 8.xまたはSUSE 15.xを使用している場合は、AppIndicatorのサポートを有効にするために、GNOMEシェル用の互換性のある拡張機能をインストールします。

a. `gnome-shell --version` コマンドを実行して、GNOMEシェルのバージョンを確認します。

b. `<https://extensions.gnome.org/extension/615/appindicator-support>` からGNOMEシェル用の互換性のある拡張機能をダウンロードします。たとえば、シェルバージョンが3.28の場合、拡張機能のバージョンとして24または26を選択できます。



c. ダウンロードしたパッケージを解凍します。パッケージ内の **metadata.json** ファイルにある **"uuid"** の値が appindicatorsupport@rgcjonas.gmail.com に設定されていることを確認します。

d. `mv` コマンドを実行して、appindicatorsupport@rgcjonas.gmail.com ディレクトリを `/usr/share/gnome-shell/extensions/` の下の場所に移動します。

e. `chmod a+r metadata.json` コマンドを実行して、**metadata.json** ファイルを他のユーザーが読み取り可能にします。

> **ヒント:**
>
> デフォルトでは、appindicatorsupport@rgcjonas.gmail.com ディレクトリ内の **metadata.json** ファイルは、rootユーザーのみが読み取り可能です。画面共有をサポートするには、**metadata.json** ファイルを他のユーザーも読み取り可能にする必要があります。

f. GNOME Tweaksをインストールします。

g. デスクトップ環境で、`Alt+F2`、`r`、`Enter` キーを順番に押すか、`killall -SIGQUIT gnome-shell` コマンドを実行してGNOMEシェルをリロードします。

h. デスクトップ環境でGNOME Tweaksを実行し、Tweaksツールで **KStatusNotifierItem/AppIndicator Support** を有効にします。

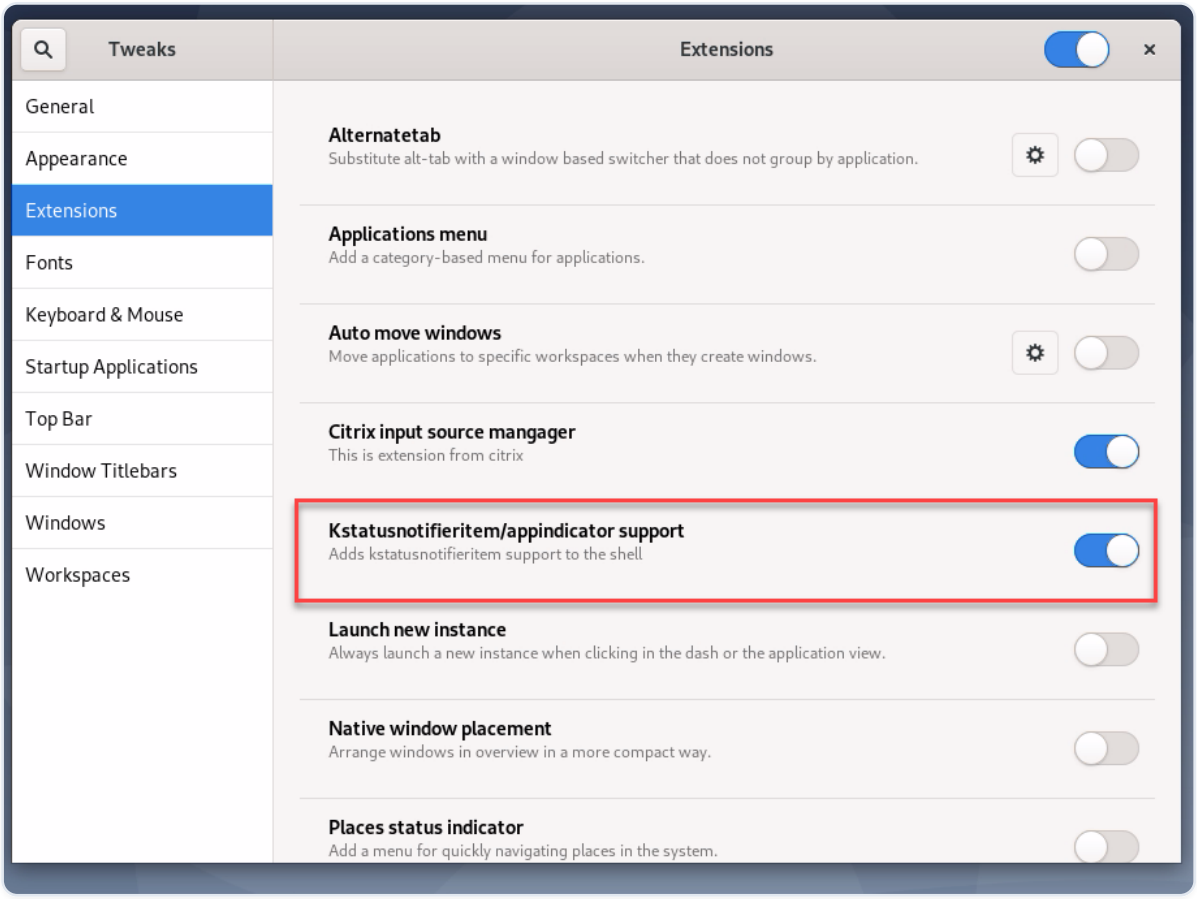
2. GNOMEがインストールされたDebian 11.3を使用している場合は、GNOMEシステムトレイアイコンをインストールして有効にするために、次の手順を完了してください。

   a. `sudo apt install gnome-shell-extension-appindicator` コマンドを実行します。GNOMEが拡張機能を認識するには、一度ログアウトしてから再度ログインする必要がある場合があります。

   b. **アクティビティ**画面でTweaksを検索します。

   c. Tweaksツールで**Extensions**を選択します。

   d. **Kstatusnotifieritem/appindicator support**を有効にします。



グラフィックの構成と微調整

この記事では、Linux VDAのグラフィック構成と微調整に関するガイダンスを提供します。

詳細については、システム要件およびインストール概要セクションを参照してください。

構成

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト値を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きする他の設定は、優先されます。

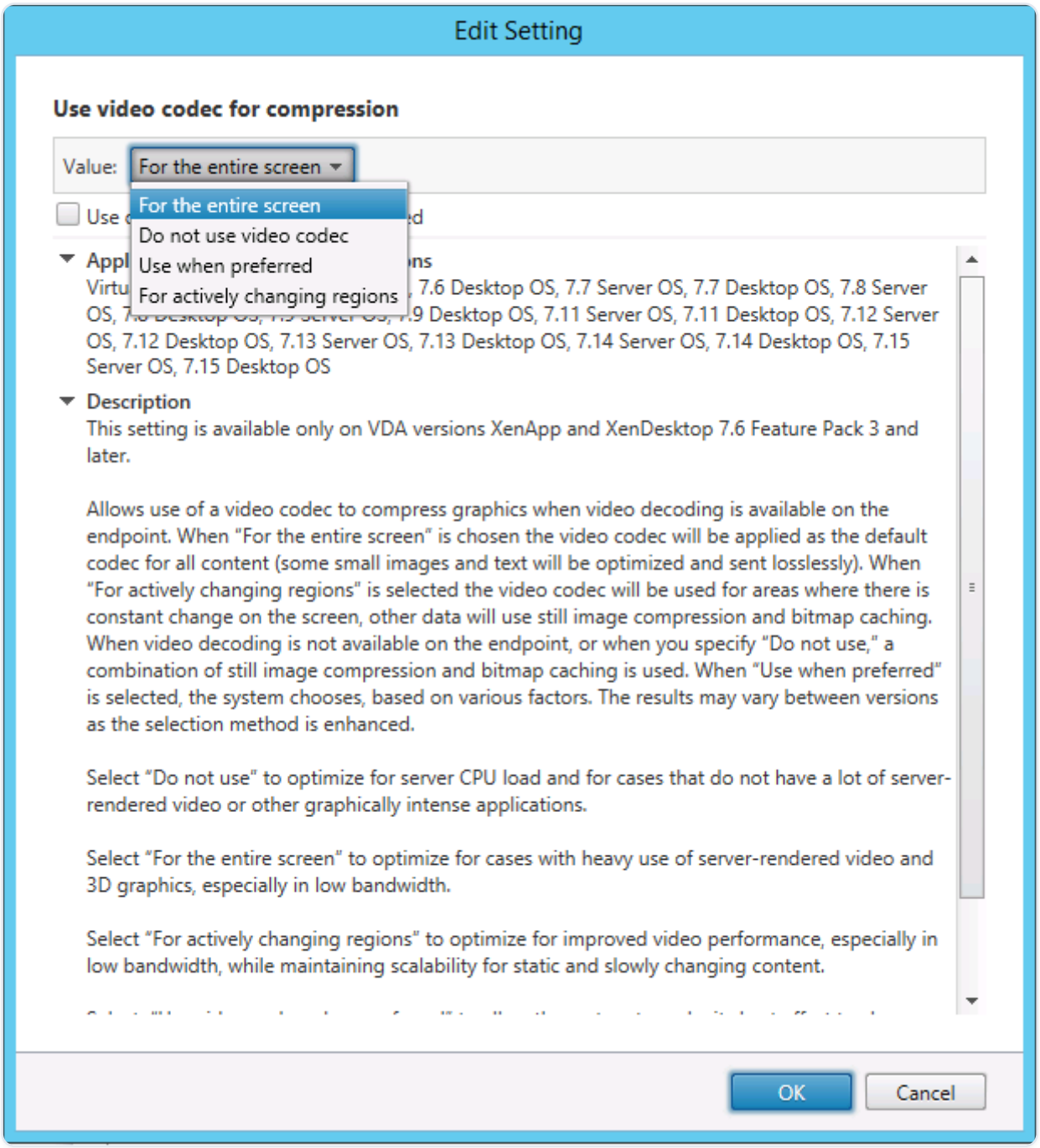
デフォルトでは、**3Dグラフィックワークロード向けに最適化**は無効になっています。

圧縮用ビデオコーデック

Thinwireは、Linux VDAで使用されるディスプレイリモート処理テクノロジーです。このテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。

この**圧縮にビデオコーデックを使用**グラフィックポリシーは、デフォルトのグラフィックモードを設定し、さまざまなユースケースに対して以下のオプションを提供します。

- **優先する場合に利用**。この設定はデフォルトです。追加の構成は不要です。これにより、すべてのCitrix®接続でThinwireが選択され、一般的なデスクトップワークロードのスケーラビリティ、帯域幅、および優れた画質のために最適化されます。
- **画面全体に対して**。ThinwireをフルスクリーンH.264またはH.265で提供し、特に3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上を最適化します。**画面全体に対して**が選択されている場合、または**優先する場合に利用**が選択され、3Dグラフィックワークロード向けに最適化が有効になっている場合に、セッションウォーターマークがサポートされます。
- **アクティブに変更される領域に対して**。Thinwireのアダプティブディスプレイテクノロジーは、動く画像（ビデオ、移動中の3D）を識別します。画像が動いている画面の部分でのみH.264を使用します。H.264ビデオコーデックの選択的な使用により、HDX Thinwireは、H.264ビデオコーデックを使用して頻繁に更新される画面の一部を検出し、エンコードできます。静止画圧縮（JPEG、RLE）とビットマップキャッシュは、テキストや写真画像を含む画面の残りの部分で引き続き使用されます。ユーザーは、ビデオコンテンツの帯域幅消費量の削減と品質の向上、およびロスレステキストまたは高品質の画像を他の場所で組み合わせるという利点を得られます。この機能を有効にするには、**圧縮にビデオコーデックを使用**ポリシーを**優先する場合に利用**（デフォルト）または**アクティブに変更される領域に対して**に設定します。詳細については、グラフィックポリシー設定を参照してください。



ディスプレイリモート処理のパフォーマンスを微調整するために、以下の視覚表示ポリシー設定を含む他のいくつかのポリシー設定を使用できます。

- シンプルなグラフィックの優先色深度
- ターゲットフレームレート
- 視覚品質

H.264 ハードウェアエンコーディング

ビデオコーデックにハードウェアエンコーディングを使用ポリシーは、利用可能な場合、GPU ハードウェアアクセラレーションを使用してビデオコーデックで画面要素を圧縮することを許可

します。GPUハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

GPUハードウェアアクセラレーションは、ハードウェアリソースの使用率を最適化し、1秒あたりのフレーム数（FPS）のパフォーマンスを大幅に向上させます。

バージョン2210以降、GPUハードウェアアクセラレーションは以下のグラフィックモードをサポートします。

- 優先する場合に使用
- 画面全体向け
- 頻繁に変化する領域向け

視覚的にロスレスな圧縮を許可する

視覚的にロスレスな圧縮を許可ポリシーは、グラフィックに対して真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用することを許可します。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、**視覚品質**設定の値の使用方法を変更します。

視覚的にロスレスな圧縮を許可ポリシーはデフォルトで無効になっています。視覚的にロスレスな圧縮を有効にするには、**視覚的にロスレスな圧縮を許可**を**有効**に設定し、**視覚品質**ポリシーを**ロスレスにビルド**に設定します。

圧縮にビデオコーデックを使用ポリシーが**ビデオコーデックを使用しない**に設定されている場合、視覚的にロスレスな圧縮は静止画エンコーディングに適用されます。**圧縮にビデオコーデックを使用**ポリシーが**ビデオコーデックを使用しない**以外のグラフィックモードに設定されている場合、視覚的にロスレスな圧縮はH.264エンコーディングに適用されます。

以下のクライアントはセレクティブH.264をサポートしています。

- Citrix Receiver for Windows バージョン4.9から4.12まで
- Citrix Receiver for Linux 13.5から13.10まで
- Windows向け Citrix Workspace™ app 1808 およびそれ以降のバージョン
- Linux向け Citrix Workspace app 1808 およびそれ以降のバージョン

視覚品質および**圧縮にビデオコーデックを使用**ポリシー設定の詳細については、「視覚表示ポリシー設定」および「グラフィックポリシー設定」を参照してください。

H.265ビデオコーデックのサポート

7.18リリース以降、Linux VDAはリモートグラフィックとビデオのハードウェアアクセラレーションのためにH.265ビデオコーデックをサポートしています。

この機能は、以下で使用できます。

- Citrix Receiver for Windows のバージョン 4.10 から 4.12 まで
- Windows向けCitrix Workspaceアプリ1808以降

この機能を利用するには、Linux VDAとクライアントの両方で有効にします。クライアントのGPUがDXVAインターフェイスを使用したH.265デコードをサポートしていない場合、**グラフィックのH.265デコード**ポリシー設定は無視され、セッションはH.264ビデオコーデックの使用にフォールバックします。詳しくは、「H.265ビデオエンコード」を参照してください。

VDAでH.265ハードウェアエンコードを有効にするには：

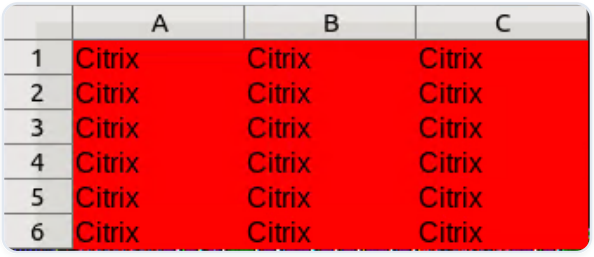
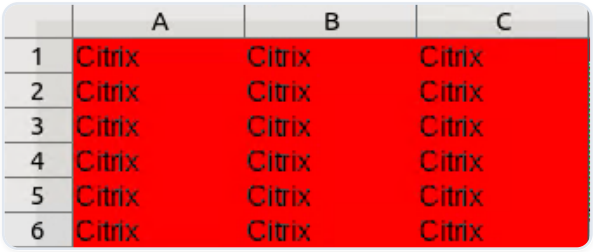
1. **ビデオコーデックにハードウェアエンコードを使用する**ポリシーを有効にします。
2. **3Dグラフィックワークロード向けに最適化**ポリシーを有効にします。
3. **圧縮にビデオコーデックを使用する**ポリシーがデフォルトであるか、**画面全体**に設定されていることを確認します。
4. **視覚品質**ポリシーが、**ロスレスビルド**または**常にロスレス**に**設定されていない**ことを確認します。

クライアントでH.265ハードウェアエンコードを有効にするには、「H.265ビデオエンコード」を参照してください。

YUV444ソフトウェアエンコードのサポート

Linux VDAはYUV444ソフトウェアエンコードをサポートしています。YUVエンコードスキームは、各ピクセルに輝度と色の両方の値を割り当てます。YUVでは、**Y**が輝度またはルミナンス値を表し、**UV**が色またはクロミナンス値を表します。この機能は、Citrix Receiver for Windows 4.10〜4.12、およびCitrix Workspaceアプリ1808 for Windows以降で使用できます。

各Y、U、またはVの一意の値は、8ビット、つまり1バイトのデータで構成されます。YUV444データ形式は、ピクセルあたり24ビットを送信します。YUV422データ形式は、2つのピクセル間でUおよびV値を共有するため、ピクセルあたりの平均送信レートは16ビットになります。次の表は、YUV444とYUV420の直感的な比較を示しています。

YUV444	YUV420
	

VDAでYUV444ソフトウェアエンコーディングを有効にするには:

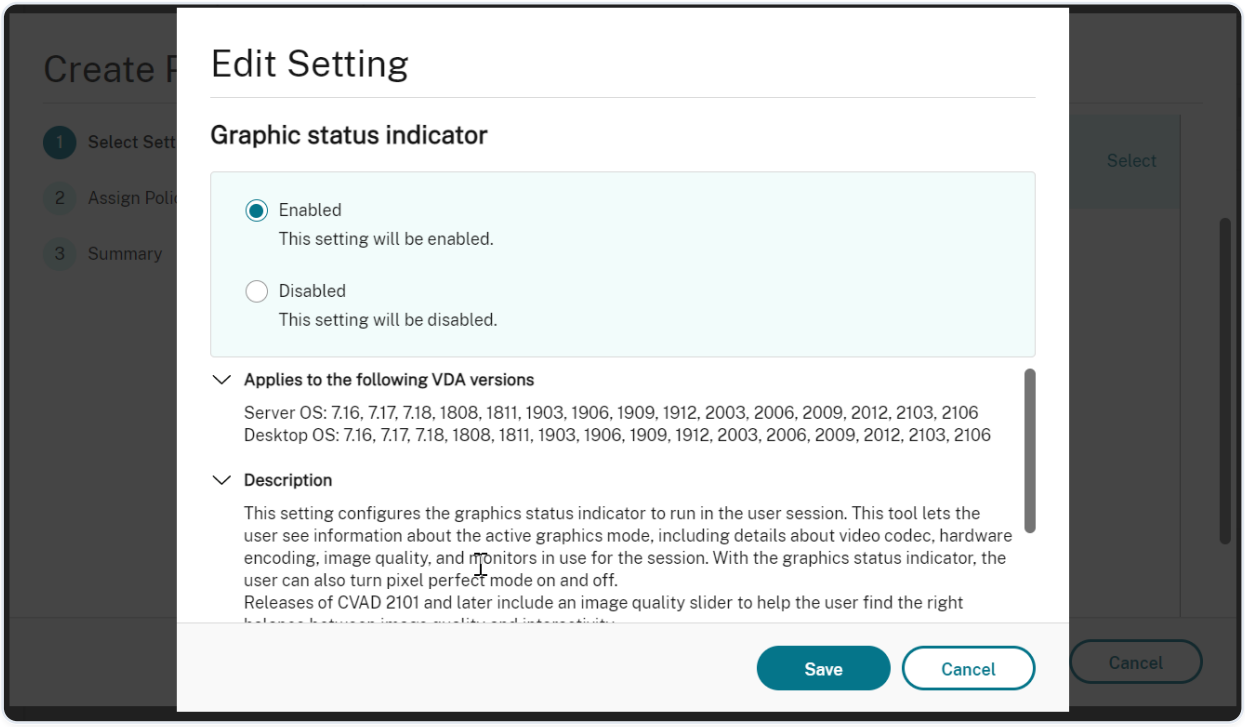
1. 「**ビデオコーデックを使用して圧縮**」ポリシーが「**画面全体**」に設定されていることを確認します。
2. 「**視覚品質**」ポリシーが「**常にロスレス**」または「**ロスレスに構築**」に設定されていることを確認します。

グラフィック品質スライダー

仮想Linuxセッションで実行されるグラフィックステータスインジケーターツールに、グラフィック品質スライダーを含めました。このスライダーは、画像品質と対話性の間の適切なバランスを見つけるのに役立ちます。

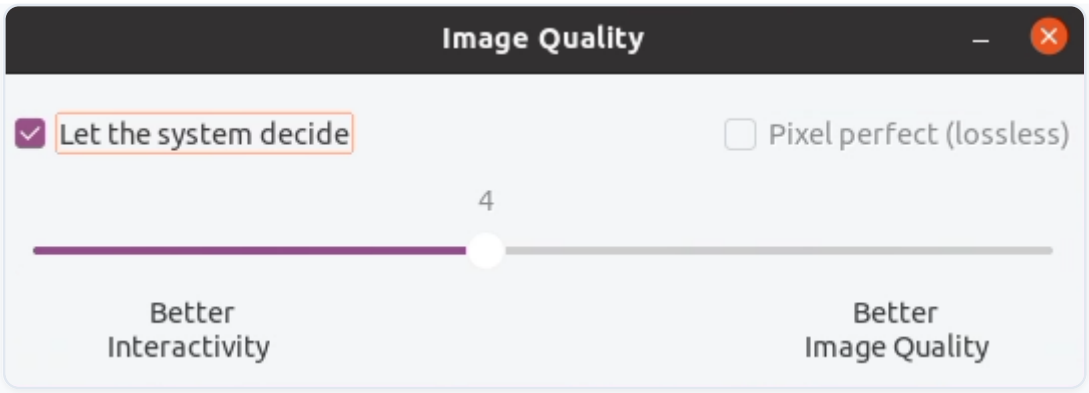
スライダーを使用するには、次の手順を実行します:

1. Citrix Studioで「**グラフィックステータスインジケーター**」ポリシーを有効にします。



2. ターミナルを開き、`ctxslider`コマンドを実行します。スライダーUIが表示されます。

> **注:**
>
> 「**視覚品質**」ポリシーを「**常にロスレス**」または「**ロスレスに構築**」に設定している場合、スライダーUIは表示されません。



次の選択肢が利用可能になりました:

- 画像の品質を変更するには、スライダーを動かします。スライダーは0～9の範囲をサポートしています。
- システム定義の設定を使用するには、**システムに決定させる**を選択します。
- ロスレスモードに切り替えるには、**ピクセルパーフェクト**を選択します。

帯域幅の見積もりに基づいて平均ビットレートを調整する

Citrixは、帯域幅の見積もりに基づいて平均ビットレートを調整することにより、HDX™ 3D Pro ハードウェアエンコーディングを強化します。

HDX 3D Proハードウェアエンコーディングが使用されている場合、VDAはネットワークの帯域幅を断続的に推定し、それに応じてエンコードされたフレームのビットレートを調整できます。この新機能は、シャープネスと流暢さのバランスを取るメカニズムを提供します。

この機能はデフォルトで有効になっています。無効にするには、次のコマンドを実行します。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "DisableReconfigureEncoder" -d "0x00000001" --force
```

この機能を使用するだけでなく、シャープネスと流暢さの間で調整するために、次のコマンドを実行することもできます。**AverageBitRatePercent**および**MaxBitRatePercent**パラメーターは、

帯域幅使用率のパーセンテージを設定します。設定する値が高いほど、グラフィックはシャープになり、流暢さは低下します。推奨される設定範囲は50～100です。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "AverageBitRatePercent" -d "90" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "MaxBitRatePercent" -d "100" --force
```

平均ビットレート調整では、画面が静止している場合、新しいフレームが送信されないため、最新のフレームは低品質の状態を維持します。シャープ化サポートは、最新のフレームを最高品質で再構成してすぐに送信することにより、この問題に対処できます。

Linux VDA Thinwireでサポートされているポリシーの完全なリストについては、ポリシーサポートリストを参照してください。

Linux VDAでのマルチモニターサポートの構成については、CTX220128を参照してください。

並列処理

Thinwireは、特定のタスクを並列化することで、1秒あたりのフレーム数（FPS）を向上させることができますが、全体的なCPU消費量がわずかに増加するというオーバーヘッドがあります。この機能はデフォルトで無効になっています。この機能を有効にするには、VDAで次のコマンドを実行します。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"ParallelProcessing" -d "0x00000001" --force
```

トラブルシューティング

使用中のグラフィックモードを確認する

使用中のグラフィックモードを確認するには、次のコマンドを実行します（**0**はTW+、**1**は全画面ビデオコーデックを意味します）。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

結果は次のようになります。

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000000" --force
```

H.264が使用中であることを確認する

H.264が使用中であることを確認するには、次のコマンドを実行します（**0**は未使用、**1**は使用中を意味します）。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

たとえば、結果は次のようになります。

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000000" --force
```

H.265が使用中であることを確認する

全画面H.265が使用中であることを確認するには、次のコマンドを実行します（**0**は未使用、**1**は使用中を意味します）。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

たとえば、結果は次のようになります。

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H265" -d "0x00000000" --force
```

どのYUVエンコードスキームが使用中であるかを確認する

どのYUVエンコードスキームが使用中であるかを確認するには、次のコマンドを実行します（**0**はYUV420、**1**はYUV422、**2**はYUV444を意味します）。

> **注:**
>
> **YUVFormat**の値は、ビデオコーデックが使用中の場合にのみ意味があります。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

たとえば、結果は次のようになります。

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000000" --force`

YUV444ソフトウェアエンコーディングが使用中であることを確認する

YUV444ソフトウェアエンコーディングが使用中であることを確認するには、次のコマンドを実行します。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

YUV444が使用中の場合、結果は次のようになります。

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000000" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000002" --force`

HDX 3D Proが有効になっていることを確認する

HDX 3D Pro が有効になっていることを確認するには、次のコマンドを実行します。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition



sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode



sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
```

HDX 3D Pro が有効になっている場合、結果は次のようになります。

`create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State" -t "REG_SZ" -v "ProductEdition" -d "<PLT or ENT>" --force`

`create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "StackSessionMode" -d "0x00000000" --force`

`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "3DPro" -d "0x00000000" --force`

HDX 3D Pro に必要な NVIDIA ライブラリがロードされていることを確認するには、Linux VDA で **nvidia-smi** コマンドを実行します。結果は次のようになります。

```
Tue Apr 12 10:42:03 2016

+-----------------------------------------------------+

| NVIDIA-SMI 361.28     Driver Version: 361.28         |

|-------------------------------+----------------------
+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |

|
===============================+======================+==================
===|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
N/A |

| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
Default |

+-------------------------------+----------------------
+----------------------+



+-----------------------------------------------------------------------------
----+

| Processes:                                                       GPU
```

```
Memory |

|  GPU       PID  Type  Process name
Usage      |

|
=============================================================================
===|

|    0      2164  C+G   /usr/local/bin/ctxgfx
106MiB |

|    0      2187    G   Xorg
85MiB |

+-----------------------------------------------------------------------------
----+
```

3D Pro でハードウェアエンコードが使用されていることを確認する

次のコマンドを実行します (**0** は使用されていないことを意味します。**1** は使用中であることを意味します):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

3D Pro が使用されている場合、結果は次のようになります。

`create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force`

NVIDIA GRID グラフィックドライバーが正しくインストールされていることを確認する

NVIDIA GRID グラフィックドライバーが正しくインストールされていることを確認するには、**nvidia-smi** を実行します。結果は次のようになります。

```
+-----------------------------------------------------+

| NVIDIA-SMI 352.70     Driver Version: 352.70         |

|-------------------------------+----------------------
+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
```

```
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |

|
==============================+======================+==================
===|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
Off |

| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
Default |

+-------------------------------+----------------------
+----------------------+




+-----------------------------------------------------------------------------
----+

| Processes:                                                       GPU
Memory |

|  GPU       PID  Type  Process name
Usage      |

|
=============================================================================
===|

|  No running processes found
                                 |

+-----------------------------------------------------------------------------
----+
```

カードの正しい構成を設定します。

`etc/X11/ctx-nvidia.sh`

HDX 3D Pro マルチモニターの再描画に関する問題

プライマリモニター以外の画面で再描画の問題が発生している場合は、NVIDIA GRID ライセンスが利用可能であることを確認してください。

Xorg エラーログを確認する

Xorg のログファイルは、**/var/log/** フォルダーに **Xorg.{DISPLAY}.log** のような名前で保存されています。

既知の問題と制限事項

vGPU の場合、Citrix Hypervisor™ のローカルコンソールに ICA デスクトップセッション画面が表示される

回避策: 次のコマンドを実行して、VM のローカル VGA コンソールを無効にします。

Citrix Hypervisor 8.1 以降の場合:

```
[root@xenserver® ~]# xe vgpu-param-set uuid=vgpu-uuid
extra_args=disable_vnc=1
```

Citrix Hypervisor 8.1 より前のバージョン:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

Gnome 3 デスクトップのポップアップがログオン時に遅い

これは Gnome 3 デスクトップセッションの起動における制限事項です。

シトリックス ワークスペース アプリのウィンドウサイズを変更すると、一部のOpenGL/WebGL アプリケーションが適切にレンダリングされない

Citrix Workspaceアプリのウィンドウサイズを変更すると、画面解像度が変更されます。NVIDIA独自のドライバーは一部の内部状態を変更し、アプリケーションがそれに応じて応答する必要がある場合があります。たとえば、WebGLライブラリ要素の**lightgl.js**は、「**このテクスチャへのレンダリングはサポートされていません（不完全なフレームバッファ）**」というエラーを発生させる可能性があります。

HDX™ 画面共有

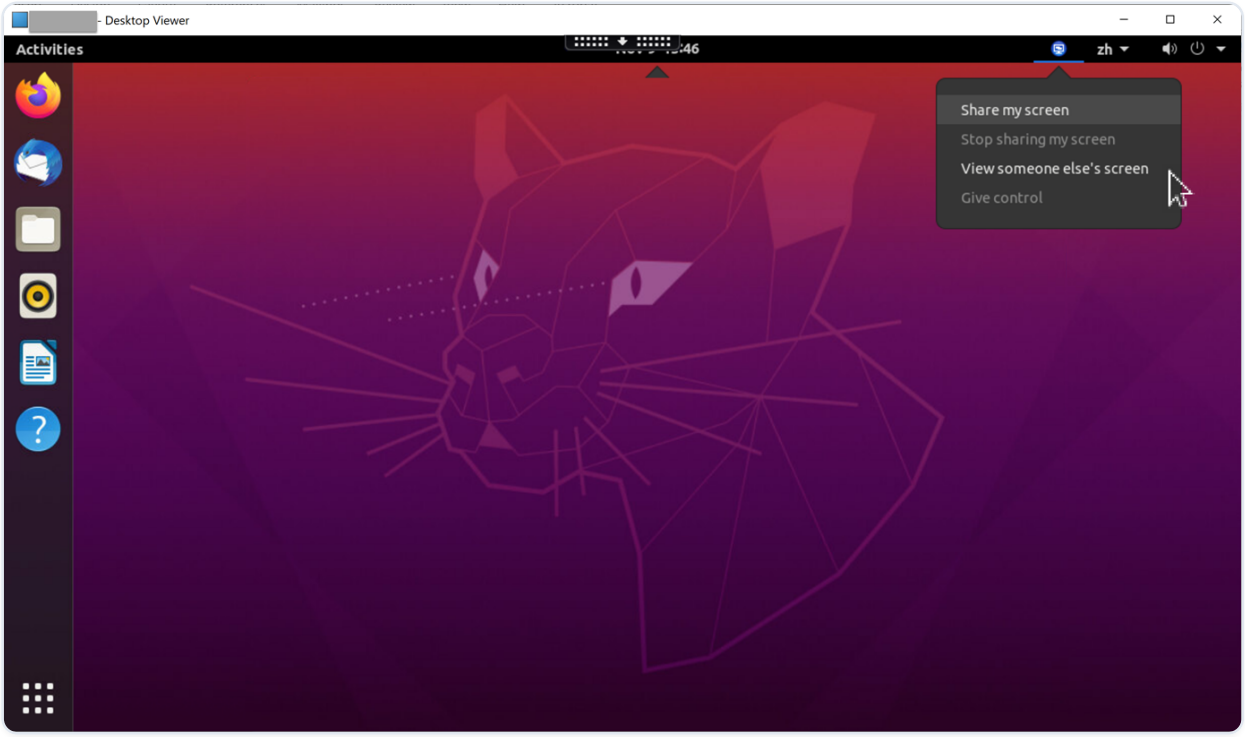
概要

Linux VDAを使用すると、仮想デスクトップの画面を、他の仮想デスクトップ上のセッションユーザーと共有できます。

次の例では、画面を共有し、他のユーザーの画面を表示する手順について説明します。

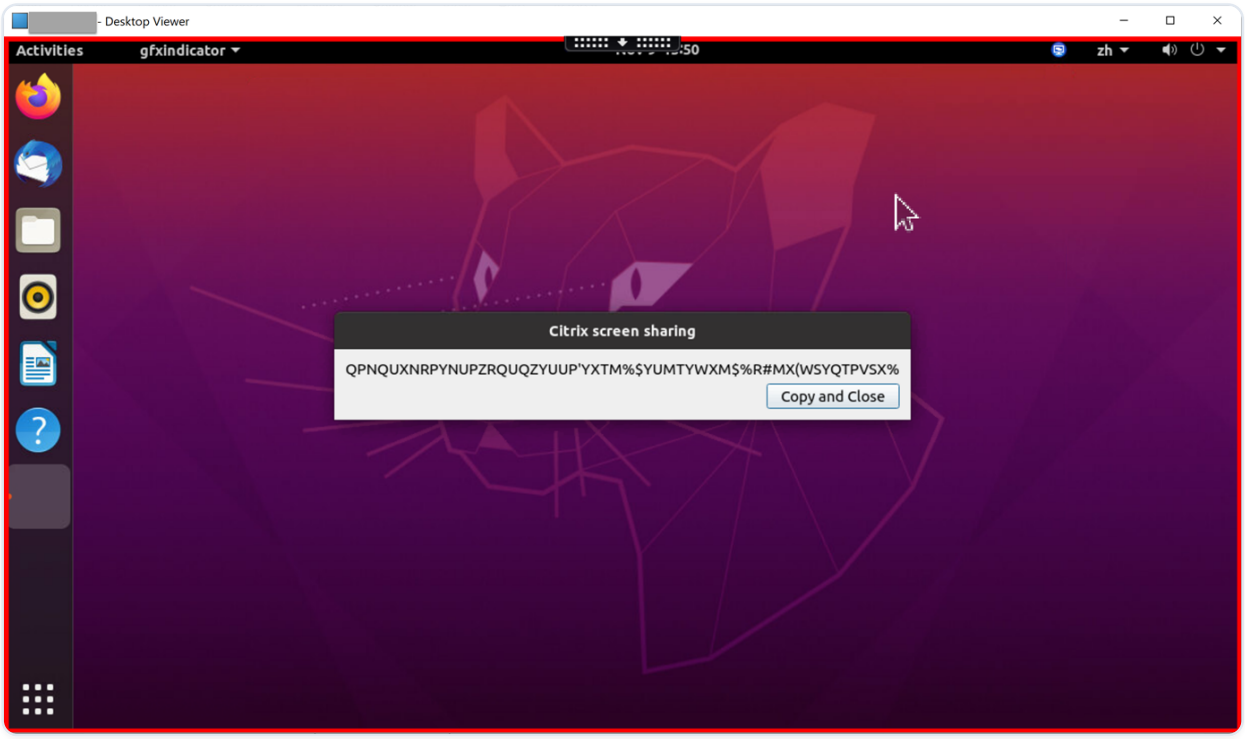
画面を共有するには:

1. 仮想デスクトップの通知領域で、**画面共有**アイコンをクリックし、**画面を共有**を選択します。



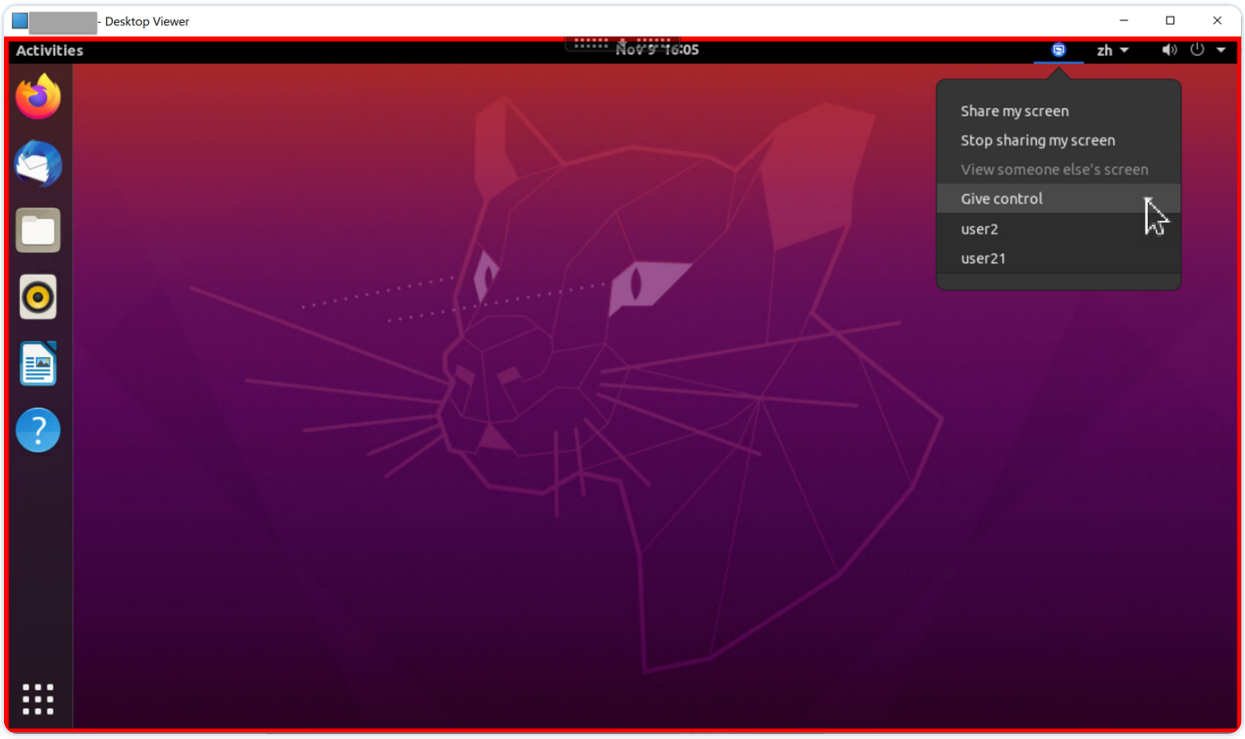
2. **コピーして閉じる**をクリックします。

   現在の画面共有コードは、画面共有を停止して再開するまで保持されます。

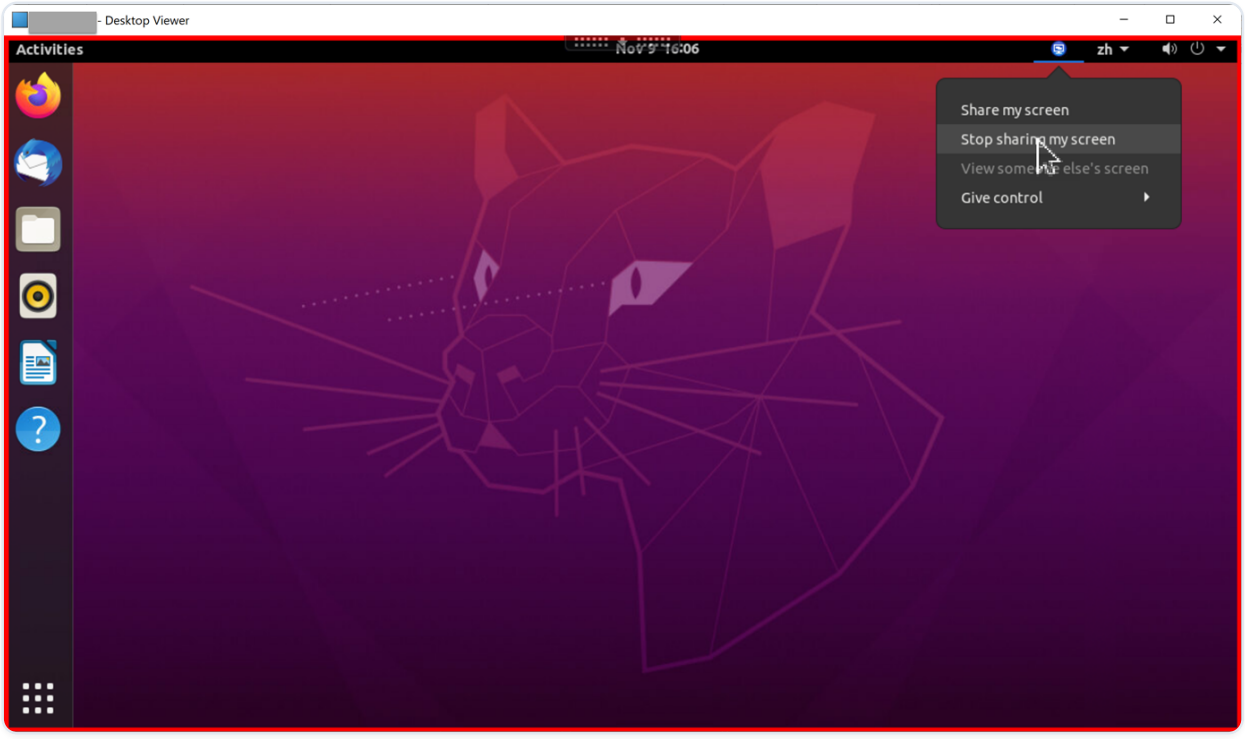


> **ヒント:**
>
> 画面を共有している間、画面の周囲に赤い枠が表示され、共有が進行中であることを示します。

3. 画面を共有したい他の仮想デスクトップ上のセッションユーザーと、コピーしたコードを共有します。
4. 閲覧者に画面を制御させるには、**制御を許可**を選択し、その後、閲覧者の名前を選択します。制御を停止するには、閲覧者の名前の選択を解除します。

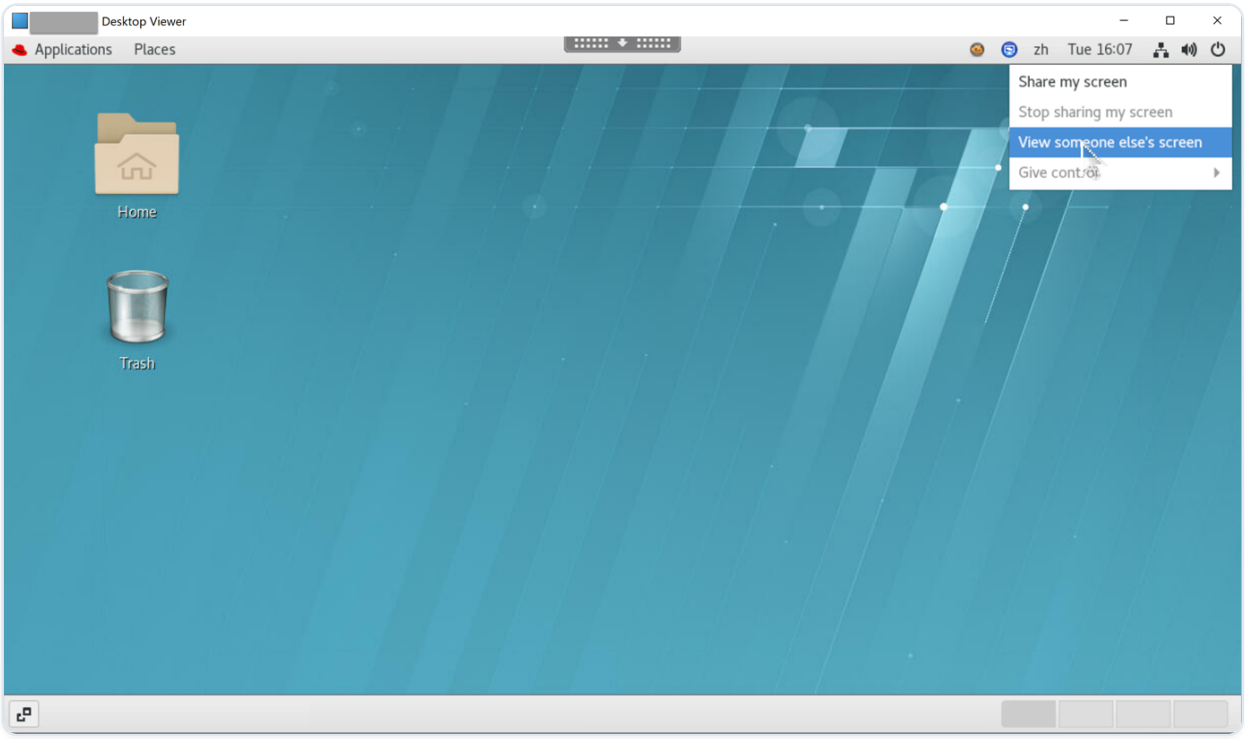


5. 画面共有を停止するには、**画面共有を停止**を選択します。

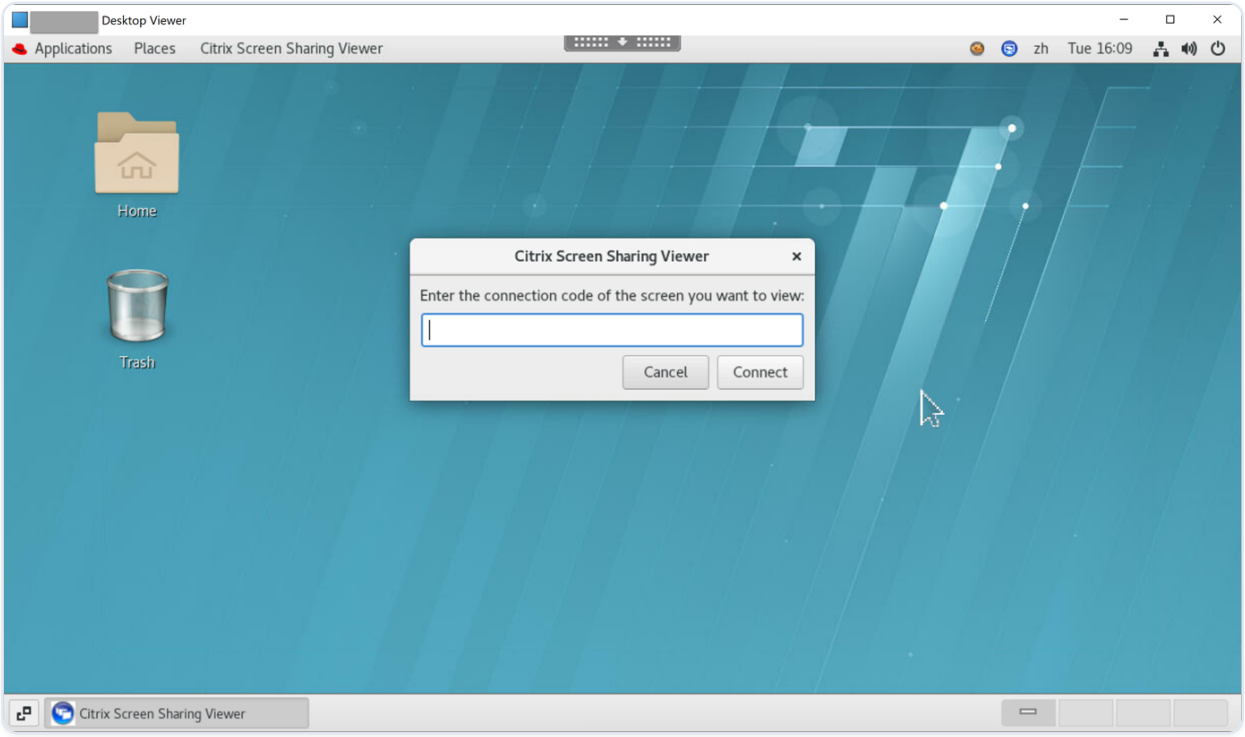


他のユーザーの画面を表示するには:

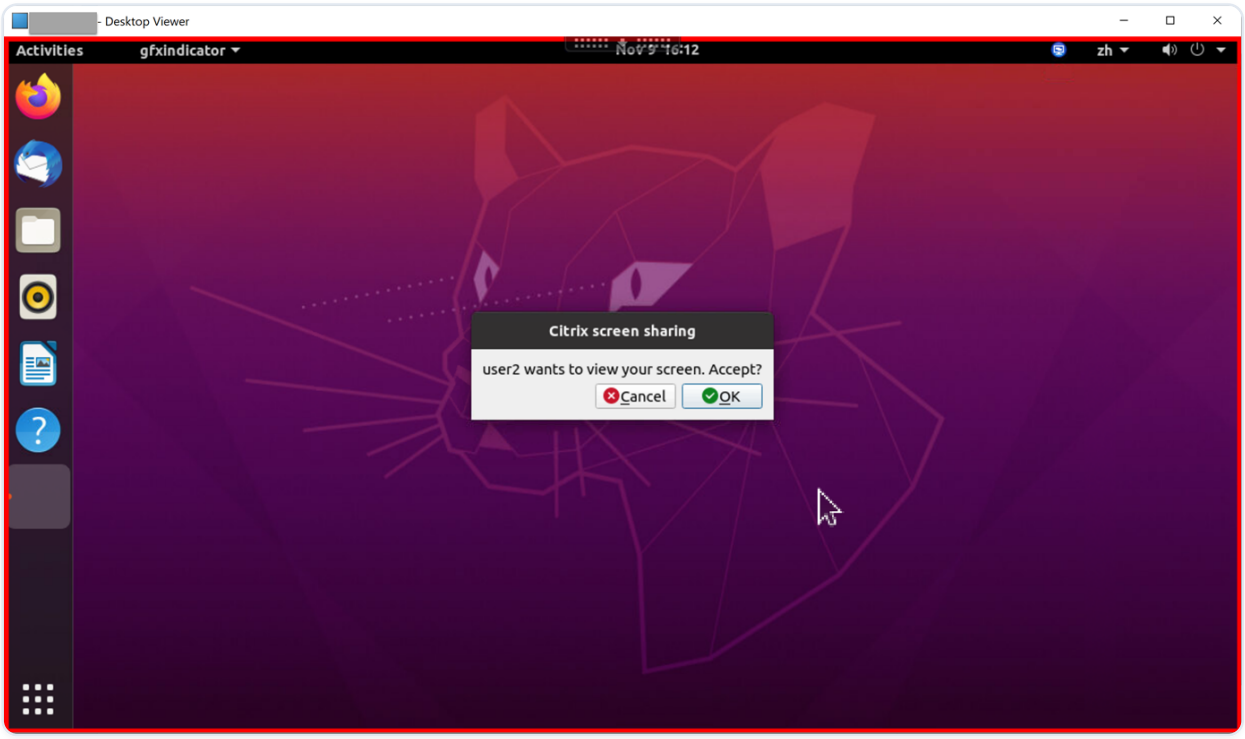
1. 仮想デスクトップの通知領域で、**画面共有**アイコンをクリックし、**他のユーザーの画面を表示**を選択します。



2. 表示したい画面の接続コードを入力し、**接続**をクリックします。



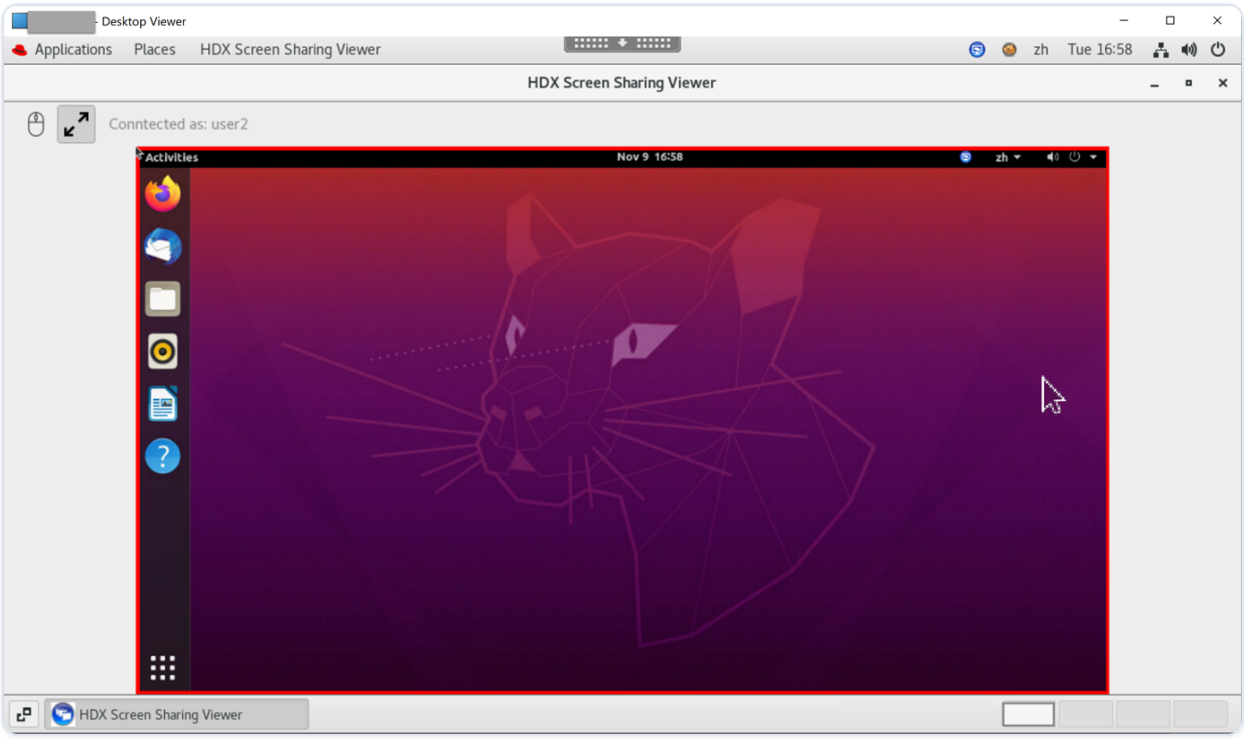
3. 画面共有者がリクエストを承認するまで待ちます。例:



ヒント:

- 共有者側では、Linuxシステムがリクエストの通知を発行します。
- 共有者が30秒以内にリクエストを承認しない場合、リクエストは期限切れとなり、プロンプトが表示されます。

4. 画面共有者が**OK**をクリックしてリクエストを承認すると、共有画面がDesktop Viewerに表示されます。自動的に割り当てられたユーザー名でビューアーとして接続されます。



5. 共有画面の制御を要求するには、左上隅にあるマウスアイコンをクリックします。

> **ヒント:**
>
> - 共有者が30秒以内にリクエストを承認しない場合、リクエストは期限切れとなります。
> - 共有画面を一度に制御できるビューアーは1人だけです。
>
> 共有画面の制御を解除するには、マウスアイコンをもう一度クリックします。

共有画面の制御を解除する(/en-us/linux-virtual-delivery-agent/2303/media/release-control-over-shared-screen.png)

6. ディスプレイのスケーリングを無効にするか、ウィンドウサイズに合わせてスケーリングするには、マウスアイコンの横にあるアイコンをクリックします。

ウィンドウのスケーリング(/en-us/linux-virtual-delivery-agent/2303/media/window-scaling.png)

構成

画面共有機能はデフォルトで無効になっています。これを有効にするには、次の設定を完了します。

1. Citrix Studioでグラフィックステータスインジケーターポリシーを有効にします。

2. Citrix Virtual Apps and Desktops™ 2112以降の場合、Citrix Studioで**ScreenSharing**ポリシーを有効にします。
3. (オプション) Citrix Virtual Apps™ and Desktops 2109以前の場合、次のコマンドを実行してLinux VDAで画面共有を有効にします。

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v
"EnableScreenSharing" -d "0x00000001"
```

4. ファイアウォールでポート52525～52625を許可します。
5. (オプション) RHEL 8.x、Debian 11、またはGNOMEがインストールされたSUSE 15.xを使用している場合は、AppIndicatorサポートを有効にするために、GNOMEシェル用の互換性のある拡張機能をインストールします。

   a. `gnome-shell --version`コマンドを実行して、GNOMEシェルのバージョンを確認します。

   b. `<https://extensions.gnome.org/extension/615/appindicator-support>`からGNOMEシェル用の互換性のある拡張機能をダウンロードします。たとえば、シェルバージョンが3.28の場合、拡張機能のバージョンとして24または26を選択できます。

   GNOMEシェル拡張機能(/en-us/linux-virtual-delivery-agent/2303/media/gnome-extension.png)

   c. ダウンロードしたパッケージを解凍します。パッケージ内の**metadata.json**ファイルの**「uuid」**値が**appindicatorsupport@rgcjonas.gmail.com**に設定されていることを確認します。

   d. `mv`コマンドを実行して、appindicatorsupport@rgcjonas.gmail.comディレクトリを`/usr/share/gnome-shell/extensions/`の下の場所に移動します。

   e. `chmod a+r metadata.json`コマンドを実行して、**metadata.json**ファイルを他のユーザーが読み取れるようにします。

> **ヒント:**
>
> デフォルトでは、appindicatorsupport@rgcjonas.gmail.com ディレクトリ内の **metadata.json** ファイルは、rootユーザーのみが読み取り可能です。画面共有をサポートするには、**metadata.json** ファイルを他のユーザーも読み取り可能にしてください。

f. GNOME Tweaksをインストールします。

g. デスクトップ環境で、`Alt+F2`、`r`、`Enter`のキーを順番に押すか、`killall -SIGQUIT gnome-shell`コマンドを実行してGNOMEシェルをリロードします。

h. デスクトップ環境でGNOME Tweaksを実行し、Tweaksツールで**KStatusNotifierItem/AppIndicator Support**を有効にします。

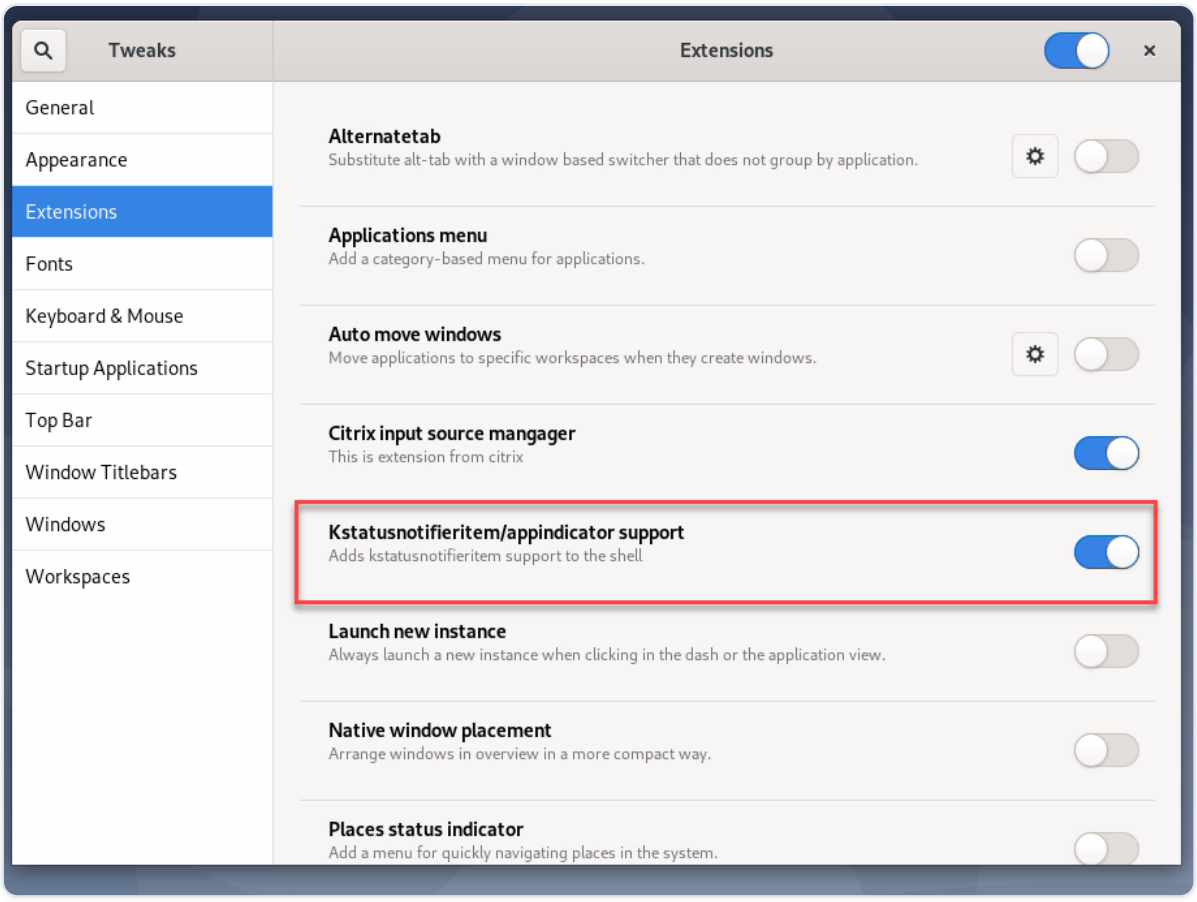
6. (オプション) GNOMEがインストールされたDebian 11.3を使用している場合は、以下の手順でGNOMEシステムトレイアイコンをインストールして有効にします。

a. `sudo apt install gnome-shell-extension-appindicator`コマンドを実行します。GNOMEが拡張機能を表示するには、一度ログアウトしてから再度ログインする必要がある場合があります。

b. **アクティビティ**画面でTweaksを検索します。

c. Tweaksツールで**拡張機能**を選択します。

d. **Kstatusnotifieritem/appindicator support**を有効にします。



考慮事項

- 画面共有機能はH.265ビデオコーデックをサポートしていません。

- 画面共有機能はアプリセッションでは利用できません。
- デスクトップセッションのユーザーは、デフォルトで最大10人の視聴者とセッション画面を共有できます。最大視聴者数は`ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v "ScreenSharingViewerMaxNum" -d <hex_value>`で構成可能です。最大数に達すると、ユーザーが追加の接続要求を受け入れようとしたときにプロンプトが表示されます。

非仮想化GPU

Linux VDAドキュメントでは、非仮想化GPUは以下を指します。

- リモートPCアクセスシナリオで使用されるGPU
- ハイパーバイザーからパススルーされたGPU

この記事では、非仮想化GPU向けにHDX™ 3D Proを有効にする方法について説明します。

前提条件

- HDX 3D Proを有効にします。これを行うには、Linux VDAのインストール時に`CTX_XDL_HDX_3D_PRO`を`Y`に設定します。環境変数については、「ステップ8：インストールを完了するためのランタイム環境の設定」を参照してください。
- NVIDIA Linux Capture SDKがサポートするGPUの場合、HDX 3D Proを有効にすると、ハードウェアアクセラレーションがデフォルトで有効になります。追加の設定は不要です。
- NVIDIA Linux Capture SDKがサポートしないGPUの場合、`XDamage`をインストールします。たとえば、Ubuntu 20.04にXDamageをインストールするには、`sudo apt-get install -y libxdamage1`を実行します。通常、XDamageはXServerの拡張機能として存在します。

構成

Xorg構成ファイルの変更

NVIDIA非仮想化GPUの場合

構成ファイルは自動的にインストールおよび設定されます。

その他のGPUの場合

`/etc/X11/`にインストールされている4つのテンプレート構成ファイルを変更する必要があります。

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf

- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

ctx-driver_name-1.conf を例として、テンプレート構成ファイルを変更するには、次の手順を実行します。

1. ***driver_name*** を実際のドライバー名に置き換えます。

   たとえば、ドライバー名が `intel` の場合、構成ファイル名を `ctx-intel-1.conf` に変更できます。

2. ビデオドライバー情報を追加します。

   各テンプレート構成ファイルには、「Device」という名前のセクションが含まれており、コメントアウトされています。このセクションでは、ビデオドライバー情報について説明します。ビデオドライバー情報を追加する前に、このセクションを有効にしてください。このセクションを有効にするには：

   a. 構成情報については、GPUメーカーが提供するガイドを参照してください。ネイティブ構成ファイルを生成できます。ネイティブ構成ファイルを使用して、GPUがローカル環境で動作することを確認してください。

   b. ネイティブ構成ファイルの「Device」セクションを **ctx-driver_name-1.conf** にコピーします。

3. 次のコマンドを実行してレジストリキーを設定し、Linux VDAが手順1で設定された構成ファイル名を認識できるようにします。

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
   "REG_SZ" -v "DriverName" -d "intel" --force
   ```

XDamageを有効にする

NVIDIA Linux Capture SDK のリリースノートのサポートされているハードウェアセクションに記載されていないGPUを使用している場合は、次の方法で `XDamage` を有効にします。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

リモートPCアクセスVDAのモニターブランキング

Linux VDAは、非仮想化GPUを使用するリモートPCアクセスVDA向けに物理モニターブランキングをサポートしています。

この機能をサポートする完全にテスト済みのLinuxディストリビューションには、Ubuntu 20.04とDebian 11.3が含まれます。

この機能はデフォルトで無効になっています。有効にするには、次の2つの手順を完了してください。

1. お使いのLinuxディストリビューションに基づいて、`evdi-dkms`パッケージをインストールします。

   ```
   sudo apt install evdi-dkms
   ```

2. EVDIへのグラフィックディスプレイオフロードを有効にします。

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
   -v "Evdi" -d "0x00000001" --force
   ```

3. Intel GPUを使用している場合は、ディスプレイマネージャーを無効にします。そうしないと、Intel GPUがディスプレイマネージャーによって占有され、Citrix®リモートセッションで利用できなくなります。

   ```
   sudo systemctl disable --now gdm
   ```

トラブルシューティング

グラフィック出力がない、または文字化けしている

3Dアプリケーションをローカルで実行でき、すべての構成が正しい場合、グラフィック出力がない、または文字化けしているのはバグの結果です。デバッグのためにトレース情報を収集するには、/opt/Citrix/VDA/bin/setlog を使用し、GFX_X11 を verbose に設定します。

ハードウェアエンコーディングが機能しない

`Xdamage`を使用する場合、ソフトウェアエンコーディングのみがサポートされます。

セッションウォーターマーク

セッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗むユーザーへの抑止力として、セッションデスクトップに表示されます。ウォーターマークは、テキストレイヤーまたはアルファチャネル付きのPNG画像として指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示されます。

> **重要:**

> セッションウォーターマークはセキュリティ機能ではありません。データ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性は保証しません。代わりに、必要に応じてこの機能を他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、画面イメージが取得されたセッションの、ログオン資格情報によって追跡されるユーザーのIDです。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、以下のセッションウォーターマークポリシー設定を使用して、画面上の配置とウォーターマークの外観を構成します。

セッションウォーターマークポリシー設定

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイにはセッション固有の情報を表示する不透明なウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、**クライアントIPアドレスを含める** は無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、**接続時間を含める** は無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、フォントサイズが小さくなったり、切り捨てられたりする可能性があり、ウォーターマークの効果が低下します。

デフォルトでは、**ログオンユーザー名を含める** は有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、**VDAホスト名を含める** は有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、**VDA IPアドレスを含める** は無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。**値** ドロップダウンメニューから **複数** または **単一** を選択します。 追加のスタイルオプションについては、この記事の「**ウォーターマークカスタムテキスト**」セクションを参照してください。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、**セッションウォーターマークスタイル** は **複数** です。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

ウォーターマークのカスタムテキスト

値はデフォルトで空です。空でない文字列を入力するか、文字列を形成する構文を設定するか、またはその組み合わせを使用してセッションウォーターマークに表示できます。空でない文字列は、1行あたり最大25個のUnicode文字をサポートします。25文字を超える文字列は切り捨てられます。

例えば、ポリシーを次の値に設定できます。

```
<date>
<time><newline><username><style=single><fontsize=40><font=Ubuntu><position=center><rotation
Linux VDA<newline>Version 2207
```

すべての構文オプションの説明については、次の表を参照してください。

構文オプション	説明	有効な設定（大文字と小文字を区別）	デフォルト値	備考
`<style>`	ウォーターマークのレイアウトスタイル	`xstyle`、`single`、`tile`、`horizontal`	`xstyle`	-
`<position>`	ウォーターマークの位置	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	レイアウトスタイルが**single**に設定されている場合にのみ有効です。
`<rotation>`	ウォーターマークの特定の角度への回転	-180–180	0	-
`<transparency>`	ウォーターマークの不透明度	0–100	17	-

構文オプション	説明	有効な設定（大文字と小文字を区別）	デフォルト値	備考
`<font>`	-	システムでサポートされているフォント	ゴシック体	-
`<fontsize>`	-	20–50	0 (自動計算)	-
`<fontzoom>`	`<fontsize>` と `<image>` で設定したフォントと画像サイズの割合	0 –	100	-
`<image>`	PNGウォーターマーク	VDA上のPNG画像へのパス	該当なし	この構文はPNGウォーターマークを構成します。アルファチャネルを持つPNGのみがサポートされています。PNGウォーターマークが使用されている場合、`<style>`、`<position>`、`<rotation>`、`<transparency>`、および `<fontzoom>` の構文オプションのみが有効になります。
`<date>`	セッション接続日 (YYYY/MM/DD) のプレースホルダー	該当なし	該当なし	-

構文オプション	説明	有効な設定（大文字と小文字を区別）	デフォルト値	備考
`<time>`	セッション接続時刻 (HH:MM) のプレースホルダー	該当なし	該当なし	-
`<domain>`	ユーザーアカウントドメインのプレースホルダー	該当なし	該当なし	-
`<username>`	現在のログオンユーザー名 (ユーザーアカウントドメインを除く) のプレースホルダー	該当なし	該当なし	-
`<hostname>`	VDAのホスト名のプレースホルダー	該当なし	該当なし	-
`<clientip>`	クライアントのIPアドレスのプレースホルダー	該当なし	該当なし	-
`<serverip>`	VDAのIPアドレスのプレースホルダー	該当なし	該当なし	-

注:

ウォーターマークのカスタムテキストが有効な構文設定で指定されている場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。

> 構文オプションを指定しないか、サポートされていない値に設定した場合、その既定値が使用されます。

制限事項

- セッションウォーターマークは、以下のいずれかのケースでサポートされます。
  - **ビデオコーデックを圧縮に使用**が**画面全体**に設定されている場合。
  - **ビデオコーデックを圧縮に使用**が**推奨される場合に使用**に設定されており、3Dグラフィックワークロード向けに最適化が有効になっている場合。
- ブラウザコンテンツリダイレクトが使用されているセッションでは、セッションウォーターマークはサポートされません。セッションウォーターマーク機能を使用するには、ブラウザコンテンツリダイレクトが無効になっていることを確認してください。
- レガシーNVIDIAドライバーを使用し、セッションが全画面ハードウェアアクセラレーションH.264またはH.265エンコードモードで実行されている場合、セッションウォーターマークはサポートされず、表示されません。(この場合、レジストリでNvCaptureTypeが2に設定されています。)
- セッションシャドウイングではウォーターマークは表示されません。
- Print Screenキーを押して画面をキャプチャした場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。画面キャプチャがコピーされないように対策を講じることをお勧めします。

Thinwire プログレッシブ表示

セッションの対話性は、低帯域幅または高遅延の接続で低下する可能性があります。たとえば、Webページのスクロールが遅くなったり、応答しなくなったり、途切れたりすることがあります。キーボードとマウスの操作は、グラフィックの更新に遅れることがあります。

バージョン7.17までは、ポリシー設定を使用して、セッションを**低**視覚品質に構成するか、より低い色深度（16ビットまたは8ビットグラフィック）を設定することで、帯域幅の消費を削減できました。ただし、ユーザーが弱い接続を使用していることを知っている必要がありました。HDX Thinwireは、ネットワークの状態に基づいて静止画の品質を動的に調整しませんでした。

バージョン7.18以降、HDX Thinwireは、以下のいずれかのケースで、デフォルトでプログレッシブ更新モードに切り替わります。

- 利用可能な帯域幅が2 Mbpsを下回る。
- ネットワーク遅延が200 msを超える。

このモードでは：

たとえば、プログレッシブ更新モードがアクティブな以下のグラフィックでは、文字**F**と**e**に青いアーティファクトがあり、画像は高度に圧縮されています。このアプローチにより、帯域幅の消費が大幅に削減され、画像とテキストをより迅速に受信できるようになり、セッションの対話性が向上します。

Thinwire プログレッシブ表示 1 の画像(/en-us/linux-virtual-delivery-agent/2303/media/thinwireprogressivedisplay.png)

セッションとの対話を停止すると、劣化した画像とテキストは徐々にロスレスにシャープ化されます。たとえば、以下のグラフィックでは、文字に青いアーティファクトが含まれなくなり、画像は元の品質で表示されます。

Thinwire プログレッシブ表示 2 の画像(/en-us/linux-virtual-delivery-agent/2303/media/thinwireprogressivedisplay2.png)

画像の場合、シャープ化にはランダムなブロック状の方法が使用されます。テキストの場合、個々の文字または単語の一部がシャープ化されます。シャープ化プロセスは複数のフレームにわたって行われます。このアプローチにより、単一の大きなシャープ化フレームによる遅延の発生が回避されます。

一時的な画像（ビデオ）は、引き続きアダプティブディスプレイまたはSelective H.264で管理されます。

プログレッシブモードの使用方法

デフォルトでは、プログレッシブモードは、**視覚品質**ポリシー設定の**高**、**中**（デフォルト）、**低**に対してスタンバイ状態です。

プログレッシブモードは、次の場合に強制的にオフ（使用不可）になります。

- **視覚品質** = **常にロスレス** または **ロスレスにビルド**
- **単純なグラフィックの優先色深度** = 8ビット
- **圧縮にビデオコーデックを使用** = **画面全体** (全画面H.264が必要な場合)

プログレッシブモードがスタンバイ状態の場合、デフォルトでは以下のいずれかの条件が発生したときに有効になります。

- 利用可能な帯域幅が2 Mbpsを下回る
- ネットワーク遅延が200 msを超える

モード切り替えが発生した後、たとえネットワークの状態が悪化しても、そのモードで最低10秒間は維持されます。

プログレッシブモードの動作を変更する

次のコマンドを実行して、プログレッシブモードの動作を変更できます。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplay" -d "<value>" --force
```

ここで、\<value\>は次のとおりです。

0 = 常にオフ（いかなる状況でも使用しない）

1 = 自動（ネットワークの状態に基づいて切り替え、デフォルト値）

2 = 常にオン

自動モード（1）の場合、次のいずれかのコマンドを実行して、プログレッシブモードが切り替わるしきい値を変更できます。

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
```

ここで、\<value\>は\<Kbps単位のしきい値\>です（デフォルト = 2,048）。

例: 4096 = 帯域幅が4 Mbpsを下回った場合にプログレッシブモードをオンにする

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayLatencyThreshold" -d "<value>" --force
```

ここで、\<value\> は \<しきい値 (ミリ秒)\> です (デフォルト = 200)

例: 100 = ネットワーク遅延が100ミリ秒を下回った場合にプログレッシブモードをオンにする.

一般的なコンテンツリダイレクト

クライアントドライブマッピングとクライアントフォルダーリダイレクト

場合	その場合
ホスト (VDA) でクライアントドライブマッピングのみを有効にする,	クライアント側のフルボリュームは、ホームディレクトリの **ctxmnt** サブディレクトリの下のセッションに自動的にマップされます。
ホスト (VDA) でクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイス (クライアント) でそれを構成する,	ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

USBデバイスリダイレクト

USB デバイスは、Citrix Workspace™ app と Linux VDA デスクトップ間で共有されます。USB デバイスがデスクトップにリダイレクトされると、ローカルに接続されているかのように USB デバイスを使用できます。

クライアントドライブマッピング

クライアントドライブマッピングとクライアントフォルダーリダイレクトを使用して、クライアント側のファイルをホスト側のセッションでアクセス可能にすることができます。クライアントドライブマッピングとクライアントフォルダーリダイレクトの比較は次のとおりです。

条件	結果
ホスト (VDA) でクライアントドライブマッピングのみを有効にすると、,	クライアント側のフルボリュームは、ホームディレクトリ内の **ctxmnt** サブディレクトリの下のセッションに自動的にマップされます。
ホスト (VDA) でクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイス (クライアント) でそれを構成すると、,	ユーザーによって指定されたローカルボリュームの一部がリダイレクトされます。

クライアントドライブマッピングを有効にする

クライアントドライブマッピングを有効にするには、Citrix Studioで **Client drive redirection** ポリシーを **Allowed** に設定します。ポリシーの詳細については、「ファイルリダイレクトポリシー設定」を参照してください。

クライアントフォルダーリダイレクトを有効にし、リダイレクトするフォルダーを指定する

クライアントフォルダーリダイレクトを有効にするには、VDAで次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\Client Folder Redirection" -t "REG_DWORD" -v "CFROnlyModeAvailable" -d "0x00000001" --force
```

クライアントからホスト側のセッションにリダイレクトするフォルダーを指定するには、ユーザーデバイスで次の手順を実行します。

1. Citrix Workspace™アプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、**CtxCFRUI.exe** を起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

USBデバイスリダイレクト

USBデバイスはCitrix Workspace™アプリとLinux VDAデスクトップ間で共有されます。USBデバイスがデスクトップにリダイレクトされると、ローカルに接続されているかのようにUSBデバイスを使用できます。

> **ヒント:**
>
> ネットワーク遅延が100ミリ秒未満の場合は、USBデバイスリダイレクトを使用することをお勧めします。ネットワーク遅延が200ミリ秒を超える場合は、USBデバイスリダイレクトを使用しないでください。

> USBデバイスリダイレクトには、主に次の3つの機能領域があります。

- オープンソースUSB/IPプロジェクト
- Citrix USBセッションモジュール
- Citrix USBサービスモジュール

オープンソースUSB/IPプロジェクト:

USB/IPプロジェクトは、Linuxカーネルドライバーと、カーネルドライバーと通信してすべてのUSBデータを取得できるいくつかのユーザーモードライブラリで構成されています。

Linux VDAは、オープンソースのUSB/IPプロジェクトに基づいてUSBデバイスリダイレクトを実装し、USB/IPのカーネルドライバーとユーザーモードライブラリを再利用します。ただし、Linux VDAとCitrix Workspaceアプリ間のすべてのUSBデータ転送は、Citrix ICA USBプロトコルによってカプセル化されます。

Citrix USBセッションモジュール:

Citrix USBセッションモジュールは、USB/IPカーネルモジュールとCitrix Workspaceアプリ間の通信ブリッジとして機能します。

Citrix USBサービスモジュール:

Citrix USBサービスモジュールは、USBデバイスの接続や切断など、USBデバイスに対するすべての操作を管理します。

USBデバイスリダイレクトの仕組み

通常、USBデバイスがLinux VDAに正常にリダイレクトされると、システム /dev パスに1つ以上のデバイスノードが作成されます。ただし、リダイレクトされたデバイスがアクティブなLinux VDAセッションで利用できない場合があります。USBデバイスは適切に機能するためにドライバーに依存しており、一部のデバイスは特別なドライバーを必要とします。ドライバーが提供されていない場合、リダイレクトされたUSBデバイスはアクティブなLinux VDAセッションからアクセスできません。USBデバイスの接続性を確保するには、ドライバーをインストールし、システムを適切に構成してください。

Linux VDAは、クライアントから正常にリダイレクトされるUSBデバイスのリストをサポートしています。

サポートされているUSBデバイス

> **ヒント:**
>
> USB 3.0ポートのサポートを追加しました。クライアントデバイスのUSB 3.0ポートにUSB 3.0デバイスを挿入できます。

> 以下のデバイスは、このバージョンのLinux VDAをサポートすることが確認されています。その他のデバイスも自由に使用できますが、予期しない結果が生じる可能性があります。

USB大容量記憶装置	VID:PID	ファイルシステム
`Netac Technology Co., Ltd`	0dd8:173c	FAT32, NTFS
`Kingston Datatraveler 101 II`	0951:1625	FAT32, NTFS
`Kingston Datatraveler GT101 G2`	1567:8902	FAT32, NTFS
`SanDisk SDCZ80 flash drive`	0781:5580	FAT32, NTFS
`WD HDD`	1058:10B8	FAT32, NTFS
`Toshiba Kingston DataTraveler 3.0 USB device`	0930:6545	FAT32, NTFS
`Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0`	FFFF:5678	FAT32, NTFS
`TD-RDF5A Transcend USB device`	8564:4000	FAT32, NTFS

注:

Amazon Linux 2、CentOS、RHEL、Rocky Linux、SUSE で NTFS を使用するには、まず、これらのディストリビューションで NTFS サポートを有効にします。

USB 3D マウス	VID:PID
`3DConnexion SpaceMouse Pro`	046d: c62b

USB スキャナー	VID:PID
`Epson Perfection V330 photo`	04B8: 0142

ユビコ USB	VID:PID
`Yubico YubiKey OTP+FIDO+CCID -Keyboard, HID`	1050:0407

WEBカメラ USB	VID:PID
`Logitech composite USB device – WebCam, Audio`	0460:0825

USBデバイスリダイレクトの構成

USB/IPカーネルモジュールのインストールまたはコンパイル (CentOS、RHEL、Rocky Linuxのみ)

Linux VDA は、USB デバイスリダイレクトの仮想ホストコントローラーとして USB/IP を使用します。ほとんどの場合、USB/IP カーネルモジュールは Linux カーネルバージョン 3.17 以降でリリースされているため、デフォルトでカーネルモジュールをビルドする必要はありません。ただし、USB/IP カーネルモジュールは CentOS、RHEL、Rocky Linux では利用できません。これらの Linux ディストリビューションで USB デバイスリダイレクトを使用するには、USB/IP カーネルモジュールをインストールまたはコンパイルする必要があります。お使いの Linux ディストリビューションに基づいて、`<https://pkgs.org/download/kmod-usbip>` から USB/IP をダウンロードしてインストールしてください。

USBデバイスリダイレクトポリシーの設定

Citrixポリシーは、USBデバイスリダイレクトが有効か無効かを制御します。デバイスの種類は、Delivery Controller™ポリシーを使用して指定することもできます。Linux VDAのUSBデバイスリダイレクトを構成する場合は、次のポリシーとルールを構成します。

- クライアントUSBデバイスリダイレクトポリシー
- クライアントUSBデバイスリダイレクト規則

USBデバイスリダイレクトを有効にする

Citrix Studioで、クライアントからのUSBデバイスリダイレクトを有効 (または無効) にします (ワークステーションホストのみ)。

設定の編集ダイアログで:

1. **許可**を選択します。
2. **OK**をクリックします。

USBデバイスリダイレクトを有効にする(/en-us/linux-virtual-delivery-agent/2303/media/client-usb-redirection-policy.png)

USBデバイスリダイレクトルールを設定する

USBリダイレクトポリシーを有効にした後、Linux VDAで許可（または拒否）されるデバイスを指定して、Citrix Studioを使用してリダイレクトルールを設定します。

クライアントUSBデバイスリダイレクトルールダイアログで:

1. **新規**をクリックしてリダイレクトルールを追加するか、**編集**をクリックして既存のルールを確認します。
2. ルールを作成（または編集）した後、**OK**をクリックします。

クライアントUSBデバイスリダイレクトルール設定(/en-us/linux-virtual-delivery-agent/2303/media/client-usb-redirection-rule.png)

USBデバイスリダイレクトの問題をトラブルシューティングする

このセクションの情報を使用して、Linux VDAの使用中に発生する可能性のあるさまざまな問題をトラブルシューティングします。

リダイレクトされたUSBディスクをアンマウントできない

Linux VDAは、Citrix Workspaceアプリからリダイレクトされたすべてのディスクを管理者権限で管理し、リダイレクトされたデバイスに所有者のみがアクセスできるようにします。その結果、デバイスは管理者権限でのみアンマウントできます。

デバイスをアンマウントできない(/en-us/linux-virtual-delivery-agent/2303/media/unable-to-mount-disk.png)

USBディスクのリダイレクトを停止するとファイルが失われる

Citrix Workspaceアプリのツールバーを使用してUSBディスクのリダイレクトをすぐに停止すると、ディスク上で変更または作成したファイルが失われる可能性があります。この問題は、ファイルシステムにデータを書き込む際に、システムがファイルシステム内のメモリキャッシュをマウントするため発生します。データはディスク自体には書き込まれません。Citrix Workspaceアプリのツールバーを使用してリダイレクトを停止すると、データがディスクにフラッシュされる時間がなくなり、データが失われます。

この問題を解決するには、USBリダイレクトを停止する前に、ターミナルで**sync**コマンドを使用してデータをディスクにフラッシュします。

Citrix Workspaceアプリのツールバーにデバイスがない

Citrix Workspaceアプリのツールバーにデバイスが表示されない場合があり、これはUSBリダイレクトが行われていないことを示しています。

Workspaceアプリのツールバーにあるデバイスタブ(/en-us/linux-virtual-delivery-agent/2303/media/client-usb-redirection-troubleshoot.png)

この問題が発生した場合は、以下を確認してください。

- USBデバイスリダイレクトを許可するようにポリシーが構成されている。
- Citrix USBサービスモジュールが実行されている。

ポリシーが正しく設定されていない場合は、この記事の「USBデバイスリダイレクトポリシーの設定」セクションを参照して修正してください。

Citrix USBサービスモジュールが実行されていない場合は、次の手順を実行してください。

1. 次のコマンドを使用して、お使いのLinuxディストリビューションでUSB/IPカーネルモジュールが利用可能かどうかを確認します。

   ```
   modinfo usbip-core
   ```

2. 出力が次のように表示される場合は、お使いのLinuxディストリビューションに基づいてUSB/IPカーネルモジュールをインストールまたはコンパイルしてください。

   ```
   modinfo: ERROR: Module usbip-core not found.
   ```

   - Amazon Linux 2、CentOS、RHEL、およびRocky Linuxについては、この記事の「USB/IPカーネルモジュールのインストールまたはコンパイル」セクションを参照してください。
   - SUSEの場合は、`<https://software.opensuse.org/package/usbip>`からUSB/IPパッケージをダウンロードしてインストールします。
   - Ubuntu/Debianの場合は、USB/IPカーネルモジュールをコンパイルしてインストールするために、次の手順を実行してください。

     a. USB/IPカーネルモジュールのソースコードをダウンロードします。

        `<https://github.com/torvalds/linux/tree/master/drivers/usb/usbip>`にあるLinuxカーネルリポジトリに移動し、ターゲットのLinuxカーネルバージョン（v4.15

以降）タグを選択して、`<https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip>` のようなリンクを取得します。

DownGit にアクセスし、前のリンクを入力して、USB/IP ソースコードをダウンロードするためのダウンロードリンクを作成します。

b. 次のコマンドを使用してソースファイルを解凍します。

```
unzip ${USBIP_SRC}.zip



cd usbip
```

c. **Makefile** ファイルを次のように変更します。

```
# SPDX-License-Identifier: GPL-2.0



ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG



obj-$(CONFIG_USBIP_CORE) += usbip-core.o



usbip-core-y := usbip_common.o usbip_event.o



obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o



vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o



#obj-$(CONFIG_USBIP_HOST) += usbip-host.o
```

```
#usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o



#obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o



#usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.o
vudc_transfer.o vudc_main.o
```

d. ソースコードをコンパイルします。

```
apt-get install linux-headers-`uname -r`



make -C /lib/modules/`uname -r`/build M=$PWD
```

e. USB/IP カーネルモジュールをインストールします。

```
cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
```

f. USB/IP カーネルモジュールをロードするために、**ctxusbsd** サービスを再起動します。

```
service ctxusbsd restart
```

Citrix Workspace アプリのツールバーに USB デバイスが表示されるが、*ポリシーによって制限されています* と表示される場合の、リダイレクトの失敗

この問題が発生した場合は、次の操作を行います。

- リダイレクトを有効にするように Linux VDA ポリシーを構成します。
- Citrix Workspace アプリのレジストリに追加のポリシー制限が構成されていないか確認します。レジストリパスの **DeviceRules** を確認して、この設定によってデバイスへのアクセスが拒否されていないことを確認します。

  HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\ICA Client\\GenericUSB

USB デバイスは正常にリダイレクトされますが、セッションで使用できません

通常、リダイレクトできるのは (/ja-jp/linux-virtual-delivery-agent/2303/configure/general-content-redirection/usb-redirection.html#supported-usb-devices) のみです。他のデバイスもアクティブな Linux VDA セッションにリダイレクトされる場合があります。リダイレクトされたデバイスごとに、ユーザーが所有するノードがシステム **/dev** パスに作成されます。ただし、ユーザーがデバイスを正常に使用できるかどうかは、ドライバーと構成によって決まります。所有されている（接続されている）がアクセスできないデバイスが見つかった場合は、そのデバイスを無制限のポリシーに追加します。

> **注:**
>
> USB ドライブの場合、Linux VDA はディスクを構成してマウントします。ユーザー（およびインストールした所有者のみ）は、追加の構成なしでディスクにアクセスできます。サポートされているデバイスリストにないデバイスの場合、そうではない可能性があります。

キーボード

このセクションには、次のトピックが含まれています。

- クライアントIME
- クライアントIMEユーザーインターフェイス同期
- 動的キーボードレイアウト同期
- ソフトキーボード
- 複数言語入力のサポート

クライアント入力方式エディター (IME)

概要

中国語、日本語、韓国語などの2バイト文字は、IMEを介して入力する必要があります。これらの文字は、WindowsネイティブのCJK IMEなど、クライアント側でCitrix Workspace™アプリと互換性のある任意のIMEを使用して入力します。

インストール

この機能は、Linux VDAをインストールすると自動的にインストールされます。

使用方法

通常どおり、Citrix Virtual AppsまたはCitrix Virtual Desktops™セッションを開きます。

クライアントIME機能の使用を開始するには、クライアント側で必要に応じて入力方式を変更します。

既知の問題

- クライアントIME機能を使用してGoogleスプレッドシートのセルに文字を入力する前に、そのセルをダブルクリックする必要があります。
- クライアントIME機能は、パスワードフィールドでは自動的に無効になりません。
- IMEユーザーインターフェイスは、入力領域でカーソルに追従しません。

クライアントIMEユーザーインターフェイスの同期

概要

これまで、クライアントIMEのユーザーインターフェイス（変換ウィンドウや候補ウィンドウを含む）は、画面の左上隅に配置されていました。カーソルに追従せず、テキスト入力領域のカーソルから離れた場所に表示されることがありました。

以前のクライアントIMEユーザーインターフェイスの画像(/en-us/linux-virtual-delivery-agent/2303/media/composition-and-candidate-windows.png)

Citrix®は、クライアントIMEの使いやすさを向上させ、ユーザーエクスペリエンスを次のようにさらに改善します。

現在のクライアントIMEユーザーインターフェイスの画像(/en-us/linux-virtual-delivery-agent/2303/media/synced-composition-and-candidate-windows.png)

この機能を使用するための前提条件

1. Linux VDAでIntelligent Input Bus (`IBus`) を有効にします。Linux OSで `IBus` を有効にする方法については、OSベンダーのドキュメントを参照してください。例：
   - ウブントゥ: `<https://help.ubuntu.com/community/ibus>`
   - CentOS、RHEL: `<https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods>`
   - デビアン: `<https://wiki.debian.org/I18n/ibus>`

- SUSE: `<https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang>`

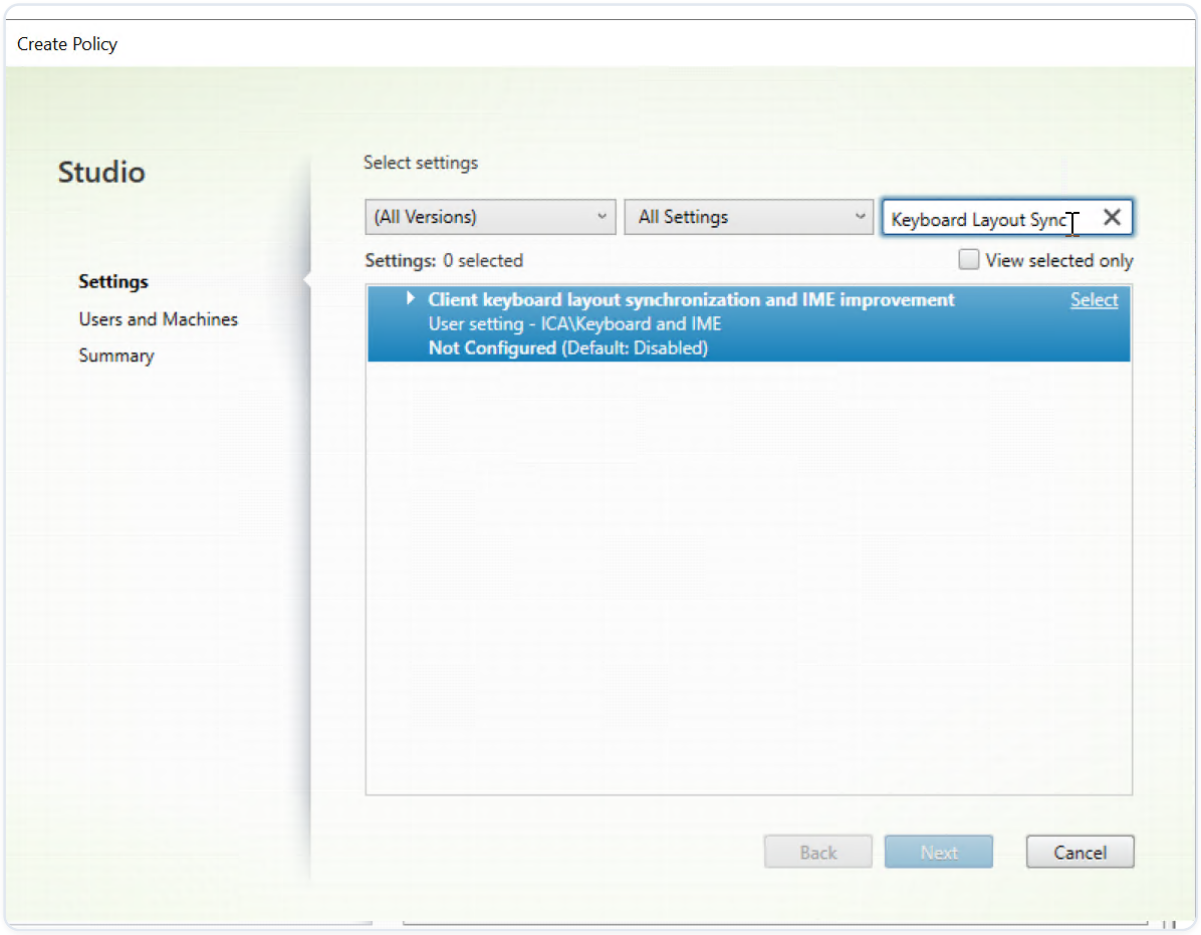
2. この機能は自動的にインストールされますが、使用する前に有効にする必要があります。

機能の有効化と無効化

クライアントIMEユーザーインターフェイス同期機能は、デフォルトで無効になっています。この機能を有効または無効にするには、**Client Keyboard Layout Sync and IME Improvement**ポリシーを設定するか、`ctxreg`ユーティリティを使用してレジストリを編集します。

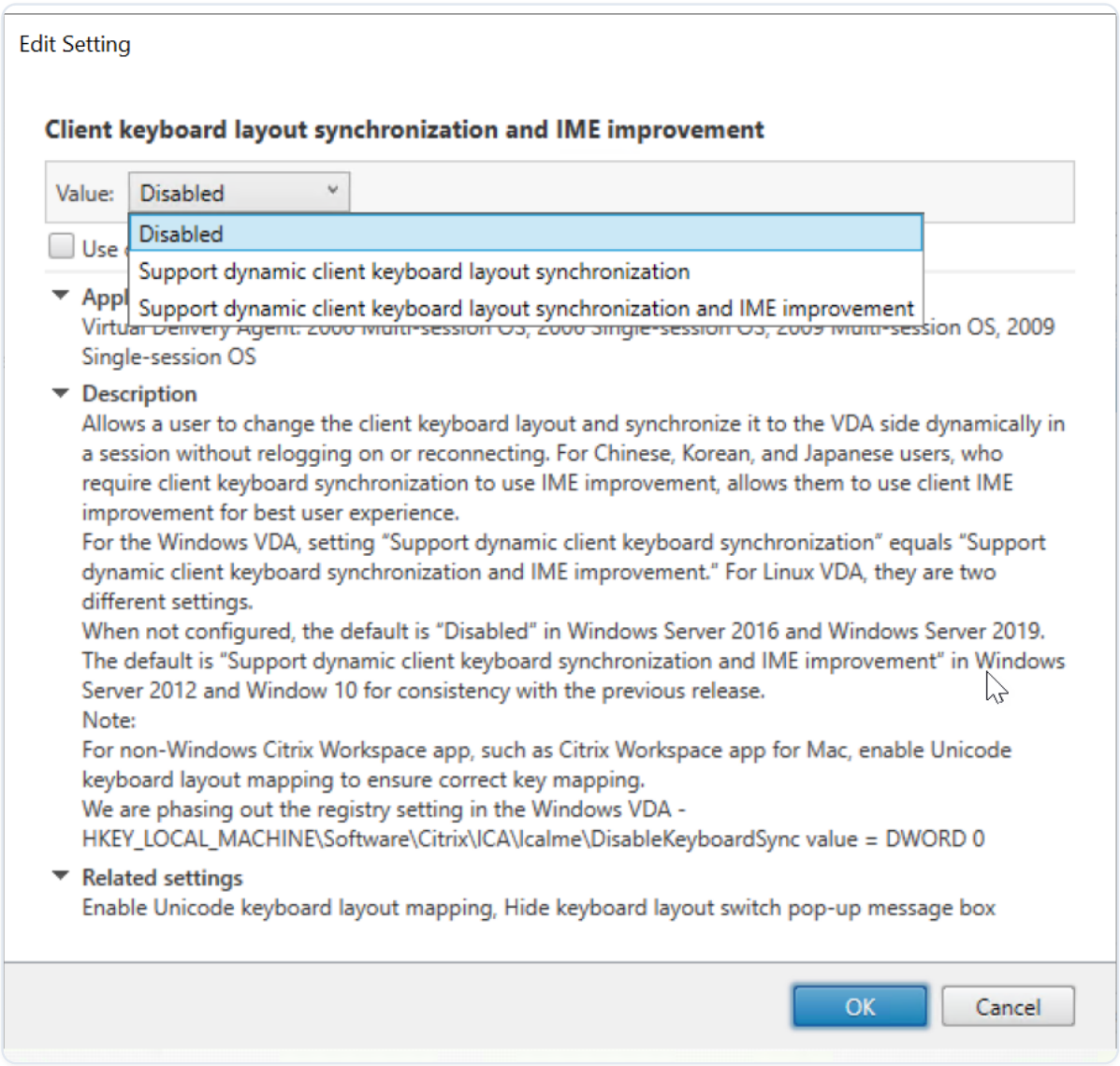
> **注:**
>
> **Client Keyboard Layout Sync and IME Improvement**ポリシーは、レジストリ設定よりも優先され、指定したユーザーオブジェクトおよびマシンオブジェクト、またはサイト内のすべてのオブジェクトに適用できます。特定のLinux VDA上のレジストリ設定は、そのVDA上のすべてのセッションに適用されます。

- クライアントIMEユーザーインターフェース同期機能を有効または無効にするには、**Client Keyboard Layout Sync and IME Improvement**ポリシーを設定します。
  a. Studioで、**ポリシー**を右クリックし、**ポリシーの作成**を選択します。
  b. **Client Keyboard Layout Sync and IME Improvement**ポリシーを検索します。



c. ポリシー名の横にある**選択**をクリックします。

d. ポリシーを設定します。



次の3つのオプションがあります。

- **無効**: 動的キーボードレイアウト同期とクライアントIMEユーザーインターフェース同期を無効にします。
- **動的クライアントキーボードレイアウト同期をサポート**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`にある**SyncKeyboardLayout**レジストリキーのDWORD値に関係なく、動的キーボードレイアウト同期を有効にします。
- **動的クライアントキーボードレイアウト同期とIME改善をサポート**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`にある**SyncKeyboardLayout**および**SyncClientIME**レジストリキーのDWORD値に関係なく、動的キーボードレイアウト同期とクライアントIMEユーザーインターフェース同期の両方を有効にします。

- クライアントIMEユーザーインターフェース同期機能を有効または無効にするには、`ctxreg`ユーティリティを介してレジストリを編集します。

  この機能を有効にするには、次のコマンドを実行します。

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v  "SyncClientIME" -d "0x00000001"
  ```

  この機能を無効にするには、次のコマンドを実行します。

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncClientIME" -d "0x00000000"
  ```

動的キーボードレイアウト同期

以前は、Linux VDA とクライアントデバイスのキーボードレイアウトは同じである必要がありました。たとえば、クライアントデバイスでキーボードレイアウトが英語からフランス語に変更されたが、VDA では変更されなかった場合、キーマッピングの問題が発生する可能性がありました。

Citrix® は、VDA のキーボードレイアウトをクライアントデバイスのキーボードレイアウトと自動的に同期することで、この問題に対処します。クライアントデバイスのキーボードレイアウトが変更されるたびに、VDA のレイアウトもそれに追従します。

> **注:**
>
> Citrix Workspace™ app for HTML5 は、動的なキーボードレイアウト同期機能をサポートしていません。

構成

動的なキーボードレイアウト同期機能は、デフォルトで無効になっています。この機能を有効または無効にするには、**Client Keyboard Layout Sync and IME Improvement** ポリシーを設定するか、`ctxreg` ユーティリティを使用してレジストリを編集します。

> **注:**

Client Keyboard Layout Sync and IME Improvement ポリシーは、レジストリ設定よりも優先され、指定したユーザーおよびマシンオブジェクト、またはサイト内のすべてのオブジェクトに適用できます。特定の Linux VDA のレジストリ設定は、その VDA 上のすべてのセッションに適用されます。

- 動的なキーボードレイアウト同期機能を有効または無効にするには、**Client Keyboard Layout Sync and IME Improvement** ポリシーを設定します。

  a. Studio で、**Policies** を右クリックし、**Create Policy** を選択します。

  b. **Client Keyboard Layout Sync and IME Improvement** ポリシーを検索します。

  クライアントキーボードレイアウト同期およびIME改善ポリシーの画像(/en-us/linux-virtual-delivery-agent/2303/media/client-keyboard-and-ime-policy.png)

  c. ポリシー名の横にある **Select** をクリックします。

  d. ポリシーを設定します。

  Client Keyboard Layout Sync and IME Improvement ポリシーの設定画像(/en-us/linux-virtual-delivery-agent/2303/media/setting-client-keyboard-and-ime-policy.png)

  3つのオプションがあります。

  - **Disabled**: 動的なキーボードレイアウト同期とクライアントIMEユーザーインターフェイス同期を無効にします。
  - **Support dynamic client keyboard layout synchronization**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar` の **SyncKeyboardLayout** レジストリキーのDWORD値に関係なく、動的なクライアントキーボードレイアウト同期を有効にします。
  - **動的クライアントキーボードレイアウト同期とIMEの改善をサポート**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`にある**SyncKeyboardLayout**および**SyncClientIME**レジストリキーのDWORD値に関係なく、動的キーボードレイアウト同期とクライアントIMEユーザーインターフェイス同期の両方を有効にします。

- `ctxreg`ユーティリティを介してレジストリを編集し、動的キーボードレイアウト同期機能を有効または無効にします。

  この機能を有効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
" -v "SyncKeyboardLayout" -d "0x00000001"
```

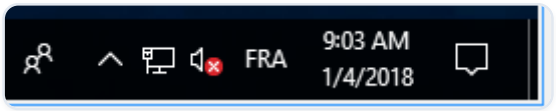
この機能を無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
" -v "SyncKeyboardLayout" -d "0x00000000"
```

使用方法

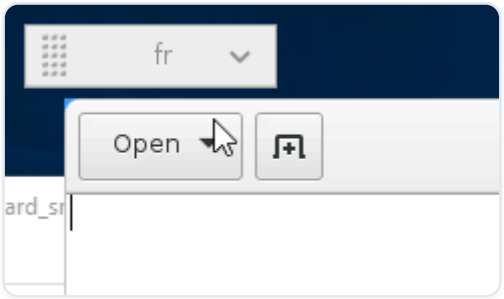
この機能を有効にすると、セッション中にクライアントデバイスのキーボードレイアウトが変更された場合、セッションのキーボードレイアウトもそれに応じて変更されます。

たとえば、クライアントデバイスのキーボードレイアウトをフランス語（FR）に変更した場合：

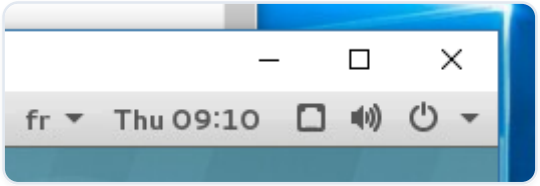


すると、Linux VDAセッションのキーボードレイアウトも「fr」に変更されます。

アプリケーションセッションでは、言語バーを有効にしている場合、この自動変更を確認できます。



デスクトップセッションでは、タスクバーでこの自動変更を確認できます。



ソフトキーボード

ソフトキーボード機能は、Linux仮想デスクトップまたはアプリケーションセッションで利用できます。入力フィールドに入ると自動的に表示され、入力フィールドを離れると自動的に非表示になります。

ソフトキーボード(/en-us/linux-virtual-delivery-agent/2303/media/soft-keyboard.png)

> **注:**
>
> この機能は、iOSおよびAndroid版のCitrix Workspace™アプリでサポートされています。

機能の有効化と無効化

この機能はデフォルトで無効になっています。**ctxreg**ユーティリティを使用して、この機能を有効または無効にします。特定のLinux VDAでの機能構成は、そのVDA上のすべてのセッションに適用されます。

この機能を有効にするには：

1. コマンドを実行します。

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
   "Enabled" -d "0x00000001"
   ```

2. Citrix Studioで、**Automatic keyboard display**ポリシーを**Allowed**に設定します。
3. （オプション）RHEL 7およびCentOS 7の場合、次のコマンドを実行して、Intelligent Input Bus (`IBus`)をデフォルトのIMサービスとして構成します。

   ```
   echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
   ```

この機能を無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

> **注:**
>
> 上記の設定は、新しいセッションにログオンするか、現在のセッションからログオフして再度ログオンしたときに有効になります。

制限事項

- この機能は、Google Chrome、LibreOffice、およびその他のアプリでは期待どおりに動作しない場合があります。
- ソフトキーボードを手動で非表示にした後、再度表示するには、入力フィールド以外の場所をクリックしてから、現在の入力フィールドを再度クリックします。
- Webブラウザで1つの入力フィールドから別の入力フィールドにクリックしても、ソフトキーボードが表示されない場合があります。この問題を回避するには、入力フィールド以外の場所をクリックしてから、目的の入力フィールドをクリックします。
- この機能は、Unicode文字および2バイト文字（中国語、日本語、韓国語などの文字）をサポートしていません。
- ソフトウェアキーボードは、パスワード入力フィールドでは使用できません。
- ソフトウェアキーボードが現在の入力フィールドと重なる場合があります。その場合は、アプリウィンドウを移動するか、画面をスクロールして、入力フィールドにアクセスしやすい位置に移動してください。
- Citrix WorkspaceアプリとHuaweiタブレット間の互換性の問題により、物理キーボードが接続されていても、Huaweiタブレットにソフトウェアキーボードが表示されます。

複数の言語入力のサポート

Linux VDAバージョン1.4以降、Citrixは公開アプリケーションのサポートを追加しました。ユーザーはLinuxデスクトップ環境なしで目的のLinuxアプリケーションにアクセスできます。

しかし、Linux VDAのネイティブ言語バーは、Linuxデスクトップ環境と高度に統合されているため、公開アプリケーションでは利用できませんでした。その結果、ユーザーは中国語、日本語、韓国語などのIMEを必要とする言語でテキストを入力できませんでした。また、アプリケーションセッション中にキーボードレイアウトを切り替えることもできませんでした。

これらの問題に対処するため、この機能はテキスト入力を受け付ける公開アプリケーションに言語バーを提供します。言語バーを使用すると、ユーザーはサーバー側のIMEを選択し、アプリケーションセッション中にキーボードレイアウトを切り替えることができます。

構成

この機能を有効または無効にするには、**ctxreg**ユーティリティを使用します（デフォルトでは無効）。特定のLinux VDAサーバーでの機能構成は、そのVDAで公開されているすべてのアプリケーションに適用されます。

構成キーは「HKEY_LOCAL_MACHINE \\SYSTEM\\CurrentControlSet\\Control\\Citrix\\LanguageBar」で、タイプはDWORDです。

この機能を有効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000001"
```

この機能を無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000000"
```

使用方法

使用方法は簡単です。

1. 機能を有効にします。
2. テキスト入力を受け付ける公開アプリケーションにアクセスします。言語バーがアプリケーションとともにセッションに表示されます。
3. ドロップダウンメニューから、目的の言語（入力ソース）を追加するために**地域と言語**を選択します。

   地域と言語の画像(/en-us/linux-virtual-delivery-agent/2303/media/select-region-language-dialog-box.png)
4. ドロップダウンメニューからIMEまたはキーボードレイアウトを選択します。
5. 選択したIMEまたはキーボードレイアウトを使用して言語を入力します。

> **注:**

- VDA側の言語バーでキーボードレイアウトを変更する場合は、クライアント側（Citrix Workspace™アプリを実行中）でも同じキーボードレイアウトが使用されていることを確認してください。
- **地域と言語**ダイアログボックスで設定を行う前に、**accountsservice**パッケージをバージョン0.6.37以降にアップグレードする必要があります。

IMEまたはキーボードレイアウトを選択するイメージ(/en-us/linux-virtual-delivery-agent/2303/media/region-language-dialog-box.png)

マルチメディア

このセクションには、次のトピックが含まれています。

- オーディオ機能(/ja-jp/linux-virtual-delivery-agent/2303/configure/multimedia/audio-features.html)
- ブラウザコンテンツリダイレクト
- HDX Webカメラビデオ圧縮(/ja-jp/linux-virtual-delivery-agent/2303/configure/multimedia/hdx-webcam-video-compression.html)

オーディオ機能

アダプティブオーディオ

アダプティブオーディオはデフォルトで有効になっています。以下のCitrix Workspace™アプリクライアントをサポートしています。

- Citrix Workspace app for Windows – 2109以降のバージョン
- Citrix Workspace app for Linux – 2109以降のバージョン
- Citrix Workspace app for Mac – 2109以降のバージョン

リストにないクライアントを使用すると、アダプティブオーディオはレガシーオーディオにフォールバックします。

アダプティブオーディオを使用すると、VDA上でオーディオ品質ポリシーを手動で構成する必要はありません。アダプティブオーディオは、ネットワークの状態に基づいてオーディオサンプリングビットレートを動的に調整し、プレミアムなオーディオエクスペリエンスを提供します。

以下の表は、アダプティブオーディオとレガシーオーディオの比較を示しています。

アダプティブオーディオ	レガシーオーディオ
最大オーディオサンプルレート: 48 kHz	最大オーディオサンプルレート: 8 kHz
ステレオチャネル	モノラルチャネル

ヒント:

RHEL 8.xでPulseAudio 13.99以降を使用してください。

ブラウザコンテンツリダイレクト

概要

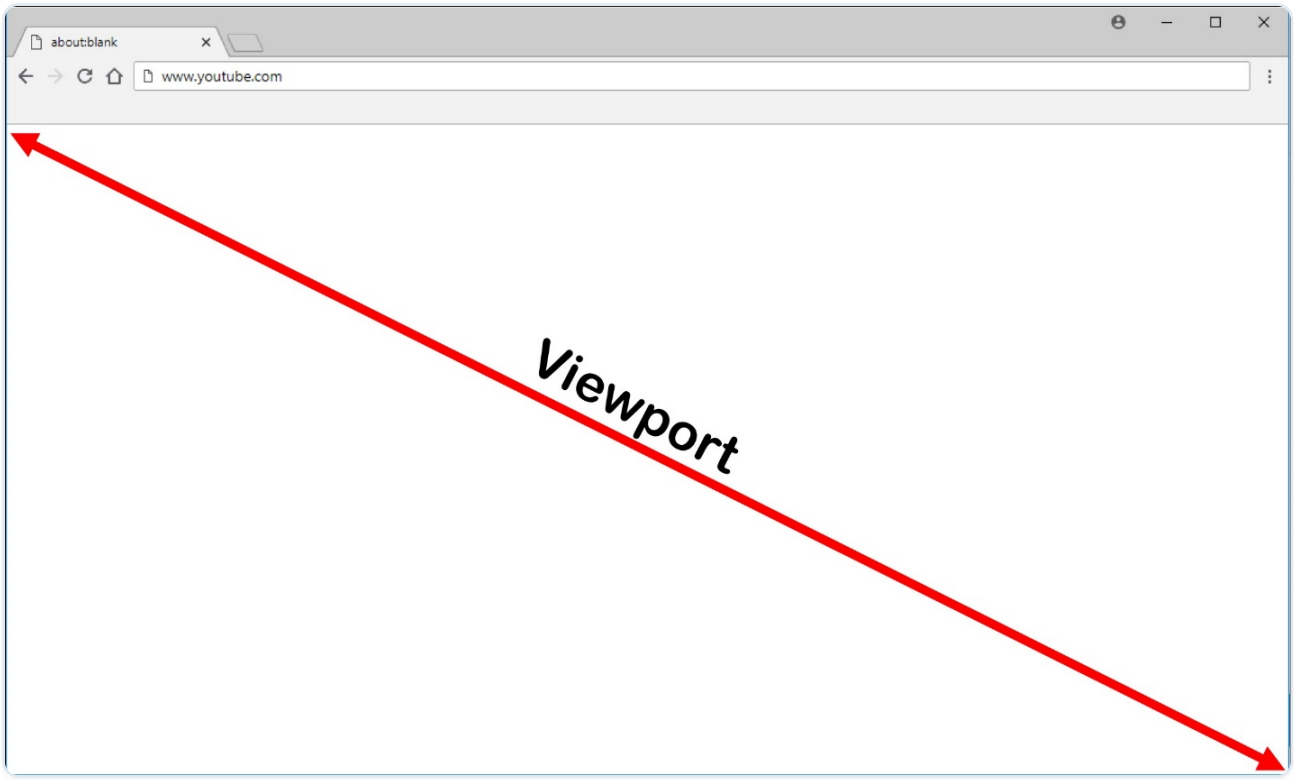
Linux VDA は Google Chrome でブラウザコンテンツリダイレクトをサポートしています。ブラウザコンテンツリダイレクトは、許可リストにあるウェブページをクライアント側でレンダリングする機能を提供します。この機能は、Citrix Workspace™ アプリを使用してクライアント側に適切なレンダリングエンジンをインスタンス化し、そのエンジンが URL から HTTP および HTTPS コンテンツを取得します。

注:

許可リストを使用して、どのウェブページをクライアント側にリダイレクトするかを指定できます。逆に、ブロックリストを使用して、どのウェブページをクライアント側にリダイレクトしないかを指定できます。

このオーバーレイウェブレイアウトエンジンは、VDA ではなくクライアント上で実行され、クライアントの CPU、GPU、RAM、およびネットワークを使用します。

ブラウザのビューポートのみがリダイレクトされます。ビューポートとは、ブラウザ内でコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、お気に入りバー、ステータスバーなどの項目は含まれません。これらの項目は、VDA 上のブラウザで引き続き実行されます。



システム要件

Windows クライアント:

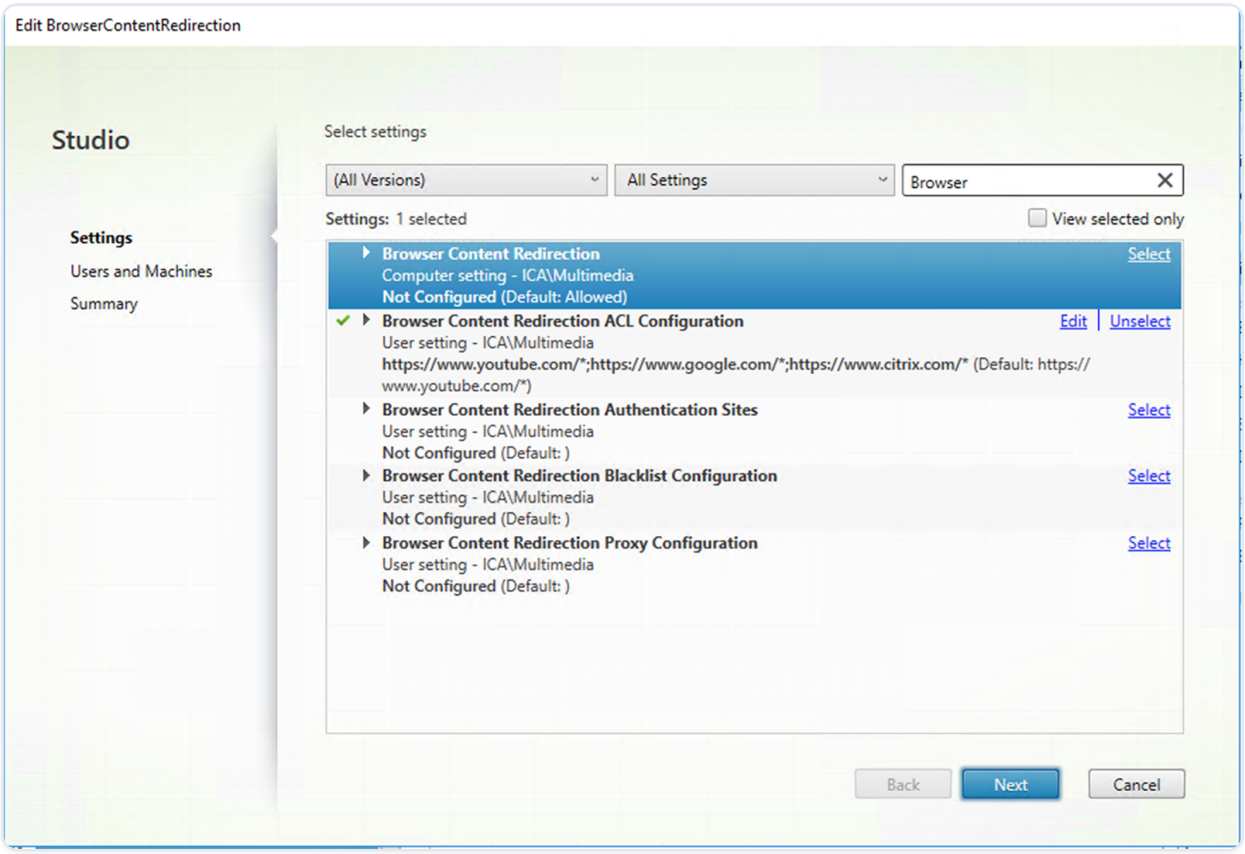
- Citrix Workspaceアプリ 1809 for Windows以降

リナックス VDA：

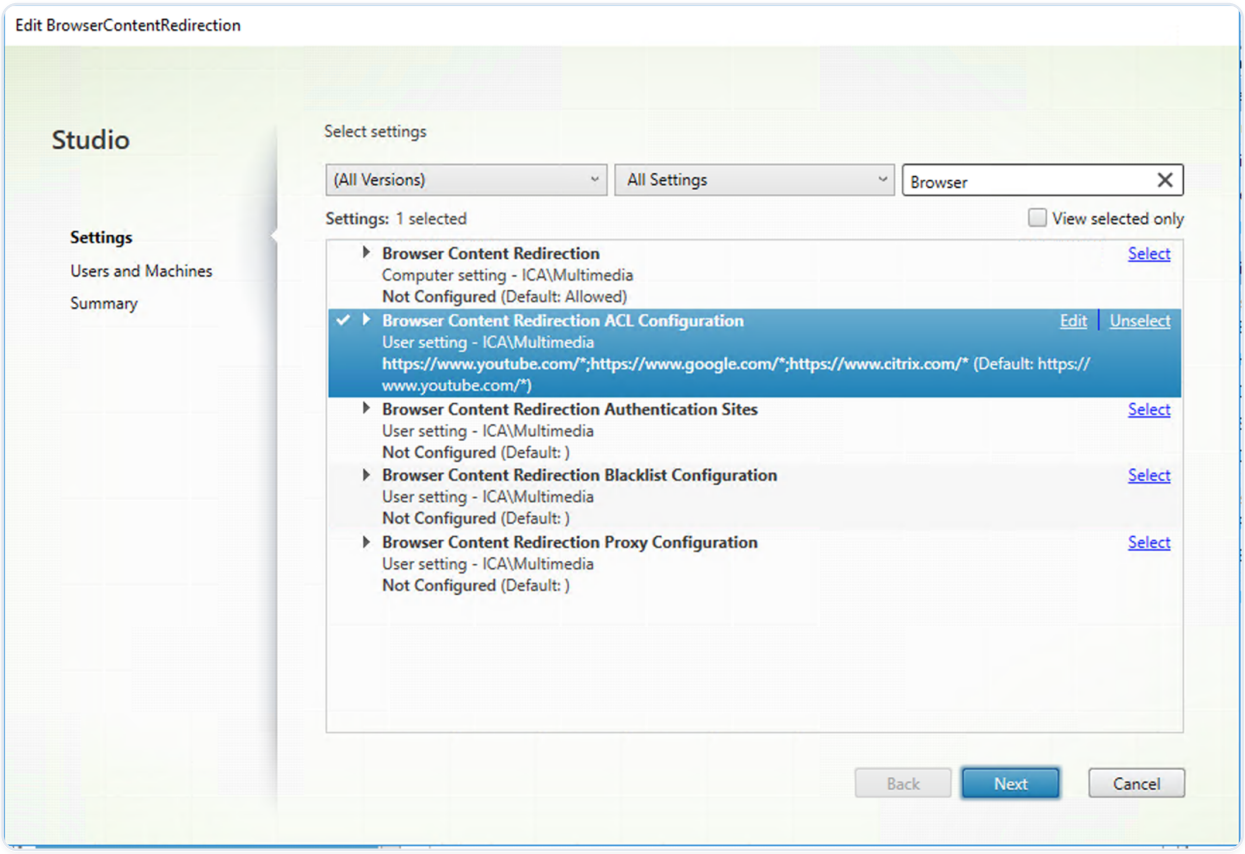
- VDA 上のブラウザ: Citrix® ブラウザコンテンツリダイレクト拡張機能が追加された Google Chrome v66 以降

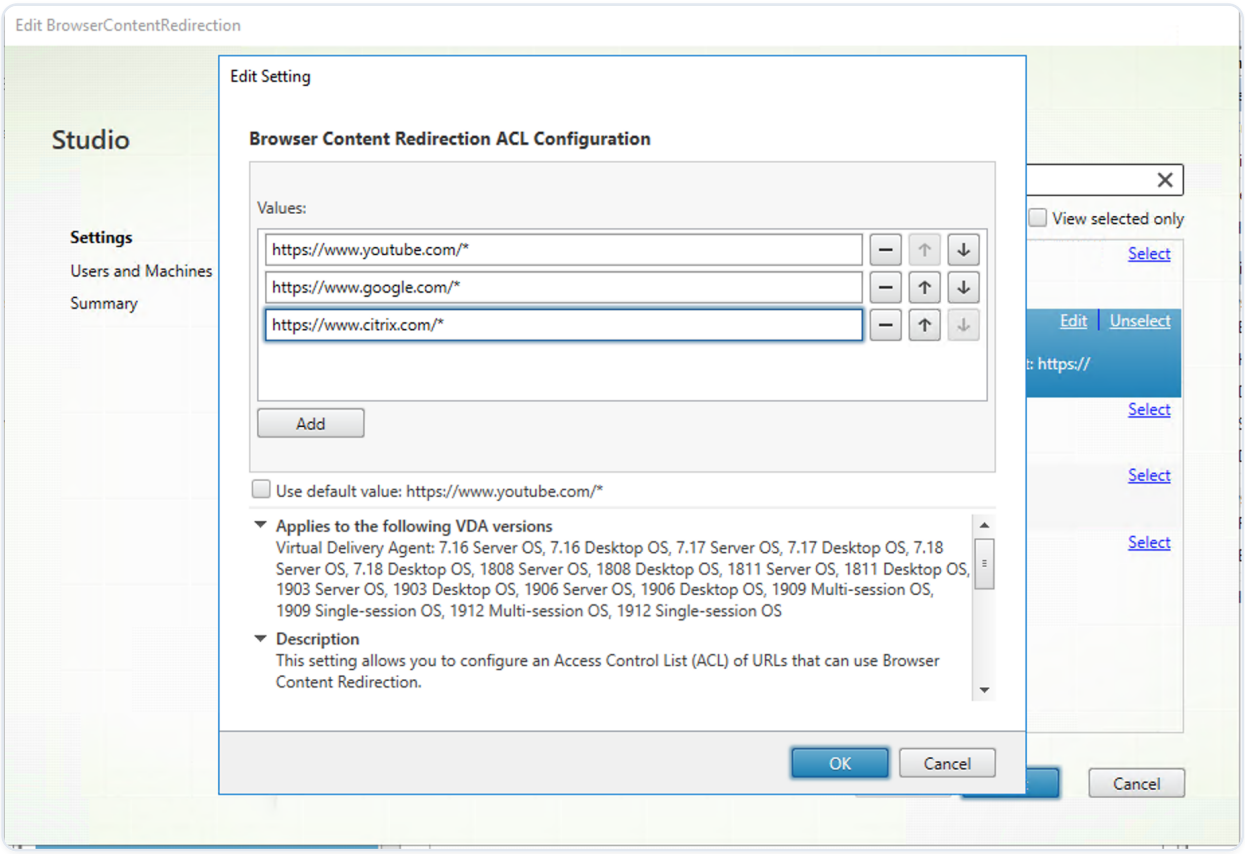
ブラウザコンテンツリダイレクトの構成

1. Citrix Studio で、ブラウザコンテンツリダイレクトの URL の許可リストとブロックリストを指定するポリシーを構成します。ブラウザコンテンツリダイレクトは、デフォルトで **許可** に設定されています。



ブラウザコンテンツリダイレクト ACL 構成 設定は、ブラウザコンテンツリダイレクトを使用できる URL の許可リストを指定します。





ブラウザコンテンツリダイレクトブラックリスト構成 設定は、ブラウザコンテンツリダイレクトを使用できない URL のブロックリストを指定します。

ブロックリストを設定するイメージ(/en-us/linux-virtual-delivery-agent/2303/media/block-list.png)

> **注:**
>
> Linux VDAは現在、**Browser Content Redirection Proxy Configuration**設定をサポートしていません。

2. VDAで**Add to Chrome**をクリックして、Chromeウェブストアから Citrix ブラウザコンテンツリダイレクト拡張機能を追加します。これにより、VDA上のブラウザが、アクセスしようとしているURLが許可リストまたはブロックリストのいずれかに一致するかどうかを検出するのに役立ちます。

> **重要:**
>
> この拡張機能はクライアントには必要ありません。VDAにのみ追加してください。

> \>

> Chrome拡張機能はユーザーごとにインストールされます。拡張機能を追加または削除するためにゴールデンイメージを更新する必要はありません。

> ChromeウェブストアからCitrixブラウザコンテンツリダイレクト拡張機能を追加するイメージ(/en-us/linux-virtual-delivery-agent/2303/media/add-to-chrome.png)

許可リスト（例: `https://www.mycompany.com/`）にはURLとの一致が見つかるが、ブロックリストには見つからない場合、仮想チャネル（CTXCSB）がCitrix Workspaceアプリにリダイレクトが必要であることを指示し、URLを中継します。その後、Citrix Workspaceアプリはローカルレンダリングエンジンをインスタンス化し、ウェブサイトを表示します。

その後、Citrix Workspaceアプリはウェブサイトを仮想デスクトップのブラウザコンテンツ領域にシームレスにブレンドし直します。

ビューポートとクライアントのイメージ(/en-us/linux-virtual-delivery-agent/2303/media/viewport-desktop-viewer.png)

1. Citrixブラウザコンテンツリダイレクト拡張機能のアイコン

   拡張機能アイコンの色は、Chrome拡張機能のステータスを示します。色は次の3つのいずれかです。

   - 緑：アクティブで接続済み
   - 灰色：現在のタブで非アクティブ/アイドル状態
   - 赤：破損/動作していません

2. クライアントでレンダリングされる、または仮想デスクトップにブレンドされるビューポート
3. リナックス ブイディーエー
4. Windowsクライアント

リダイレクトのシナリオ

Citrix Workspaceアプリがコンテンツをフェッチするシナリオを次に示します。

リダイレクトのシナリオの画像(/en-us/linux-virtual-delivery-agent/2303/media/browser-viewport-redirection-scenarios.png)

- **サーバーフェッチとサーバーレンダリング:** サイトを許可リストに追加しなかったか、リダイレクトが失敗したため、リダイレクトは行われません。VDAでWebページをレンダリングし、Thinwireを使用してグラフィックをリモート処理するようにフォールバックします。フォールバック動作を制御するには、ポリシーを使用します。このシナリオでは、VDAで高いCPU、RAM、帯域幅の消費が発生します。
- **クライアントフェッチとクライアントレンダリング:** Citrix WorkspaceアプリがWebサーバーに直接接続するため、インターネットアクセスが必要です。このシナリオでは、Citrix Virtual Apps and Desktops™サイトからすべてのネットワーク、CPU、およびRAMの使用をオフロードします。

フォールバックメカニズム

クライアントのリダイレクトが失敗する場合があります。たとえば、クライアントマシンに直接インターネットアクセスがない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

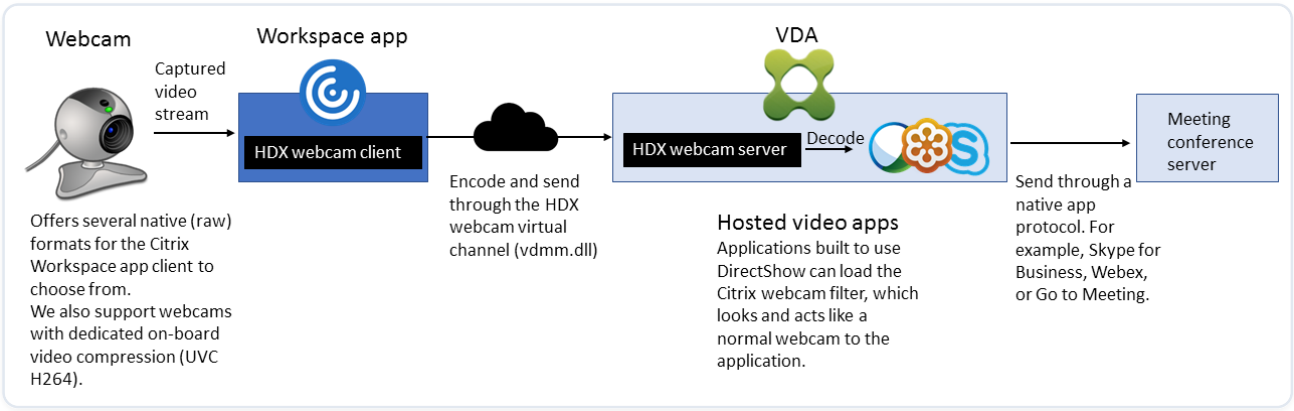
HDX™ Webカメラビデオ圧縮

概要

Linux VDAセッションで実行されているビデオ会議アプリケーションのユーザーは、HDX Webカメラビデオ圧縮を使用してWebカメラを使用できるようになりました。この機能はデフォルトで有効になっています。可能な場合は常にHDX Webカメラビデオ圧縮を使用することをお勧めします。

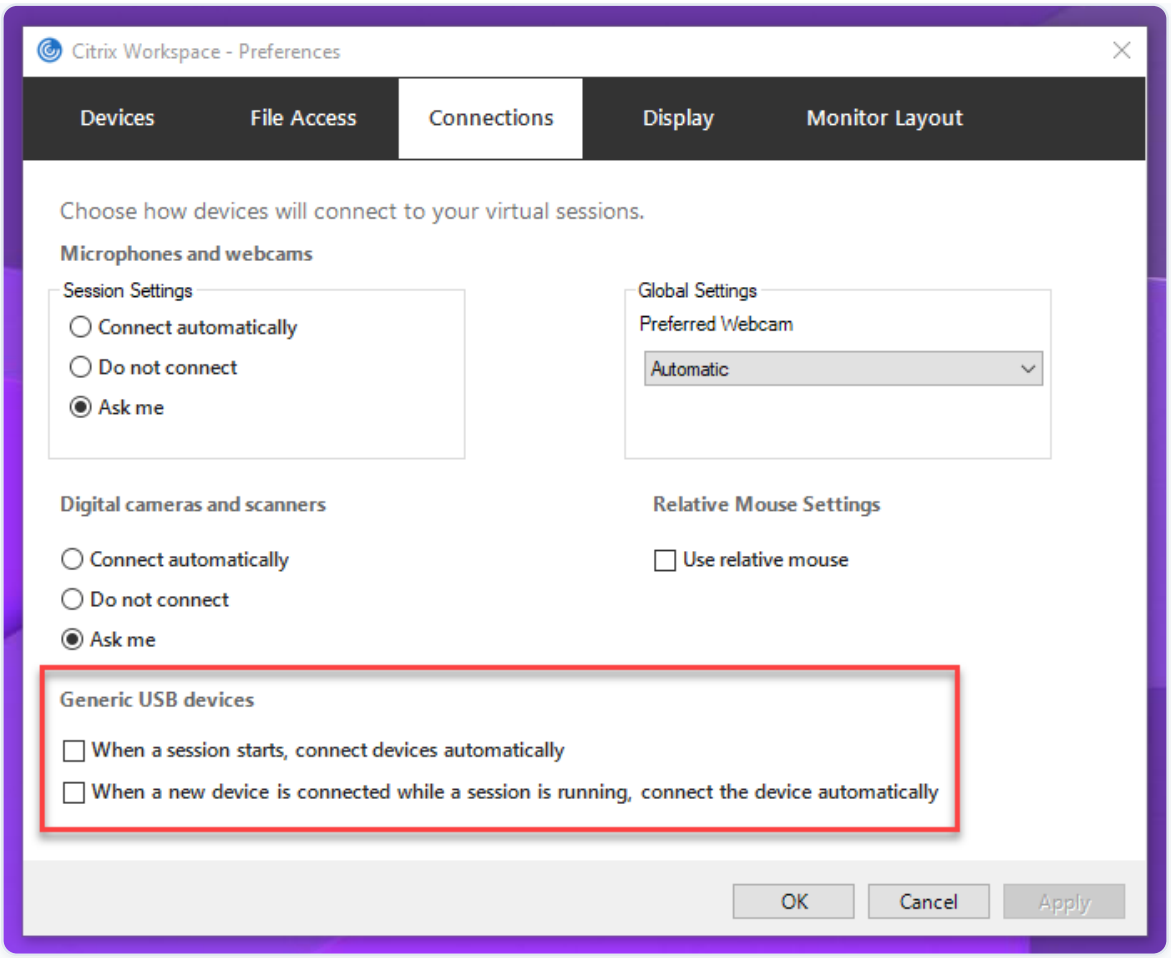
HDX Webカメラビデオ圧縮は、**最適化された** Webカメラモードとも呼ばれます。このタイプのWebカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。HDX Webカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはWebカメラとの通信を処理します。クライアントは、ビデオを適切に表示できるサーバーにのみビデオを送信します。サーバーはWebカメラを直接処理しませんが、その統合により、デスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復力を向上させるためにビデオを圧縮します。



注:

- この機能は、Azureマシンで機能が依存する**videodev**カーネルモジュールが不足しているため、Azureマシンでは利用できません。
- この機能は、Citrix WorkspaceアプリクライアントからのH.264ビデオのみをサポートします。
- サポートされているWebカメラの解像度は、48x32から1920x1080の範囲です。
- Webカメラを使用しているときに、Citrix Workspace™アプリのツールバーから**Generic USB devices**を選択しないでください。そうしないと、予期しない問題が発生する可能性があります。



サポートされているCitrix Workspaceアプリ

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサ
Windows版 Citrix Workspaceアプリ	Windows向けCitrix Workspaceアプリは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Windows向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、32ビットアプリのみが最適化されたHDX Webカメラビデオ圧縮を使用できます。

完全にテストされたWebカメラ

Webカメラによって、フレームレート、明るさ、コントラストのレベルが異なります。Citrix®は、初期機能検証のために以下のWebカメラを使用しています。

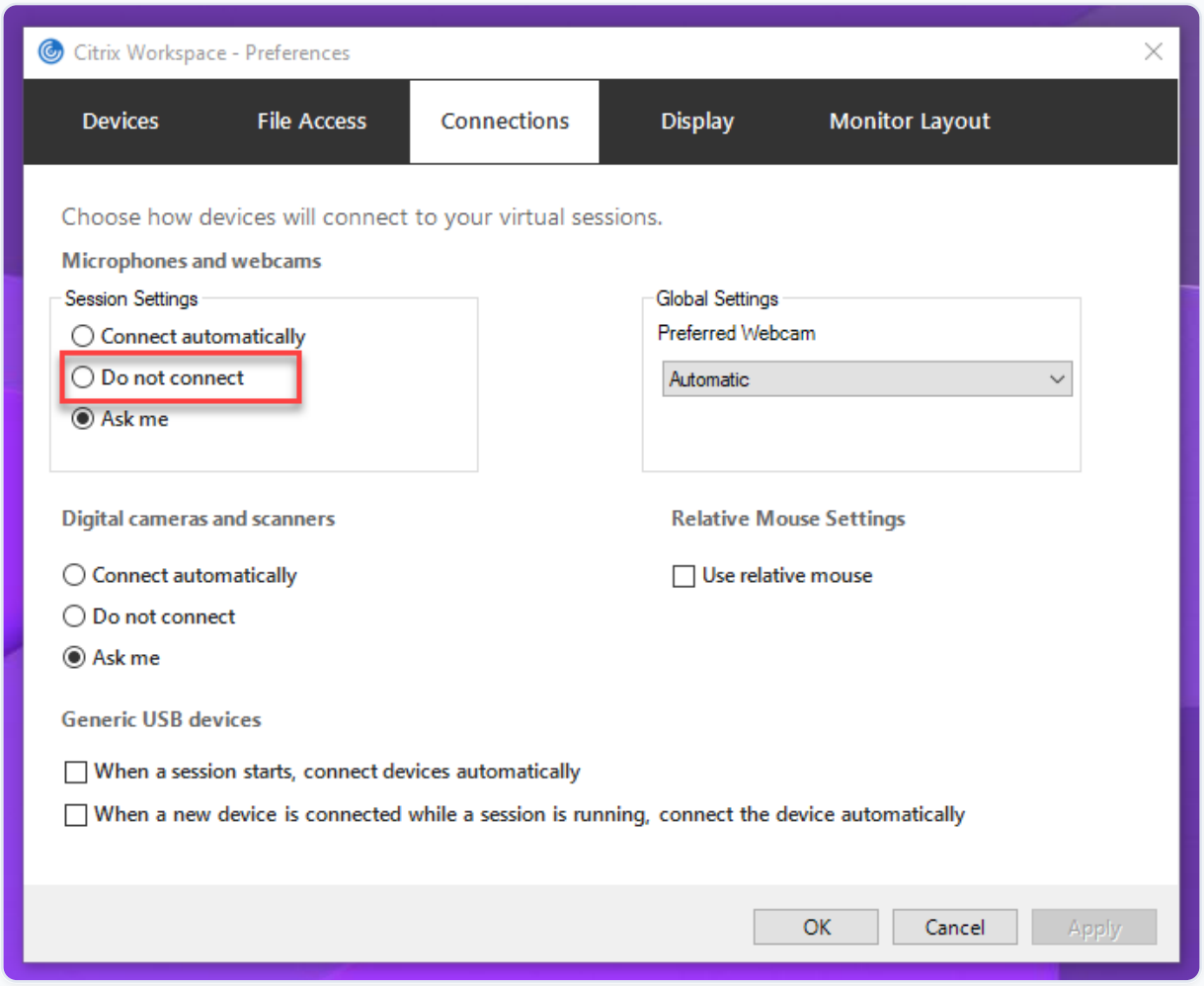
- ロジクール HD ウェブカメラ C270
- ロジクール ウェブカメラ C930e
- マイクロソフト LifeCam HD-3000

構成

この機能はデフォルトで有効になっています。これを使用するには、以下の検証と構成を完了してください。

ヒント:

Citrix Workspace app ユーザーは、Desktop Viewer の **マイクとWebカメラ** 設定で **接続しない** を選択することで、デフォルト設定を上書きできます。



1. VDA のインストールが完了したら、VDA が Delivery Controller™ に登録でき、公開された Linux デスクトップセッションが Windows 資格情報を使用して正常に起動できることを確認します。
2. VDA がインターネットにアクセスできることを確認し、`sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` コマンドを実行して Web カメラの設定を完了します。VDA がインターネットにアクセスできない場合は、手順 3 に進みます。

   > **注:**
   >
   > `uname -r` とカーネルヘッダーの間でカーネルの不一致が発生する可能性があります。この不一致により、ctxwcamcfg.sh スクリプトが失敗します。HDX Web カメラビデオ圧縮を適切に使用するには、**sudo apt-get dist-upgrade** を実行し、VDA を再起動してから、ctxwcamcfg.sh スクリプトを再実行します。

   > VDA が Debian に展開されている場合は、最新のカーネルバージョンで実行されていることを確認してください。そうでない場合は、次のコマンドを実行して最新のカーネルバージョンに更新します。

   ```
   sudo apt-get update

   sudo apt-get dist-upgrade

   sudo reboot
   ```

   VDA が SUSE 15.3、SUSE 15.2、または SUSE 12.5 に展開されている場合は、次のコマンドを実行して最新のカーネルバージョンに更新し、再起動します。

   ```
   zypper up kernel-default

   reboot
   ```

   ctxwcamcfg.sh スクリプトは、次のことを支援します。

   a. VDA に `kernel-devel` および Dynamic Kernel Module Support (DKMS) プログラムをインストールします。

- `kernel-devel` は、対応するバージョンの仮想 Web カメラカーネルモジュールをビルドするために使用されます。
- DKMS は、仮想 Web カメラカーネルモジュールを動的に管理するために使用されます。

> **注:**
>
> RHEL および CentOS に上記のプログラムをインストールする場合、`ctxwcamcfg.sh` スクリプトは VDA に次のリポジトリをインストールして有効にします。
>
> - Enterprise Linux 用追加パッケージ (EPEL)
> - アールピーエム・フュージョン

b. `<https://github.com/umlaeute/v4l2loopback>` から `v4l2loopback` オープンソースコードをダウンロードし、DKMS を使用して `v4l2loopback` を管理します。

`v4l2loopback` は、V4L2 ループバックデバイスを作成できるカーネルモジュールです。

c. `sudo service ctxwcamsd restart` コマンドを実行します。Linux VDA の Web カメラサービス (`ctxwcamsd`) が再起動し、HDX Web カメラビデオ圧縮機能のために `v4l2loopback` カーネルモジュールをロードします。

3. VDAにインターネットアクセスがない場合、v4l2loopbackカーネルモジュールを別のマシンでビルドし、VDAにコピーします。

a. インターネットアクセスがあり、VDAと同じカーネルバージョンを持つビルドマシンを準備します。`uname -r`コマンドはカーネルバージョンを見つけるのに役立ちます。

b. ビルドマシンで、`sudo mkdir -p /var/xdl`コマンドを実行します。

c. VDAから`/var/xdl/configure_*`をビルドマシンの`/var/xdl/`にコピーします。

d. ビルドマシンで、`sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh`コマンドを実行してカーネルモジュールをビルドします。コマンドが正常に実行されると、`/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/`パスの下にv4l2loopback.koファイルが作成されます。ctxwcamcfg.shスクリプトの実行中に発生する可能性のあるエラーは無視してください。

e. v4l2loopback.koをビルドマシンからVDAにコピーし、`/opt/Citrix/VDA/lib64/`の下に配置します。

f. VDAで、`sudo service ctxwcamsd restart`コマンドを実行してWebカメラサービスを再起動し、v4l2loopbackカーネルモジュールをロードします。

ドメイン参加していないLinux VDA

概要

ドメイン参加していないVDAは、VDAおよびユーザー認証のためにVDAをActive Directoryドメインに参加させる必要性をなくします。ドメイン参加していないVDAを作成する際、VDAをクラウドコントロールプレーンに登録するための公開鍵と秘密鍵のペアを生成します。したがって、Active Directoryドメインへの参加は不要になります。ユーザーがドメイン参加していないVDAからセッションを起動すると、VDAはユーザーがCitrix Workspaceアプリにログオンするために使用するユーザー名を使用して、ローカルマッピングアカウントを作成します。VDAは、ローカルマッピングアカウントがSSOおよびセッション再接続に使用するランダムなパスワードを割り当てます。ランダムなパスワードを変更すると、SSOおよびセッション再接続は失敗します。SSOを無効にするには、「SSO以外の認証」を参照してください。

重要:

- ドメイン参加していないVDAは、Citrix DaaSでサポートされています。
  - コントロールプレーンはCitrix DaaS上に展開する必要があります。
  - ドメイン参加していないVDAは、パブリッククラウドまたはオンプレミスのデータセンターに展開できます。Citrix DaaSのコントロールプレーンが、ドメイン参加していないVDAを管理します。
  - Citrix Cloud ConnectorをバイパスするようにRendezvous V2を構成できます。そうしないと、VDAをコントロールプレーンに接続するためにCloud Connectorをインストールする必要があります。
- ドメイン参加していないVDAを作成するには、Machine Creation Services™ (MCS)を使用する必要があります。
  - MCSはベアメタルサーバーをサポートしていません。

ドメイン参加していないLinux VDAで利用可能な機能

ドメイン参加していないVDAで指定された属性を持つローカルユーザーを作成する

ドメイン参加していないVDAでホストされているセッションを開くと、VDAはデフォルトの属性を持つローカルユーザーを自動的に作成します。VDAは、Citrix Workspace™アプリにログオンするために使用したユーザー名に基づいてローカルユーザーを作成します。ユーザーのユーザー識別子（UID）、グループID（GID）、ホームディレクトリ、ログインシェルなどのユーザー属性を指定することもできます。この機能を使用するには、次の手順を実行します。

1. この機能を有効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\LocalMappedAccount" -t
"REG_DWORD" -v "CreateWithUidGid" -d "0x00000001" --force
```

2. VDAのインストールパスにある`/var/xdl/getuidgid.sh`スクリプトで、次の属性を指定します。

属性	必須またはオプション	説明
`uid`	必須	ユーザー識別子 (UID) は、Linux がシステム上の各ユーザーに割り当てる番号です。これにより、ユーザーがアクセスできるシステムリソースが決まります。
`gid`	必須	グループ識別子 (GID) は、特定のグループを表すために使用される番号です。
`homedir`	オプション	Linux ホームディレクトリは、特定のユーザーのためのディレクトリです。
`shell`	オプション	ログインシェルは、ユーザーがユーザーアカウントにログインしたときに与えられるシェルです。

以下は、`getuidgid.sh`スクリプトの例です。

注:

スクリプトで指定された属性が有効であることを確認してください。

```
#!/bin/bash



################################################################################
########

#

# Citrix Virtual Apps™ & Desktops For Linux Script: Get uid and gid for
the user

#

# Copyright (c) Citrix Systems, Inc. All Rights Reserved.

#



export LC_ALL="en_US.UTF-8"



function get_uid_gid_for_user()

{

echo "uid:12345"

echo "gid:1003"

echo "homedir:/home/$1"

echo "shell:/bin/sh"

}
```

```
get_uid_gid_for_user $1
```

非SSO認証

デフォルトでは、Linux VDA はシングルサインオン (SSO) が有効になっています。ユーザーは、Citrix Workspace アプリと VDA セッションに、1組の資格情報を使用してログオンします。 ユーザーが異なる資格情報セットを使用して VDA セッションにログオンするようにするには、Linux VDA で SSO を無効にします。詳しくは、「非SSO認証」を参照してください。

Azure Active Directory を使用した認証

Azure に展開するドメイン非参加型 VDA は、AAD IDサービスと統合してユーザー認証を提供します。詳しくは、「Azure Active Directory を使用した認証」を参照してください。

ランデブー V2

ドメイン非参加型 VDA は、Citrix Cloud Connector をバイパスするために Rendezvous V2 を使用することがサポートされています。詳しくは、「Rendezvous V2」を参照してください。

ドメイン非参加型 Linux VDA の作成

MCSを使用して、Citrix DaaSでドメイン非参加のLinux VDAを作成します。詳しくは、「ドメイン非参加のLinux VDAを作成する」を参照してください。

ポリシーサポートリスト

Linux VDA ポリシーサポートリスト

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
クリップボードのクライアントからセッションへの転送サイズを制限	LimitClipboardTransferC2H	ユーザー	ICA®	無効 (0)
クリップボードのセッションからクライアント	LimitClipboardTransferH2C	ユーザー	ICA	無効 (0)

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
への転送サイズを制限				
クライアントのローカル時間を使用	UseLocalTimeOfClient	ユーザー	ICA\タイムゾーン制御	サーバーのタイムゾーンを使用する
ICAラウンドトリップ計算	IcaRoundTripCheckEnabled	コンピューター	ICA\エンドユーザー監視	有効 (1)
ICAラウンドトリップ計算間隔	IcaRoundTripCheckPeriod	コンピューター	ICA\エンドユーザー監視	15
アイドル接続のICAラウンドトリップ計算	IcaRoundTripCheckWhenIdle	コンピューター	ICA\エンドユーザー監視	無効 (0)
セッション全体の帯域幅制限	LimitOverallBw	ユーザー	ICA\帯域幅	0
オーディオリダイレクトの帯域幅制限	LimitAudioBw	ユーザー	ICA\帯域幅	0
オーディオリダイレクトの帯域幅制限パーセント	LimitAudioBwPercent	ユーザー	ICA\帯域幅	0
クライアントUSBデバイスリダイレクトの帯域幅制限	LimitUSBBw	ユーザー	ICA\帯域幅	0
クライアントUSBデバイスリダイレクトの帯域幅パーセント	LimitUSBBwPercent	ユーザー	ICA\帯域幅	0

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
クリップボードリダイレクトの帯域幅制限	LimitClipbdBW	ユーザー	ICA\帯域幅	0
クリップボードリダイレクトの帯域幅制限パーセント	LimitClipbdBWPercent	ユーザー	ICA\帯域幅	0
ファイルリダイレクト帯域幅制限	LimitCdmBw	ユーザー	ICA\帯域幅	0
ファイルリダイレクト帯域幅制限率	LimitCdmBwPercent	ユーザー	ICA\帯域幅	0
プリンターリダイレクト帯域幅制限	LimitPrinterBw	ユーザー	ICA\帯域幅	0
プリンターリダイレクト帯域幅制限率	LimitPrinterBwPercent	ユーザー	ICA\帯域幅	0
WebSockets接続	AcceptWebSocketsConnections	コンピューター	ICA\WebSockets	禁止
WebSockets ポート番号	WebSocketsPort	コンピューター	ICA\WebSockets	8008
WebSockets 信頼済みオリジンサーバーリスト	WSTrustedOriginServerList	コンピューター	ICA\WebSockets	*
ICA キープアライブ	SendICAKeepAlives	コンピューター	**ICA キープアライブ**	ICA キープアライブメッセージ

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
				を送信しない (0)
ICA キープアライブタイムアウト	ICAKeepAliveTimeout	コンピューター	**ICA キープアライブ**	60秒
ICAリスナーポート番号	IcaListenerPortNumber	コンピューター	ICA	1494
HDX™アダプティブトランスポート	HDXoverUDP	コンピューター	ICA	優先(2)
セッションの信頼性接続	AcceptSessionReliabilityConnections	コンピューター	ICA\セッション信頼性	許可(1)
再接続UIの透過レベル	ReconnectionUiTransparencyLevel	コンピューター	ICA\自動クライアント再接続	80%
セッションの信頼性ポート番号	SessionReliabilityPort	コンピューター	ICA\セッションの信頼性	2598
セッションの信頼性タイムアウト	SessionReliabilityTimeout	コンピューター	ICA\セッションの信頼性	180 秒
クライアント自動再接続	AllowAutoClientReconnect	ユーザー	ICA\クライアント自動再接続	許可 (1)
クライアントオーディオリダイレクト	AllowAudioRedirection	ユーザー	オーディオ	許可 (1)
クライアントプリンターリダイレクト	AllowPrinterRedir	ユーザー	印刷	許可 (1)

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
PDFユニバーサルプリンターの自動作成	AutoCreatePDFPrinter	ユーザー	印刷	無効 (0)
プリンタードライバーのマッピングと互換性	DriverMappingList	ユーザー	印刷	`"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"`
クライアントクリップボードのリダイレクト	AllowClipboardRedir	ユーザー	クリップボード	許可 (1)
クライアントUSBデバイスのリダイレクト	AllowUSBRedir	ユーザー	USB	禁止 (0)
クライアントUSBデバイスのリダイレクト規則	USBDeviceRules	ユーザー	USB	"\0"
動的画像圧縮	MovingImageCompressionConfiguration	ユーザー	シンワイヤー	有効 (1)
追加の色圧縮	ExtraColorCompression	ユーザー	シンワイヤー	無効 (0)
目標最小フレームレート	TargetedMinimumFramesPerSecond	ユーザー	シンワイヤー	10 フレーム/秒
目標フレームレート	FramesPerSecond	ユーザー	シンワイヤー	30 フレーム/秒
視覚品質	VisualQuality	ユーザー	シンワイヤー	中 (3)

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
圧縮にビデオコーデックを使用	VideoCodec	ユーザー	シンワイヤー	優先する場合に使用 (3)
ビデオコーデックにハードウェアエンコードを使用	UseHardwareEncodingForVideoCodec	ユーザー	シンワイヤー	有効 (1)
視覚的にロスレスな圧縮を許可	AllowVisuallyLosslessCompression	ユーザー	シンワイヤー	無効 (0)
3Dグラフィックワークロード向けに最適化	OptimizeFor3dWorkload	ユーザー	シンワイヤー	無効 (0)
シンプルなグラフィックの優先色深度	PreferredColorDepth	ユーザー	シンワイヤー	24ビット/ピクセル (1)
オーディオ品質	SoundQuality	ユーザー	オーディオ	高 – 高品位オーディオ (2)
クライアントマイクのリダイレクト	AllowMicrophoneRedir	ユーザー	オーディオ	許可 (1)
セッションの最大数	MaximumNumberOfSessions	コンピューター	負荷管理	250
同時ログオンの許容数	ConcurrentLogonsTolerance	コンピューター	負荷管理	2
Controller の自動更新を有効にする	EnableAutoUpdateOfControllers	コンピューター	バーチャル デリバリー エージェント の 設定	許可 (1)
クリップボード選択更新モード	ClipboardSelectionUpdateMode	ユーザー	クリップボード	3

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
プライマリ選択更新モード	PrimarySelectionUpdateMode	ユーザー	クリップボード	3
Speexの最大品質	MaxSpeexQuality	ユーザー	オーディオ	5
クライアントドライブの自動接続	AutoConnectDrives	ユーザー	ファイルリダイレクト/CDM	有効 (1)
クライアント光学ドライブ	AllowCdromDrives	ユーザー	ファイルリダイレクト/CDM	許可 (1)
クライアント固定ドライブ	AllowFixedDrives	ユーザー	ファイルリダイレクト/CDM	許可 (1)
クライアントフロッピーディスクドライブ	AllowFloppyDrives	ユーザー	ファイルリダイレクト/CDM	許可 (1)
クライアントネットワークドライブ	AllowNetworkDrives	ユーザー	ファイルリダイレクト/CDM	許可 (1)
クライアントドライブリダイレクト	AllowDriveRedir	ユーザー	ファイルリダイレクト/CDM	許可 (1)
読み取り専用クライアントドライブアクセス	ReadOnlyMappedDrive	ユーザー	ファイルリダイレクト/CDM	無効 (0)
キーボードの自動表示	AllowAutoKeyboardPopUp	ユーザー	MRVC	無効 (0)
デスクトップとクライアント間のファイル転送を許可	AllowFileTransfer	ユーザー	ファイル転送	許可

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
デスクトップからファイルをダウンロード	AllowFileDownload	ユーザー	ファイル転送	許可
デスクトップにファイルをアップロード	AllowFileUpload	ユーザー	ファイル転送	許可
セッションアイドルタイマー	EnableSessionIdleTimer	ユーザー	セッションタイマー	有効 (1)
セッションアイドルタイマー間隔	SessionIdleTimerInterval	ユーザー	セッションタイマー	1440分
切断されたセッションタイマー	EnableSessionDisconnectTimer	ユーザー	セッションタイマー	無効 (0)
切断されたセッションタイマーの間隔	SessionDisconnectTimerPeriod	ユーザー	セッションタイマー	1440分

注:

Windows Virtual Delivery Agent (VDA) のみがUser Datagram Protocol (UDP) 経由のオーディオをサポートします。Linux VDA はサポートしません。詳細については、「User Datagram Protocol (UDP) 経由のオーディオのリアルタイム転送」を参照してください。

Citrix Studio でセッション接続タイマーを構成するには、以下のCitrixポリシー設定を使用できます:

- **セッションアイドルタイマー**: アイドルセッションの時間制限を適用するかどうかを決定します。

- **セッションアイドルタイマーの間隔**: アイドルセッションの時間制限を設定します。**セッションアイドルタイマー**が**有効**で、設定された時間内にアクティブなセッションがユーザー入力を受信しなかった場合、セッションは切断されます。
- **切断されたセッションタイマー**: 切断されたセッションの時間制限を適用するかどうかを決定します。
- **切断されたセッションタイマーの間隔**: 切断されたセッションがログオフされるまでの間隔を設定します。

いずれかのポリシー設定を更新する場合は、展開全体で一貫性があることを確認してください。

アイドルセッションの時間制限が期限切れになると、警告メッセージが表示されます。例については、次のスクリーンショットを参照してください。**OK**を押すと警告メッセージは閉じますが、セッションをアクティブに保つことはできません。セッションをアクティブに保つには、ユーザー入力を提供してアイドルタイマーをリセットしてください。

警告メッセージ(/en-us/linux-virtual-delivery-agent/2303/media/warning-message-idle-session-timeout.png)

以下のポリシーは、Citrix Studioバージョン7.12以降で構成できます。

- MaxSpeexQuality

  値 (整数):

  既定値: 5

  詳細:

  オーディオリダイレクトは、オーディオ品質が中または低の場合（ポリシー「オーディオ品質」を参照）、Speexコーデックでオーディオデータをエンコードします。Speexは非可逆コーデックであり、入力音声信号の忠実度を犠牲にして圧縮を実現します。他の音声コーデックとは異なり、品質とビットレートの間のトレードオフを制御できます。Speexのエンコードプロセスは、ほとんどの場合、0から10までの範囲の品質パラメーターによって制御されます。品質が高いほど、ビットレートも高くなります。

  最大Speex品質は、オーディオ品質と帯域幅制限（ポリシー「オーディオリダイレクト帯域幅制限」を参照）に基づいて、オーディオデータをエンコードするための最適なSpeex品質を選択します。オーディオ品質が中の場合、エンコーダーは広帯域モードになり、サンプリングレートが高くなります。オーディオ品質が低い場合、エンコーダーは狭帯域モードになり、サンプリングレートが低くなります。同じSpeex品質でも、モードによってビットレートが異なります。最適なSpeex品質とは、最大値が次の条件を満たす場合です。

- 最大Speex品質以下であること。
- そのビットレートが帯域幅制限以下であること。

関連設定: オーディオ品質、オーディオリダイレクト帯域幅制限

- PrimarySelectionUpdateMode

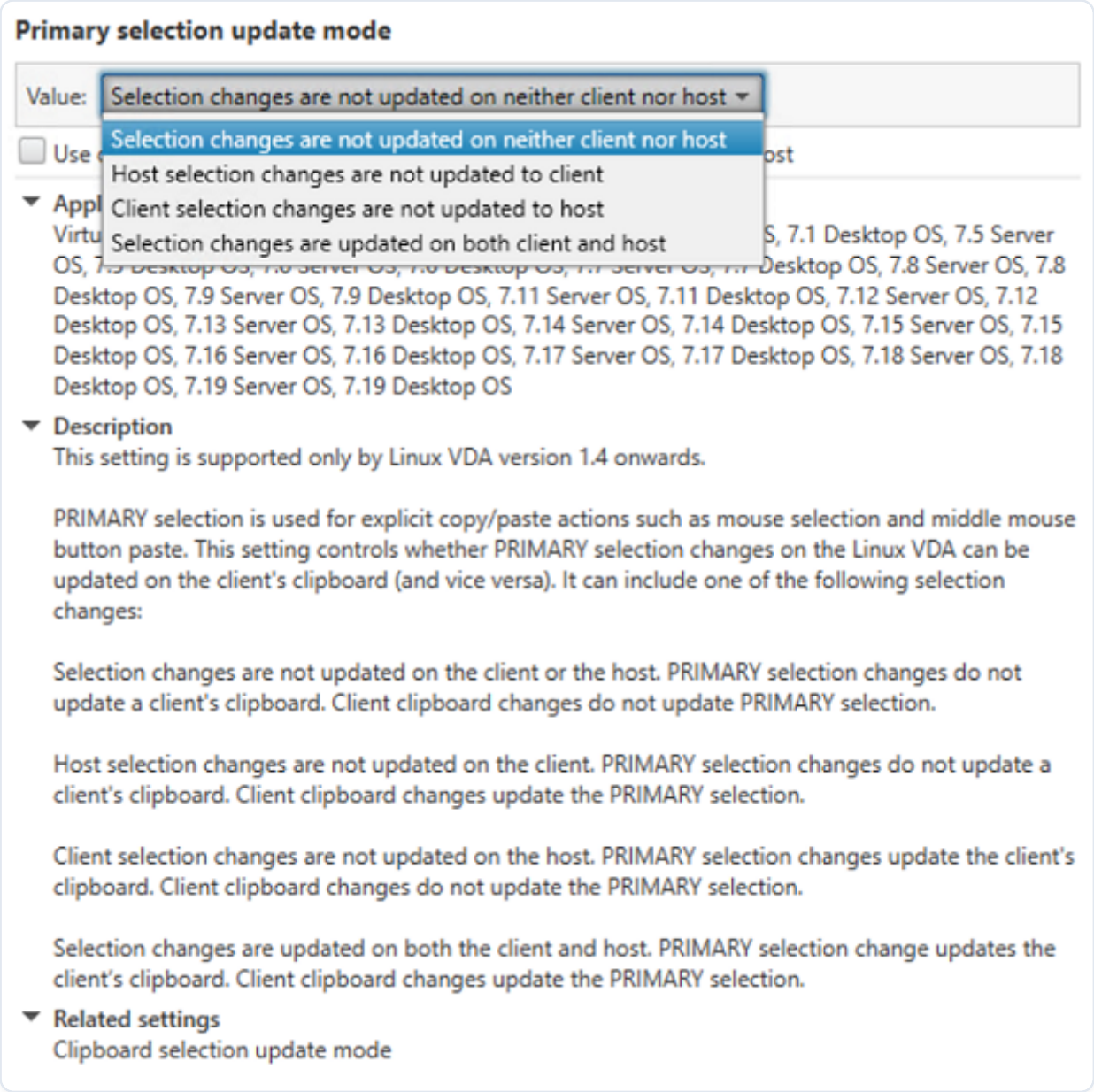
  値 (enum):

  既定値: 3

  詳細:

  プライマリ選択は、データを選択し、マウスの中央ボタンを押して貼り付けるときに使用されます。

  このポリシーは、Linux VDAとクライアントでのプライマリ選択の変更が、相互にクリップボードを更新できるかどうかを制御します。4つの値オプションがあります。



- **クライアントとホストのどちらでも選択の変更は更新されません**

  Linux VDAでのプライマリ選択の変更は、クライアントのクリップボードを更新しません。クライアントでのプライマリ選択の変更は、Linux VDAのクリップボードを更新しません。

- **ホストの選択変更はクライアントに更新されません**

  Linux VDAでのプライマリ選択の変更は、クライアントのクリップボードを更新しません。クライアントでのプライマリ選択の変更は、Linux VDAのクリップボードを更新します。

- **クライアントの選択変更はホストに更新されません**

Linux VDAでのプライマリ選択の変更は、クライアントのクリップボードを更新します。クライアントでのプライマリ選択の変更は、Linux VDAのクリップボードを更新しません。

- **選択変更はクライアントとホストの両方で更新されます**

  Linux VDAでのプライマリ選択の変更は、クライアントのクリップボードを更新します。クライアントでのプライマリ選択の変更は、Linux VDAのクリップボードを更新します。このオプションがデフォルト値です。

関連設定: クリップボード選択更新モード

- ClipboardSelectionUpdateMode

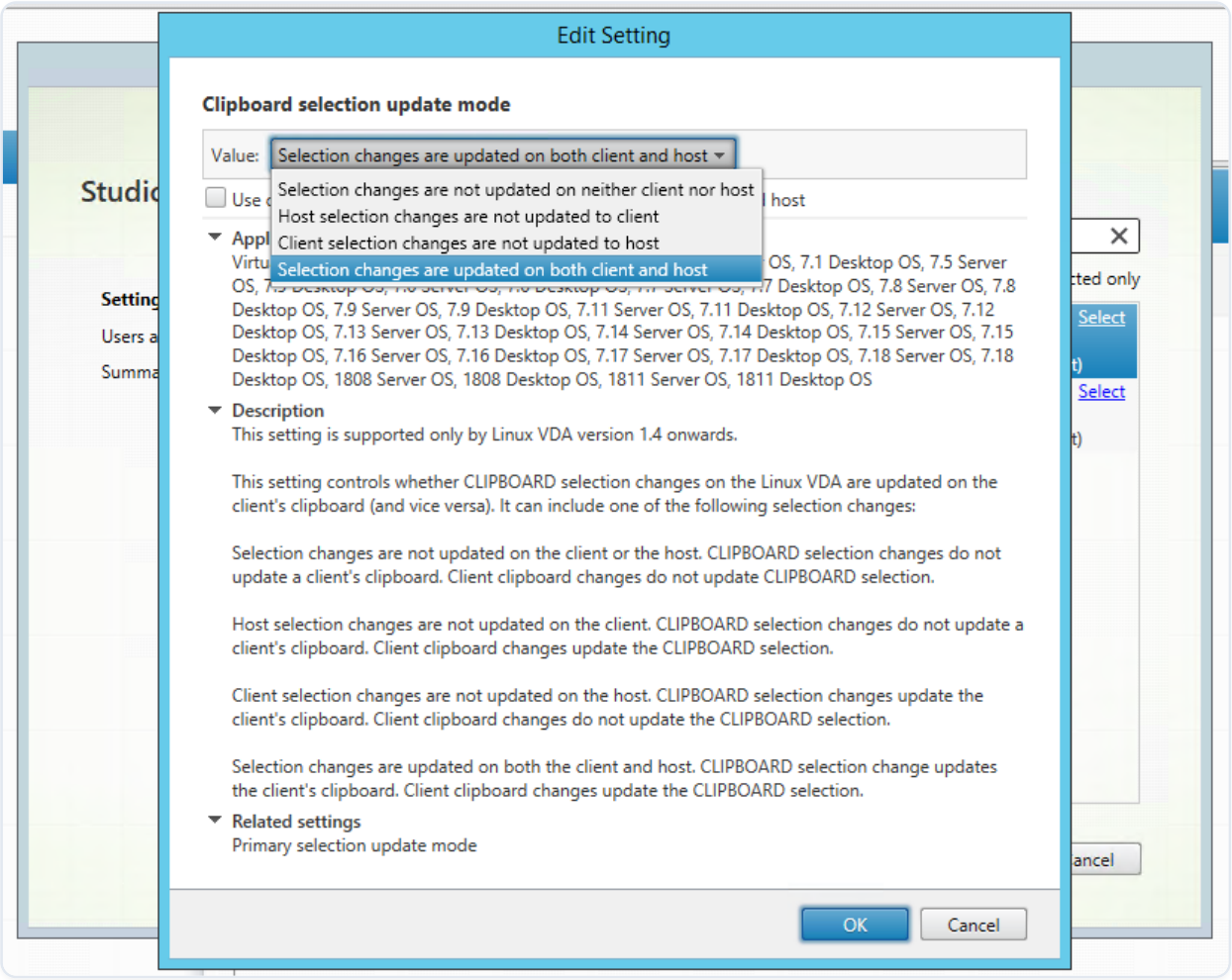
値 (enum):

デフォルト値: 3

詳細:

クリップボード選択は、データをいくつか選択し、ショートカットメニューから「コピー」を選択するなどして、明示的にクリップボードに「コピー」するよう要求する場合に使用されます。クリップボード選択は主にMicrosoft Windowsのクリップボード操作に関連して使用されますが、プライマリ選択はLinux固有のものです。

このポリシーは、Linux VDAとクライアントでのクリップボード選択の変更が、互いのクリップボードを更新できるかどうかを制御します。4つの値オプションがあります。



- **選択変更はクライアントとホストのどちらにも更新されません**

  Linux VDAでのクリップボード選択の変更は、クライアントのクリップボードを更新しません。クライアントでのクリップボード選択の変更は、Linux VDAのクリップボードを更新しません。

- **ホストの選択変更はクライアントに更新されません**

  Linux VDAでのクリップボード選択の変更は、クライアントのクリップボードを更新しません。クライアントでのクリップボード選択の変更は、Linux VDAのクリップボードを更新します。

- **クライアントの選択変更はホストに更新されません**

  Linux VDAでのクリップボード選択の変更は、クライアントのクリップボードを更新します。クライアントでのクリップボード選択の変更は、Linux VDAのクリップボードを更新しません。

- **選択変更はクライアントとホストの両方で更新されます**

Linux VDAでのクリップボード選択の変更は、クライアントのクリップボードを更新します。クライアントでのクリップボード選択の変更は、Linux VDAのクリップボードを更新します。このオプションがデフォルト値です。

関連設定: プライマリ選択更新モード

> **注:**
>
> Linux VDA は、クリップボード選択とプライマリ選択の両方をサポートしています。Linux VDA とクライアント間のコピーと貼り付けの動作を制御するには、クリップボード選択更新モードとプライマリ選択更新モードの両方を同じ値に設定することをお勧めします。

印刷

このセクションには、次のトピックが含まれています。

- 印刷のベストプラクティス
- PDF印刷

印刷のベストプラクティス

この記事では、印刷のベストプラクティスに関する情報を提供します。

インストール

Linux VDAには、**cups**フィルターと**foomatic**フィルターの両方が必要です。これらのフィルターは、VDAのインストール時にインストールされます。ディストリビューションに基づいて、フィルターを手動でインストールすることもできます。例：

RHEL 7の場合：

```
sudo yum –y install cups



sudo yum -y install foomatic-filters
```

印刷ポリシー設定

クライアントプリンターリダイレクト

この設定は、クライアントプリンターがVDAセッションにマップされるかどうかを制御します。デフォルトでは、クライアントプリンターのマッピングは許可されています。

クライアントプリンターを自動作成

この設定は、VDAセッションにマップできるクライアントプリンターを指定します。デフォルトでは、**すべてのクライアントプリンターを自動作成**に設定されており、これはすべてのクライアントプリンターがVDAセッションにマップされることを意味します。この設定の詳細については、Citrix Virtual Apps and Desktopsのドキュメントにあるクライアントプリンターの自動作成を参照してください。

PDFユニバーサルプリンターの自動作成

PDF印刷機能を使用するには、このポリシーを**有効**に設定します。

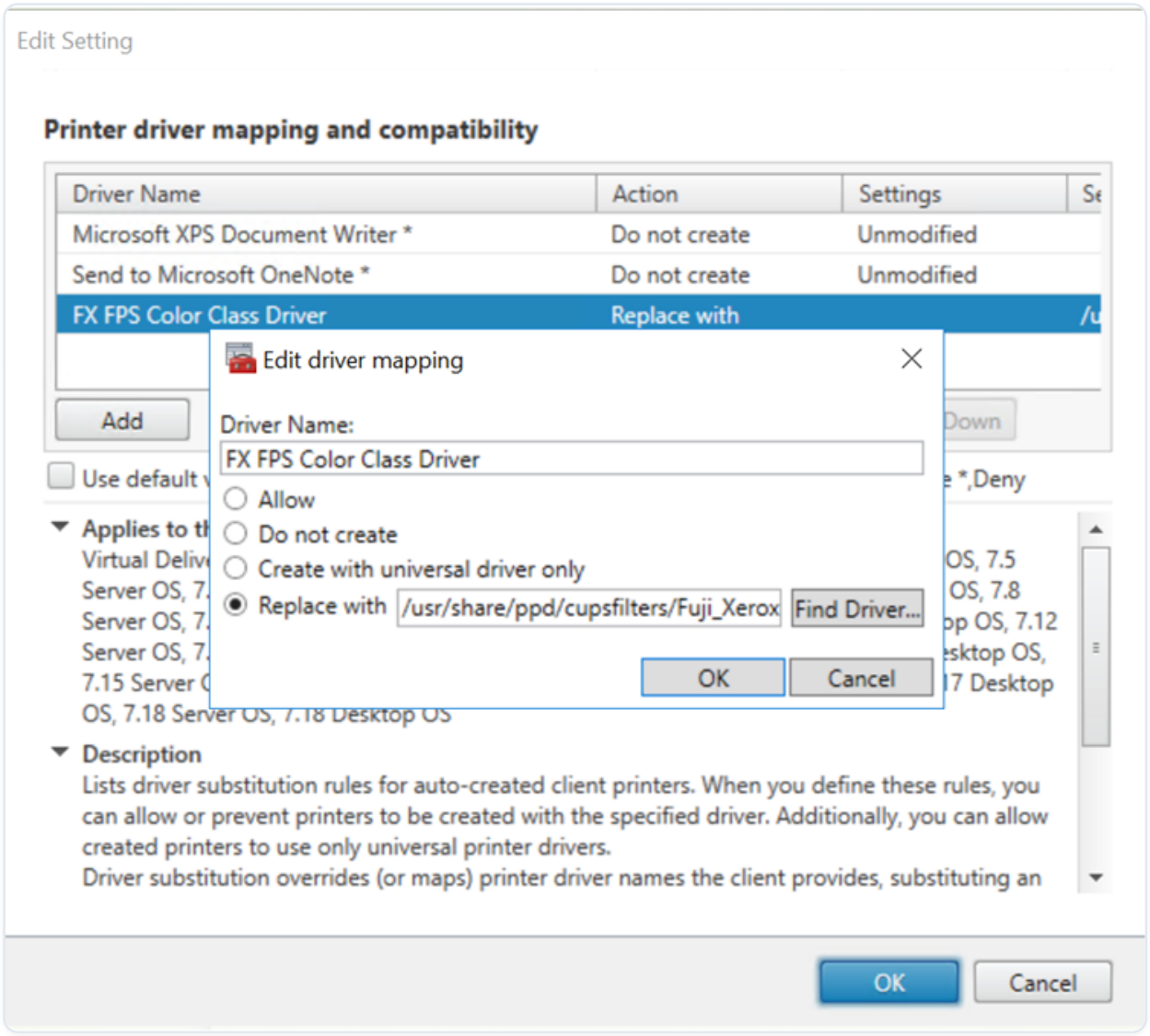
プリンタードライバーのマッピングと互換性

Citrixは、3種類のユニバーサルプリンタードライバー（postscript、pcl5、pcl6）を提供しています。ただし、ユニバーサルプリンタードライバーがクライアントプリンターと互換性がない場合があります。この場合、以前のリリースでは、~/.CtxlpProfile$CLIENT_NAME構成ファイルを編集するしかありませんでした。バージョン1906以降では、代わりにCitrix Studioで**プリンタードライバーのマッピングと互換性**ポリシーを構成することを選択できます。

Citrix Studioで**プリンタードライバーのマッピングと互換性**ポリシーを構成するには：

1. **プリンタードライバーのマッピングと互換性**ポリシーを選択します。
2. 「**追加**」をクリックします。
3. **ドライバー名**にクライアントプリンターのドライバー名を入力します。Citrix Workspace™ app for Linuxを使用している場合は、代わりにプリンター名を入力します。

4\. **置換**を選択し、VDA上のドライバーファイルの絶対パスを入力します。



注:

- PPDドライバーファイルのみがサポートされています。
- **プリンタードライバーのマッピングと互換性**ポリシーの他のオプションはサポートされていません。**次で置き換える**のみが有効になります。

使用方法

公開デスクトップと公開アプリケーションの両方から印刷できます。すべてのクライアントプリンターをVDAセッションにマップできます。プリンター名はデスクトップとアプリケーションで異なります。

- 公開デスクトップの場合:

`<client printer name>:$CLIENT_NAME:dsk$SESSION_ID`

- 公開アプリケーションの場合:

`<client printer name>:$CLIENT_NAME:app$SESSION_ID`

> **注:**
>
> 同じユーザーが公開デスクトップと公開アプリケーションの両方を開いた場合、両方のプリンターがセッションで利用可能になります。公開アプリケーションセッションでデスクトッププリンターに印刷したり、公開デスクトップでアプリケーションプリンターに印刷したりすることはできません。

トラブルシューティング

印刷できません

印刷が正しく機能しない場合は、印刷デーモンである**ctxlpmngt**とCUPSフレームワークを確認してください。

印刷デーモンである**ctxlpmngt**はセッションごとのプロセスであり、セッションの期間中実行されている必要があります。次のコマンドを実行して、印刷デーモンが実行されていることを確認します。**ctxlpmngt**が実行されていない場合は、コマンドラインから手動で**ctxlpmngt**を開始します。

```
ps –ef | grep ctxlpmngt
```

印刷がまだ機能しない場合は、**CUPS**フレームワークを確認してください。**ctxcups**サービスはプリンター管理に使用され、Linux CUPSフレームワークと通信します。これはマシンごとに1つのプロセスであり、次のコマンドを実行して確認できます。

```
service ctxcups status
```

CUPSログを収集するための追加手順

CUPSログを収集するには、次のコマンドを実行してCUPSサービスファイルを構成します。そうしないと、CUPSログは**hdx.log**に記録されません。

```
sudo service cups stop
```

```
sudo vi /etc/systemd/system/printer.target.wants/cups.service


PrivateTmp=false


sudo service cups start


sudo systemctl daemon-reload
```

注:

この構成は、問題が発生したときに完全な印刷ログを収集するためだけに行われます。通常の状況では、CUPSのセキュリティを破るため、この構成はお勧めしません。

印刷出力が文字化けする

互換性のないプリンタードライバーは、出力の文字化けを引き起こす可能性があります。ユーザーごとのドライバー構成が利用可能で、**~/.CtxlpProfile$CLIENT_NAME**構成ファイルを編集することで構成できます。

```
[DEFAULT_PRINTER]


printername=


model=


ppdpath=
```

```
drivertype=
```

重要:

「**printername**」は、現在のクライアント側のデフォルトプリンターの名前を含むフィールドです。これは読み取り専用の値です。編集しないでください。

ppdpath、**model**、**drivertype** の各フィールドは、マップされたプリンターに対して1つしか有効にならないため、同時に設定することはできません。

- ユニバーサルプリンタードライバーがクライアントプリンターと互換性がない場合は、**model=** オプションを使用してネイティブプリンタードライバーのモデルを構成します。**lpinfo** コマンドを使用して、プリンターの現在のモデル名を見つけることができます。

  ```
  lpinfo –m

  …

  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  ```

  その後、プリンターに合わせてモデルを設定できます。

  ```
  model=xerox/ph3115.ppd.gz
  ```

- ユニバーサルプリンタードライバーがクライアントプリンターと互換性がない場合は、ネイティブプリンタードライバーのPPDファイルパスを構成します。**ppdpath** の値は、ネイティブプリンタードライバーファイルの絶対パスです。

  たとえば、/home/tester/NATIVE_PRINTER_DRIVER.ppd の下に **ppd driver** があります。

  ```
  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
  ```

- Citrix が提供するユニバーサルプリンタードライバーには3種類あります（postscript、pcl5、pcl6）。プリンターのプロパティに基づいてドライバーの種類を構成できます。

  たとえば、クライアントのデフォルトプリンタードライバーの種類がPCL5の場合、**drivertype** を次のように設定します。

  ```
  drivertype=pcl5
  ```

出力サイズがゼロ

異なる種類のプリンターを試してください。また、CutePDF や PDFCreator のような仮想プリンターを試して、この問題がプリンタードライバーに関連しているかどうかを確認してください。

印刷ジョブは、クライアントのデフォルトプリンターのプリンタードライバーに依存します。現在アクティブなドライバーの種類を特定することが重要です。クライアントプリンターがPCL5ドライバーを使用しているのに、Linux VDAがPostscriptドライバーを選択すると、問題が発生する可能性があります。

プリンタードライバーの種類が正しい場合は、次の手順を実行して問題を特定できます。

1. 公開デスクトップセッションにログオンします。
2. **vi ~/.CtxlpProfile$CLIENT_NAME** コマンドを実行します。
3. Linux VDAにスプールファイルを保存するために、次のフィールドを追加します。

   ```
   deletespoolfile=no
   ```

4. 構成の変更を読み込むには、ログオフして再度ログオンします。
5. 問題を再現するためにドキュメントを印刷します。印刷後、スプールファイルは **/var/spool/cups-ctx/$logon_user/$spool_file** に保存されます。
6. スプールが空かどうかを確認します。スプールファイルがゼロの場合、問題が発生しています。詳細については、Citrixサポートに連絡してください（印刷ログを提供してください）。

7. スプールサイズがゼロでない場合は、ファイルをクライアントにコピーします。スプールファイルの内容は、クライアントのデフォルトプリンターのプリンタードライバーの種類によって異なります。マップされたプリンター（ネイティブ）ドライバーがPostScriptの場合、スプールファイルはLinux OSで直接開くことができます。内容が正しいかどうかを確認してください。

   スプールファイルがPCLの場合、またはクライアントOSがWindowsの場合は、スプールファイルをクライアントにコピーし、別のプリンタードライバーを使用してクライアント側のプリンターで印刷します。

8. マップされたプリンターを別のプリンタードライバーを使用するように変更します。次の例では、PostScriptクライアントプリンターを例として使用します。

   a. アクティブなセッションにログオンし、クライアントデスクトップでブラウザーを開きます。

   b. 印刷管理ポータルを開きます。

      ```
      localhost:631
      ```

   c. マップされたプリンター **CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID** と **Modify Printer** を選択します。この操作には管理者権限が必要です。

   d. **cups-ctx** 接続を保持し、**Continue** をクリックしてプリンタードライバーを変更します。

   e. **Make** および **Model** フィールドで、Citrix UPDドライバーとは異なるプリンタードライバーを選択します。たとえば、CUPS-PDF仮想プリンターがインストールされている場合は、Generic CUPS-PDF Printerドライバーを選択します。変更を保存します。

   f. このプロセスが成功した場合、マップされたプリンターが新しく選択されたドライバーを使用できるように、**.CtxlpProfile$CLIENT_NAME** でドライバーのPPDファイルパスを構成します。

既知の問題

Linux VDAでの印刷中に、以下の問題が確認されています。

CTXPSドライバーは一部のPLCプリンターと互換性がありません

印刷出力の破損が発生した場合は、プリンタードライバーをメーカー提供のネイティブドライバーに設定してください。

大容量ドキュメントの印刷パフォーマンスが遅い

ローカルクライアントプリンターで大容量ドキュメントを印刷すると、ドキュメントはサーバー接続を介して転送されます。低速接続では、転送に時間がかかる場合があります。

他のセッションから表示されるプリンターおよび印刷ジョブの通知

Linuxには、Windowsオペレーティングシステムと同じセッションの概念がありません。そのため、すべてのユーザーがシステム全体の通知を受け取ります。これらの通知は、CUPS構成ファイル: **/etc/cups/cupsd.conf** を変更することで無効にできます。

ファイルに構成されている現在のポリシー名を見つけます。

`DefaultPolicy default`

ポリシー名が *default* の場合は、以下の行をデフォルトポリシーのXMLブロックに追加します。

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

     … …
```

```
    <Limit Create-Printer-Subscription>

        Require user @OWNER

        Order deny,allow

    </Limit>

    <Limit All>

        Order deny,allow

    </Limit>

</Policy>
```

PDF印刷

PDF印刷をサポートするCitrix Workspace™アプリのバージョンを使用すると、Linux VDAセッション内から変換されたPDFを印刷できます。セッションの印刷ジョブは、Citrix Workspaceアプリがインストールされているローカルマシンに送信されます。ローカルマシンでは、お好みのPDFビューアを使用してPDFを開き、お好みのプリンターで印刷できます。

Linux VDAは、以下のバージョンのCitrix WorkspaceアプリでPDF印刷をサポートしています。

- Citrix Receiver for HTML5 バージョン2.4～2.6.9、Citrix Workspaceアプリ1808 for HTML5以降

- Citrix Receiver for Chrome バージョン2.4～2.6.9、Citrix Workspaceアプリ1808 for Chrome以降
- Citrix Workspaceアプリ1905 for Windows以降

構成

PDF印刷をサポートするCitrix Workspaceアプリのバージョンを使用する以外に、Citrix Studioで以下のポリシーを設定してください。

- **Client Printer Redirection** を **Allowed** に設定します（デフォルトで **Allowed**）。
- **Auto-create PDF Universal Printer** を **Enabled** に設定します（デフォルトで **Disabled**）。
- 「**クライアントプリンターの自動作成**」を「**すべてのクライアントプリンターを自動作成**」に設定します。

これらのポリシーを有効にすると、起動したセッション内で **Print** をクリックしたときに、プリンターを選択するための印刷プレビューがローカルマシンに表示されます。デフォルトプリンターの設定については、Citrix Workspaceアプリのドキュメントを参照してください。

リモートPCアクセス

概要

リモートPCアクセスは、Citrix Virtual Apps and Desktopsの拡張機能です。これにより、組織は従業員が物理的なオフィスPCに安全にリモートアクセスすることを容易に許可できます。ユーザーがオフィスPCにアクセスできれば、業務に必要なすべてのアプリケーション、データ、リソースにアクセスできます。

リモートPCアクセスは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps™ and Desktopsと同じコンポーネントを使用します。リモートPCアクセスを展開および構成するための要件とプロセスは、Citrix Virtual Apps and Desktopsを展開するために必要な要件とプロセスと同じです。この統一性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDXを使用してリモートオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

詳細については、Citrix Virtual Apps and Desktopsのドキュメントのリモートアクセスを参照してください。

考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX™ 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできません。この画面が表示されることは、潜在的なセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。自動ユーザー割り当てでは、ユーザーがPCにローカルでログオンすると、自動的にマシンに割り当てられます。このログオンは管理者の介入なしに行われます。クライアント上のCitrix Workspace™アプリは、リモートPCアクセスデスクトップセッション内で、ユーザーがオフィスPC上のアプリケーションとデータにアクセスするのに役立ちます。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

構成

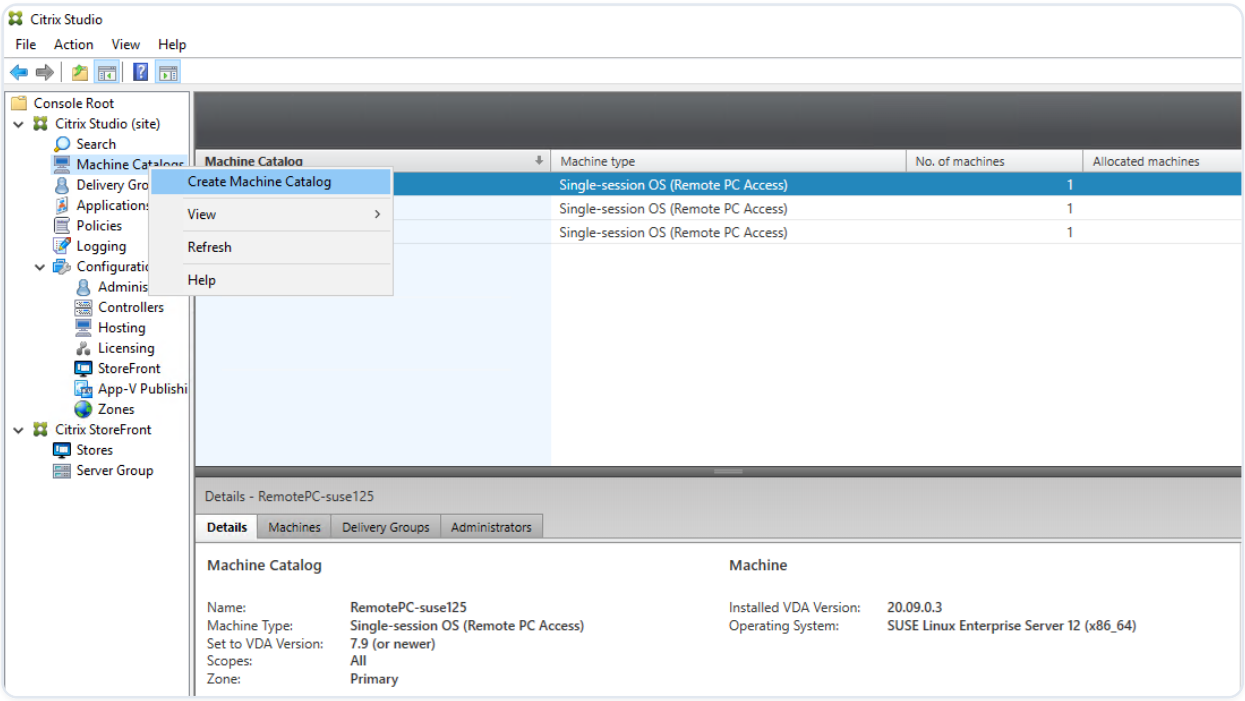
Linux PCセッションを配信するには、ターゲットPCにLinux VDAをインストールし、**リモートPCアクセス**タイプのマシンカタログを作成し、アクセスを要求するユーザーがマシンカタログ内のPCを利用できるようにデリバリーグループを作成します。次のセクションで手順を詳しく説明します。

ステップ1 - ターゲットPCにLinux VDAをインストールする

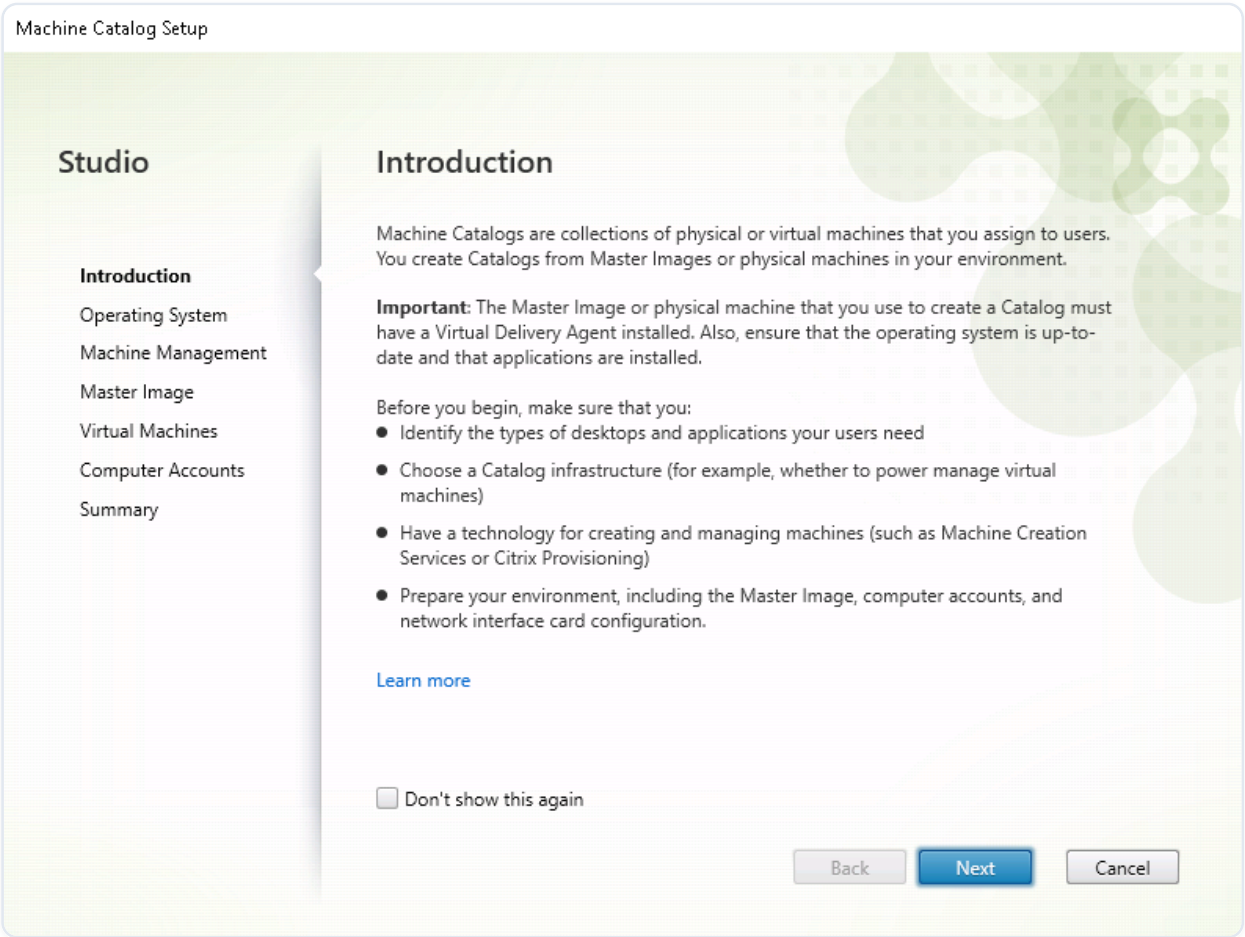
Linux VDAをインストールするには、簡易インストールを使用することをお勧めします。インストール中に、`CTX_XDL_VDI_MODE`変数の値を`Y`に設定します。

ステップ2 - リモートPCアクセスタイプのマシンカタログを作成する

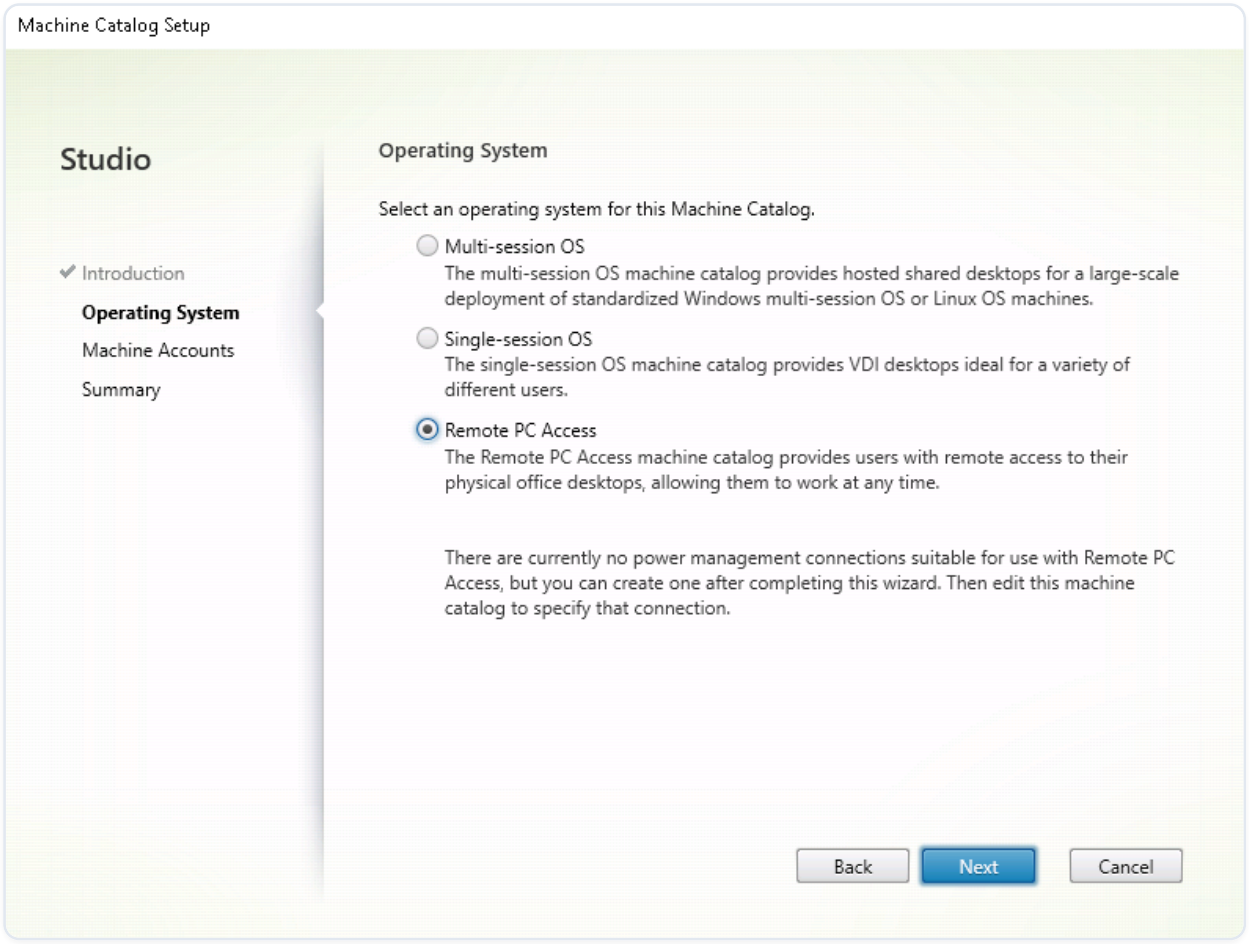
1. Citrix Studioで、**マシンカタログ**を右クリックし、ショートカットメニューから**マシンカタログの作成**を選択します。



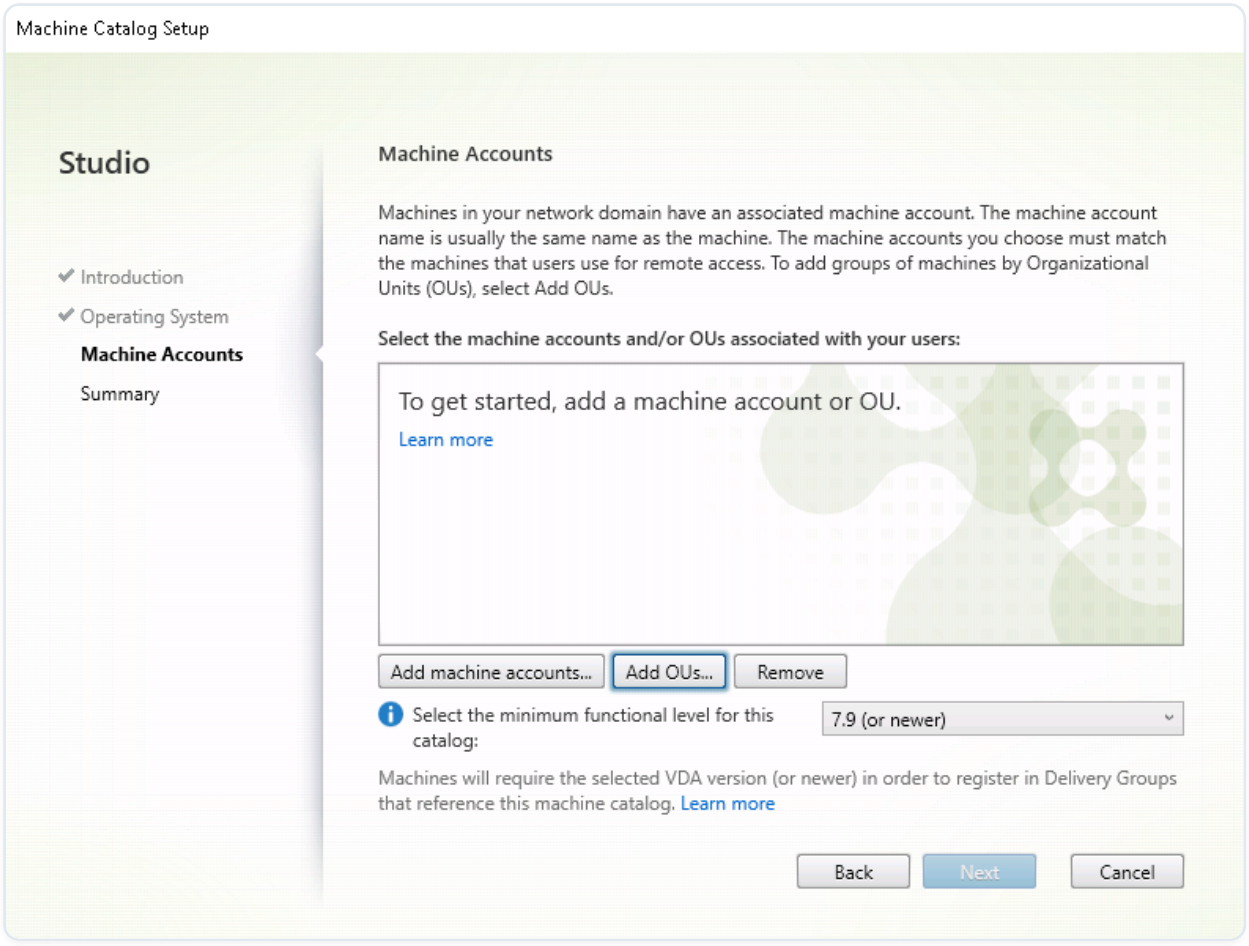
2. **はじめに**ページで**次へ**をクリックします。



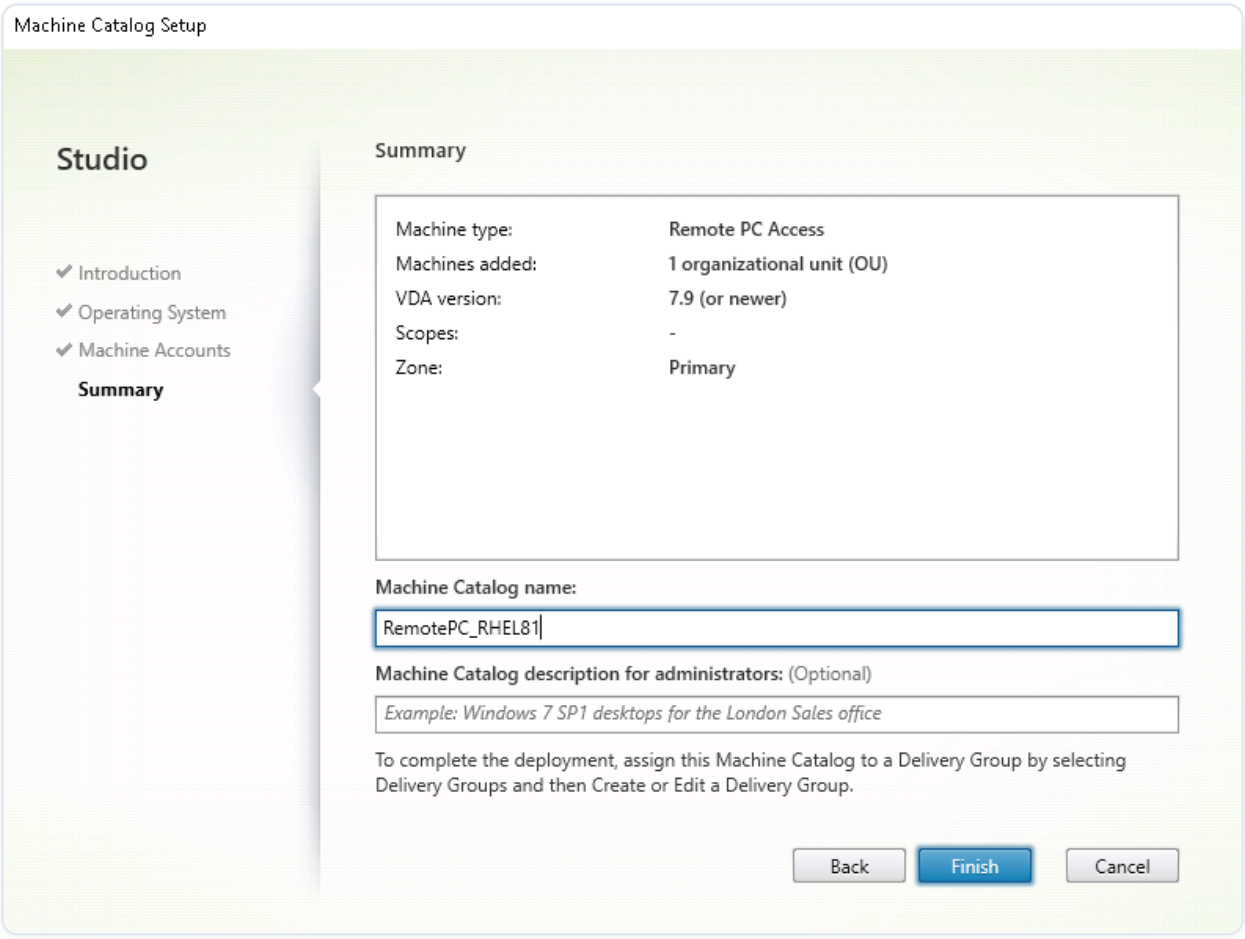
3. **オペレーティングシステム**ページで**リモートPCアクセス**を選択します。



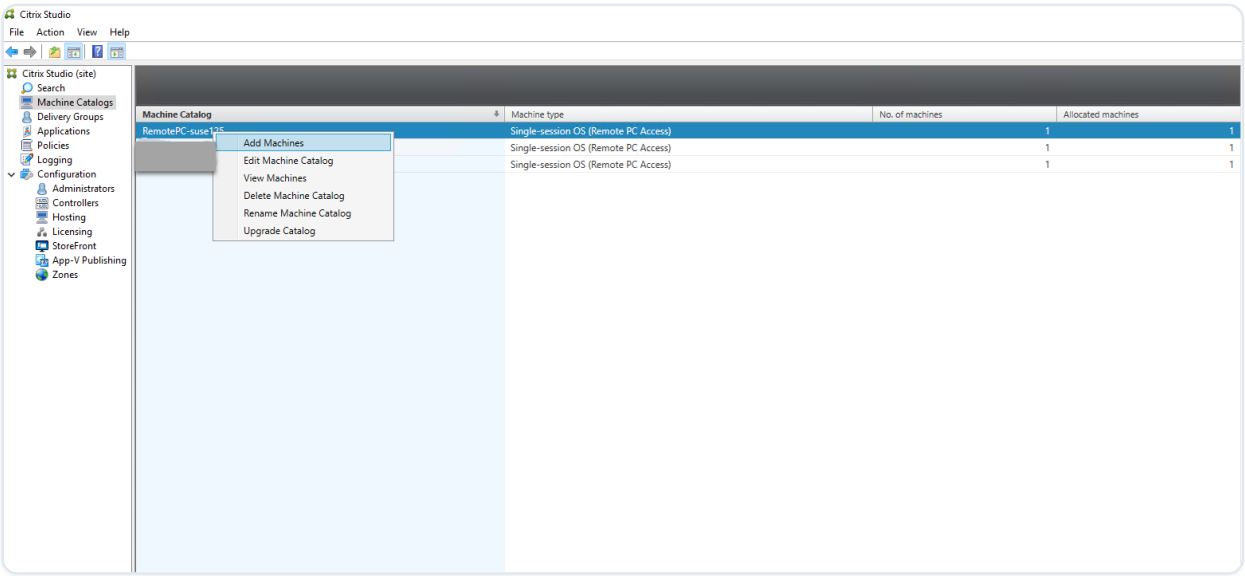
4. 「**OUの追加**」をクリックしてターゲットPCを含むOUを選択するか、「**マシンアカウントの追加**」をクリックして個々のマシンをマシンカタログに追加します。



5. マシンカタログに名前を付けます。

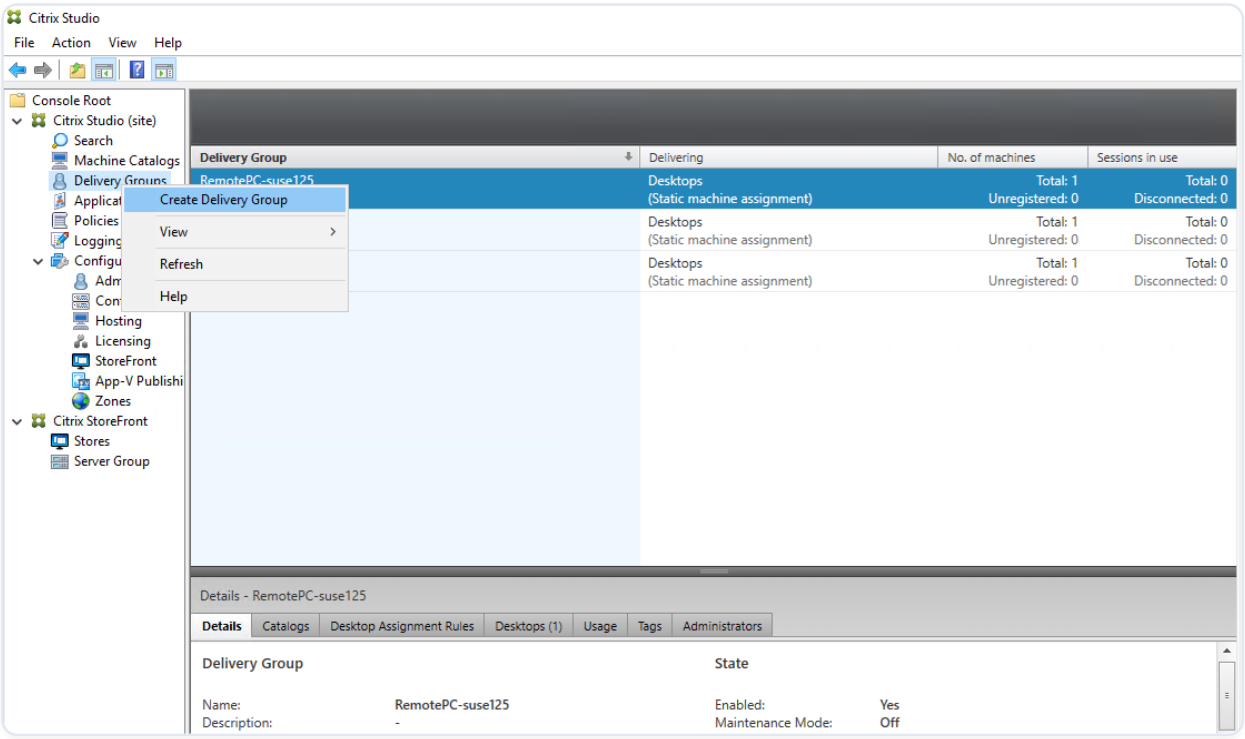


6. (オプション) マシンカタログを右クリックして、関連する操作を実行します。

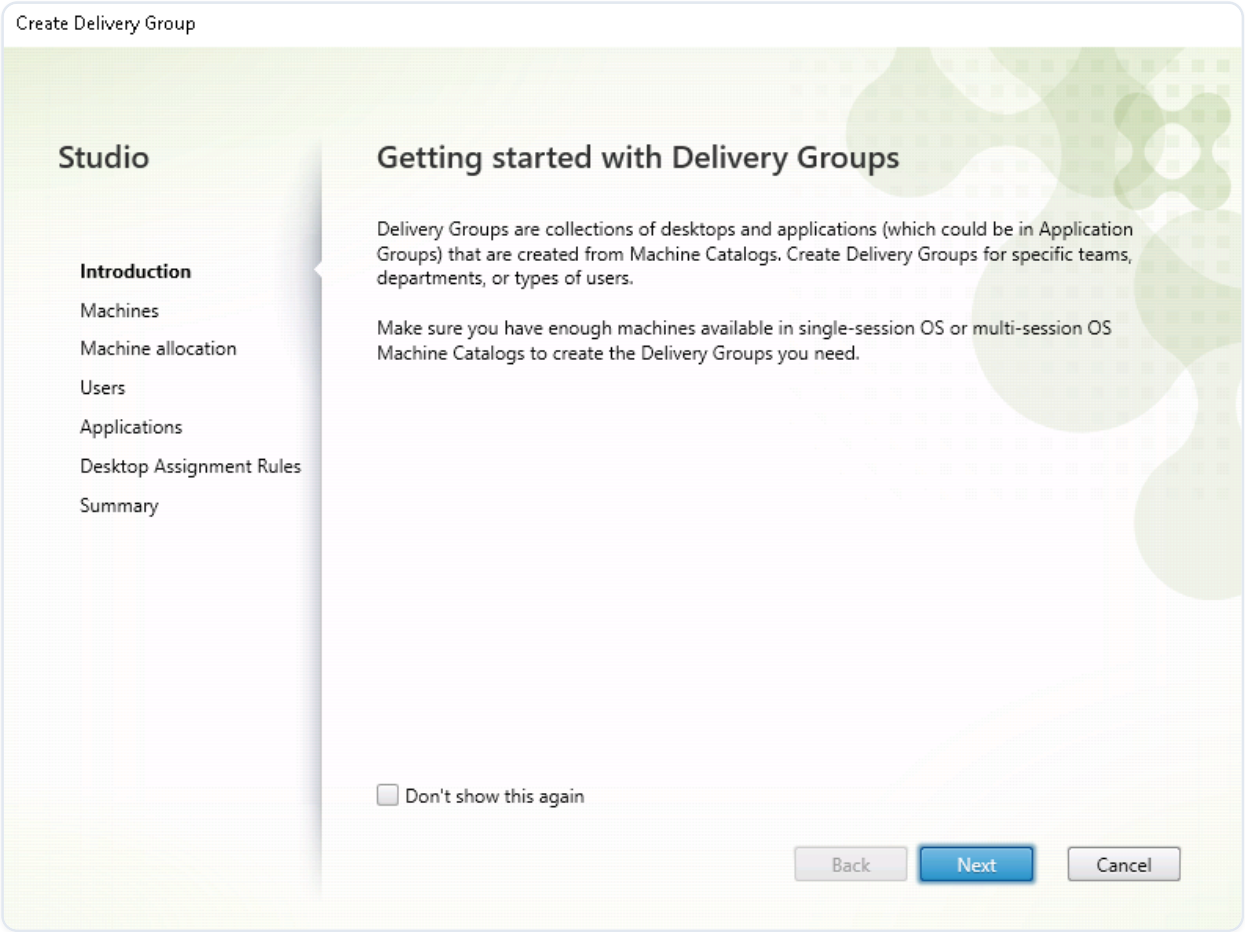


ステップ3 - マシンカタログ内のPCを、アクセスを要求するユーザーが利用できるようにするデリバリーグループを作成する

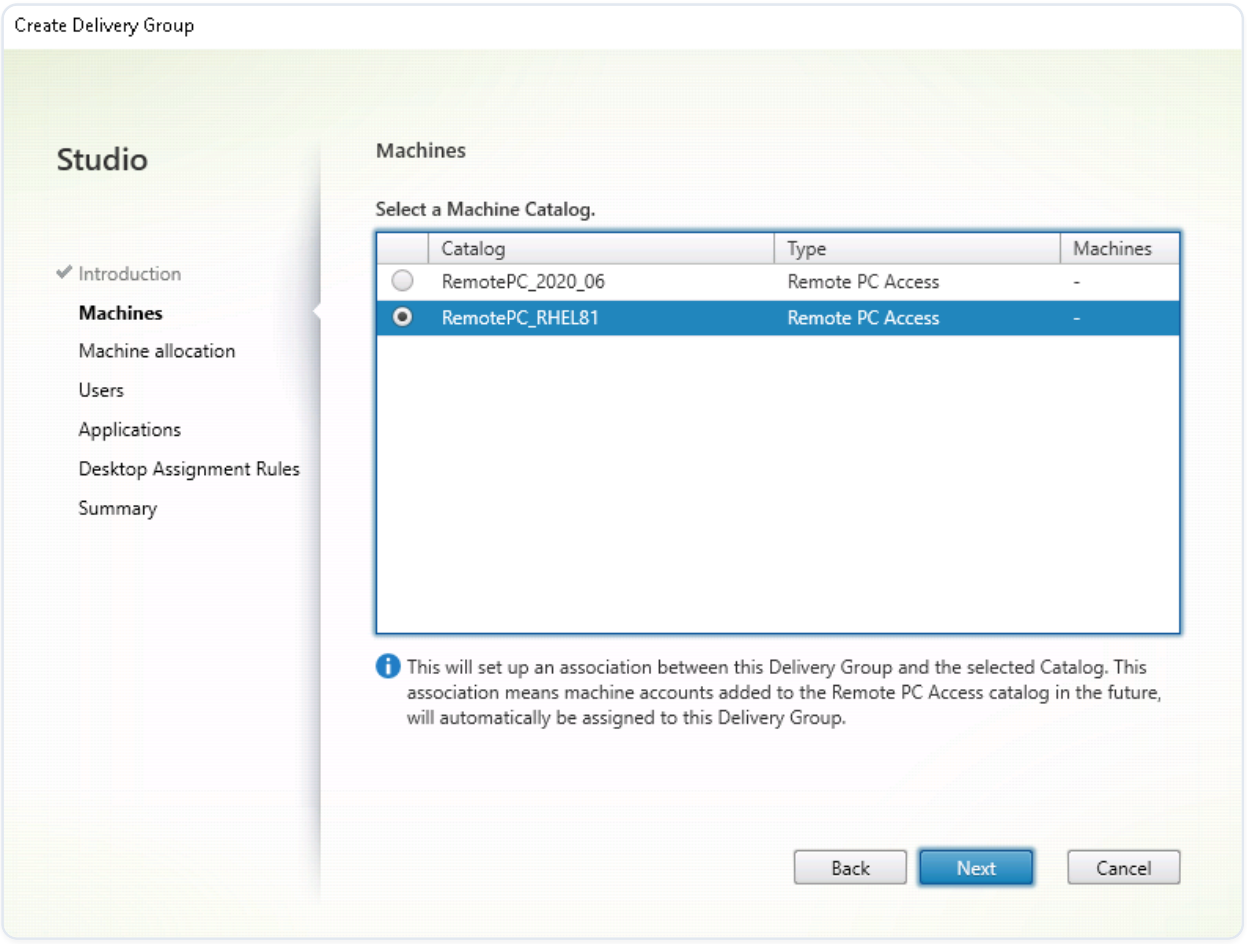
1. Citrix Studioで、**デリバリーグループ**を右クリックし、ショートカットメニューから**デリバリーグループの作成**を選択します。



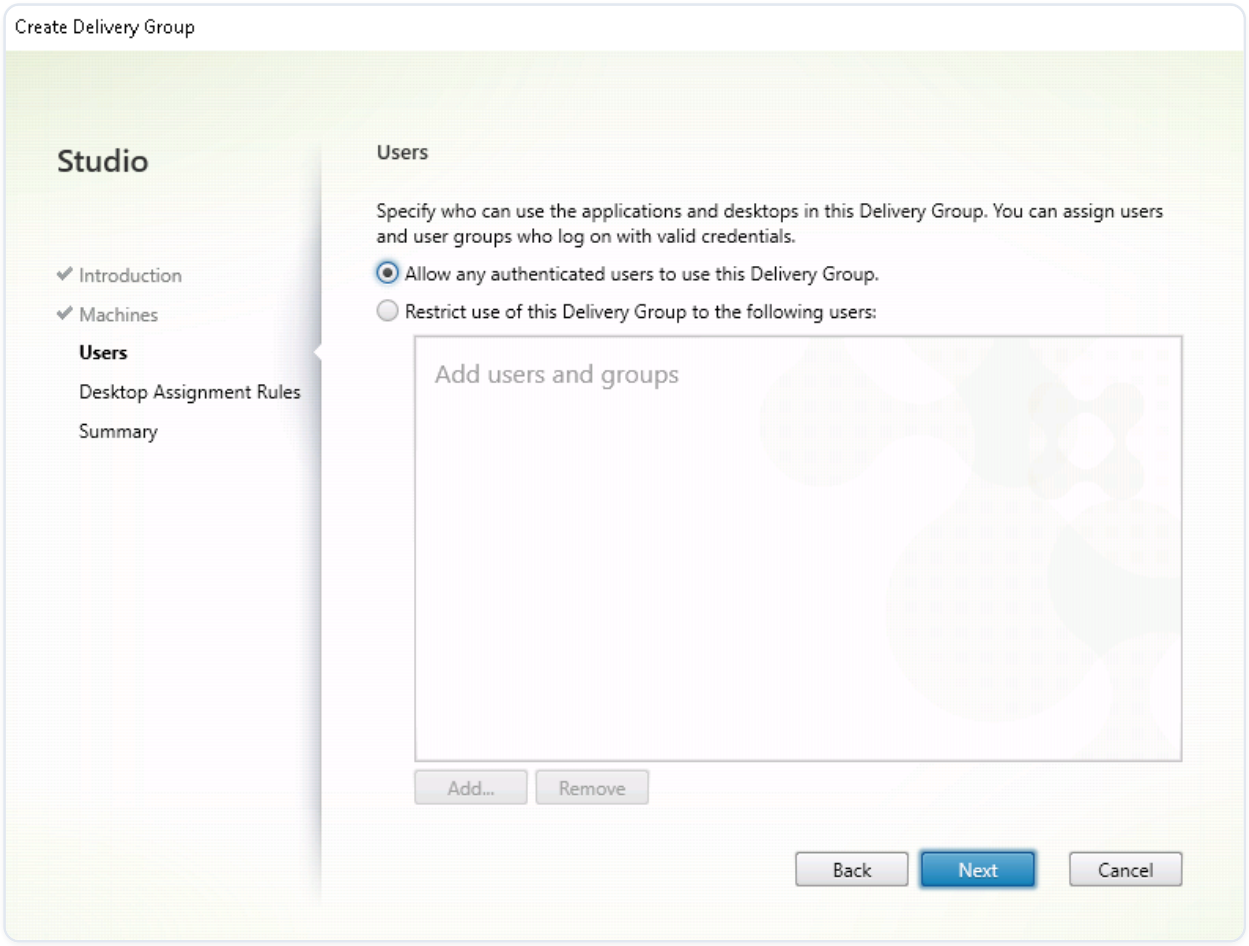
2. 「**デリバリーグループの開始**」ページで「**次へ**」をクリックします。



3. ステップ2で作成したマシンカタログを選択し、デリバリーグループに関連付けます。



4. マシンカタログ内のPCにアクセスできるユーザーを追加します。追加したユーザーは、クライアントデバイス上のCitrix Workspaceアプリを使用して、PCにリモートでアクセスできます。



Wake on LAN (ウェイク・オン・ラン)

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:

  - シトリックス DaaS™（旧称 シトリックス Virtual Apps and Desktops サービス）
  - シトリックス Virtual Apps and Desktops 2012 以降

- 物理PC:
  - VDAバージョン2012以降
  - BIOSおよびNICでWake on LANが有効になっていること

Wake on LANの構成

現在、統合Wake on LANの構成はPowerShellを使用してのみサポートされています。

Wake on LANを構成するには:

1. まだ Remote PC Access マシンカタログがない場合は、作成します。
2. まだ Wake on LAN ホスト接続がない場合は、作成します。

> **注:**
>
> Wake on LAN機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合、ホスト接続を作成します。

3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

   Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection
```

```
$hypHc = New-Item -Path xdhyp:\Connections `

             -Name $connectionName `

             -HypervisorAddress "N/A" `

             -UserName "woluser" `

             -Password "wolpwd" `

             -ConnectionType Custom `

             -PluginId VdaWOLMachineManagerFactory `

             -CustomProperties "<CustomProperties></CustomProperties>" `

             -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

5. マシンカタログ内の各VMで、BIOSおよびNICのWake on LANを有効にします。

   注： Wake on LANを有効にする方法は、マシンの構成によって異なります。

   - BIOSでWake on LANを有効にするには：

     a. BIOSに入り、Wake on LAN機能を有効にします。

        BIOSにアクセスする方法は、マザーボードの製造元と、その製造元が選択したBIOSベンダーによって異なります。

     b. 設定を保存してマシンを再起動します。

   - NICでWake on LANを有効にするには：

     a. NICがマジックパケットをサポートしているかどうかを確認するには、`sudo ethtool <NIC>`コマンドを実行します。

        `<NIC>`はNICのデバイス名です（例：`eth0`）。`sudo ethtool <NIC>`コマンドは、NICの機能に関する出力を提供します。

        - 出力に`Supports Wake-on: <letters>`のような行があり、`<letters>`に文字`g`が含まれている場合、NICはWake on LANマジックパケット方式をサポートしています。
        - 出力に`Wake-on: <letters>`のような行があり、`<letters>`に文字`g`が含まれていて、文字`d`が含まれていない場合、Wake on LANマジックパケット方式は有効になっています。ただし、`<letters>`に文字`d`が含まれている場合、Wake on LAN機能が無効になっていることを示します。この場合、`sudo ethtool -s <NIC> wol g`コマンドを実行してWake on LANを有効にしてください。

b. ほとんどのディストリビューションでは、起動ごとに`sudo ethtool -s <NIC> wol g`コマンドが必要です。このオプションを永続的に設定するには、お使いのディストリビューションに基づいて以下の手順を完了してください。

Ubuntu:

インターフェース構成ファイル`/etc/network/interfaces`に`up ethtool -s <NIC> wol g`行を追加します。例:

```
# ifupdown has been replaced by netplan(5) on this system. See

# /etc/netplan for current configuration.

# To re-enable ifupdown on this system, you can run:

# sudo apt install ifupdown

auto eth0

iface eth0 inet static

           address 10.0.0.1

           netmask 255.255.240.0

           gateway 10.0.0.1

           up ethtool -s eth0 wol g
```

RHEL/SUSE:

インターフェース構成ファイル`/etc/sysconfig/network-scripts/ifcfg-<NIC>`に次の`ETHTOOL_OPTS`パラメーターを追加します:

```
ETHTOOL_OPTS="-s ${DEVICE} wol g"
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。

- ある PC が別の PC を起動するには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用している必要があります。PC が同じマシンカタログ内にあるか、異なるマシンカタログ内にあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンに Wake on LAN ホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットはグローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内に少なくとも1台のPCが電源オンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動できるようにするには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Studioで表示されます。ただし、Studio内でそのプロパティを編集することはサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。
  - ユーザーが自分のPCへのセッションを起動しようとし、VDAが未登録の場合
  - 管理者がStudioまたはPowerShellから手動で電源オンコマンドを送信する場合
- デリバリーコントローラーはPCの電源状態を認識しないため、Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーはVDA登録状態を使用して、PCがオンかオフかを判断します。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

セッション

このセクションには、次のトピックが含まれています。

- アダプティブトランスポート
- 一時ホームディレクトリでのログオン
- アプリケーションの公開
- セッションの信頼性
- ランデブー V1
- ランデブー V2
- TLS を使用したユーザーセッションの保護
- DTLS を使用したユーザーセッションの保護

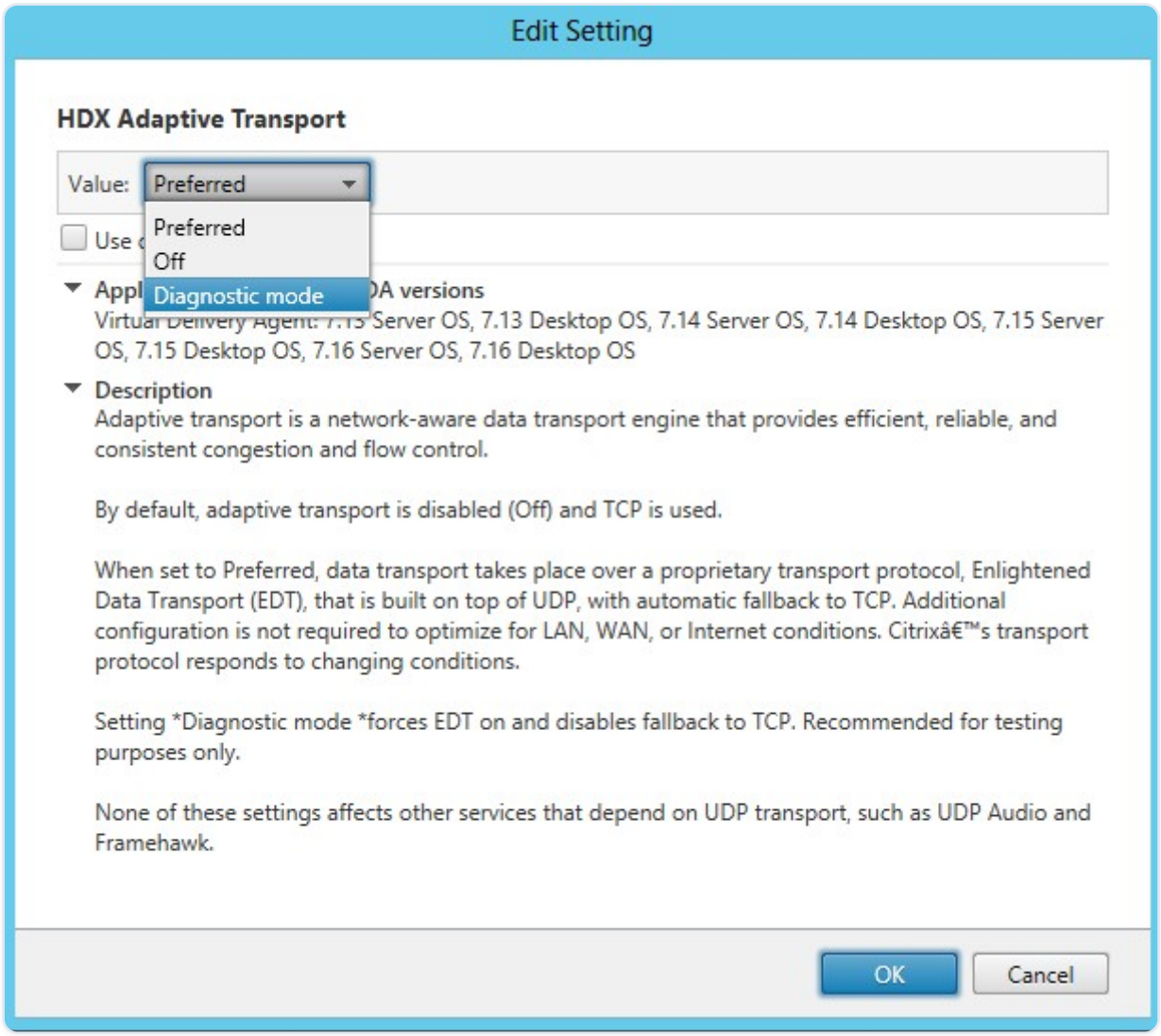
アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktopsのデータ転送メカニズムです。これは、より高速で、拡張性が高く、アプリケーションの対話性を向上させ、困難な長距離WANおよびインターネット接続でより対話的になります。アダプティブトランスポートの詳細については、アダプティブトランスポートを参照してください。

アダプティブトランスポートを有効にする

Citrix Studioで、**HDX™ Adaptive Transport**ポリシーが**Preferred**または**Diagnostic mode**に設定されていることを確認します。**Preferred**はデフォルトで選択されています。

- **Preferred**: 可能な場合はEnlightened Data Transport (EDT)を介したアダプティブトランスポートが使用され、TCPへのフォールバックが行われます。
- **Diagnostic mode**: EDTが強制的にオンになり、TCPへのフォールバックが無効になります。



アダプティブトランスポートを無効にする

アダプティブトランスポートを無効にするには、Citrix Studioで**HDX Adaptive Transport**ポリシーを**Off**に設定します。

アダプティブトランスポートが有効になっているか確認する

UDPリスナーが実行されているかどうかを確認するには、次のコマンドを実行します。

```
netstat -an | grep "1494\|2598"
```

通常、出力は次のようになります。

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```

```
udp        0      0 :::1494                 :::*
```

EDT MTU検出

EDTは、セッションを確立する際に最大転送単位 (MTU) を自動的に決定します。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化が防止されます。

最小要件:

- リナックス VDA 2012
- Citrix Workspace™ アプリ 1911 Windows用
- シトリックス ADC:
  - 13.0.52.24
  - 12.1.56.22
- セッションの信頼性を有効にする必要があります

この機能をサポートしないクライアントプラットフォームまたはバージョンを使用している場合、環境に適したカスタムEDT MTUを構成できます。詳細については、Knowledge Centerの記事CTX231821を参照してください。

警告:

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、**レジストリエディター**の誤った使用によって生じる問題が解決されることを保証できません。**レジストリエディター**の使用は、お客様ご自身の責任において行ってください。編集する前にレジストリを必ずバックアップしてください。

VDAでのEDT MTU検出の有効化または無効化

EDT MTU検出はデフォルトで無効になっています。

- EDT MTU検出を有効にするには、次のコマンドを使用して`MtuDiscovery`レジストリキーを設定し、VDAを再起動して、VDAが登録されるのを待ちます。

`/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t "REG_DWORD" -v "MtuDiscovery" -d "0x00000001" --force`

- EDT MTU検出を無効にするには、`MtuDiscovery`レジストリ値を削除します。

クライアントでのEDT MTU検出の制御

ICA®ファイルに`MtuDiscovery`パラメーターを追加することで、クライアントでEDT MTU検出を選択的に制御できます。この機能を無効にするには、`Application`セクションの下に以下を設定します。

`MtuDiscovery=Off`

この機能を再度有効にするには、ICAファイルから`MtuDiscovery`パラメーターを削除します。

> **重要:**
>
> このICAファイルパラメーターが機能するには、VDAでEDT MTU検出を有効にする必要があります。VDAでEDT MTU検出が有効になっていない場合、ICAファイルパラメーターは効果がありません。

セッションログオン画面のカスタム背景とバナーメッセージ

以下のコマンドを使用して、セッションの**ログオン**画面にカスタム背景またはバナーメッセージを追加できます。セッションの**ログオン**画面に背景とバナーメッセージの両方を追加するには、バナーメッセージを背景画像に埋め込むことができます。

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "LogonDisplayString" -d "<text of custom logon banner message>" --force
```

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "BackgroundImagePath" -d "<path to your custom logon screen background image>" --force
```

SUSE 15.4でこの機能を使用するには、`<http://download.opensuse.org/distribution/leap/15.3/repo/oss/>`から`imlib2`をインストールしてください。

> **ヒント:**

> LogonDisplayStringを使用してカスタムバナーメッセージを追加すると、ログオン画面の背景はデフォルトで青色になります。

セッションユーザーによるカスタムデスクトップ環境

CTX_XDL_DESKTOP_ENVIRONMENT 変数を使用して、セッションユーザーのデスクトップ環境を指定できます。2209リリース以降、セッションユーザーは独自のデスクトップ環境をカスタマイズできます。この機能を有効にするには、事前にVDAにデスクトップ環境をインストールする必要があります。

次の表は、セッションユーザーによるカスタムデスクトップ環境をサポートするLinuxディストリビューションとデスクトップ環境の対応表を示しています。

LINUXディストリビューション	サポートされているデスクトップ
Debian11.3	マテ、ジーノーム、ジーノーム・クラシック、ケーディーイー
RHEL 8.6, RHEL 8.4	マテ、ジーノーム、ジーノーム・クラシック
RHEL 7.9	マテ、ジーノーム、ジーノーム・クラシック、ケーディーイー
ロッキー・リナックス 8.6	マテ、ジーノーム、ジーノーム・クラシック、ケーディーイー
SUSE 15.4	マテ、ジーノーム、ジーノーム・クラシック
ウブントゥ 22.04、ウブントゥ 20.04、ウブントゥ 18.04	メイト、グノーム、グノームクラシック、ケーディーイー

デスクトップ切り替えコマンド

ターゲットのデスクトップ環境に切り替えるには、セッション内で対応するコマンドを実行します。

ターゲットのデスクトップ環境が次の場合は、	次のコマンドを実行します。
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`

ターゲットのデスクトップ環境が次の場合は、	次のコマンドを実行します。
グノームクラシック	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

KDEのヒント

- KDEの起動時にMagnusがロードされることがあります。回避策として、`sudo apt remove magnus`を実行してMagnusパッケージを削除できます。
- KDEの起動中に発生するQT警告を無効にするには、ルートユーザーとして`/usr/share/qt5/qtlogging.ini`を編集し、次のエントリを追加します。

```
qt.qpa.xcb.xcberror.error=false

qt.qpa.xcb.warning=false

qt.qpa.xcb.error=false
```

- KDEでは画面のロック解除が失敗する場合があります。回避策として、デスクトップの自動ロック機能を無効にすることをお勧めします。

一時ホームディレクトリでのログオン

Linux VDA上のマウントポイントが失敗した場合に備えて、一時ホームディレクトリを指定できます。一時ホームディレクトリが指定されている場合、マウントポイントが失敗すると、セッションログオン中にプロンプトが表示されます。ユーザーデータは一時ホームディレクトリの下に保存されます。

次の表は、ホームディレクトリ設定に役立つレジストリキーについて説明しています。

レジストリキー	説明	コマンド
`LogNoHome`	ユーザーがホームディレクトリなしでセッションにログオンできるかどうかを制御しま	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"`

レジストリキー	説明	コマンド
	す。デフォルト値は1で、「はい」を意味します。値が0に設定されている場合、ホームディレクトリなしでのセッションログオンは無効になります。	`-t "REG_DWORD" -v "LogNoHome" -d "0x00000001" --force`
`HomeMountPoint`	Linux VDA上にローカルマウントポイントを設定します。たとえば、`/mnt/home`がマウントポイントの場合、ユーザーのホームディレクトリは`/mnt/home/domain/<user_name>`です。マウントポイントが環境内のユーザーホームディレクトリと同じであることを確認してください。	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "HomeMountPoint" -d "<A directory where the NFS share is to be mounted>" --force`
`TempHomeDirectoryPath`	マウントポイントが失敗した場合に備えて、Linux VDA上に一時ホームディレクトリを設定します。デフォルト値は`/tmp`です。このレジストリキーは`HomeMountPoint`に依存します。システムがマウントポイントが利用できないことを検出した場合にのみ有効になります。ユーザーの一時ホームディレクトリは`/tmp/CTXSmf_user_id`です。	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "TempHomeDirectoryPath" -d "</tmp by default>" --force`
`RemoveHomeOnLogoff`	ユーザーログオフ時に一時ホームディレクトリを削除するかどうかを制御します。1は「はい」、0は「いいえ」を意味します。	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "RemoveHomeOnLogoff" -d "0x00000000" --force`

アプリケーションの公開

Linux VDAバージョン7.13で、Citrixはサポートされているすべてのプラットフォームにシームレスアプリケーション機能を追加しました。この機能を使用するために、特定のインストール手順は必要ありません。

ヒント:

Linux VDAバージョン1.4で、Citrixは非シームレス公開アプリケーションとセッション共有のサポートを追加しました。

Citrix Studioを使用したアプリケーションの公開

デリバリーグループを作成するとき、または既存のデリバリーグループにアプリケーションを追加するときに、Linux VDAにインストールされているアプリケーションを公開できます。このプロセスは、Windows VDAにインストールされているアプリケーションを公開するのと同様です。詳しくは、Citrix Virtual Apps and Desktopsのドキュメント（使用しているCitrix Virtual Apps and Desktopsのバージョンに基づく）を参照してください。

注:

- デリバリーグループを構成するときは、デリバリーの種類が**デスクトップとアプリケーション**または**アプリケーション**に設定されていることを確認してください。
- アプリケーションの公開は、Linux VDA バージョン 1.4 以降でサポートされています。ただし、Linux VDA は、デスクトップとアプリを同じマシンに配信することをサポートしていません。この問題に対処するため、アプリとデスクトップの配信には個別のデリバリーグループを作成することをお勧めします。
- シームレスアプリケーションを使用するには、StoreFrontでシームレスモードを無効にしないでください。シームレスモードはデフォルトで有効になっています。「TWIMode=Off」を設定してすでに無効にしている場合は、「TWIMode=On」に変更するのではなく、この設定を削除してください。そうしないと、公開されたデスクトップを起動できない可能性があります。

制限事項

Linux VDAは、単一ユーザーによる同じアプリケーションの複数の同時インスタンスの起動をサポートしていません。

アプリセッションでは、アプリケーションに固有のショートカットのみが期待どおりに機能します。

既知の問題

アプリケーションの公開中に、以下の既知の問題が確認されています。

- 非矩形ウィンドウはサポートされていません。ウィンドウの角にサーバー側の背景が表示される場合があります。
- 公開されたアプリケーションのウィンドウコンテンツのプレビューはサポートされていません。
- 複数のLibreOfficeアプリケーションを実行すると、これらのアプリケーションはプロセスを共有するため、最初に起動されたものだけがCitrix Studioに表示されます。
- 「Dolphin」のような公開されたQt5ベースのアプリケーションでは、アイコンが表示されない場合があります。この問題を解決するには、`<https://wiki.archlinux.org/title/Qt>`の記事を参照してください。

ランデブー V1

Citrix Gatewayサービスを使用する場合、Rendezvousプロトコルにより、トラフィックはCitrix Cloud™ Connectorsをバイパスし、Citrix Cloudコントロールプレーンに直接かつ安全に接続できます。

考慮すべきトラフィックには2つの種類があります。1) VDA登録およびセッションブローカリングのための制御トラフィック、2) HDX™セッションのトラフィックです。

Rendezvous V1では、HDXセッションのトラフィックがCloud Connectorsをバイパスできますが、VDA登録およびセッションブローカリングのためのすべての制御トラフィックをプロキシするには、引き続きCloud Connectorsが必要です。

要件

- Citrix Workspace™およびCitrix Gatewayサービスを使用した環境へのアクセス。
- コントロールプレーン：Citrix DaaS（旧Citrix Virtual Apps and Desktops™サービス）。
- Linux VDAバージョン2112以降。

  - バージョン2112は、非透過型HTTPプロキシに必要な最小バージョンです。
  - バージョン2204は、透過型およびSOCKS5プロキシに必要な最小バージョンです。

- CitrixポリシーでRendezvousプロトコルを有効にします。詳しくは、「Rendezvousプロトコルポリシー設定」を参照してください。
- VDAは、すべてのサブドメインを含め、`https://*.nssvc.net`にアクセスできる必要があります。その方法ですべてのサブドメインをホワイトリストに登録できない場合は、代わりに`https://*.c.nssvc.net`と`https://*.g.nssvc.net`を使用してください。詳しくは、Citrix Cloudドキュメントの「インターネット接続要件」セクション（Virtual Apps and Desktopサービスの下）およびKnowledge Centerの記事「CTX270584」を参照してください。
- Cloud Connectorsは、セッションを仲介する際にVDAのFQDNを取得する必要があります。この目標を達成するには、サイトのDNS解決を有効にします。Citrix DaaS Remote PowerShell SDKを使用して、コマンド`Set-BrokerSite -DnsResolutionEnabled $true`を実行します。Citrix DaaS Remote PowerShell SDKについて詳しくは、「SDKとAPI」を参照してください。

プロキシ構成

VDAは、HTTPおよびSOCKS5プロキシを介したRendezvous接続の確立をサポートしています。

プロキシに関する考慮事項

Rendezvousでプロキシを使用する場合は、次の点を考慮してください。

- 非透過型HTTPプロキシとSOCKS5プロキシがサポートされています。
- パケットの復号と検査はサポートされていません。VDAとGateway Service間のICA®トラフィックが傍受、復号、検査されないように例外を設定してください。そうしないと、接続が切断されます。
- HTTPプロキシは、NegotiateおよびKerberos認証プロトコルを使用して、マシンベースの認証をサポートします。プロキシサーバーに接続すると、Negotiate認証スキームが自動的にKerberosプロトコルを選択します。Kerberosは、Linux VDAがサポートする唯一のスキームです。

> **注:**
>
> Kerberosを使用するには、プロキシサーバーのサービスプリンシパル名（SPN）を作成し、それをプロキシのActive Directoryアカウントに関連付ける必要があります。VDAはセッション確立時に`HTTP/<proxyURL>`の形式でSPNを生成します。このとき、プロキ

> シURLは**Rendezvous proxy**ポリシー設定から取得されます。SPNを作成しない場合、認証は失敗します。

- SOCKS5プロキシでの認証は現在サポートされていません。SOCKS5プロキシを使用する場合は、Gateway Serviceアドレス（要件で指定）宛てのトラフィックが認証をバイパスできるように例外を設定する必要があります。
- SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

透過型プロキシ

Rendezvousでは透過型HTTPプロキシがサポートされています。ネットワークで透過型プロキシを使用している場合、VDAに追加の設定は必要ありません。

非透過型プロキシ

ネットワークで非透過型プロキシを使用する場合は、Rendezvous proxy configuration設定を構成します。この設定が有効になっている場合、VDAが使用するプロキシを認識できるように、HTTPまたはSOCKS5プロキシアドレスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`

Rendezvousの検証

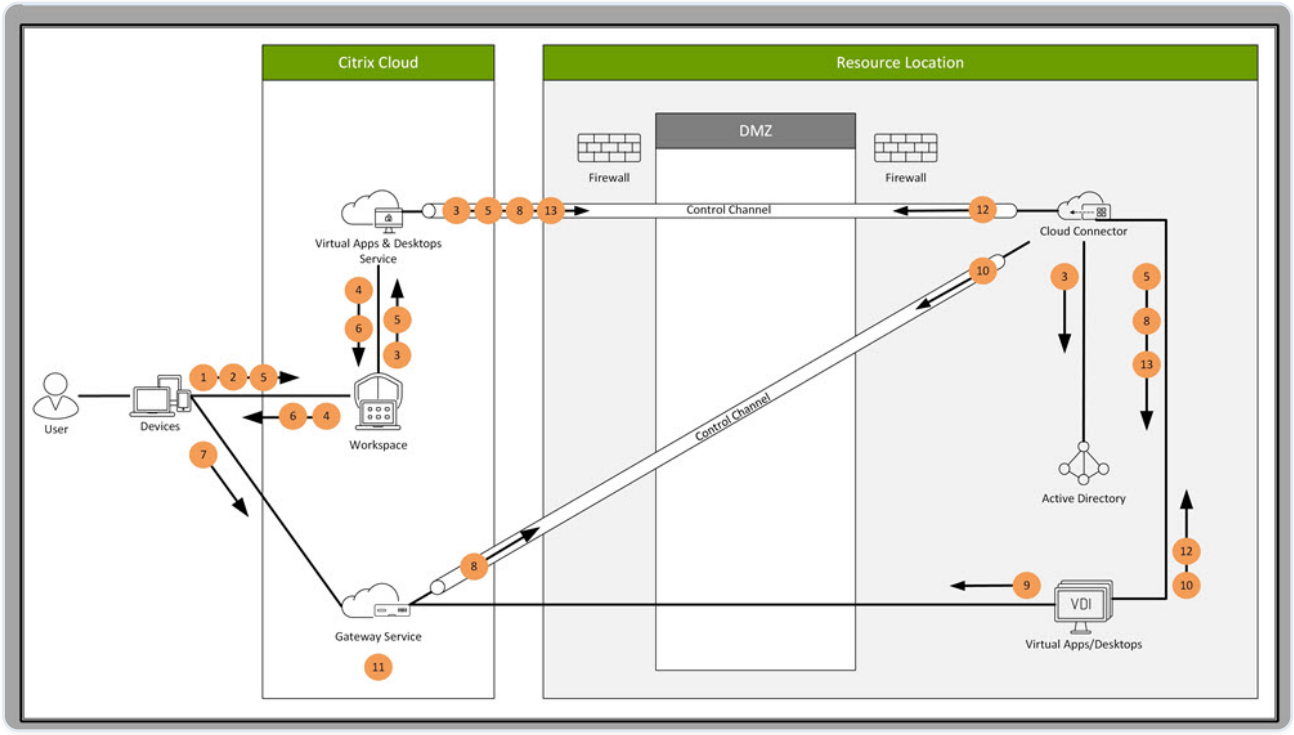
すべての要件を満たしている場合は、Rendezvousが使用されているかどうかを検証するために、次の手順に従ってください。

1. VDAでターミナルを起動します。
2. `/opt/Citrix/VDA/bin/ctxquery -f iP`を実行します。
3. TRANSPORT PROTOCOLSは接続の種類を示します。
    - TCP ランデブー: TCP - TLS - CGP - ICA
    - EDT ランデブー: UDP - DTLS - CGP - ICA
    - Cloud Connector経由のプロキシ: TCP - PROXY - SSL - CGP - ICA または UDP - PROXY - DTLS - CGP - ICA

> **ヒント:**
>
> Rendezvousが有効な状態でVDAがCitrix Gatewayサービスに直接到達できない場合、VDAはCloud Connectorを介してHDXセッションをプロキシするようにフォールバックします。

Rendezvousの仕組み

この図は、Rendezvous接続フローの概要です。



フローを理解するには、以下の手順に従ってください。

1. Citrix Workspaceに移動します。
2. Citrix Workspaceで資格情報を入力します。
3. オンプレミスのActive Directoryを使用している場合、Citrix DaaS™は、Cloud Connectorチャネルを使用してActive Directoryで資格情報を認証します。
4. Citrix Workspaceは、Citrix DaaSから列挙されたリソースを表示します。
5. Citrix Workspaceからリソースを選択します。Citrix DaaSは、受信セッションの準備をするようVDAにメッセージを送信します。
6. Citrix Workspaceは、Citrix Cloudによって生成されたSTAチケットを含むICAファイルをエンドポイントに送信します。
7. エンドポイントはCitrix Gatewayサービスに接続し、VDAに接続するためのチケットを提供し、Citrix Cloudがそのチケットを検証します。
8. Citrix Gatewayサービスは、接続情報をCloud Connectorに送信します。Cloud Connectorは、その接続がRendezvous接続であるかどうかを判断し、その情報をVDAに送信します。
9. VDAはCitrix Gatewayサービスへの直接接続を確立します。

10. VDAとCitrix Gatewayサービス間の直接接続が不可能な場合、VDAはCloud Connectorを介して接続をプロキシします。
11. Citrix Gatewayサービスは、エンドポイントデバイスとVDA間の接続を確立します。
12. VDAは、Cloud Connectorを介してCitrix DaaSでライセンスを検証します。
13. Citrix DaaSは、Cloud Connectorを介してセッションポリシーをVDAに送信します。これらのポリシーが適用されます。

ランデブー V2

Citrix Gatewayサービスを使用する場合、Rendezvousプロトコルにより、トラフィックはCitrix Cloud™ Connectorをバイパスし、Citrix Cloudコントロールプレーンに直接かつ安全に接続できます。

考慮すべきトラフィックには、1) VDA登録とセッションブローカリングのための制御トラフィック、2) HDX™セッショントラフィックの2種類があります。

Rendezvous V1では、HDXセッショントラフィックがCloud Connectorをバイパスできますが、VDA登録とセッションブローカリングのためのすべての制御トラフィックをCloud Connectorがプロキシする必要があります。

Rendezvous V2は、シングルセッションおよびマルチセッションLinux VDAで、標準ADドメイン参加マシンと非ドメイン参加マシンの両方での使用がサポートされています。非ドメイン参加マシンでは、Rendezvous V2により、HDXトラフィックと制御トラフィックの両方がCloud Connectorをバイパスできます。

要件

Rendezvous V2を使用するための要件は次のとおりです。

- Citrix Workspace™およびCitrix Gatewayサービスを使用した環境へのアクセス。
- コントロールプレーン：Citrix DaaS（旧Citrix Virtual Apps and Desktops™サービス）。
- VDAバージョン2201以降。
    - バージョン2204は、HTTPおよびSOCKS5プロキシの最低要件です。
- CitrixポリシーでRendezvousプロトコルを有効にします。詳しくは、Rendezvousプロトコルポリシー設定を参照してください。
- VDAは、すべてのサブドメインを含む`https://*.nssvc.net`にアクセスできる必要があります。その方法ですべてのサブドメインをホワイトリストに登録できない場合は、代わりに`https://*.c.nssvc.net`と`https://*.g.nssvc.net`を使用してください。詳しくは、

Citrix Cloudドキュメントのインターネット接続要件セクション（Virtual Apps and Desktop サービスの下）およびKnowledge Centerの記事CTX270584を参照してください。

- VDAは、前述のアドレスに接続できる必要があります。
  - TCP Rendezvousの場合はTCP 443で。
  - EDT Rendezvousの場合はUDP 443で。

プロキシの構成

VDAは、Rendezvousを使用する際に、制御トラフィックとHDXセッショントラフィックの両方でプロキシ経由の接続をサポートします。両方の種類のトラフィックで要件と考慮事項が異なるため、慎重に確認してください。

制御トラフィックのプロキシに関する考慮事項

- HTTPプロキシのみがサポートされています。
- パケットの復号と検査はサポートされていません。VDAとCitrix Cloudコントロールプレーン間の制御トラフィックが傍受、復号、または検査されないように例外を設定してください。そうしないと、接続は失敗します。
- プロキシ認証はサポートされていません。
- 制御トラフィックのプロキシを構成するには、レジストリを次のように編集します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ProxySettings" -d "http://<URL or IP>:<port>" --force
```

HDXトラフィックのプロキシに関する考慮事項

- HTTPおよびSOCKS5プロキシがサポートされています。
- EDTはSOCKS5プロキシでのみ使用できます。
- HDXトラフィックのプロキシを構成するには、Rendezvous proxy configurationポリシー設定を使用します。
- パケットの復号と検査はサポートされていません。VDAとCitrix Cloudコントロールプレーン間のHDXトラフィックが傍受、復号、または検査されないように例外を設定してください。そうしないと、接続は失敗します。
- HTTPプロキシは、NegotiateおよびKerberos認証プロトコルを使用することで、マシンベースの認証をサポートしています。プロキシサーバーに接続すると、Negotiate認証スキームは自動

的にKerberosプロトコルを選択します。KerberosはLinux VDAがサポートする唯一のスキームです。

> **注:**
>
> Kerberosを使用するには、プロキシサーバーのサービスプリンシパル名 (SPN) を作成し、プロキシのActive Directoryアカウントに関連付ける必要があります。VDAはセッション確立時に`HTTP/<proxyURL>`の形式でSPNを生成します。ここで、プロキシURLは**Rendezvous proxy**ポリシー設定から取得されます。SPNを作成しない場合、認証は失敗します。

- SOCKS5プロキシでの認証は現在サポートされていません。SOCKS5プロキシを使用している場合、Gateway Serviceアドレス (要件で指定) 宛てのトラフィックが認証をバイパスできるように例外を設定する必要があります。
- SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

透過型プロキシ

Rendezvousでは透過型HTTPプロキシがサポートされています。ネットワークで透過型プロキシを使用している場合、VDAに追加の構成は必要ありません。

Rendezvous V2の構成方法

環境でRendezvousを構成する手順は次のとおりです。

1. すべての要件が満たされていることを確認します。
2. VDAのインストール後、次のコマンドを実行して必要なレジストリキーを設定します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"GctRegistration" -d "0x00000001" --force
```

3. VDAマシンを再起動します。
4. Citrixポリシーを作成するか、既存のポリシーを編集します。
   - Rendezvousプロトコル設定を**許可**に設定します。
   - Citrixポリシーフィルターが適切に設定されていることを確認します。このポリシーは、Rendezvousを有効にする必要があるマシンに適用されます。

- Citrixポリシーが別のポリシーを上書きしないように、正しい優先順位を持っていることを確認します。

Rendezvousの検証

セッションがRendezvousプロトコルを使用しているかどうかを確認するには、ターミナルで`/opt/Citrix/VDA/bin/ctxquery -f iP`コマンドを実行します。

表示されるトランスポートプロトコルは、接続の種類を示します。

- TCP ランデブー: TCP - TLS - CGP - ICA
- EDT ランデブー: UDP - DTLS - CGP - ICA
- Cloud Connector を介したプロキシ: TCP - PROXY - SSL - CGP - ICA または UDP - PROXY - DTLS - CGP - ICA

Rendezvous V2 が使用されている場合、プロトコルバージョンは 2.0 と表示されます。

> **ヒント:**
>
> Rendezvous が有効になっている状態で VDA が Citrix Gateway サービスに直接到達できない場合、VDA は HDX セッションを Cloud Connector 経由でプロキシするようにフォールバックします。

DTLS を使用したユーザーセッションの保護

DTLS 暗号化は、7.18 リリース以降、完全にサポートされている機能です。デフォルトでは、この機能は Linux VDA で有効になっています。詳細については、「Transport Layer Security」を参照してください。

DTLS 暗号化を有効にする

アダプティブトランスポートが有効になっていることを確認する

Citrix Studio で、**HDX™ Adaptive Transport** ポリシーが **Preferred** または **Diagnostic mode** に設定されていることを確認します。

Linux VDA で SSL 暗号化を有効にする

Linux VDA で、**/opt/Citrix/VDA/sbin** にある **enable_vdassl.sh** ツールを使用して SSL 暗号化を有効（または無効）にします。このツールで利用可能なオプションについては、`/opt/Citrix/VDA/sbin/enable_vdassl.sh –h` コマンドを実行してください。

注:

Linux VDA は DTLS 1.0 と DTLS 1.2 の両方をサポートしており、デフォルトでは DTLS 1.2 を使用します。Citrix Workspace アプリでどのバージョンの DTLS が使用されているかを確認してください。Linux VDA と Citrix Workspace アプリの両方で同じバージョンの DTLS が使用されていることを確認してください。Citrix Workspace アプリが DTLS 1.0 のみをサポートしている場合（例：Citrix Receiver for Windows 4.11）、**enable_vdassl.sh** ツールを使用して、**SSLMinVersion** を **TLS_1.0** に、**SSLCipherSuite** を **COM** または **ALL** に設定します。

TLS を使用してユーザーセッションを保護する

バージョン 7.16 以降、Linux VDA はセキュアなユーザーセッションのための TLS 暗号化をサポートしています。TLS 暗号化はデフォルトで無効になっています。

TLS 暗号化を有効にする

セキュアなユーザーセッションのために TLS 暗号化を有効にするには、Linux VDA と Delivery Controller™ (Controller) の両方に証明書をインストールし、TLS 暗号化を有効にします。

Linux VDA に証明書をインストールする

PEM 形式のサーバー証明書と CRT 形式のルート証明書を取得します。サーバー証明書には、以下のセクションが含まれています。

- 証明書
- 暗号化されていない秘密鍵
- 中間証明書 (オプション)

サーバー証明書の例:

サーバー証明書の例 (/en-us/linux-virtual-delivery-agent/2303/media/example-server-certificate.png)

TLS 暗号化を有効にする

LINUX VDA で TLS 暗号化を有効にする

Linux VDA では、**/opt/Citrix/VDA/sbin** ディレクトリにある `enable_vdassl.sh` スクリプトを使用して TLS 暗号化を有効 (または無効) にします。スクリプトで利用可能なオプションについては、`/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` コマンドを実行してください。

SSL を有効にするスクリプト (/en-us/linux-virtual-delivery-agent/2303/media/script-for-enabling-ssl.png)

ヒント: 各 Linux VDA サーバーにサーバー証明書をインストールし、各 Linux VDA サーバーおよびクライアントにルート証明書をインストールする必要があります。

コントローラーでTLS暗号化を有効にする

> **注:**
>
> TLS暗号化はデリバリーグループ全体に対してのみ有効にできます。特定のアプリケーションに対してはTLS暗号化を有効にできません。

コントローラー上のPowerShellウィンドウで、ターゲットデリバリーグループのTLS暗号化を有効にするには、次のコマンドを順に実行します。

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

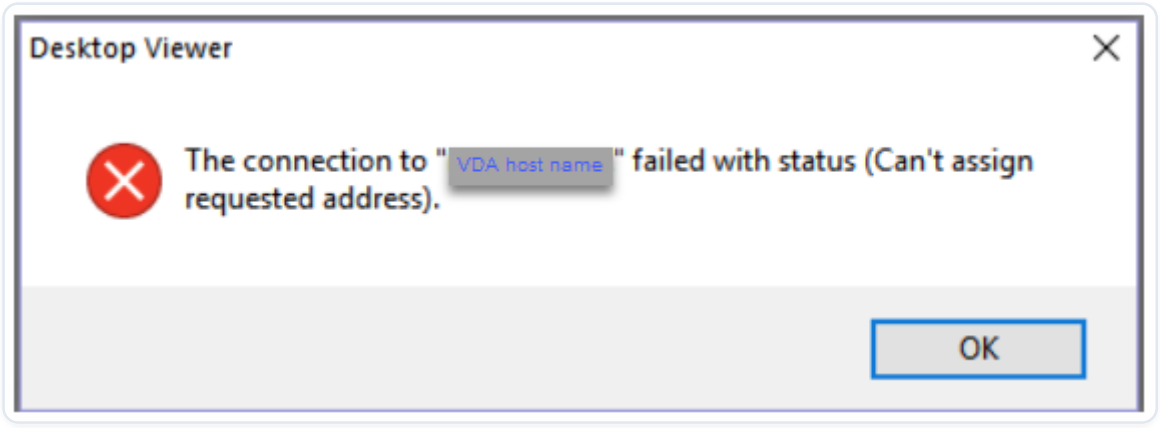
> **注:**
>
> ICA®セッションファイルにVDA FQDNのみが含まれるようにするには、`Set-BrokerSite –DnsResolutionEnabled $true`コマンドも実行できます。このコマンドはDNS解決を有効にします。DNS解決を無効にすると、ICAセッションファイルはVDAのIPアドレスを開示し、`SSLProxyHost`や`UDPDTLSPort`などのTLS関連項目に対してのみFQDNを提供します。

コントローラーでTLS暗号化を無効にするには、次のコマンドを順に実行します。

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $false`
3. `Set-BrokerSite –DnsResolutionEnabled $false`

トラブルシューティング

公開されたデスクトップセッションにアクセスしようとすると、Windows向けCitrix Workspace™アプリで次の「要求されたアドレスを割り当てることができません」というエラーが発生する場合があります。



回避策として、次のようなエントリを**hosts**ファイルに追加します。

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

Windowsマシンでは、**hosts**ファイルは通常、`C:\Windows\System32\drivers\etc\hosts`にあります。

セッションの信頼性

Citrix® は、サポートされているすべての Linux プラットフォームにセッションの信頼性機能を提供します。セッションの信頼性は、デフォルトで有効になっています。

セッションの信頼性により、ネットワークの中断時でもICAセッションがシームレスに再接続されます。セッションの信頼性の詳細については、「自動クライアント再接続とセッションの信頼性」を参照してください。

注: セッションの信頼性接続を介して送信されるデータは、デフォルトでプレーンテキストです。セキュリティ上の理由から、TLS暗号化を有効にすることをお勧めします。TLS暗号化の詳細については、「TLSを使用したユーザーセッションの保護」を参照してください。

構成

Citrix Studioのポリシー設定

Citrix Studioでセッションの信頼性について、次のポリシーを設定できます。

- セッションの信頼性接続
- セッションの信頼性タイムアウト

- セッションの信頼性ポート番号
- 再接続UIの透過レベル

詳細については、「セッションの信頼性ポリシー設定」および「自動クライアント再接続ポリシー設定」を参照してください。

注: **セッションの信頼性接続**または**セッションの信頼性ポート番号**ポリシーを設定した後、設定を有効にするには、VDAサービスとHDX™サービスをこの順序で再起動してください。

Linux VDAでの設定

- **セッションの信頼性TCPリスナーの有効化/無効化**

デフォルトでは、セッションの信頼性TCPリスナーは有効になっており、ポート2598でリッスンしています。リスナーを無効にするには、次のコマンドを実行します。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "fEnableWinStation" -d "0x00000000"
```

注: 設定を有効にするには、HDXサービスを再起動してください。TCPリスナーを無効にしても、セッションの信頼性は無効になりません。**セッションの信頼性接続**ポリシーを通じて機能が有効になっている場合、セッションの信頼性は他のリスナー（SSLなど）を介して引き続き利用できます。

- **セッションの信頼性ポート番号**

次のコマンドを使用して、セッションの信頼性ポート番号を設定することもできます（例としてポート番号2599を使用）。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "PortNumber" -d  "2599"
```

注: 設定を有効にするには、HDXサービスを再起動してください。ポート番号が**Citrix Studio**のポリシー設定で設定されている場合、Linux VDAでの設定は無視されます。VDA上のファイアウォールが、設定されたポートを介したネットワークトラフィックを禁止しないように構成されていることを確認してください。

- **サーバーからクライアントへのキープアライブ間隔**

セッション中にアクティビティがない場合（たとえば、マウスの動きや画面の更新がない場合）、Linux VDAとクライアントの間でキープアライブメッセージが送信されます。キープアライブメッセージは、クライアントがまだ応答しているかどうかを検出するために使用されます。クライアントからの応答がない場合、クライアントが再接続するまでセッションは中断されます。この設定は、連続するキープアライブメッセージ間の秒数を指定します。デフォルトでは、この設定は構成されていません。これを構成するには、次のコマンドを実行します（例として10秒を使用）。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpServerToClientKeepAlive"  -d  "10"  --force
```

- **クライアントからサーバーへのキープアライブ間隔**

この設定は、ICA®クライアントからLinux VDAに送信される連続するキープアライブメッセージ間の秒数を指定します。デフォルトでは、この設定は構成されていません。これを構成するには、次のコマンドを実行します（例として10秒を使用）。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpClientToServerKeepAlive"  -d  "10"  --force
```

トラブルシューティング

ポリシー設定でセッションの信頼性を有効にした後、セッションを起動できない。

この問題を回避するには、次の操作を行います。

1. Citrix Studioでポリシー設定を通じてセッションの信頼性を有効にした後、VDAサービスとHDXサービスがこの順序で再起動されていることを確認してください。
2. VDAで、次のコマンドを実行して、セッションの信頼性TCPリスナーが実行されていることを確認します（例としてポート2598を使用）。

   ```
   netstat -an | grep 2598
   ```

   セッションの信頼性ポートにTCPリスナーがない場合は、次のコマンドを実行してリスナーを有効にします。

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations
\cgp"   -v  "fEnableWinStation" -d "0x00000001"
```

セッション録画 (実験的機能)

実験的機能として、Linux VDAでホストされているセッションを録画および再生できます。

セッション録画を有効または無効にする

Linux VDAのセッション録画を有効または無効にするには、**SmAudAllowed**をそれぞれ**1**または**0**に設定します。以下のコマンドを使用できます。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "SmAudAllowed" -d "0x00000001" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "SmAudAllowed" -d "0x00000000" --force
```

注:

Linux VDAでセッション録画を有効にすると、ユーザーがセッションにログオンしたときに、セッションが録画されていることが通知されます。

録画ファイルのサイズを指定する

録画のサイズが大きくなると、録画ファイルのダウンロードに時間がかかり、再生中にシークスライダーを使用して移動する際の応答が遅くなります。ファイルサイズを制御するには、ファイルのしきい値制限を指定します。録画がこの制限に達すると、現在のファイルは閉じられ、録画を続行するために追加のファイルが作成されます。このアクションは「ロールオーバー」と呼ばれます。

以下のコマンドを使用して、ロールオーバーの2つのしきい値を指定できます。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "RolloverFileSizeInMB" -d "0x00000032" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "RolloverTimeInHours" -d "0x0000000c" --force
```

- **RolloverFileSizeInMB**。現在のファイルが指定されたサイズに達すると閉じられ、新しいファイルが開きます。デフォルトでは、サイズが50 MBを超えるとロールオーバーが発生します。サポートされる値：10～300。
- **RolloverTimeInHours**。指定された期間に達すると、現在のファイルが閉じられ、新しいファイルが開きます。デフォルトでは、セッションが12時間録画されるとロールオーバーが発生します。サポートされる値：1～24。

ロールオーバーは、上記の2つの条件のうち最初に満たされたときに発生します。たとえば、ファイルサイズに17 MB、期間に6時間を指定したとします。録画が3時間で17 MBに達すると、セッション録画はファイルを閉じて新しいファイルを開きます。

多数の小さなファイルが作成されるのを防ぐため、ファイルサイズに指定された値にかかわらず、少なくとも1時間が経過するまでロールオーバーは発生しません。この規則の例外は、ファイルサイズが300 MBを超過する場合です。

録画の保存場所を指定する

録画ファイルはデフォルトで`/var/xdl/session_recordings`に保存されます。別のパスを指定するには、以下のコマンドを実行します。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v
"Path" -d "<your custom storage path>" --force
```

録画はローカルドライブまたはネットワークパスを指すマウントポイントに保存できます。設定したストレージパスに適切なアクセス許可を設定し、ユーザー`ctxsrvr`にそのパスへの書き込み許可を付与してください。

録画を表示

録画を表示するには、以下の手順に従ってSession Recording PlayerまたはSession Recording Web Playerをインストールしてください。

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsダウンロードページにアクセスし、製品ファイルをダウンロードします。ファイルを解凍します。
2. SessionRecordingPlayer.msiとSessionRecordingWebPlayer.msiをダブルクリックし、指示に従ってインストールを完了します。

> **ヒント:**
>
> Session Recording Web Playerを使用するには、Session Recordingサーバーにのみインストールし、録画がSession Recordingサーバーで利用可能であることを確認してください。詳細については、Citrix Session Recordingのドキュメントを参照してください。

制限事項

- 仮想アプリセッションの場合、録画通知が中央に表示されない場合があります。

仮想チャネルSDK（実験的）

Linux VDA用仮想チャネルソフトウェア開発キット（SDK）を使用すると、VDA上で実行するサーバー側アプリケーションを作成できます。詳しくは、Linux VDA用Citrix仮想チャネルSDKドキュメントを参照してください。

Linux VDA用Citrix仮想チャネルSDKは、Citrix Virtual Apps and Desktopsダウンロードページからダウンロードできます。適切なバージョンのCitrix Virtual Apps and Desktopsを展開し、**コンポーネント**をクリックしてLinux VDAのダウンロードを選択してください。

Wayland (実験的)

実験的な機能として、Linux VDAは、RHEL 9.1/9.0、Rocky Linux 9.1/9.0、およびUbuntu 22.04上のGNOMEでWaylandをサポートしています。Waylandでは、以下の機能が完全にテストされています。

- オーディオ
- クリップボード
- クライアントドライブマッピング (CDM)

- 印刷
- USBデバイスリダイレクト

> **注:**
>
> - HDX™ 3D Proはサポートされていません。
> - Linux仮想アプリセッションはサポートされていません。

Waylandを有効にする

Waylandを使用するには、次のコマンドを実行してレジストリキー **EnableWayland** を **1** に設定します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Wayland" -t "REG_DWORD" -v
"EnableWayland" -d "0x00000001" --force
```

デフォルトでは、レジストリキー **EnableWayland** は **0** に設定されており、これはX11が使用されることを意味します。

Waylandが使用中であるかを確認する

1. Linuxでターミナルウィンドウを開きます。
2. **echo $XDG_SESSION_TYPE** コマンドを実行します。

Waylandが使用中の場合、出力に **'wayland'** が表示されます。

制限事項

Waylandを使用している場合、以下の制限が確認されています。

- クライアントデバイスのキーボードレイアウトは、VDAのキーボードレイアウトと同期されません。
- RHEL 9.1/9.0またはRocky Linux 9.1/9.0上のセッションからログオフするのに約20秒かかります。

Linux Virtual Delivery Agentのドキュメント履歴

次の表に、Linux Virtual Delivery Agent 2303のドキュメントに対する重要な変更点を示します。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

DATE	変更	説明
20 Mar 2023	Linux Virtual Delivery Agent 2303の初期リリース	「新機能」を参照してください。