新機能

リリース日: July 07, 2022

7.15の新機能

累積更新プログラム9 (CU9) は、Linux VDA 7.15 LTSRの最新リリースです。CU9では、Linux VDA 7.15 CU8と比較して、1つの修正が追加されています。

PDF印刷

以前は実験的な機能として提供されていましたが、PDF印刷は、このリリースで完全にサポートされる機能になりました。これにより、Citrix Receiver for ChromeおよびHTML5のユーザーは、Linux VDAセッション内で変換されたPDFを印刷できます。

システムの動作変更

このリリース以降、Linux VDAのアップグレード後にctxsetup.shスクリプトを実行する必要はありません。

修正された問題

CU9で修正された問題

- SUSEまたはRHELでLinux VDAをアンインストールすると、/opt/Citrix/の場所に空のフォルダーが削除されない場合があります。

CU8で修正された問題

- チャネルバインディングが有効な場合、Linux VDAをDelivery Controller™に登録しようとすると失敗する場合があります。

CU6で修正された問題

- マウスとキーボードが同じウィンドウにフォーカスされていない場合、またはマウスがフォーカスを変更できない場合、Linuxセッションが応答しなくなることがあります。

- 取り外し可能なUSBドライブをLinux VDAに汎用的にリダイレクトしようとすると失敗する場合があります。この問題は、USBドライブがNTFS（New Technology File System）形式の場合に発生します。
- Linux VDAは、**ターゲットフレームレート** (FramesPerSecond) 設定で指定された1秒あたりのフレーム数に達しない場合があります。この問題は、Linux VDAにGPUがインストールされている場合に発生します。

CU5で修正された問題

- クリップボード機能を使用してクライアントとセッション間でコンテンツをコピーアンドペーストしようとすると失敗する場合があります。
- Linux VDAでセッションを起動してアクションを実行すると、セッションが切断される場合があります。

CU4で修正された問題

- エンドポイントからコンテンツをコピーしてLinux VDAで実行中のアプリケーションに貼り付けようとすると、コンテンツがコピーされない場合があります。
- SUSE Linux Enterprise Server 11 Service Pack 4でキーボードが機能しない場合があります。その結果、キーストロークが画面に表示されず、キーボードレイアウトが正しく設定されません。
- Linux VDAのユーザーセッションで**ctxctl**プロセスが実行に失敗する場合があります。

CU3 で修正された問題

- Linux VDA が Citrix® ポリシーを適用できない場合があります。この問題は、NetScaler® Gateway で Access Control 要素接続タイプを使用するようにポリシーを構成した場合に発生します。

CU2 で修正された問題

- Delivery Controller を使用した Linux VDA の登録が断続的に失敗する場合があります。
- Red Hat Enterprise Linux Server 7.3 で実行されている Citrix Director 7.13 は、マシンのセッション詳細を表示しない場合があります。次のエラーメッセージが表示されます:

  データを取得できません。
- Linux VDA が Delivery Controller に登録された後、しばらくすると登録解除される場合があります。

- Linux VDA のセッション表示を確認するために使用される特定のサードパーティ製アプリケーションが、すべてのピクセルを表示しない場合があります。
- 複数の LDAP サーバーがある場合、ポリシーが更新されセッションがタイムアウトした後、Linux VDA でアプリケーションを起動しようとすると失敗する場合があります。
- セッションが Linux VDA に接続されている場合、ctxhdx プロセスが予期せず **segfault** エラーで終了する場合があります。
- Linux VDA 7.16 Early Access Release を使用している場合、ブローカーエージェントがアプリケーション名を取得できない場合があります。この失敗により、Director に **Agent Requested** エラーが表示され、その後再登録が開始されます。

CU1 で修正された問題

- Linux VDA が Delivery Controller に登録された後、しばらくすると登録解除される場合があります。
- Linux VDA のセッション表示を確認するために使用される特定のサードパーティ製アプリケーションが、すべてのピクセルを表示しない場合があります。
- 複数の LDAP サーバーがある場合、ポリシーが更新されセッションがタイムアウトした後、Linux VDA でアプリケーションを起動しようとすると失敗する場合があります。

7.15 LTSRで修正された問題

このLinux VDAリリースでは、以下の問題が解決されました。

- DNS IPアドレスを入力すると、簡易インストールによってLinux VDAがネットワークから切断される可能性があります。
- ビデオ再生中に、Citrix Receiver™ for WindowsからCitrix Receiver for Androidへのセッションローミングが失敗します。

既知の問題

このリリースで以下の問題が確認されています。

- XenAppおよびXenDesktop 7.15 LTSR CU6と統合されたCitrix Scoutは、Linux VDA 7.15からログを収集できません。Linux VDA 7.15は、Citrix Scoutがログの収集に使用するCitrix Telemetry Serviceをサポートしていません。
- `indicator-datetime-service`プロセスは$TZ環境変数を消費しません。クライアントとセッションが異なるタイムゾーンにある場合、Ubuntu 16.04 Unity DesktopのUnityパネルにはクライアントの時刻が表示されません。

- 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た後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。
- 英語以外の言語では、UTF-8エンコーディングのみがサポートされています。
- Citrix Receiver™ for AndroidのCAPS LOCKの状態は、セッションローミング中に反転する場合があります。既存の接続をCitrix Receiver for Androidにローミングすると、CAPS LOCKの状態が失われる可能性があります。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ます。
- Citrix Receiver for Macを使用してLinux VDAに接続する場合、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。Citrix Receiver for Macは、デフォルトで左右のOptions/Altキーの両方にAltGrを送信します。この動作はCitrix Receiver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への戻り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ます。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ます。

  ```
  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および場合によっては他のサービスのサービスチケットが削除されます。ただし、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。
- Citrix Receiver for Windows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 Desktop バージョン 7.15 (PDFダウンロード)

このLinux VDAリリースには、ドキュメントに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。

システム要件

Linuxディストリビューション

Linux VDAは、以下のLinuxディストリビューションをサポートしています。

- スースー リナックス エンタープライズ:
  - デスクトップ 12 サービスパック 2
  - サーバー 12 サービスパック 2
  - サーバー 11 サービスパック 4
- レッドハット エンタープライズ リナックス
  - ワークステーション 7.3
  - ワークステーション 6.9
  - ワークステーション 6.6
  - サーバー 7.3
  - サーバー 6.9
  - サーバー 6.6
- セントオーエス リナックス
  - CentOS 7.3
  - CentOS 6.6
- ウブントゥ リナックス
  - Ubuntu Desktop 16.04 (4.4.x カーネル搭載)
  - Ubuntu Server 16.04 (4.4.x カーネル搭載)

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、次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
RHEL 7.3、CentOS 7.3	1.17
RHEL 6.9	1.17
RHEL 6.6、CentOS 6.6	1.15
ウブントゥ 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

Ubuntu 16.04でHWE Xorgサーバー1.19を使用しないでください。

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。

注:

Citrix®のLinux OSプラットフォームおよびバージョンに対するサポートは、OSベンダーからのサポートが終了すると期限切れになります。

重要:

GnomeおよびKDEデスクトップはSUSE、RHEL、CentOSでサポートされています。Unityデスクトップ はUbuntuのみでサポートされています。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。

XenDesktop®

Linux VDAは、現在サポートされているすべてのXenDesktopバージョンと互換性があります。XenDesktop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。ただし、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。

> **注:**
>
> Linux VDAはXenDesktopバージョン7.0以前とは互換性がありません。

シトリックス レシーバー™

以下のバージョンのCitrix Receiverがサポートされています。

- シトリックス レシーバー for ユニバーサル Windows プラットフォーム バージョン 1.0
- Citrix Receiver for Windows バージョン4.8以降
- Citrix Receiver for Linux バージョン 13.5
- Citrix Receiver for Mac OSX バージョン 12.6
- シトリックス レシーバー フォー アンドロイド バージョン 3.11
- Citrix Receiver for iOS バージョン 7.2
- シトリックス レシーバー フォー クローム バージョン 2.5
- Citrix Receiver for HTML5 バージョン 2.5 (Access Gateway 経由のみ)

ハイパーバイザー

Linux VDAゲストVMのホストには、以下のハイパーバイザーがサポートされています。

- XenServer®
- VMware ESXおよびESXi
- マイクロソフト ハイパーV
- ニュータニックス AHV

ベアメタルホスティングもサポートされています。

> **ヒント:**
>
> サポートされているプラットフォームのリストについては、ベンダーのドキュメントを参照してください。

Active Directory統合パッケージ

Linux VDAは、以下のActive Directory統合パッケージおよび製品をサポートしています。

- サンバ ウィンバインド
- クエスト認証サービス v4.1 以降
- セントリファイ ダイレクトコントロール
- SSSD

> **ヒント:**
>
> サポートされているプラットフォームのリストについては、Active Directory 統合パッケージのベンダーのドキュメントを参照してください。

HDX™ 3D プロ

HDX 3D Pro をサポートするには、以下のハイパーバイザー、Linux ディストリビューション、および NVIDIA GRID™ GPU が必要です。

ハイパーバイザー

以下のハイパーバイザーがサポートされています。

- XenServer
- VMware ESX および ESXi
- ニュータニックス AHV

Linux ディストリビューション

以下の Linux ディストリビューションは HDX 3D Pro をサポートしています。

- Red Hat Enterprise Linux - ワークステーション 7.3
- レッドハット エンタープライズ リナックス - サーバー 7.3
- Red Hat Enterprise Linux - ワークステーション 6.9
- レッドハット エンタープライズ リナックス - サーバー 6.9
- Red Hat Enterprise Linux - ワークステーション 6.6
- レッドハット エンタープライズ リナックス - サーバー 6.6

- SUSE Linux Enterprise Desktop 12 サービスパック 2
- SUSE Linux Enterprise Server 12 サービスパック 2
- Ubuntu Linux デスクトップ 16.04
- Ubuntu Linux サーバー 16.04

GPU

以下のGPUがGPUパススルーでサポートされています:

- エヌビディア GTX750Ti
- エヌビディア GRID - Tesla M60
- NVIDIA GRID - K2

以下のGPUがvGPUでサポートされています:

- NVIDIA GRID の Tesla M60
- NVIDIA GRID の Tesla M10

インストール概要

Linux Virtual Delivery Agent (VDA) のインストールは、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同じ一般的な手順に従います。

1. インストールの準備をします。
2. ハイパーバイザーを準備します。
3. Linux 仮想マシン (VM) を Windows ドメインに追加します。
4. Linux VDA をインストールします。
5. Linux VDA を構成します。
6. XenApp または XenDesktop でマシンカタログを作成します。
7. XenApp® または XenDesktop でデリバリーグループを作成します。

バリエーションと特定のコマンドは、ディストリビューションごとに文書化されています。

デリバリーコントローラーの構成

XenDesktop 7.6およびそれ以前のバージョンでは、Linux VDAをサポートするために変更が必要です。これらのバージョンでは、ホットフィックスまたは更新スクリプトが必要です。インストールと検証の手順については、この記事で説明します。

Delivery Controller™の構成を更新する

XenDesktop 7.6 SP2の場合、Linux仮想デスクトップ用ブローカーを更新するためにホットフィックスアップデート2を適用します。ホットフィックスアップデート2は、こちらから入手できます:

CTX142438: ホットフィックスアップデート2 - Delivery Controller 7.6 (32ビット) 用 – 英語

XenDesktop 7.6 SP2より前のバージョンでは、**Update-BrokerServiceConfig.ps1**という名前のPowerShellスクリプトを使用してBroker Serviceの構成を更新できます。このスクリプトは、次のパッケージで入手できます:

- シトリックス-リナックスブイディーエー-スクリプト.zip

ファーム内のすべてのDelivery Controllerで、次の手順を繰り返します:

1. **Update-BrokerServiceConfig.ps1**スクリプトをDelivery Controllerマシンにコピーします。
2. ローカル管理者としてWindows PowerShellコンソールを開きます。
3. **Update-BrokerServiceConfig.ps1**スクリプトを含むフォルダーに移動します。
4. **Update-BrokerServiceConfig.ps1**スクリプトを実行します:

```
.\Update-BrokerServiceConfig.ps1
```

ヒント:

デフォルトでは、PowerShellはPowerShellスクリプトの実行を防止するように構成されています。スクリプトの実行に失敗した場合は、再試行する前にPowerShellの実行ポリシーを変更してください:

```
Set-ExecutionPolicy Unrestricted
```

Update-BrokerServiceConfig.ps1スクリプトは、Linux VDAで必要となる新しいWCFエンドポイントを使用してBroker Service構成ファイルを更新し、Broker Serviceを再起動します。スクリプトはBroker Service構成ファイルの場所を自動的に特定します。元の構成ファイルのバックアップは、ファイル名に**.prelinux**が付加されて同じディレクトリに作成されます。

これらの変更は、同じDelivery Controllerファームを使用するように構成されたWindows VDAのブローカー処理には影響しません。単一のControllerファームで、Windows VDAとLinux VDAの両方のセッションをシームレスに管理およびブローカー処理できます。

Delivery Controller の構成を確認する

必要な構成変更が Delivery Controller に適用されると、**EndpointLinux** 文字列が **%PROGRAMFILES%\\Citrix\\Broker\\Service\\BrokerService.exe.config** ファイルに 5 回表示されます。

Windows コマンドプロンプトから、ローカル管理者としてログオンして確認します。

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config
```

簡単インストール

簡単インストールは、Linux VDAバージョン7.13以降で正式にサポートされています。簡単インストールを使用すると、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できます。

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
RHEL 7.3	はい	はい	はい
RHEL 6.9	はい	はい	はい
RHEL 6.6	はい	はい	はい
CentOS 7.3	はい	はい	はい
ウブントゥ 16.04	はい	はい	はい
SUSE 12.2	はい	いいえ	はい

簡単インストールの使用

この機能を使用するには、次の手順を実行します。

1. 構成情報とLinuxマシンを準備します。
2. Linux VDA パッケージをインストールします。

   Citrix® の Web サイトにアクセスし、お使いの Linux ディストリビューションに基づいて適切な Linux VDA パッケージをダウンロードします。
3. Linux VDA のインストールを完了するために、ランタイム環境をセットアップします。

ステップ 1: 構成情報と Linux マシンを準備する

簡易インストール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
- Active Domain の FQDN - 完全修飾ドメイン名

> **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ます。
> - セッションを起動するには、X Window System 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ます。

ステップ 2: 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。

RHEL および CentOS ディストリビューションの場合:

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

Ubuntu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
```

SUSEディストリビューションの場合:

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

ステップ3：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パッケージをインストールした後、ctxinstall.shスクリプトを使用して実行環境を構成します。このスクリプトは、対話モードまたはサイレントモードで実行できます。

対話モード:

手動で構成するには、次のコマンドを実行し、各プロンプトで関連するパラメーターを入力します。

```
sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
```

サイレントモード:

サイレントモードで簡易インストールを使用するには、ctxinstall.sh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を示します。
- **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_ADINTEGRATIONWAY**=winbind \| sssd \| centrify – Active Directory統合方法を示します。
- **CTX_EASYINSTALL_USERNAME**=domain-user-name – ドメインユーザーの名前を示します。ドメインへの参加に使用されます。
- **CTX_EASYINSTALL_PASSWORD**=password – ドメインユーザーのパスワードを指定します。ドメインへの参加に使用されます。

ctxsetup.sh で使用される変数は次のとおりです。

- **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）をスペースで区切った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 Virtual Desktop 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。

- **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、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\>** に設定できます。
- **CTX_XDL_LDAP_LIST**=list-ldap-servers – Linux VDA は DNS をクエリして 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。不要な場合は、**\<none\>** に設定できます。
- **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 をクエリします。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。不要な場合は、**\<none\>** に設定できます。
- **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。

いずれかのパラメーターが設定されていない場合、インストールは対話モードに戻り、ユーザー入力が求められます。すべてのパラメーターが環境変数によってすでに設定されている場合、ctxinstall.sh スクリプトは回答を求めません。

サイレントモードでは、環境変数を設定してからctxinstall.shスクリプトを実行するために、次のコマンドを実行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_ADINTEGRATIONWAY=winbind | sssd | centrify

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_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_START_SERVICE=Y | N

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

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。Citrixでは、前のコマンドから**#\!/bin/bash**を最初の行として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_EASYINSTALL_HOSTNAME=host-name \
```

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


CTX_EASYINSTALL_NTPS=address-of-ntps \


CTX_EASYINSTALL_DOMAIN=domain-name \


CTX_EASYINSTALL_REALM=realm-name \


......


CTX_XDL_SEARCH_BASE=search-base-set \


CTX_XDL_START_SERVICE=Y \


/opt/Citrix/VDA/sbin/ctxinstall.sh
```

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。環境内のワークグループをカスタマイズするには、次の手順を実行します。

  a. Linux VDA マシン上に /tmp/ctxinstall.conf ファイルを作成します。

  b. ファイルに workgroup=\<your workgroup\> の行を追加します。

- 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。

- CentOS上のCentrifyの場合、簡易インストールはCentrify環境チェックツールである `adcheck` で失敗し、次のエラーを報告する可能性があります。

  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の特殊な構成が原因で発生します。この問題を解決するには、次の手順を実行します。

  a. Delivery Controller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**に正しいサブネットアドレスを追加します。

- ドメインに参加する方法として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2つあります。

  - 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。

    RHELの場合: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956>`

    CentOSの場合: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956>`

    スース：wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-suse10-x86_64.tgz?_ga=1.10831088.558673738.1478847956>`

    ウブントゥ: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956>`

- Centrifyパッケージをローカルディレクトリからフェッチします。Centrifyパッケージのディレクトリを指定するには、次の手順を実行します。

  a. Linux VDA サーバー上に /tmp/ctxinstall.conf ファイルが存在しない場合は作成します。

  b. ファイルに「centrifypkgpath=\<path name\>」の行を追加します。

  例:

```
cat /tmp/ctxinstall.conf

set “centrifypkgpath=/home/mydir”

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
```

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、この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への参加に失敗する

ドメインに参加しようとするとエラーが発生し、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で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で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、セッションを起動すると、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、サーバーOSマシンのコンソールもグレースクリーンを表示します。

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.



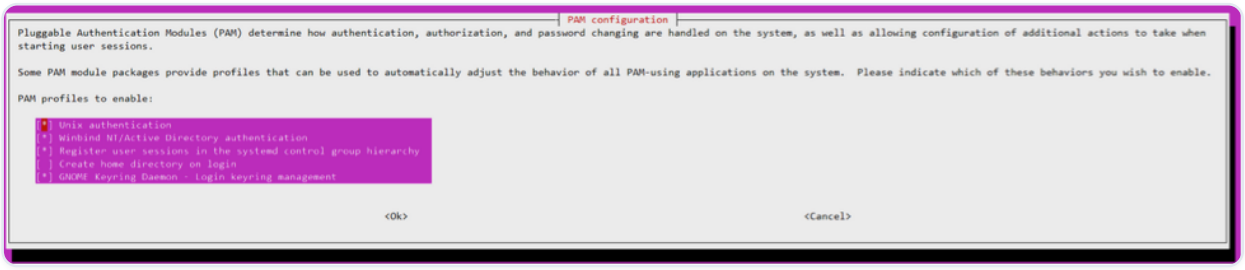
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting normally.
```

ヒント:

この問題の根本原因は、ドメイン管理者用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. 表示されるポップアップウィンドウで、「**Create home directory login**」が選択されていることを確認します。



dbusエラーによりセッションが起動できない、またはすぐに終了する

/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、Citrix 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 により SSHD がホームディレクトリにアクセスできない

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/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。

RHEL/CentOS 用 Linux Virtual Delivery Agent のインストール

手動インストールについてはこの記事の手順に従うか、自動インストールと構成には簡易インストールを使用できます。簡易インストールは、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。

> **注:**
>
> 簡易インストールは新規インストールにのみ使用してください。既存のインストールを更新するために簡易インストールを使用しないでください。

手順 1：VDA インストール用に RHEL 7/CentOS 7、RHEL 6/CentOS 6 を準備する

手順 1a：ネットワーク構成を確認する

Citrix® は、続行する前にネットワークが正しく接続され、構成されていることを推奨します。

手順 1b：ホスト名を設定する

> **注:**

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

> 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=`**ホスト名**

手順 1c：ホスト名にループバックアドレスを割り当てる

> **注:**

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

> 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、**/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 **ホスト名-FQDN ホスト名** 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** への他の参照を削除します。

> **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。

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 を実行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 を実行できない場合は、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 6.x およびそれ以前のリリースでは、クロック同期に NTP デーモン (`ntpd`) を使用しますが、RHEL 7.x のデフォルト環境では、代わりに新しい Chrony デーモン (`chronyd`) を使用します。両方のサービス間の構成および運用プロセスは似ています。

NTP サービスを構成する (RHEL 6/CentOS 6 のみ)

ルートユーザーとして、**/etc/ntp.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
```

典型的な展開では、時刻はローカルのドメインコントローラーから同期し、パブリックNTPプールサーバーから直接同期しないでください。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、NTPデーモンを再起動します。

```
sudo /sbin/service ntpd restart
```

Chronyサービスを構成する (RHEL 7/CentOS 7のみ)

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
```

典型的な展開では、時刻はローカルのドメインコントローラーから同期し、パブリックNTPプールサーバーから直接同期しないでください。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
```

手順1g: OpenJDKをインストールする

Linux VDAはOpenJDKに依存しています。通常、ランタイム環境はオペレーティングシステムのインストールの一部としてインストールされます。

正しいバージョンを確認してください:

- RHEL 7/CentOS 7:

```
sudo yum info java-1.8.0-openjdk
```

- RHEL 6/CentOS 6:

```
sudo yum info java-1.7.0-openjdk
```

プレパッケージされたOpenJDKは以前のバージョンである可能性があります。必要に応じて最新バージョンに更新してください:

- RHEL 7/CentOS 7:

```
sudo yum -y update java-1.8.0-openjdk
```

- RHEL 6/CentOS 6:

```
sudo yum -y update java-1.7.0-openjdk
```

「**~/.bashrc**」ファイルに次の行を追加して、**JAVA_HOME** 環境変数を設定します。

`export JAVA\_HOME=/usr/lib/jvm/java`

新しいシェルを開き、Java のバージョンを確認します。

```
java -version
```

> **ヒント:**
>
> 問題を回避するため、RHEL 6/CentOS 6 の場合は OpenJDK バージョン 1.7.0 または 1.8.0 のみを、RHEL 7/CentOS 7 の場合は OpenJDK バージョン 1.8.0 のみをインストールしたことを確認してください。システム上の他のすべての Java バージョンを削除してください。

手順 1h: PostgreSQL のインストール

Linux VDA には、RHEL 6 では PostgreSQL 8.4 以降、RHEL 7 では PostgreSQL 9.2 以降が必要です。

次のパッケージをインストールします。

```
sudo yum -y install postgresql-server



sudo yum -y install postgresql-jdbc
```

データベースを初期化し、マシン起動時にサービスが開始されるようにするには、次のインストール後の手順が必要です。このアクションにより、**/var/lib/pgsql/data** の下にデータベースファイルが作成されます。コマンドは PostgreSQL 8 と PostgreSQL 9 で異なります。

- RHEL 7 のみ: PostgreSQL 9

```
sudo postgresql-setup initdb
```

- RHEL 6 のみ: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
```

手順 1i: PostgreSQL の開始

マシン起動時にサービスを開始し、すぐにサービスを開始します。

- RHEL 7 のみ: PostgreSQL 9

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

- RHEL 6 のみ: PostgreSQL 8

```
sudo /sbin/chkconfig postgresql on



sudo /sbin/service postgresql start
```

次を使用して PostgreSQL のバージョンを確認します。

```
psql --version
```

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'
```

重要:

このリリースでは、gperftools-libs の新しい依存関係が追加されていますが、元のリポジトリには存在しません。`sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm` コマンドを使用して新しいリポジトリを追加します。

RHEL 6/CentOS 6 のみが影響を受けます。Linux VDA パッケージをインストールする前に、このコマンドを実行してください。

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応じて、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は、変更は不要です。

Citrix XenServer® での時刻同期の修正

XenServer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XenServer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。

一部のLinuxディストリビューションでは、XenServer 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XenServer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 - 時刻同期機能が無効になっており、それ以上の操作は不要です。

/proc/sys/xen/indepent_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するには、**/etc/sysctl.conf** ファイルを編集し、以下の行を追加します。

`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 の時刻同期機能を利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正確性を確保するため、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 VMware および XenServer とは異なります。そこでは 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の両方がシステムクロックを同期しようとする問題が発生します。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。

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仮想マシン (VM) をWindowsドメインに追加する

Linux VDAは、Active Directory (AD) ドメインにLinuxマシンを追加するためのいくつかの方法をサポートしています。

- サンバ Winbind
- 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

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が使用されている場合、セッションの起動が失敗する可能性があります。

サンバ ウィンバインド

必要なパッケージをインストールまたは更新します。

```
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 /sbin/chkconfig winbind on
```

Winbind認証を構成する

Winbindを使用して、Kerberos認証用にマシンを構成します。

```
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`

`authconfig`コマンドから返される、`winbind`サービスが起動に失敗したこと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`サービスを起動しようとしたときに発生する可能性があります。

/etc/samba/smb.confを開き、\[Global\]セクションの下に、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`

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メソッド設定は、マシンが最初にドメインに参加したときにWinbindにシステムキータブファイルを作成させます。

Windowsドメインへの参加

ドメインコントローラに到達可能である必要があり、コンピュータ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
```

REALMは、大文字のKerberosレルム名であり、**user**はコンピュータ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のPAMを構成する

デフォルトでは、Winbind PAMモジュール (pam_winbind) の構成は、Kerberosチケットキャッシュとホームディレクトリの作成を有効にしません。`/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。これらの変更には、Winbindデーモンの再起動が必要です。

```
sudo /sbin/service winbind restart
```

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。

/etc/krb5.confを開き、\[libdefaults\]セクションの下の次の設定をKEYRINGからFILEタイプに変更します。

`default_ccache_name = FILE:/tmp/krb5cc_%{uid}`

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にコンピュータオブジェクトを持つことを必要とします。

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構成の検証

KerberosがLinux VDAで正しく使用されるように構成されていることを確認するには、システムキー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、以下を使用して確認します。

```
sudo klist
```

以下を使用して、マシンのアカウントの詳細を調べます。

```
sudo net ads status
```

ユーザー認証の検証

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、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に使用されたことがないものとします。

```
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4：Linux VDAのインストール 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

Active Directory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

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=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、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時間チケットの有効期間より1時間短いです。チケットの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。そのドメインユーザーアカウントは以前に使用されたことがないものとします。

```
ssh localhost -l domain\\username



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
```

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
```

GnomeまたはKDEコンソールに直接ログオンすることで、同様のテストを実行できます。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/installation-overview/redhat.html#step-4-install-the-linux-vda)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エージェント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：

```
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。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/installation-overview/redhat.html#step-4-install-the-linux-vda)に進みます。

```
adinfo --test
```

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、Sambaでホストキータブを作成する
2. SSSD をセットアップする
3. NSS/PAM を構成する
4. Kerberos の構成を確認する
5. ユーザー認証を確認する

必要なソフトウェア

Active Directory プロバイダーは、SSSD バージョン 1.9.0 で初めて導入されました。以前のバージョンを使用している場合は、Active Directory で LDAP プロバイダーを構成するに記載されている手順に従ってください。

この記事に含まれる手順を使用する場合、次の環境がテストおよび検証済みです。

- RHEL 7.3 以降/CentOS 7.3 以降

- Linux VDA バージョン 1.3 以降

ドメインに参加し、Samba で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`、`Winbind`、または `Samba` を使用できます。

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 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。

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とKerberos認証のため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
```

REALMはKerberosレルム名（大文字）、**domain**はActive Directoryドメインの短い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、前述のコマンドに次の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`

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Kerberosレルム名（大文字）、**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。

- 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。

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

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。

sssd.conf のファイルの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`

NSS/PAMを構成する

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 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。シェルによる置換を防ぐため、ドル記号 (**$**) はバックスラッシュ (****) 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、以下を使用して確認します。

```
sudo klist
```

ユーザー認証を確認する

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するには、**getent**コマンドを使用します。

```
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、以前に使用されたことがないものです。

```
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、期限切れになっていないことを確認します。ドメイン参加の検証後、手順 4: Linux VDA のインストール に進みます。

```
klist
```

手順 4: Linux VDA のインストール

手順 4a: 古いバージョンのアンインストール

以前に古いバージョンの Linux VDA 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
```

2. パッケージをアンインストールします:

```
sudo rpm -e XenDesktopVDA
```

注:

以前の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:

バージョン 1.3 以降、インストールパスが変更されました。以前のリリースでは、インストールコンポーネントは **/usr/local/** にありました。新しい場所は **/opt/Citrix/VDA/** です。

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。

手順 4b: Linux VDA パッケージのダウンロード

Citrix Webサイトにアクセスし、お使いのLinuxディストリビューションに基づいて適切なLinux VDAパッケージをダウンロードします。

手順 4c: Linux VDA のインストール

`Yum` を使用して Linux VDA ソフトウェアをインストールします:

RHEL 7/CentOS 7 の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

RHEL 6.9の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

RHEL 6.6/CentOS 6.6の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.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。インストールする前に、次の依存関係を解決する必要があります。

RHEL 7/CentOS 7の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

RHEL 6.9の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

RHEL 6.6/CentOS 6.6の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

RHEL 7のRPM依存関係リスト:

```
postgresql-server >= 9.2



postgresql-jdbc >= 9.2
```

```
java-1.8.0-openjdk >= 1.8.0

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

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2
```

```
motif >= 2.3.4

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

openldap >= 2.4

cyrus-sasl >= 2.1
```

```
cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.6.0

gperftools-libs >= 2.4

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

RHEL 6.9のRPM依存関係リスト:

```
postgresql-jdbc >= 8.4


postgresql-server >= 8.4


java-1.7.0-openjdk >= 1.7.0


ImageMagick >= 6.5.4.7


GConf2 >= 2.28.0


system-config-firewall-base >= 1.2.27


policycoreutils-python >= 2.0.83


xorg-x11-server-utils >= 7.7


xorg-x11-xinit >= 1.0.9


ConsoleKit >= 0.4.1


dbus >= 1.2.24
```

```
dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2
```

```
cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1
```

```
rpmlib(PayloadFilesHavePrefix) <= 4.0-1


rpmlib(CompressedFileNames) <= 3.0.4-1


rpmlib(PayloadIsXz) <= 5.2-1
```

RHEL 6.6/CentOS 6.6のRPM依存関係リスト:

```
postgresql-jdbc >= 8.4


postgresql-server >= 8.4


java-1.7.0-openjdk >= 1.7.0


ImageMagick >= 6.5.4.7


GConf2 >= 2.28.0


system-config-firewall-base >= 1.2.27


policycoreutils-python >= 2.0.83


xorg-x11-server-utils >= 7.7
```

```
xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1
```

```
findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0
```

```
xorg-x11-server-Xorg >= 1.15

xorg-x11-server-Xorg < 1.16

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

手順4d：Linux VDAのアップグレード（オプション）

バージョン7.14および7.13からLinux VDAソフトウェアを`Yum`を使用してアップグレードできます。

RHEL 7/CentOS 7の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

RHEL 6.9の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

RHEL 6.6/CentOS 6.6の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

RPMパッケージマネージャーを使用してLinux VDAソフトウェアをアップグレードします:

RHEL 7/CentOS 7 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

RHEL 6.9 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

RHEL 6.6/CentOS 6.6 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

> **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。

ステップ 5: 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、ハイパーバイザーおよび VDA マシンに必須のグラフィックドライバーをインストールするための追加のインストール手順が必要です。

次を設定します。

1. シトリックス XenServer
2. ブイエムウェア ESX

選択したハイパーバイザーの手順に従ってください。

シトリックス XenServer:

この詳細セクションでは、Citrix XenServer への NVIDIA GRID ドライバーのインストールと構成について説明します。

VMware ESX の場合：

このガイドの情報に従って、VMware ESX 用の NVIDIA GRID ドライバーをインストールおよび構成してください。

VDA マシン:

各 Linux VM ゲストのドライバーをインストールおよび構成するには、次の手順に従います。

1. 開始する前に、Linux VMがシャットダウンされていることを確認してください。
2. XenCenter®で、GPUパススルーモードでGPUをVMに追加します。
3. RHEL VMを起動します。

NVIDIA GRIDドライバー用にマシンを準備するには、次のコマンドを実行します。

```
yum install gcc



yum install "kernel-devel-$(uname -r)"



systemctl set-default multi-user.target
```

NVIDIA GRIDドライバーをインストールするには、Red Hat Enterprise Linuxドキュメントの手順に従ってください。

> **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コードスニペットの画像(/en-us/linux-virtual-delivery-agent/7-15-ltsr/media/linux-vda-nvidia-smi-code-snippet.png)

カードの正しい構成を設定します。

`etc/X11/ctx-nvidia.sh`

大規模な解像度と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6：Linux VDAを構成する

パッケージをインストールした後、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

プロンプトに従って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に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、スクリプトは情報の入力を求めません。

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 Virtual Desktopサービスは、マシンの起動後に開始されます。値はデフォルトでYに設定されています。

- **CTX_XDL_ADD_FIREWALL_RULES** = **Y \| N** – Linux Virtual Desktop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 Virtual Desktop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** = **1 \| 2 \| 3 \| 4** – 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。使用するサポートされているActive Directory統合方法を指定します。
  - 1 – サンバ Winbind
  - 2 – クエスト認証サービス
  - 3 – セントリファイ ダイレクトコントロール
  - 4 – SSSD
- **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、Virtual Delivery Agent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。例: ad1.mycompany.com:389。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。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_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。

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=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set
```

```
export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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。Citrix では、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=1|2|3|4 \

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_START_SERVICE=Y|N \


/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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。

ステップ 7: 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、Linux VDA を制御するために、次のコマンドを実行できます。

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
```

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 の状態を確認する:

Linux VDA サービスの実行状態を確認するには:

```
sudo /sbin/service ctxvda status


sudo /sbin/service ctxhdx status
```

ステップ 8: XenApp または XenDesktop® で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 の方法と似ています。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場合とは異なる、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、サーバーOSオプション。
  - VDI専用デスクトップ配信モデルのデスクトップOSオプション。
- マシンが電源管理されていない設定になっていることを確認してください。
- Linux VDAではMCSがサポートされていないため、PVSまたは**別のサービスまたはテクノロジー**（既存のイメージ）展開方法を選択してください。
- 同じマシンカタログに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

ト型共有デスクトップ配信モデルが適用されます。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適用されます。

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、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9：XenApp®またはXenDesktopで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。

- 配信の種類として、デスクトップまたはアプリケーションを選択します。
- 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。

SUSE 用 Linux Virtual Delivery Agent をインストールする

手動インストールについてはこの記事の手順に従うか、自動インストールと構成にはeasy installを使用するかを選択できます。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。

> **注:**
>
> easy installは新規インストールにのみ使用してください。既存のインストールを更新するためにeasy installを使用しないでください。

ステップ1：インストールの準備

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すべての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
```

または、UIベースのYaSTツールを起動します：

```
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を構成する方法について説明します。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に基づいています。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DNSを構成する

1. YaSTネットワーク設定を開きます。

2. SLED 12のみ：**Global Options**タブで、**Network Setup Method**を**Wicked Service**に変更します。
3. **Hostname/DNS**タブを開きます。
4. **Change hostname via DHCP**のチェックを外します。
5. 「**ループバックIPにホスト名を割り当てる**」をチェックします。
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。

    - ホスト名 – マシンのDNSホスト名を追加します。
    - ドメイン名 – マシンのDNSドメイン名を追加します。
    - 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。

> **注:**
>
> Linux VDAは現在、NetBIOS名の切り捨てをサポートしていません。そのため、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。

マルチキャストDNSを無効にする

SLEDのみ、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。SLESではmDNSはデフォルトで有効になっていないため、何もする必要はありません。

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
```

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。

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 を実行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 を実行できない場合は、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。

1. YaST NTP Configuration を開き、**General Settings** タブを選択します。
2. Start NTP Daemon セクションで、**Now and on Boot** をオンにします。
3. 存在する場合は、**Undisciplined Local Clock (LOCAL)** 項目を選択し、**Delete** をクリックします。
4. **Add** をクリックして、NTP サーバーのエントリを追加します。
5. **Server Type** を選択し、**Next** をクリックします。
6. アドレスフィールドに NTP サーバーの DNS 名を入力します。このサービスは通常、Active Directory ドメインコントローラーでホストされます。
7. Options フィールドは変更しないでください。
8. NTP サービスに到達可能であることを確認するには、**Test** をクリックします。
9. 変更を保存するには、一連のウィンドウで**OK**をクリックします。

> **注:**
>
> SLES 12の実装では、AppArmorポリシーに関する既知のSUSEの問題により、NTPデーモンが起動に失敗する場合があります。詳細については、解決策を参照してください。

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ます。

- PostgreSQL
  - SLED/SLES 11: バージョン9.1以降
  - SLED/SLES 12: バージョン9.3以降
- OpenJDK 1.7.0
- OpenMotif ランタイム環境 2.3.1 以降
- カップス
  - SLED/SLES 11: バージョン1.3.7以降
  - SLED/SLES 12: バージョン1.6.0以降
- Foomaticフィルター
  - SLED/SLES 11: バージョン3.0.0以降

    - SLED/SLES 12: バージョン1.0.0以降

- ImageMagick
    - SLED/SLES 11: バージョン 6.4.3.6 以降
    - SLED/SLES 12: バージョン 6.8 以降

リポジトリを追加する

一部の必須パッケージは、すべてのSUSE Linux Enterpriseリポジトリで利用できるわけではありません。

- SLED 11: PostgreSQLはSLES 11で利用可能ですが、SLED 11では利用できません。
- SLES 11: OpenJDKとOpenMotifはSLED 11で利用可能ですが、SLES 11では利用できません。
- SLED 12: PostgreSQLはSLES 12で利用可能ですが、SLED 12では利用できません。ImageMagickはSLE 12 SDK ISOまたはオンラインリポジトリ経由で利用できます。
- SLES 12: 問題はありません。すべてのパッケージが利用可能です。ImageMagickはSLE 12 SDK ISOまたはオンラインリポジトリ経由で利用できます。

この問題を解決するには、インストール元のSLEの代替エディションのメディアから不足しているパッケージを入手してください。つまり、SLEDではSLESメディアから不足しているパッケージをインストールし、SLESではSLEDメディアから不足しているパッケージをインストールします。次のアプローチでは、SLEDとSLESの両方のISOメディアファイルをマウントし、リポジトリを追加します。

- SLED 11で、次のコマンドを実行します。

```
sudo mkdir -p /mnt/sles



sudo mount -t iso9660 path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /mnt/
sles



sudo zypper ar -f /mnt/sles sles
```

- SLES 11で、次のコマンドを実行します。

```
sudo mkdir -p /mnt/sled



sudo mount -t iso9660 path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /mnt/
sled



sudo zypper ar -f /mnt/sled sled
```

- SLED 12で、次のコマンドを実行します。

```
sudo mkdir -p /mnt/sles



sudo mount -t iso9660 path-to-iso/SLES-12-SP2-DVD-x86_64-GM-DVD1.iso /mnt/
sles



sudo zypper ar -f /mnt/sles sles
```

- SLED/SLES 12で、次のコマンドを実行します。

```
sudo mkdir -p /mnt/sdk



sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso /
mnt/sdk



sudo zypper ar -f /mnt/sdk sdk
```

Kerberosクライアントをインストールする

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、使用する 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 をインストールする

Linux VDA は OpenJDK 1.7.0 に依存しています。

ヒント:

問題を防ぐため、OpenJDK バージョン 1.7.0 のみをインストールしていることを確認してください。システム上の他のすべての Java バージョンを削除してください。

- **SLED:**

1. SLED では、Java ランタイム環境は通常、オペレーティングシステムとともにインストールされます。インストールされているかどうかを確認してください。

   ```
   sudo zypper info java-1_7_0-openjdk
   ```

2. ステータスが「期限切れ」と報告された場合は、最新バージョンに更新してください。

   ```
   sudo zypper update java-1_7_0-openjdk
   ```

3. Java のバージョンを確認してください。

   ```
   java -version
   ```

- **SLES:**

1. SLES で、Java ランタイム環境をインストールします。

   ```
   sudo zypper install java-1_7_0-openjdk
   ```

2. Java のバージョンを確認してください。

```
java -version
```

PostgreSQL をインストールする

- SLED/SLES 11 で、パッケージをインストールします。

```
sudo zypper install libecpg6


sudo zypper install postgresql-init


sudo zypper install postgresql


sudo zypper install postgresql-server


sudo zypper install postgresql-jdbc
```

データベースサービスを初期化し、マシンの起動時に PostgreSQL が開始されるようにするために、インストール後の手順が必要です。

```
sudo /sbin/insserv postgresql


sudo /etc/init.d/postgresql restart
```

- SLED/SLES 12 で、パッケージをインストールします。

```
sudo zypper install postgresql-init


sudo zypper install postgresql-server
```

```
sudo zypper install postgresql-jdbc
```

データベースサービスを初期化し、マシンの起動時に PostgreSQL が開始されるようにするために、インストール後の手順が必要です。

```
sudo systemctl enable postgresql


sudo systemctl restart postgresql
```

データベースファイルは /var/lib/pgsql/data にあります。

リポジトリを削除する

依存パッケージがインストールされたので、以前に設定した代替エディションのリポジトリを削除し、メディアをアンマウントできます。

- SLED 11 で、パッケージを削除するコマンドを実行します。

```
sudo zypper rr sles


sudo umount /mnt/sles


sudo rmdir /mnt/sles
```

- SLES 11 で、パッケージを削除するコマンドを実行します。

```
sudo zypper rr sled


sudo umount /mnt/sled
```

```
sudo rmdir /mnt/sled
```

- SLED 12 で、パッケージを削除するコマンドを実行します。

```
sudo zypper rr sles



sudo umount /mnt/sles



sudo rmdir /mnt/sles
```

- SLED/SLES 12 で、パッケージを削除するコマンドを実行します。

```
sudo zypper rr sdk



sudo umount /mnt/sdk



sudo rmdir /mnt/sd
```

手順 2：ハイパーバイザー用に Linux VM 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応じて、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 XenServer® での時刻同期の修正

XenServer 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 XenServer の両方がシステムクロックを管理しようとする問題が発生します。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は NTP と同期させる必要があります。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。

一部の Linux ディストリビューションでは、XenServer 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 XenServer 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 - 時間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 - 時間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/indepent_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** を書き込んで時間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。

```
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 での時間同期の修正

Hyper-V Linux Integration Services がインストールされている Linux VM は、Hyper-V の時間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、**統合サービス**を選択します。
3. **時刻の同期**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間同期が無効になっている VMware や XenServer とは異なります。Hyper-V の時間同期は、NTP の時間同期と共存し、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の両方がシステムクロックを同期しようとする問題が発生します。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はNTPと同期させる必要があります。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。

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：Linux仮想マシン（VM）をWindowsドメインに追加する

Linux VDAは、LinuxマシンをActive Directory (AD) ドメインに追加するためのいくつかの方法をサポートしています。

- 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

選択した方法に基づいて指示に従ってください。

サンバ・ウィンバインド

Windows ドメインに参加

ドメインコントローラーに到達可能であり、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 Windows ドメインメンバーシップを開きます。
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。
    - **Linux認証にSMB情報も使用する** 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った場合、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、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の資格情報を入力し、**OK** をクリックします。
6. 成功を示すメッセージが表示されます。
7. 一部のsambaおよびkrb5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。

YaSTは、これらの変更に一部のサービスまたはマシンの再起動が必要であることを示している場合があります。マシンを再起動することをお勧めします。

```
su -



reboot
```

SLED/SLES 12 のみ: Kerberos 資格情報キャッシュ名のパッチ適用

SLED/SLES 12 では、デフォルトの Kerberos 資格情報キャッシュ名の指定が、通常の **FILE:/tmp/krb5cc_%{uid}** から **DIR:/run/user/%{uid}/krb5cc** に変更されました。この新しい DIR キャッシュ方法は Linux VDA と互換性がないため、手動で変更する必要があります。root ユーザーとして、**/etc/krb5.conf** を編集し、設定されていない場合は **\[libdefaults\]** セクションに次の設定を追加します。

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

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
```

マシンアカウントの詳細を調べるには、次を使用します。

```
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、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
```

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して実行できます。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/installation-overview/suse.html#step-4-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ドメインユーザーのログオン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小さ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、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、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。そのドメインユーザーアカウントは以前に使用されたことがないものとします。

```
ssh localhost -l domain\\username



id -u
```

id -u コマンドによって返される uid に対して、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で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。ドメイン参加の検証後、(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/installation-overview/suse.html#step-4-install-the-linux-vda)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状態で、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 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。Centrify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：

```
su -



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、(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/installation-overview/suse.html#step-4-install-the-linux-vda)に進みます。

ステップ4：Linux VDAのインストール

ステップ4a：古いバージョンのアンインストール

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。

1. Linux VDAサービスを停止します。

   ```
   sudo /sbin/service ctxvda stop



   sudo /sbin/service ctxhdx stop
   ```

2. パッケージをアンインストールします。

   ```
   sudo rpm -e XenDesktopVDA
   ```

重要:

以前の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。

手順4b：Linux VDAパッケージをダウンロードする

Citrix Webサイトにアクセスし、お使いのLinuxディストリビューションに基づいて適切なLinux VDAパッケージをダウンロードします。

手順4c：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。

SUSE 12の場合：

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

SUSE 11の場合：

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.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。その前に、以下の依存関係を解決してください。

SUSE 12の場合：

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

SUSE 11の場合：

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
```

Step 4d: Linux VDA のアップグレード (オプション)

RPM パッケージマネージャーを使用して、バージョン 7.14 および 7.13 から Linux VDA ソフトウェアをアップグレードできます。

SUSE 12 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

SUSE 11 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
```

SUSE 12 の RPM 依存関係リスト:

```
postgresql-server >= 9.3


postgresql-jdbc >= 9.2


java-1.7.0-openjdk >= 1.7.0


ImageMagick >= 6.8


dbus-1 >= 1.8.8


dbus-1-x11 >= 1.8.8


libXpm4 >= 3.5.11


libXrandr2 >= 1.4.2


libXtst6 >= 1.2.2
```

```
motif >= 2.3

pam >= 1.1.8

bash >= 4.2

findutils >= 4.5

gawk >= 4.1

sed >= 4.2

cups >= 1.6.0

cups-filters-foomatic-rip >= 1.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1
```

```
libxml2 >= 2.9


python-requests >= 2.8.1


rpmlib(PayloadFilesHavePrefix) <= 4.0-1


rpmlib(CompressedFileNames) <= 3.0.4-1


rpmlib(PayloadIsLzma) <= 4.4.6-1
```

SUSE 11 の RPM 依存関係リスト:

```
postgresql-server >= 9.1.


postgresql-jdbc >= 9.1


java-1_7_0-openjdk >= 1.7.0.6


ImageMagick >= 6.4.3.6


ConsoleKit >= 0.2.10


dbus-1 >= 1.2.10
```

```
dbus-1-x11 >= 1.2.10

xorg-x11-libXpm >= 7.4

xorg-x11-libs >= 7.4

openmotif-libs >= 2.3.1

pam >= 1.1.5

libdrm >= 2.4.41

libpixman-1-0 >= 0.24.4

Mesa >= 9.0

openssl >= 0.9.8j

xorg-x11 >= 7.4

xorg-x11-fonts-core >= 7.4
```

```
xorg-x11-libXau >= 7.4

xorg-x11-libXdmcp >= 7.4

bash >= 3.2

findutils >= 4.4

gawk >= 3.1

sed >= 4.1

cups >= 1.3.7

foomatic-filters >= 3.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1
```

```
libxml2 >= 2.7

python-requests >= 2.0.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1
```

重要:

アップグレード後、Linux VDA マシンを再起動します。

手順 5: Linux VDA の構成

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に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への登録に使用する、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 Virtual Desktopサービスは、マシンの起動後に開始されます。この値はデフォルトでYに設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES = Y \| N** – Linux Virtual Desktop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 Virtual Desktop用に、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 = 1 \| 2 \| 3 \| 4** – 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。使用するサポートされているActive Directory統合方法を指定します。
  - 1 – サンバ Winbind
  - 2 – Quest 認証サービス
  - 3 – セントリファイ ダイレクトコントロール
  - 4 – SSSD
- **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技術のセットである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、Virtual Delivery Agent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をクエリします。DNSがLDAPサービスレコードを提供できない場合、LDAPポートを含むスペース区切りのLDAP FQDNのリストを提供できます。例：ad1.mycompany.com:389。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をクエリします。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。この変数はデフォルトで**\<none\>**に設定されています。
- **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。

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=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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。Citrix では、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=1|2|3|4 \

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_START_SERVICE=Y|N \
```

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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。

手順 6：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 を起動します。

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
```

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7：XenAppまたはXenDesktop®で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、Server OSオプション。
  - VDI専用デスクトップ配信モデルの場合は、Desktop OSオプション。
- マシンが電源管理されていないことを確認してください。
- Linux VDAではMCSがサポートされていないため、PVSまたは**別のサービスまたはテクノロジー**（既存のイメージ）の展開方法を選択してください。
- 同じマシンカタログに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、同等のホスト型共有デスクトップ配信モデルが適用されます。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適用されます。

> **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8：XenApp®またはXenDesktopで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、次の制限が適用されます。

- 配信の種類には、デスクトップまたはアプリケーションを選択します。
- 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。

> **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。

Ubuntu 用 Linux Virtual Delivery Agent のインストール

手動インストールについてはこの記事の手順に従うか、自動インストールと構成には簡易インストールを使用するかを選択できます。簡易インストールは時間と労力を節約し、手動インストールよりもエラーが発生しにくくなります。

> **注:**
>
> 簡易インストールは新規インストールにのみ使用してください。既存のインストールを更新するために簡易インストールを使用しないでください。

ステップ 1: VDA インストールのために Ubuntu を準備する

ステップ 1a: ネットワーク構成を確認する

続行する前に、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。

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ように、**/etc/hosts** ファイルの次の行を、最初の2つのエントリとして FQDN とホスト名を含むように変更します。

```
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。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、および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、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**サーバーまたは**プール**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: OpenJDKをインストールする

Linux VDAはOpenJDKに依存します。通常、ランタイム環境はオペレーティングシステムのインストールの一部としてインストールされます。次のコマンドでインストールされているかどうかを確認します。

```
sudo apt-get install -y default-jdk
```

ステップ1i: PostgreSQLをインストールする

Linux VDAは、Ubuntu 16.04でPostgreSQLバージョン9.xを必要とします。

```
sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

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

```
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 cups
```

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応じて、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 XenServer®での時刻同期の修正

XenServer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XenServer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。

一部のLinuxディストリビューションでは、XenServer 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XenServer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 - 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/indepent_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
```

この変更を再起動後も永続的に適用するには、**/etc/sysctl.conf file** 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 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正確性を保つために、この機能は NTP サービスと並行して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、**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 XenServer 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の両方がシステムクロックを同期しようとするため、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仮想マシン（VM）をWindowsドメインに追加する

Linux VDAは、LinuxマシンをActive Directory (AD) ドメインに追加するためのいくつかの方法をサポートしています。

- 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

選択した方法に基づいて指示に従ってください。

サンバ ウィンバインド

必要なパッケージをインストールまたは更新する

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

Winbindデーモンをマシンの起動時に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
```

Kerberosの構成

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。

```
[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**プロパティは、**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認証の構成

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は大文字のKerberosレルム名です。

nsswitchの構成

`/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 REALM -U user
```

ここで、**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。

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 authentication** と **Create home directory on login** の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たままになります。

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。

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。Kerberos `kinit` コマンドを実行して、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
```

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、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、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、以前に使用されたことがないものとします。

```
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ていることを確認します。

```
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、手順4：Linux VDAのインストールに進みます。

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再試行してください。

Quest認証サービス

ドメインコントローラーでQuestを構成する

Active Directory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**をチェックします。
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で使用される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**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デーモンの構成

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も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ドメインへの参加

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任意のドメインユーザーです。ドメイン名とは、ドメインのDNS名です（例: example.com）。

ドメインメンバーシップの確認

Delivery Controllerは、WindowsまたはLinuxを問わず、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、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。そのドメインユーザーアカウントは以前に使用されたことがないものとします。

```
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4: 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状態で、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任意の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 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。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:

```
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動かない場合、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 4: 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、次の設定を行います:

```
[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` プロパティは、`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 keytab 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` の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:**

adcli をインストールする:

必要なパッケージをインストールします。

```
sudo apt-get install adcli
```

adcli を使用してドメインに参加する:

古いシステム keytab 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 にとって必要です。

システム keytab を確認する:

adcli ツールの機能は限られており、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は提供されていません。システム keytab ファイルが作成されていることを確認するための最良の代替策は次のとおりです。

```
sudo klist -ket
```

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:

パッケージをインストールする:

```
sudo apt-get install samba
```

samba を構成する:

`/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。

samba を使用して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、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 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。

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 update 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は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` が 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** プロパティは、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。

ヒント:

これらの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っていることを要求します。

adcliを使用してドメインメンバーシップを確認する:

次のコマンドを実行して、ドメイン情報を表示します。

```
sudo adcli info domain-dns-name
```

Sambaを使用してドメインメンバーシップを確認する:

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、システムキータブ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
```

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、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。そ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ないものです。

```
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。ドメイン参加の検証後、手順4：Linux VDAのインストールに進みます。

手順4：Linux VDAのインストール

手順4a：Linux VDAパッケージのダウンロード

CitrixのWebサイトにアクセスし、お使いのLinuxディストリビューションに基づいて適切なLinux VDAパッケージをダウンロードします。

手順4b：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。

```
sudo dpkg -i xendesktopvda_7.15.0.404-1.ubuntu16.04_amd64.deb
```

UbuntuのDebian依存関係リスト：

```
postgresql >= 9.5


libpostgresql-jdbc-java >= 9.2


default-jdk >= 2:1.8


imagemagick >= 8:6.8.9.9
```

```
ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42
```

```
libsasl2-modules-gssapi-mit >= 2.1.~

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~
```

手順4c：Linux VDAの構成

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。

プロンプトに従って手動でスクリプトを実行することも、事前構成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への登録に使用する、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 Virtual Desktop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 Virtual Desktop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 Virtual Desktop用に、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 = 1 \| 2 \| 3 \| 4** – 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。使用するサポートされているActive Directory統合方法を指定します。
  - 1 – サンバ・ウィンバインド
  - 2 – クエスト・オーセンティケーション・サービス
  - 3 – セントリファイ・ダイレクトコントロール
  - 4 – SSSD
- **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、Virtual Delivery Agent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。例: ad1.mycompany.com:389。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_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。

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=1|2|3|4



export CTX_XDL_HDX_3D_PRO=Y|N



export CTX_XDL_VDI_MODE=Y|N
```

```
export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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。Citrix では、最初の行に **#\!/bin/bash** を指定して、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=1|2|3|4 \

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_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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 5: 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
```

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6：XenAppまたはXenDesktop®で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。
  - ホスト型共有デスクトップ配信モデルの場合は、Server OSオプション。
  - VDI専用デスクトップ配信モデルの場合は、Desktop OSオプション。
- マシンが電源管理されていないことを確認します。
- MCSはLinux VDAでサポートされていないため、PVSまたは**別のサービスまたはテクノロジー**（既存のイメージ）の展開方法を選択してください。
- 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、同等のホスト型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7：XenApp®またはXenDesktopで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。

- 配信タイプについては、「**デスクトップ**」を選択します。Ubuntu 用 Linux VDA はアプリケーション配信をサポートしていません。
- 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。
- 配信グループと、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。

Linux VDA の設定

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述します。

NISとActive Directoryを統合する

この記事では、SSSDを使用してLinux VDA上でNISをWindows Active Directory (AD)と統合する方法について説明します。Linux VDAはCitrix XenApp & XenDesktopのコンポーネントと見なされます。その結果、Windows AD環境に密接に適合します。

ADの代わりにNISをUIDおよびGIDプロバイダーとして使用する場合、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の両方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、RHEL/CentOS用Linux Virtual Delivery Agentのインストール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用Linux Virtual Delivery Agentのインストール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、システムに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とNSSの両方のモジュールを提供し、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ー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。

必要なソフトウェア

ADプロバイダーはSSSDバージョン1.9.0で初めて導入されました。

この記事に含まれる手順を使用する場合、以下の環境がテストおよび検証されています。

- RHEL 7.3以降/CentOS 7.3以降
- Linux VDAバージョン1.3以降

NISとADを統合する

NISをADと統合するには、次の手順を実行します。

1. Linux VDAをNISクライアントとして追加する
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(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/configuration/integrate-nis-with-active-directory.html#join-the-domain-and-create-a-host-keytab-using-samba)
3. SSSD をセットアップする(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/configuration/integrate-nis-with-active-directory.html#set-up-sssd)
4. NSS/PAM を構成する(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/configuration/integrate-nis-with-active-directory.html#configure-nsspam)
5. Kerberos の構成を確認する(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/configuration/integrate-nis-with-active-directory.html#verify-the-kerberos-configuration)
6. ユーザー認証を確認する(/ja-jp/linux-virtual-delivery-agent/7-15-ltsr/configuration/integrate-nis-with-active-directory.html#verify-user-authentication)

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 サービスを構成します。

```
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。

ドメインに参加し、Samba を使用してホストキー・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ます。以下に例を挙げます。

- アドクリ
- レルムディー
- ウィンバインド
- サンバ

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。

ドメインに参加し、Samba を使用してホストキー・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
```

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`

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。

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 の構成例（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 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.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`

NSS/PAM の構成

RHEL/CentOS:

authconfig を使用して SSSD を有効にします。**oddjob-mkhomedir** をインストールして、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します。

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update



sudo systemctl start sssd



sudo systemctl enable sssd
```

ヒント:

Linux VDA の設定を構成する際、SSSD には Linux VDA クライアント用の特別な設定がないことを考慮してください。**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。

Kerberos の構成を確認する

Linux VDA で 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、以下を使用して確認します。

```
sudo klist -ke
```

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、および NSS が機能するかどうかを確認します。

```
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に使用されたことがないものです。

```
sudo 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
```

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。

ヒント:

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。

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。この問題に対処するため、Citrixはアプリとデスクトップの配信用に個別のデリバリーグループを作成することを推奨しています。

注:

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。

トラブルシューティング

公開されたアプリケーションの起動に2分以上かかり、ウィンドウがシームレスモードで表示されないという問題に遭遇する場合があります。この問題が発生した場合は、Linux VDAとStoreFrontの両方でシームレスモードが有効になっていることを確認してください。

Linux VDAでシームレスモードが有効になっているかを確認するコマンド：

```
sudo /opt/Citrix/VDA/bin/ctxreg list -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix"  |  grep
"SeamlessEnabled"
```

「SeamlessEnabled = 0x00000000」と表示される場合、シームレスモードは無効になっています。有効にするには、次のコマンドを実行します：

```
sudo /opt/Citrix/VDA/bin/ctxreg update  -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix"  -v
"SeamlessEnabled" -d "0x00000001"
```

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。

- StoreFrontでシームレスモードが無効になっているにもかかわらず、Linux VDAで有効になっている場合、非シームレス公開アプリケーションは起動に失敗します。Linux VDAとStoreFrontの両方でシームレスモードを同時に有効または無効にしてください。
- 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。

- 現在、シームレスモードは以下のウィンドウマネージャーをサポートしています：Mutter (CentOS7.3\RHEL7.3\SUSE12.2)、Metacity (CentOS6.6\RHEL6.6\SUSE 11.4)、および Compiz (Ubuntu 16.04)。Kwinおよびその他のウィンドウマネージャーはサポートされていません。お使いのウィンドウマネージャーがサポートされているものに設定されていることを確認してください。
- 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/index.php/Qt>` の記事を参照してください。
- 同じICA®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は、同じグループにまとめられます。この問題を解決するには、タスクバーのプロパティでタスクバーボタンを結合しないように設定してください。

印刷

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。お使いのLinuxディストリビューションに基づいて、次のコマンドを実行します。

RHEL 7の印刷サポート:

```
sudo yum –y install cups



sudo yum -y install foomatic-filters
```

RHEL 6の印刷サポート:

```
sudo yum –y install cups



sudo yum -y install foomatic
```

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。クライアント側のデフォルトプリンターのみがLinux VDAセッションにマップされます。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る必要があります。以下を考慮してください。

- 公開デスクトップの場合:

  `CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`

- 公開アプリケーションの場合:

  `CitrixUniversalPrinter:$CLIENT_NAME:app$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

印刷できない

印刷が正しく機能しない場合は、確認すべきさまざまな項目があります。印刷デーモン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。印刷デーモンが実行されていることを確認してください。

```
ps –ef | grep ctxlpmngt
```

ctxlpmngtプロセスが実行されていない場合は、コマンドラインから**ctxlpmngt**を手動で開始します。それでも印刷が機能しない場合は、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用であり、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、次のように確認できます。

```
service ctxcups status
```

CUPS印刷時の追加ログ

Linux VDAのコンポーネントの1つとして、印刷コンポーネントのログを取得する方法は、他のコンポーネントと同様です。

RHELの場合、CUPSサービスファイルを構成するためにいくつかの追加手順が必要です。そうしないと、一部のログが**hdx.lo**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:

この設定は、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のものです。通常、この設定はCUPSのセキュリティを破るため、推奨されません。

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設定が利用可能で、**~/.CtxlpProfile$CLIENT_NAME** 設定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**、および **drivertype** の各フィールドは、マッピング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、**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。プリンターの現在のモデル名は、**lpinfo** コマンドを使用して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、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。

例えば、/home/tester/NATIVE_PRINTER_DRIVER.ppd の下に **ppd driver** がある場合：

```
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）。ネイティブプリンタードライバーが利用できない場合、ドライバータイプを構成できます。

例えば、クライアントのデフォルトプリンタードライバータイプがPCL5の場合：

```
drivertype=pcl5
```

出力サイズがゼロになる

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タイプ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タイプが正しい場合、以下の手順を実行して問題を特定できます。

この問題を特定するには：

1. ICA®セッションデスクトップにログオンします。
2. vi ~/.CtxlProfile$CLIENT_NAME
3. Linux VDA上の保存プールファイルに次のフィールドを追加します。

   ```
   deletespoolfile=no
   ```

4. ログオフして再度ログオンし、構成の変更をロードします。
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、それは問題を示しています。詳細なガイダンスについては、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ます。

   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、スプールファイルをクライアントにコピーし、クライアント側のプリンターを使用して印刷します。この手順を完了した後、他のプリンタードライバーを使用してテストします。
8. マップされたプリンターを別のサードパーティ製プリンタードライバーに変更するには、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:$ClientName:app/dek$SESSION_ID** を選択し、**プリンターの変更** をクリックします。この操作には管理者権限が必要です。

   d. cups-ctx接続を維持し、 をクリックしてプリンタードライバーを変更します。

   e. ページで、Citrix UPDドライバー（例：Citrix Universal™ Driver Postscript）の代わりに、他のPostScript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このサードパーティ製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。低速な接続では、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、選択したPDFビューアを使用してPDFを開き、選択した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有効にしてください。

- **クライアントプリンターリダイレクト**（デフォルトで有効）
- **PDFユニバーサルプリンターの自動作成**（デフォルトで無効）

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**印刷**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。

グラフィックの構成

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のセクションを参照してください。

構成パラメーター

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Thinwireには、**ctxreg**ユーティリティで調整できるグラフィック関連の構成パラメーターがいくつかあります。

Thinwire Plusを有効にする方法

Thinwire Plusは、標準VDAと3D Proの両方でデフォルトで有効になっています。

H.264を有効にする方法

オペレーティングシステムの要件に加えて、H.264にはCitrix Workspaceアプリ（旧Citrix Receiver）のバージョンの最小要件があります。クライアントが要件を満たさない場合、Thinwire Plusにフォールバックします。

オペレーティングシステム	H.264の最小要件
ウィンドウズ	3.4以降
マック オーエス テン	11.8以降
リナックス	13.0以降
アンドロイド	3.5
iOS	5.9
クローム OS	1.4

Citrix Workspace app の最新の機能マトリックスは `<https://docs.citrix.com/ja-jp/citrix-workspace-app/citrix-workspace-app-feature-matrix.html>` で入手できます。

VDA で H.264 エンコーディングをアドバタイズするには、次のコマンドを実行します。

```
sudo ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"AdvertiseH264" -d "0x00000001" --force
```

HDX™ 3D Pro でハードウェアエンコーディングを有効にする方法

HDX 3D Pro の場合、**AdvertiseH264** 設定はソフトウェア H.264 エンコーディングのみを有効にします。 ハードウェアエンコーディングを有効にするには、次のコマンドを実行します。

```
sudo ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"HardwareEncoding" -d "0x00000001" --force
```

注:

`ctxreg command can't be found` エラーが発生した場合は、完全なパスを指定して `ctxreg` コマンドを使用してください。たとえば、`sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" –force` の代わりに `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" –force` を使用します。

低帯域幅向けに Thinwire Plus を調整する方法

- MaxColorDepth

  ```
  Default 0x20, type DWORD
  ```

  このオプションは、Thinwire プロトコルを介してクライアントに転送されるグラフィックの色深度を指定します。

  帯域幅を節約するには、0x10 (シンプルなグラフィックに推奨される色深度を表します) または 0x8 (実験的な低帯域幅モード) に設定します。

- 品質

  視覚的な品質

  ```
  Default: 0x1(medium), type: DWORD, valid values: 0x0(low), 0x1(medium), 0x2(high), 0x3(build to lossless), 0x4 always lossless.
  ```

  帯域幅を節約するには、Quality を 0x0 (低) に設定します。

- その他のパラメーター

  - TargetFPS

    ターゲットフレームレート

    ```
    Default: 0x1e (30), Type: DWORD
    ```

  - MinFPS

目標最小フレームレート

```
Default: 0xa (10), Type: DWORD
```

- MaxScreenNum

  クライアントが持つことができるモニターの最大数

  ```
  Default: 0x2, Type: DWORD
  ```

  標準VDAの場合、最大10まで設定できます。3D Proの場合、許可される最大値は4です。

トラブルシューティング

使用中のエンコードを確認する

H.264エンコードが使用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（**1**はH.264を意味し、**0**はTW+を意味します）。

```
sudo ctxreg dump | grep H264
```

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 "H264" -d "0x00000001" --force`

`create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force`

3D Proでハードウェアエンコードが使用されているか確認する

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、**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
```

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`

別の方法として、**nvidia-smi**コマンドを使用します。ハードウェアエンコードが使用されている場合、出力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 |

+-----------------------------------------------------------------------------
----+
```

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** と同様の名前で保存されます。

既知の問題と制限事項

vGPU の場合、XenServer® 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。

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

NVENC API は 8Q 以外の vGPU プロファイルではサポートされていません

NVIDIA Tesla M60 カードの 8Q 以外の vGPU プロファイルは CUDA をサポートしていないため、NVENC API および Citrix® 3D Pro ハードウェアエンコーディングは利用できません。

NVIDIA K2 グラフィックカードはパススルーモードで YUV444 ハードウェアエンコーディングをサポートしていません

これは NVIDIA K2 グラフィックカードの制限です。

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の制限です。

Citrix Receiver ウィンドウのサイズ変更時に一部の 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 Receiver ウィンドウの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 **lightgl.js** は「`Rendering to this texture is not supported (incomplete frame buffer)`」というエラーを発生させる可能性があります。

非GRID 3Dグラフィック

概要

この機能強化により、Linux VDAはNVIDIA GRID 3Dカードだけでなく、非GRID 3Dカードもサポートします。

インストール

非GRID 3Dグラフィック機能を使用するには、以下を行う必要があります。

- 前提条件としてXDamageをインストールします。通常、XDamageはXServerの拡張機能として存在します。
- 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、「手順3：インストールを完了するためのランタイム環境のセットアップ」を参照してください。

構成

Xorg構成ファイル

3Dカードドライバーが NVIDIA 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。

その他の種類の3Dカード

3Dカードドライバーが NVIDIA ではない場合、`/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、以下を実行します。

1. ***driver_name***を実際のドライバー名に置き換えます。

   例えば、ドライバー名が `intel` の場合、設定ファイル名を `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。

   各テンプレート設定ファイルには、「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。このセクションにはビデオドライバー情報が記述されています。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. 設定情報については、製造元が提供する3Dカードガイドを参照してください。ネイティブ設定ファイルを生成できます。Linux VDA ICA®セッションを使用していないときに、ネイティブ設定ファイルを使用してローカル環境で3Dカードが動作することを確認してください。

   b. ネイティブ設定ファイルの「Device」セクションを**ctx-driver_name-1.conf**にコピーします。
3. Linux VDAがステップ1で設定された設定ファイル名を認識できるように、以下のコマンドを実行してレジストリキーを設定します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_SZ" -v "DriverName" -d "intel" --force
```

非GRID 3Dグラフィック機能を有効にする

非GRID 3Dグラフィック機能はデフォルトで無効になっています。XDamageEnabledを1に設定することで、以下のコマンドを実行して有効にできます。

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

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、すべての設定が正しい場合、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に設定してください。

ハードウェアエンコーディングが機能しない

この機能はソフトウェアエンコーディングのみをサポートしています。

ポリシーを構成する

インストール

インストール記事に従ってLinux VDAを準備します。

依存関係

Linux VDAパッケージをインストールする前に、これらの依存関係をインストールしてください。

RHEL/CentOS:

```
sudo yum -y install openldap



sudo yum -y install libxml2
```

```
sudo yum -y install cyrus-sasl
```

```
sudo yum -y install cyrus-sasl-gssapi
```

SLES/SELD:

```
sudo zypper install openldap2
```

```
sudo zypper install libxml2
```

```
sudo zypper install cyrus-sasl
```

```
sudo zypper install cyrus-sasl-gssapi
```

ウブントゥ:

```
sudo apt-get install -y libldap-2.4-2
```

```
sudo apt-get install -y libsasl2-2
```

```
sudo apt-get install -y libsasl2-modules-gssapi-mit
```

構成

Citrix Studioでのポリシー設定

Citrix Studioでポリシーを設定するには、次の手順を実行します。

1. **Citrix Studio**を開きます。
2. **ポリシー**パネルを選択します。
3. **ポリシーの作成** をクリックします。
4. ポリシーサポートリストに従ってポリシーを設定します。

VDA上のLDAPサーバー設定

Linux VDA上のLDAPサーバー設定は、単一ドメイン環境ではオプションですが、複数ドメインおよび複数フォレスト環境では必須です。この設定は、これらの環境でポリシーサービスがLDAP検索を実行するために必要です。

Linux VDAパッケージのインストール後、次のコマンドを実行します。

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
```

提案された形式ですべてのLDAPサーバーを入力します: LDAPポートを含む、スペースで区切られたLDAP完全修飾ドメイン名 (FQDN) のリスト (例: ad1.mycompany.com:389 ad2.mycomany.com:389)。

Linux VDAでのLDAPサーバー設定の画像(/en-us/linux-virtual-delivery-agent/7-15-ltsr/media/ldap-server-setting-on-linux-vda-new.png)

ctxregコマンドを実行して、この設定をレジストリに直接書き込むこともできます:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ListOfLDAPServers" -d "ad1.mycompany.com:389 ad2.mycomany.com:389" --
force
```

以下のポリシーはLinux VDAにのみ適用され、Citrix Studioバージョン7.12以降でのみ構成できます:

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

これらのポリシーについては、ポリシーサポートリストで説明されています。Citrix Studioバージョン7.11以前を使用している場合は、**ctxreg**コマンドを使用して、これらのポリシーをLinux VDAでローカルに構成する必要があります。

注:

値は特定の範囲に制限されています。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。

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
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
オーディオリダイレクトの帯域幅制限	LimitAudioBw	ユーザー	オーディオ	0 キロビット/秒
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	プリンターリダイレクトを許可	ユーザー	印刷	許可 (1)
クライアントクリップボードリダイレクト	クリップボードリダイレクトを許可	ユーザー	クリップボード	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
クライアントUSBデバイスのリダイレクト	USBリダイレクトを許可	ユーザー	USB	禁止 (0)
クライアントUSBデバイスリダイレクト規則	USBデバイス規則	ユーザー	USB	“\0”
動画圧縮	動画圧縮構成	ユーザー	シンワイヤー	有効 (1)
目標最小フレームレート	目標最小フレーム/秒	ユーザー	シンワイヤー	10 フレーム/秒
ターゲットフレームレート	フレーム/秒	ユーザー	シンワイヤー	30 フレーム/秒
視覚的な品質	視覚品質	ユーザー	シンワイヤー	中 (3)
圧縮にビデオコーデックを使用	ビデオコーデック	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)
単純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 – 高精細オーディオ (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)
最大セッション数	MaximumNumberOfSessions	コンピューター	負荷管理	250

STUDIOポリシー	キー名	タイプ	モジュール	デフォルト値
同時ログオン許容数	ConcurrentLogonsTolerance	コンピューター	負荷管理	2
コントローラー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 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
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
最大Speex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	ICA\ファイルリダイレクト	有効 (1)
クライアント光学ドライブ	AllowCdromDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアント固定ドライブ	AllowFixedDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアントフロッピードライブ	AllowFloppyDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアントネットワークドライブ	AllowNetworkDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアントリムーバブルドライブ	AllowRemoveableDrives	ユーザー	ICA\ファイルリダイレクト	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
クライアントドライブのリダイレクト	AllowDriveRedir	ユーザー	ICA\ファイルリダイレクト	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	ICA\ファイルリダイレクト	無効 (0)

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):

  デフォルト値: 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コーデックを使用して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することが可能です。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) に応じて、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、モードが異なるとビットレートも異なります。最適なSpeex品質とは、最大値が以下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

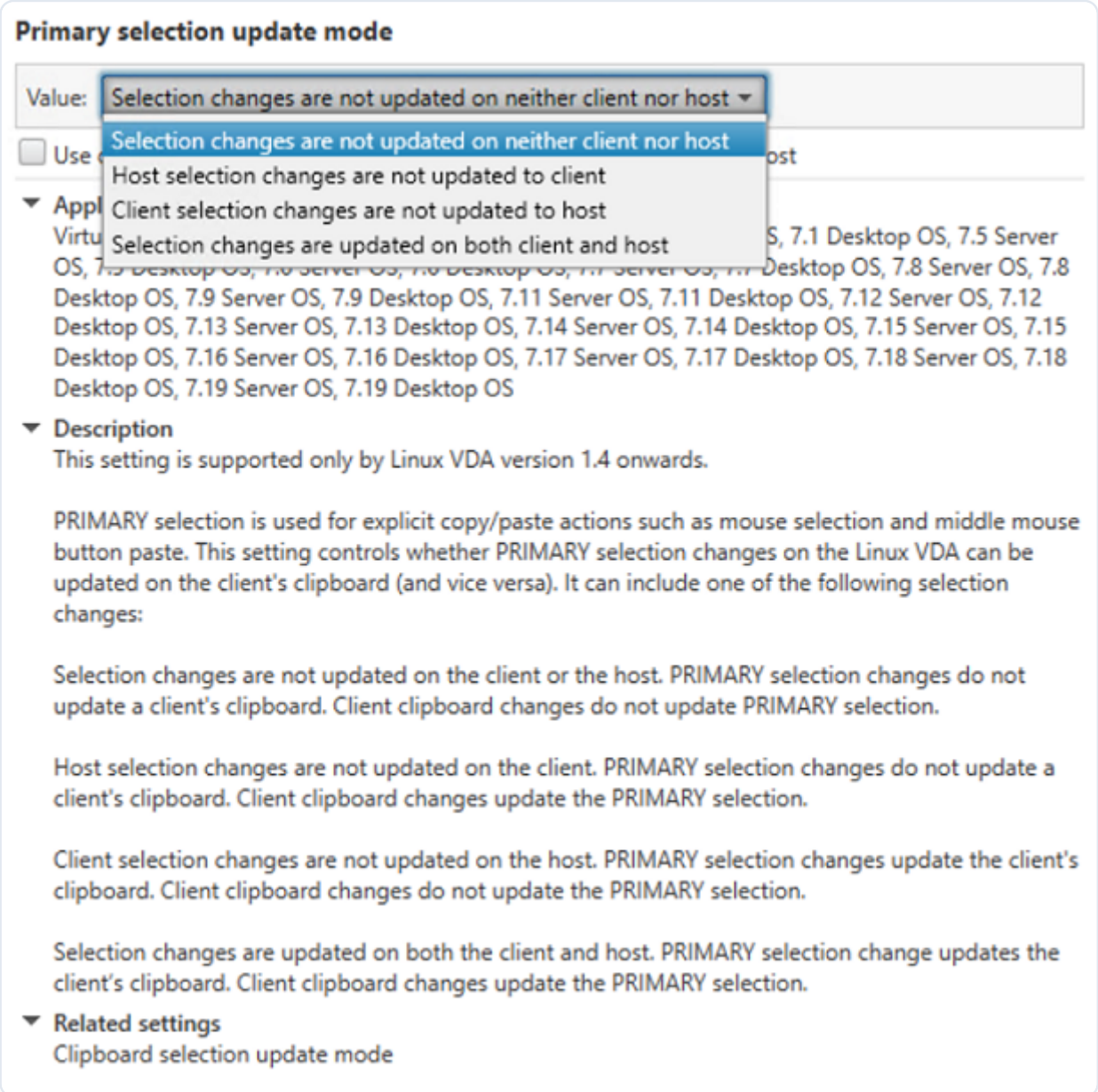
  値 (列挙型):

デフォルト値: 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。



- **選択の変更はクライアントにもホストにも更新されません**

  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。

- **ホストの選択の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の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。

- **選択の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

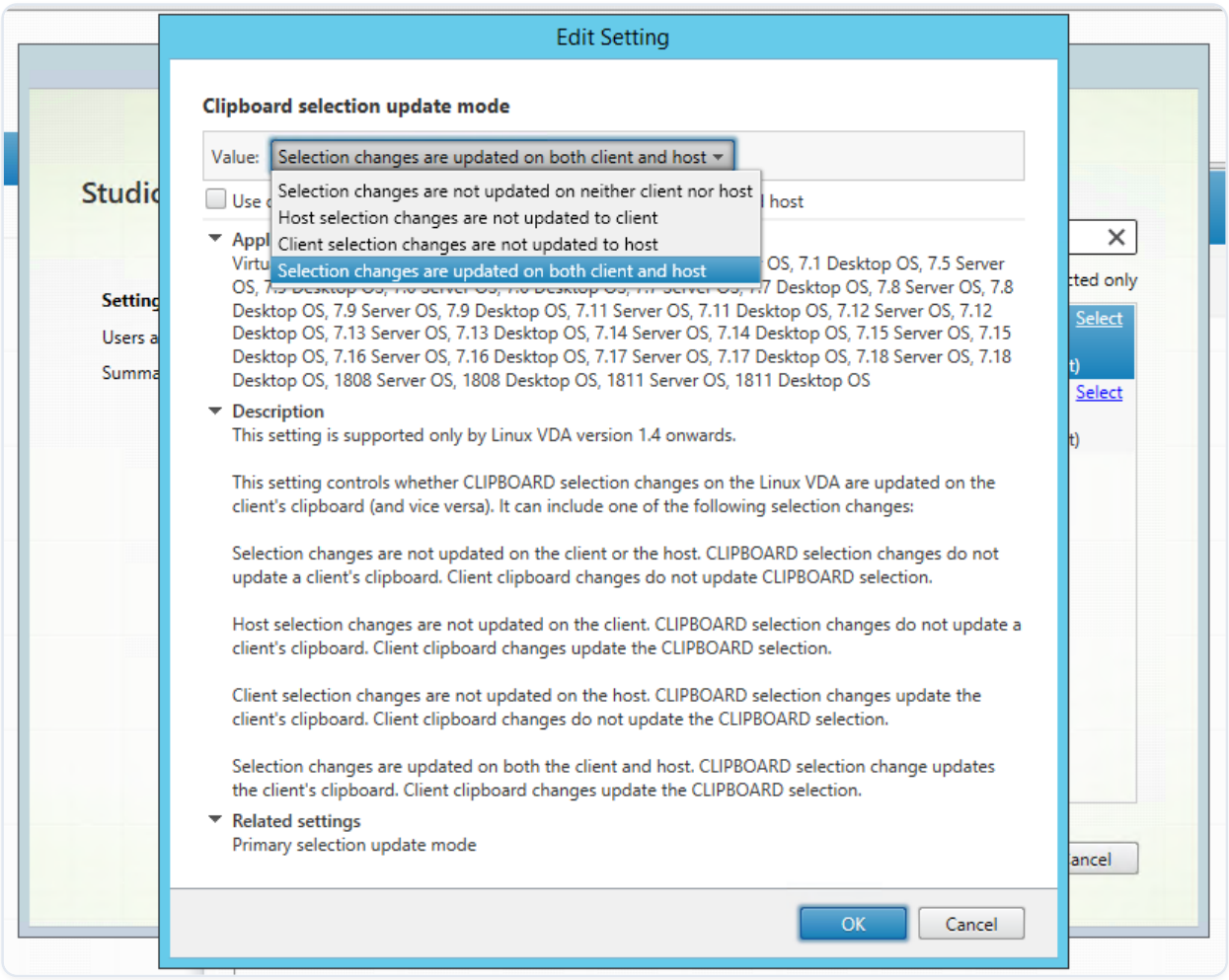
  値（列挙型）:

  デフォルト値: 3

  詳細:

  クリップボード選択は、データを選択し、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」を要求するときに使用されます。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に固有のものです。

  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相互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。



- **選択の変更はクライアントにもホスト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、クライアント上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上のクリップボードを更新しません。

- **ホストの選択の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、クライアント上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上のクリップボードを更新します。

- **クライアントの選択の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、クライアント上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上のクリップボードを更新しません。

- **選択の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、クライアント上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上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＆ペースト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。

IPv6 の構成

Linux VDA は、XenApp および XenDesktop 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 のみではありません。
- 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、IPv6 の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 netmask} を実際のネットマスク（例: 2000::/64）に置き換えます。

XenApp および XenDesktop 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。

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) の構成

CEIP に参加すると、Citrix 製品の品質とパフォーマンスの向上に役立てるため、匿名の統計情報と使用状況情報が Citrix に送信されます。

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自動的に CEIP 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

指定しない場合、CEIP は有効になります。

CEIP を無効にするには、クライアントで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 "CEIPSwitch" -d "1"
```

- **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のパスに保存されます。

Linux VDA から収集される 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する
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ルされていることを示すテキスト文字列。
HDX 3D Proの有効/無効	hdx_3d_pro	マシンでHDX 3D Proが有効になっているかどうかを示すテキスト文字列
VDIモードの有効/無効	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
LVDA主要サービスの最終再起動時刻	シーティーエックスエイチディーエックス シーティーエックスブイディーエー	`ctxhdx` および `ctxvda` サービスの最終再起動時刻。

データポイント	キー名	説明
		形式はdd-hh:mm:ssで、例: 10-17:22:19
GPUタイプ	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
アクティブセッション数	active_session_number	このデータポイントを収集した時点でのマシン上のアクティブセッションの数を示す整数
Linux OS名およびバージョン	os_name_version	マシンのLinux OS名およびバージョンを示すテキスト文字列
セッションキー	session_key	データが生成されたセッションを識別する
再接続時間コスト	econnect_time_cost	セッションの再接続時間コストを保存するために使用されます。配列のサイズは5で、このデータポイントの現在の値、最小値、最大値、実行中の合計、および更新回数を追跡します。
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がある場合があります。

データポイント	キー名	説明
セッションの継続時間	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クライアントの種類	receiver_type	セッションの起動に使用されたCitrix Receiverの種類を示す整数。
Receiverクライアントのバージョン	receiver_version	セッションの起動に使用されたCitrix Receiver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デバイスを使用する回数を示す整数

USBリダイレクトの構成

USBデバイスは、Citrix Receiver™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、ユーザーはそのUSBデバイスをローカルに接続されているかのように使用できます。

USBリダイレクトには、主に3つの機能領域があります。

- オープンソースプロジェクトの実装 (VHCI)
- VHCIサービス
- USBサービス

オープンソースVHCI:

USBリダイレクト機能のこの部分は、IPネットワークを介した汎用USBデバイス共有システムを開発します。これは、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ユーザーモードライブラリで構成されています。Linux VDAの実装では、CitrixはVHCIのカーネルドライバーを再利用します。ただし、Linux VDAとCitrix Receiver間のすべてのUSBデータ転送は、Citrix ICA®プロトコルパッケージにカプセル化されます。

VHCIサービス:

VHCIサービスは、VHCIカーネルモジュールと通信するためにCitrixが提供するオープンソースサービスです。このサービスは、VHCIとCitrix USBサービス間のゲートウェイとして機能します。

USBサービス:

USBサービスは、USBデバイス上のすべての仮想化とデータ転送を管理するCitrixモジュールを表します。

USB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セッションで使用できない場合があります。USBデバイスは正常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、クライアントとの間で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。さらに、デバイス、特にUSBディスクは適切にマウントされ、ユーザー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USBデバイス

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。

> **注:**
>
> Linux VDAはUSB 2.0プロトコルのみをサポートします。

USB大容量記憶装置	VID:PID	ファイルシステム
ネタック テクノロジー株式会社	0dd8:173c	FAT32
キングストン データトラベラー 101 II	0951:1625	FAT32

USB大容量記憶装置	VID:PID	ファイルシステム
キングストン データトラベラー GT101 G2	1567:8902	FAT32
SanDisk SDCZ80 フラッシュドライブ	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

USB 3Dマウス	VID:PID
3Dコネクション スペースマウス プロ	046d: c62b

USBスキャナー	VID:PID
エプソン パーフェクション V330 フォト	04B8: 0142

USBリダイレクトの構成

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。さらに、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。

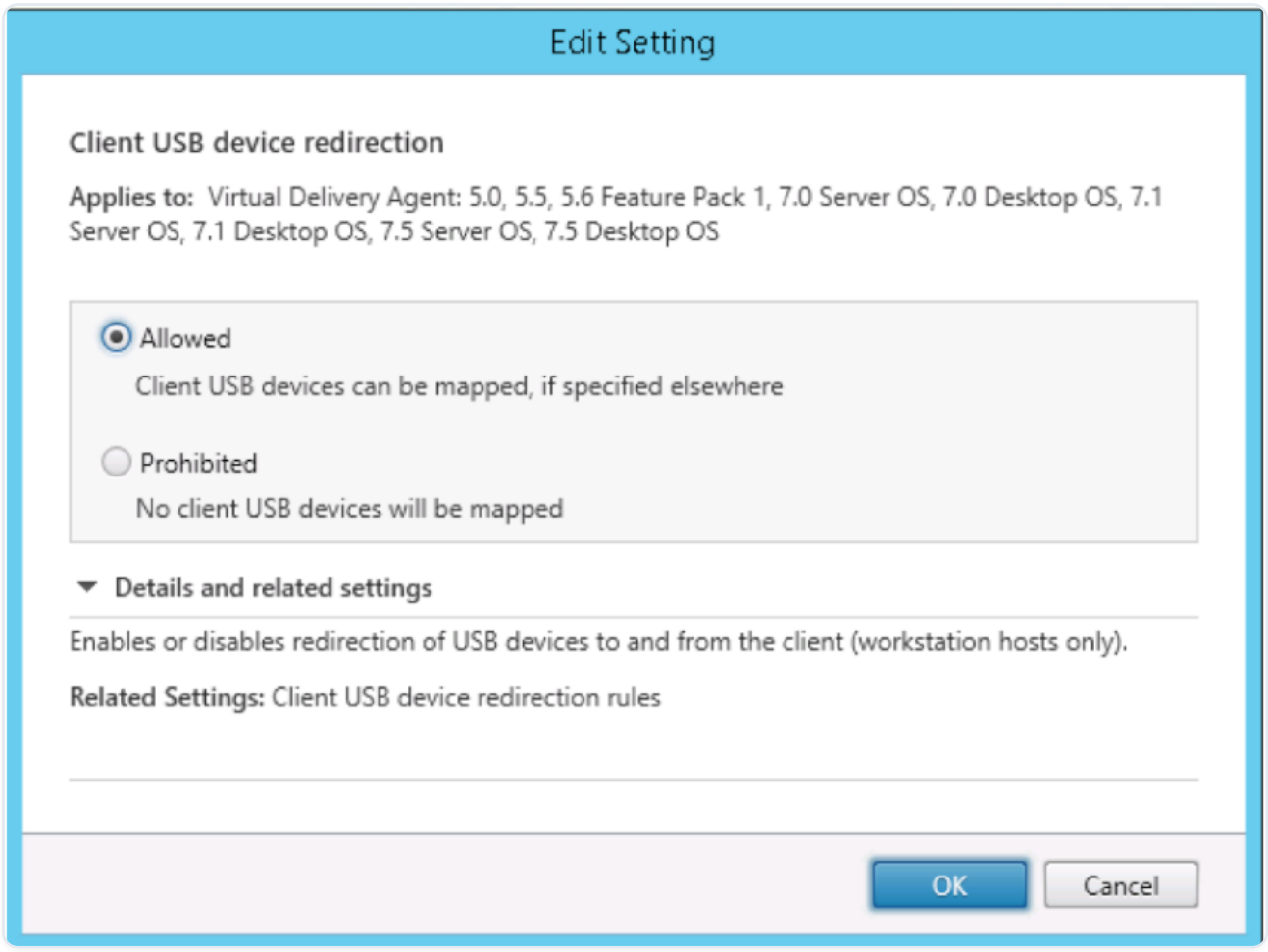
- クライアントUSBデバイスリダイレクトポリシー
- クライアントUSBデバイスリダイレクト規則

USBリダイレクトポリシーを有効にする

Citrix Studioで、クライアントとの間で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、次のようにします。

1. **許可**を選択します。
2. **OK**をクリックします。

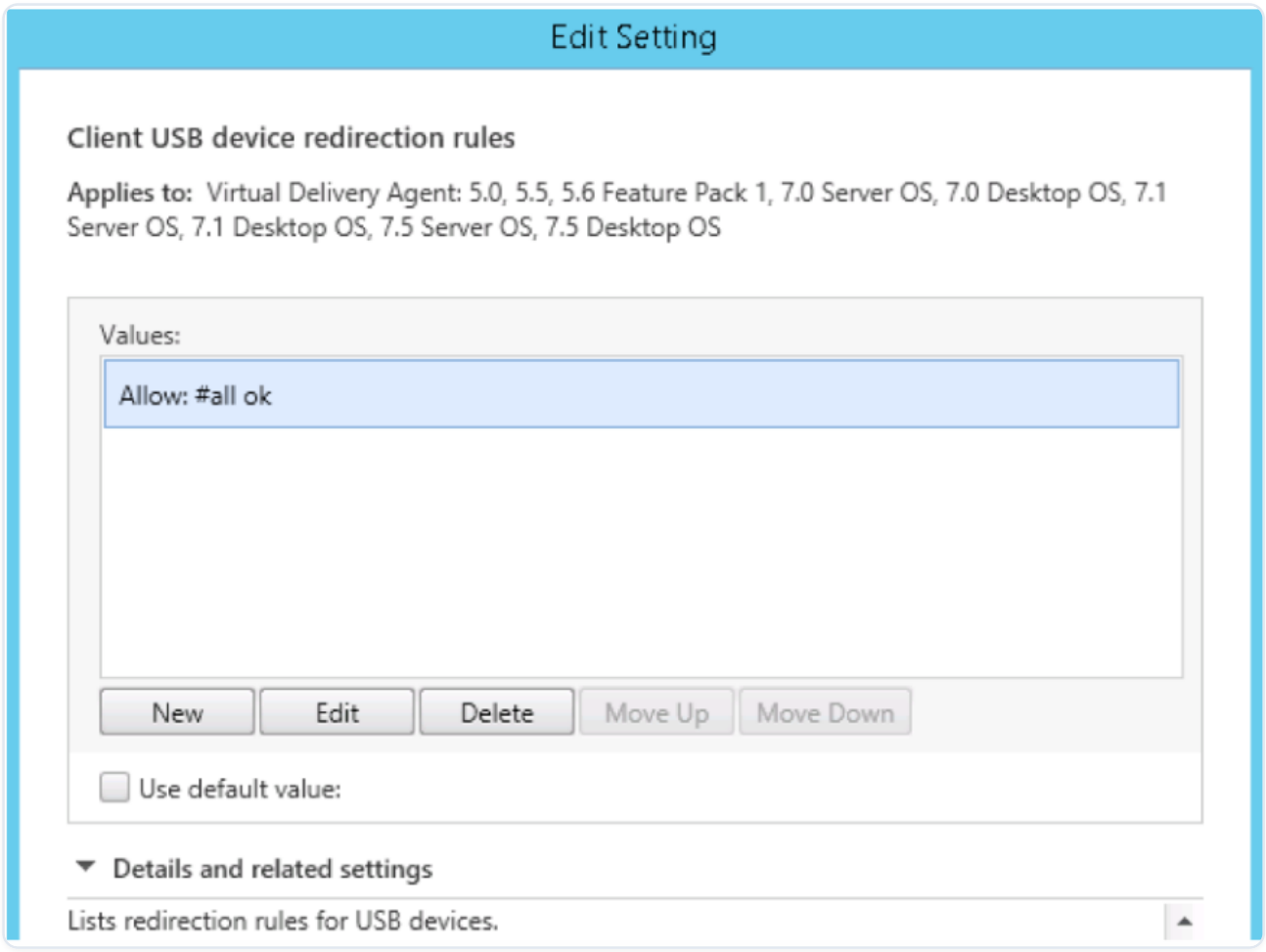


USBリダイレクト規則を設定する

USBリダイレクトポリシーを有効にした後、Citrix Studioを使用して、Linux VDAで許可（または拒否）されるデバイスを指定することで、リダイレクト規則を設定します。

クライアントUSBデバイスリダイレクト規則ダイアログで、次のようにします。

1. リダイレクト規則を追加するには**新規**をクリックし、既存の規則を確認するには**編集**をクリックします。
2. 規則を作成（または編集）した後、**OK**をクリックします。



VHCIカーネルモジュールをビルドする

USBリダイレクトは、VHCIカーネルモジュール（**usb-vhci-hcd.ko**および**usb-vhci-iocif.ko**）に依存します。これらのモジュールはLinux VDAディストリビューションの一部（RPMパッケージの一部）です。これらは公式のLinuxディストリビューションカーネルに基づいてコンパイルされ、次の表に示されています。

サポートされているLINUXディストリビューション	カーネルバージョン
RHEL 7.3	3.10.0-514.el7.x86_64
RHEL 6.6	2.6.32-504.el6.x86_64
SUSE 12.2	4.4.49-92.11-デフォルト
SUSE 11.4	3.0.101-0.47.55-デフォルト
ウブントゥ 16.04	4.4.0-45-ジェネリック

重要:

お使いのマシンのカーネルがCitrixがLinux VDA用に構築したドライバーと互換性がない場合、USBサービスが起動に失敗することがあります。この場合、独自のVHCIカーネルモジュールを構築した場合にのみ、USBリダイレクト機能を使用できます。

カーネルがCitrixによって構築されたモジュールと一致しているかを確認する

コマンドラインで、次のコマンドを実行してカーネルの一貫性を確認します。

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
```

コマンドが正常に実行された場合、カーネルモジュールは正常にロードされており、バージョンはCitrixによってインストールされたものと一致しています。

コマンドがエラーで実行された場合、カーネルはCitrixモジュールと整合性が取れていないため、再構築する必要があります。

VHCIカーネルモジュールを再構築する

カーネルモジュールがCitrixバージョンと整合性がない場合は、次の手順を実行します。

1. Citrixダウンロードサイトから LVDAソースコードをダウンロードします。「**Linux Virtual Delivery Agent (sources)**」セクションに含まれるファイルを選択します。
2. citrix-linux-vda-sources.zipファイルからファイルを復元します。VHCIソースファイルは**linux-vda-souces/vhci-hcd-1.15.tar.bz2**にあります。VHCIファイルは**tar xvf vhci-hcd-1.15.tar.bz2**を使用して復元できます。
3. ヘッダーファイルと**Module.symvers**ファイルに基づいてカーネルモジュールをビルドします。適切なLinuxディストリビューションに基づいてカーネルヘッダーファイルをインストールし、**Module.symvers**を作成するには、次の手順を使用します。

   RHEL 7.3/RHEL 6.9/RHEL 6.6:

   ```
   yum install kernel-devel
   ```

   SUSE 12.2:

```
zypper install kernel-devel



zypper install kernel-source
```

SUSE 11.4:

```
zypper install kernel-source
```

ウブントゥ 16.04:

```
apt-get install linux-headers
```

> **ヒント:**
>
> インストールが成功すると、次のようなカーネルフォルダーが作成されます。
>
> /usr/src/kernels/3.10.0-327.10.1.el7.x86_64

4. /usr/src/kernels/3.10.0-327.10.1.el7.x86_64フォルダーで、**Module.symvers**ファイルが存在することを確認します。このファイルがフォルダーにない場合は、カーネルをビルドしてこのファイルを取得するか（例: `make oldconfig`; `make prepare`; `make modules`; `make`）、**/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.***からコピーします。
5. **vhci-hcd-1.15/Makefile**ファイルで、VCHIのMakefileを変更し、KDIRをカーネルディレクトリに設定します。

```
#KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build



KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
```

6. フォルダー**vhci-hcd-1.15/**で、**make**を実行してVHCIカーネルをビルドします。

> **注:**
>
> ビルドが成功した場合、**usb-vhci-hcd.ko** と **usb-vhci-iocifc.ko** は **vhci-hcd-1.15/** フォルダーに作成されます。

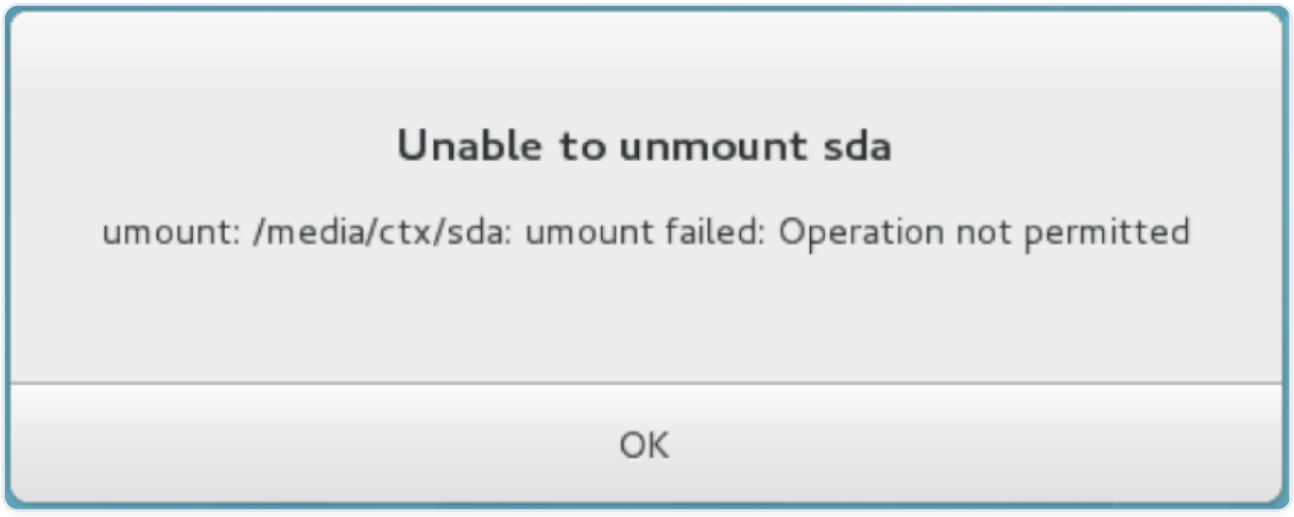
7. カーネルモジュールを新しくビルドしたものに置き換えます: **cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/**
8. USBサービスを再起動します: **service ctxusbsd restart**
9. セッションからログオフし、再度ログオンします。USBリダイレクトが機能しているか確認します。

USBリダイレクトの問題の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、Linux VDAの使用時に発生する可能性のあるさまざまな問題のトラブルシューティングを行います。

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

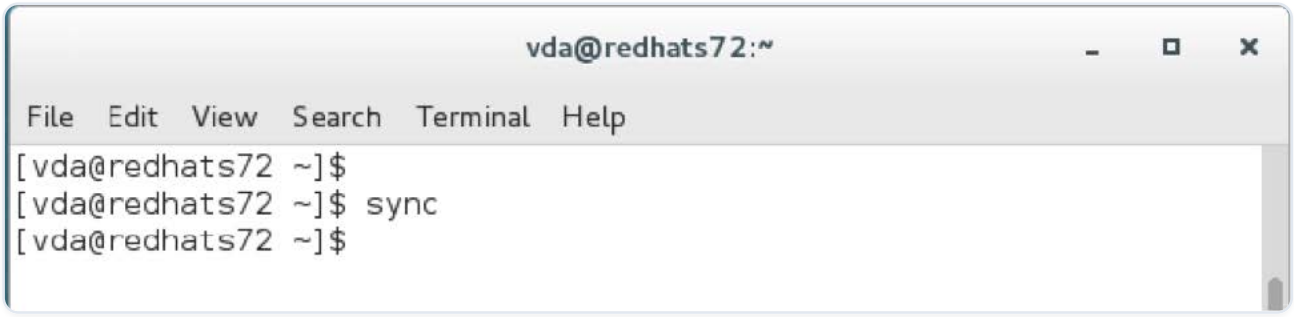
Citrix Receiverからリダイレクトされたすべてのディスクのアクセス制御のため、Linux VDAは、所有者のみがリダイレクトされたデバイスにアクセスできるように、これらすべてのデバイスを管理者権限で管理します。その結果、ユーザーは管理者権限なしではデバイスをアンマウントできません。



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

USBディスクをセッションにリダイレクトし、それを変更しようとした場合（たとえば、ディスク上にいくつかのファイルを作成する）、その後Citrix Receiverのツールバーを使用してすぐにリダイレクトを停止すると、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 Receiver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 Receiverのツールバーにデバイスがない

Citrix Receiverのツールバーにデバイスが表示されないことがあり、これはUSBリダイレクトが行われていないことを示します。この問題が発生した場合は、以下を確認してください。

- USB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
- カーネルモジュールはカーネルと互換性があります

受信側ツールバーのデバイスタブの画像(/en-us/linux-virtual-delivery-agent/7-15-ltsr/media/client-usb-redirection-troubleshoot.png)

> **注:**
>
> **デバイス**タブは、Citrix Receiver for Linuxでは利用できません。

Citrix ReceiverのツールバーにUSBデバイスが表示されるが、「*ポリシー制限*」と表示されている場合の、リダイレクトの失敗

この問題は、デバイスのポリシー構成が原因で発生します。このような場合は、次の手順を実行します。

- 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 Receiver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。デバイスはCitrix Receiverのレジストリ設定によってブロックされている可能性があります。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、サポートされているUSBデバイスのみがリダイレクトできます。ただし、場合によっては、他の種類のデバイスがアクティブなLinux VDAセッションにリダイレクトされることがあります。このような状況では、リダイレクトされたすべてのデバイスに対して、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てください。

> **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（およびそれを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。これは、サポートされているデバイスリストにないデバイスには当てはまらない場合があります。

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を使用して入力してください。

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XenDesktop®またはXenAppセッションを開きます。

クライアントIME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てください。

既知の問題

- Googleスプレッドシートのセルに文字を入力するためにクライアントIME機能を使用する前に、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は、SUSE 11ディストリビューションではサポートされていません。

HDX™ インサイト

概要

HDX Insight は Citrix Application Delivery Management (ADM) の一部であり、広く普及している業界標準の AppFlow に基づいています。これにより、IT 部門は、NetScaler または Citrix SD-WAN™ アプリケーションネットワーキングファブリックを通過する Citrix ICA トラフィックに対する前例のないエンドツーエンドの可視性を提供することで、卓越したユーザーエクスペリエンスを実現できます。

このリリースでは、Linux VDA は HDX Insight 機能を部分的にサポートしています。エンドユーザーエクスペリエンス管理 (EUEM) 機能が実装されていないため、時間期間に関連するデータポイントは利用できません。

インストール

依存パッケージのインストールは不要です。

使用方法

HDX Insight は、Citrix Workspace™ アプリと Linux VDA の間で NetScaler® を介して渡される ICA メッセージを分析します。

Linux VDA を使用して NetScaler Insight Center の展開をセットアップし、HDX Insight 機能を有効にする必要があります。既存の構成、設定、またはデータを失うことなく、NetScaler Insight Center の展開を Citrix ADM に移行できます。詳細については、「NetScaler Insight Center から Citrix ADM への移行」を参照してください。

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、NetScaler で AppFlow® が有効になっていないか、Insight Center で NetScaler のインスタンスが誤って構成されています。

- 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、管理者にお問い合わせの上、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しばらく起動されていることを確認してください。

既知の問題

時間期間に関連するデータポイントを表示できません。 EUEM機能が実装されていないため、時間期間に関連するデータポイント（ICA RTTなど）は利用できず、N/Aと表示されます。

トレースオン

概要

ログの収集と問題の再現は、診断を遅らせ、ユーザーエクスペリエンスを低下させます。トレースオン機能は、このような作業を軽減します。Linux VDAでは、トレースはデフォルトで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るようになりました。デフォルトでは、Linux VDAをインストールして構成すると、`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

トレースオンは、**/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。ルート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、**Log Output Path**は**/var/log/xdl/hdx.log**に設定されており、**Max Log Size**は200 MBに設定されています。また、**Log Output Path**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**Warnings**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します。

```
setlog levels
```

次のコマンドを使用して、すべてのログレベル（Disable、Inherited、Verbose、Information、Warnings、Errors、Fatal Errorsを含む）を設定できます。

```
setlog level <class> [<level>]
```

`<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、これを all に設定します。

```
setlog level all error



Setting log class ALL to 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します。

```
setlog flags
```

単一のログフラグを表示または設定します。

```
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 **/var/xdl/.ctxlog** ファイルを使用して構成されますが、このファイルは root ユーザーのみが作成できます。他のユーザーにはこのファイルへの書き込み権限がありません。Citrix は、root ユーザーが他のユーザーに書き込み権限を与えないことを推奨します。これに従わない場合、任意のまたは悪意のある構成が `ctxlogd` になる可能性があり、これにより、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（誤って削除された場合など）、`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、root 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。

認証されていないセッションを構成する

この記事の情報を使用して、認証されていない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:

認証されていないセッションを構成する際は、セッションの事前起動は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、Citrix Receiver™ for Androidでもサポートされていません。

認証されていないストアを作成する

Linux VDAで認証されていないセッションをサポートするには、StoreFrontを使用して認証されていないストアを作成します。

デリバリーグループで認証されていないユーザーを有効にする

認証されていないストアを作成したら、デリバリーグループで認証されていないユーザーを有効にして、認証されていないセッションをサポートします。デリバリーグループで認証されていないユーザーを有効にするには、XenAppおよびXenDesktopのドキュメントの手順に従ってください。

認証されていないセッションのアイドル時間を設定する

認証されていない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：

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime
 -d 0x00000005
```

認証されていないユーザーの最大数を設定する

認証されていない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認証されていない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：

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber
 -d  0x00000020
```

重要:

認証されていないセッションの数を制限します。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

認証されていないセッションを構成する際は、次の点を考慮してください。

- **認証されていない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ます（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 を使用する認証されていない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、認証されていない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場合があります。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、**/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 **KDE Action Restrictions** パラメーターが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。

LDAPS の設定

セキュアLDAP (LDAPS) を使用すると、Active Directory管理ドメイン向けにセキュアな軽量ディレクトリアクセスプロトコルを有効にし、SSL (Secure Socket Layer)/TLS (Transport Layer Security) を介した通信を提供できます。

デフォルトでは、クライアントとサーバーアプリケーション間のLDAP通信は暗号化されていません。SSL/TLS (LDAPS) を使用するLDAPにより、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: Linux VDAのDelivery Controller™への登録
- ポリシーサービス: ポリシー評価

LDAPSの設定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
- リナックス VDA で エルダップス 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を設定する

- SSSDを設定する
- Winbindを設定する
- Centrifyを設定する
- Questを設定する

AD/LDAPサーバーでLDAPSを有効にする

Microsoftの認証局 (CA) またはMicrosoft以外のCAのいずれかから、適切にフォーマットされた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、LDAP over SSL/TLS (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、Microsoftサポートサイトの「How to enable LDAP over SSL with a third-party certification authority」を参照してください。

マルチティア (2層または3層など) の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LDAPS認証に適した証明書が自動的に提供されるわけではありません。

マルチティア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、Microsoft TechNetサイトの「LDAP over SSL (LDAPS) Certificate」の記事を参照してください。

クライアント使用向け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「How to export Root Certification Authority Certificate」を参照してください。

Linux VDAでLDAPSを有効または無効にする

Linux VDAでLDAPSを有効または無効にするには、次のスクリプトを (管理者としてログインして) 実行します。

このコマンドの構文は次のとおりです。

- 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
```

- SSL/TLSなしの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
```

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に準拠するいくつかのサードパーティ製ソフトウェアコンポーネント（SSSD、Winbind、Centrify、Questなど）もセキュアな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署名とシーリングを使用してセキュアな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、セキュアな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。また、ほとんどの場合、LDAPS（ポート636上のSSL経由のLDAP）は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ています。影響を受ける構成ファイルは**ldap.conf**と**smb.conf**です。ファイルを次のように変更します。

```
ldap.conf:



TLS_REQCERT never



smb.conf:



ldap ssl = start tls



ldap ssl ads = yes



client ldap sasl wrapping = plain
```

あるいは、セキュアなLDAPはSASL GSSAPI署名とシーリングによって構成できますが、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。

```
smb.conf:



ldap ssl = off
```

```
ldap ssl ads = no
```

```
client ldap sasl wrapping = seal
```

セントリファイ

CentrifyはポートLDAPSをサポートしていません。ただし、ポート389で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LDAPSをサポートしていませんが、異なる方法を使用してポート389でセキュア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、次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、それが 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ました**

  enable_ldaps.sh を使用せずに誤って LDAPS 関連のキーが更新された場合、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、LDAP トラフィックが SSL/TLS で暗号化されていません**

  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 トラフィックがありません**

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 を使用してください。

- **/opt/Citrix/VDA/sbin/enable_ldaps.sh スクリプトを実行してルート CA 証明書をインポートできませんでした**

  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ます。一般的に、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、Citrix® は base64 エンコードされた PEM 形式を推奨します。

- **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。

Xauthority の構成

Linux VDA は、インタラクティブなリモート処理のために X11 ディスプレイ機能 (`xterm` および `gvim` を含む) を使用する環境をサポートします。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、次の2つの方法があります。

- **Xhost**。デフォルトでは、Xhost は localhost 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、特定のマシンで 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 Cookie に資格情報を保存するために使用されます。XServer インスタンス (Xorg) が起動されると、その特定のディスプレイへの接続を認証するために Cookie 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、次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
- Cookie 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 に設定します。
- Xorg の Cookie 番号のいずれかを含む `.Xauthority` ファイルを取得します。

Xauthority の構成

リモート X11 ディスプレイ用に Linux VDA で Xauthority を有効にするには、次の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® セッションの起動後、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、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、`~/.Xauthority` ファイルがデフォルトで使用されます。

- 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、次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、Linux VDA の IP アドレス（例：10.158.11.11）と公開デスクトップのディスプレイ番号（例：160）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。

   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 + \<ディスプレイ番号\> 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。

Linux Virtual Delivery Agentのドキュメント履歴

次の表に、Linux Virtual Delivery Agent 7.15のドキュメントに対する重要な変更点を示します。これらのアップデート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。

日付	変更	説明
07 Jul 2022	累積更新プログラム9（CU9） のリリース	Linux Virtual Delivery Agent 7.15の新機能
11 Aug 2021	累積更新プログラム8（CU8） のリリース	Linux Virtual Delivery Agent 7.15の新機能
30 Jun 2020	累積更新プログラム6（CU6） のリリース	Linux Virtual Delivery Agent 7.15の新機能
22 Oct 2019	累積更新プログラム5（CU5） のリリース	Linux Virtual Delivery Agent 7.15の新機能
23 Apr 2019	累積更新プログラム4（CU4） のリリース	Linux Virtual Delivery Agent 7.15の新機能
13 Apr 2017	Linux Virtual Delivery Agent 7.15のリリース	Linux Virtual Delivery Agent 7.15の新機能