Linux Virtual Delivery Agent 7.15

Contents

新機能 **3**

解決された問題 **3**

既知の問題 **5**

サードパーティ製品についての通知 **7**

システム要件 **7**

インストールの概要 **11**

Delivery Controller の構成 **11**

簡単インストール **12**

Linux Virtual Delivery Agent for RHEL/CentOS のインストール **24**

Linux Virtual Delivery Agent for SUSE のインストール **55**

Linux Virtual Delivery Agent for Ubuntu のインストール **79**

Linux VDA の構成 **104**

NIS の **Active Directory** との統合 **105**

公開アプリケーション **111**

印刷 **112**

PDF 印刷 **118**

グラフィックの構成 **119**

GRID 以外の **3D** グラフィック **124**

ポリシーの設定 **126**

ポリシーサポート一覧 **128**

IPv6 の構成 **134**

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 **135**

USB リダイレクトの設定 **138**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

クライアント入力システム（**IME**） **147**

HDX Insight **147**

トレースオン **149**

認証が不要なセッションの構成 **152**

LDAPS の構成 **154**

Xauthority の構成 **158**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

新機能

October 6, 2022

リリース日：2022 年 7 月 7 日

バージョン **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 以降に報告された問題が 1 件修正されています。

PDF 印刷

これまで実験的に導入されていたPDF 印刷機能は、このリリースで本格的に導入されます。この機能によって、Citrix Receivers for Chrome および Citrix Receivers for HTML5 は、Linux VDA セッションで変換された PDF を印刷できるようになります。

システムの動作の変更

このリリースでは、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。

解決された問題

August 8, 2022

CU9 で解決された問題

- SUSE または RHEL で Linux VDA をアンインストールしても、/opt/Citrix/にある空のフォルダーが削除されない場合があります。[CVADHELP-18241]

CU8 で解決された問題

- チャネルバインドを有効にすると、Linux VDA を Delivery Controller に登録しようとして失敗する場合があります。[CVADHELP-14481]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CU6 で解決された問題

- マウスやキーボードが同じウィンドウで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の変更に失敗すると、Linux セッションが応答しなくなることがあります。[CVADHELP-12768]
- リムーバブル USB ドライブを Linux VDA に汎用リダイレクトしようとすると失敗する可能性があります。この問題は、USB ドライブが NTFS（New Technology File System）でフォーマットされている場合に発生します。[CVADHELP-13675]
- Linux VDA は、ターゲットフレーム数（FramesPerSecond）設定で指定されたフレーム数/秒を達成できない場合があります。この問題は、GPU が Linux VDA にインストールされている場合に発生します。[CVADHELP-14267]

CU5 で解決された問題

- 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して貼り付けようとすると失敗する場合があります。[LD2047]
- Linux VDA でセッションを起動して操作を実行すると、セッションが切断される場合があります。[LD2257]

CU4 で解決された問題

- エンドポイントからコンテンツをコピーして、Linux VDA で実行されている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。[LC8760]
- キーボードは SUSE Linux Enterprise Server 11 Service Pack 4 では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。[LC9906]
- Linux VDA のユーザーセッションで **ctxctl** プロセスを実行できない場合があります。[LD0353]

CU3 で解決された問題

- Linux VDA が Citrix ポリシーを適用しない可能性があります。この問題は、NetScaler Gateway でアクセス制御要素の接続タイプを使用するようにポリシーを設定した場合に発生します。[LC9842]

CU2 で解決された問題

- Delivery Controller を使用した Linux VDA の登録が断続的に失敗することがあります。[LC7982]
- Red Hat Enterprise Linux Server 7.3 で動作している Citrix Director 7.13 で、マシンのセッションの詳細が表示されないことがあります。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。[LC8204]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Linux VDA は、Delivery Controller に登録してしばらくすると、登録を解除することがあります。[LC8205]
- Linux VDA のセッション表示を確認するために使用される一部のサードパーティアプリケーションでは、すべてのピクセルが表示されないことがあります。[LC8419]
- 複数の LDAP サーバーがある場合、ポリシーが更新されて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ことがあります。[LC8444]
- セッションが Linux VDA に接続されている場合、ctxhdx プロセスが **segfault** エラーで予期せず終了することがあります。[LC8611]
- Linux VDA 7.16 Early Access Release を使用すると、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ことがあります。この問題により、Director がエージェント要求エラーを表示し、その後再登録が開始されます。[LC9243]

CU1 で解決された問題

- Linux VDA は、Delivery Controller に登録してしばらくすると、登録を解除することがあります。[LC8205]
- Linux VDA のセッション表示を確認するために使用される一部のサードパーティアプリケーションでは、すべてのピクセルが表示されないことがあります。[LC8419]
- 複数の LDAP サーバーがある場合、ポリシーが更新されて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ことがあります。[LC8444]

7.15 LTSR で解決された問題

このリリースの Linux VDA では、次の問題が解決されています。

- DNS サーバーの IP アドレスを入力すると、簡単インストール機能が Linux VDA をネットワークから切断することがあります。[LNXVDA-2152]
- ビデオの再生中、Citrix Receiver for Windows から Citrix Receiver for Android へのセッションのローミングが失敗します。[LNXVDA-2164]

既知の問題

August 8, 2022

このリリースでは、次の問題が確認されています:

- XenApp および XenDesktop 7.15 LTSR CU6 に統合された 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `indicator-datetime-service`プロセスで $TZ 環境変数が使用されません。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。[LNXVDA-2128]
- Ubuntu のグラフィック：HDX 3D Pro で、Desktop Viewer をサイズ変更した後、アプリケーションの周囲に黒い枠が表示されたり、まれに背景が黒く表示される場合があります。
- Linux VDA 印刷リダイレクトで作成されたプリンターは、セッションからログアウト後、削除されることがあります。
- ディレクトリにファイルやサブディレクトリが多数含まれていると、CDM ファイルが見つからないクライアント側のファイルやディレクトリが非常に多い場合、この問題が生じることがあります。
- このリリースでは、英語以外の言語には UTF-8 エンコードのみがサポートされます。
- セッションのローミング時、Citrix Receiver for Android で CapsLock が通常とは反対の状態になる場合があります。Citrix Receiver for Android への既存の接続をローミングすると、Caps Lock 状態が失われる場合があります。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 に接続している場合、Alt キーを使用するショートカットキーが機能しないことがあります。Citrix Receiver for Mac では、左右どちらの option/alt キーを押しても、デフォルトでは AltGr が送信されます。Citrix Receiver の設定でこの動作を変更することはできますが、結果はアプリケーションによって異なります。
- Linux VDA をドメインに再度追加すると、登録できません。再度追加することにより、Kerberos キーの新しいセットが生成されます。しかし、ブローカーは、Kerberos キーの以前のセットに基づいた、キャッシュに存在する期限切れの VDA サービスチケットを使用する可能性があります。VDA がブローカーに接続しようとするときに、ブローカーは VDA に返すセキュリティコンテキストを確立できないことがあります。通常見られる現象は、VDA 登録の失敗です。

  この問題は、VDA サービスチケットが最終的に期限切れとなって更新されると自動的に解決します。ただし、サービスチケットの期限は長いので、それまでに時間がかかることがあります。

  この問題を回避するには、ブローカーのチケットキャッシュを消去します。ブローカーを再起動するか、管理者としてコマンドプロンプトからブローカーで次のコマンドを実行します。

  ```
  klist -li 0x3e4 purge
  <!--NeedCopy-->
  ```

  このコマンドにより、Citrix Broker Service を実行する Network Service プリンシパルが LSA キャッシュに保持するサービスチケットはすべて削除されます。これにより、ほかの VDA のサービスチケットが削除されます。また、その他のサービスのサービスチケットも削除される可能性があります。ただし、この処理は悪影響を及ぼしません。これらのサービスチケットは、再度必要になった時に 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がサポートされません。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を接続した場合は、アプリケーションが応答しなくなって再起動する必要が生じる可能性があります。録音中にキャプチャデバイスが取り外されると、同様の問題が発生する可能性があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Receiver for Windows でオーディオ録音中にオーディオの歪みが生じることがあります。

サードパーティ製品についての通知

August 15, 2022

Linux Virtual Desktop バージョン 7.15（PDF のダウンロード）

Linux VDA のこのリリースには、ドキュメント内で定義された条件の下でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

システム要件

November 11, 2021

Linux ディストリビューション

Linux VDA では、次の Linux ディストリビューションがサポートされています:

- SUSE Linux Enterprise
  - Desktop 12 Service Pack 2
  - Server 12 Service Pack 2
  - Server 11 Service Pack 4
- Red Hat Enterprise Linux
  - Workstation 7.3
  - Workstation 6.9
  - Workstation 6.6
  - Server 7.3
  - Server 6.9
  - Server 6.6
- CentOS Linux
  - CentOS 7.3
  - CentOS 6.6
- Ubuntu Linux

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ubuntu Desktop 16.04（4.4.x カーネル）
- Ubuntu Server 16.04（4.4.x カーネル）

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 のバージョンについては、次の表を参照してください。詳しくは、「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
Ubuntu 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

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

すべての場合で、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 社の Linux OS のプラットフォームおよびバージョンのサポートは、OS ベンダーのサポートの期限が切れた時点で終了します。
>
> 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 でのみサポートされます。1 つまたは複数のデスクトップをインストールする必要があります。

XenDesktop

Linux VDA は、現在サポートされているすべての XenDesktop の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、および製品のバージョンごとのサポートが停止される時期について詳しくは、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 の構成手順は、Windows VDA と多少異なります。ただし、Delivery Controller ファームは Windows デスクトップと Linux デスクトップを両方とも仲介できます。

> 注:
>
> Linux VDA は、XenDesktop バージョン 7.0 以前には対応していません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Receiver

次のバージョンの Citrix Receiver がサポートされます。

- Citrix Receiver for UWP（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
- Citrix Receiver for Android バージョン 3.11
- Citrix Receiver for iOS バージョン 7.2
- Citrix Receiver for Chrome バージョン 2.5
- Citrix Receiver for HTML5 バージョン 2.5（Access Gateway 経由でのみサポート）

ハイパーバイザー

Linux VDA ゲスト仮想マシンをホストする次のハイパーバイザーがサポートされます。

- XenServer
- VMware ESX および ESXi
- Microsoft Hyper-V
- Nutanix AHV

ベアメタルホスティングもサポートされます。

> ヒント：
>
> サポートされるプラットフォームの一覧については、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 では、以下の Active Directory 統合パッケージおよび製品がサポートされています：

- Samba Winbind
- Quest Authentication Services v4.1 以降
- Centrify DirectControl
- SSSD

> ヒント：
>
> サポート対象プラットフォームの一覧については、Active Directory 統合パッケージのベンダーが提供しているドキュメントを参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX 3D Pro

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ます。

- XenServer
- VMware ESX および ESXi
- Nutanix AHV

Linux ディストリビューション

HDX 3D Pro では、以下の Linux ディストリビューションがサポートされます。

- Red Hat Enterprise Linux - Workstation 7.3
- Red Hat Enterprise Linux - Server 7.3
- Red Hat Enterprise Linux - Workstation 6.9
- Red Hat Enterprise Linux - Server 6.9
- Red Hat Enterprise Linux - Workstation 6.6
- Red Hat Enterprise Linux - Server 6.6
- SUSE Linux Enterprise Desktop 12 Service Pack 2
- SUSE Linux Enterprise Server 12 Service Pack 2
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

GPU

以下の GPU が GPU パススルーとしてサポートされます。

- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2

以下の GPU が vGPU としてサポートされます。

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

インストールの概要

February 20, 2019

Linux Virtual Delivery Agent（VDA）のインストールは、サポートされるすべての Linux ディストリビューションと同じ手順を使用します。

1. インストールの準備。
2. ハイパーバイザーの準備。
3. Windows ドメインへの Linux 仮想マシン（VM）の追加。
4. Linux VDA のインストール。
5. Linux VDA の構成。
6. XenApp または XenDesktop でマシンカタログを作成
7. XenApp または XenDesktop でデリバリーグループを作成

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記載されています。

Delivery Controller の構成

May 6, 2020

XenDesktop 7.6 以前のバージョンで Linux VDA をサポートするには、変更を加える必要があります。そのため、これらのバージョンでは、Hotfix またはアップデートスクリプトが必要です。これらのインストールと確認については、このセクションで説明しています。

Delivery Controller 構成の更新

XenDesktop 7.6 SP2 の場合、Hotfix Update 2 を適用して、Linux Virtual Desktop 用のブローカーを更新します。Hotfix Update 2 は、以下から入手できます。

- CTX142438: Hotfix Update 2 - Delivery Controller 7.6（32 ビット）用 - 英語
- CTX142439: Hotfix Update 2 - Delivery Controller 7.6（64 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ブローカーサービス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から入手できます。

- citrix-linuxvda-scripts.zip

次の手順をサーバーファーム内の各 Delivery Controller で繰り返します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. **Update-BrokerServiceConfig.ps1** スクリプトを Delivery Controller マシンにコピーします。
2. ローカル管理者のコンテキストで 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を参照します。
4. **Update-BrokerServiceConfig.ps1** スクリプトを実行します:

```
.\Update-BrokerServiceConfig.ps1
<!--NeedCopy-->
```

> ヒント:
>
> デフォルトでは、PowerShell は PowerShell スクリプトを実行できないように構成されています。スクリプトの実行に失敗する場合は、再試行する前に PowerShell 実行ポリシーを変更します。
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--NeedCopy-->
> ```

Update-BrokerServiceConfig.ps1 スクリプトを実行すると、Linux VDA に必要とされる新しい WCF エンドポイントを使用してブローカーサービス構成ファイルが更新され、ブローカーサービスが再起動します。このスクリプトでは、自動的にブローカーサービス構成ファイルの場所が特定されます。元の構成ファイルのバックアップが、**.prelinux** という拡張子のファイル名で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 の仲介には影響しません。単一の Controller ファームは、Windows VDA と Linux VDA の両方とのセッションをシームレスに管理し、仲介できます。

Delivery Controller 構成の確認

必要な構成変更が Delivery Controller に適用されているかどうかを確認するには、**%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config** ファイル中に **EndpointLinux** ストリングが 5 回出現していることを確認します。

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

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\
findstr EndpointLinux BrokerService.exe.config
<!--NeedCopy-->
```

簡単インストール

June 20, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

簡単インストールは、Linux VDA Version 7.13 以降で正式にサポートされています。簡単インストール機能は、必要なパッケージをインストールして、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

	Winbind	SSSD	Centrify
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
Ubuntu 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、以下の手順に従ってください:

1. 構成ファイル情報および 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 Web サイトにアクセスし、環境の 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には Runtime Environment をセットアップします。

手順 **1**: 構成ファイル情報および **Linux** マシンを準備する

簡単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 がインストールされ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
- 領域名 - Kerberos 領域名
- アクティブドメインの FQDN - 完全修飾ドメイン名

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要:
>
> - Linux VDA をインストールするには、Linux マシンでリポジトリが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 システムおよび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。

手順 **2**: **Linux VDA** パッケージのインストール

次のコマンドを実行して、Linux VDA の環境をセットアップします。

RHEL および CentOS ディストリビューション

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

Ubuntu ディストリビューション

```
sudo dpkg -i <PATH>/<Linux VDA deb>
sudo apt-get install -f
<!--NeedCopy-->
```

SUSE ディストリビューションの場合:

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

手順 **3**: **Runtime Environment** をセットアップしてインストールを完了する

Linux VDA パッケージのインストール後、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:

手動構成を実行するには、次のコマンドを実行し、プロンプトごとに関連パラメーターを入力します。

```
sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--NeedCopy-->
```

サイレントモード:

サイレントモードで簡単インストールを使用するには、ctxinstall.sh を実行する前に以下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指定します。
- **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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_EASYINSTALL_DOMAIN**=domain-name - ドメインの NetBIOS 名。
- **CTX_EASYINSTALL_REALM**=realm-name - Kerberos 領域名。
- **CTX_EASYINSTALL_FQDN**=ad-fqdn-name
- **CTX_EASYINSTALL_ADINTEGRATIONWAY**=winbind | sssd | centrify - Active Directory の統合方式を指定
- **CTX_EASYINSTALL_USERNAME**=domain-user-name - ドメインに参加させるために使用されるドメインユーザーの名前を指定します。
- **CTX_EASYINSTALL_PASSWORD**=password - ドメインに参加させるために使用されるドメインユーザーのパスワードを指定します。

次の変数は、ctxsetup.sh で使用されます。

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** - Linux VDA では、DNS CNAME レコードを使用して、Delivery Controller 名を指定できます。
- **CTX_XDL_DDC_LIST** = list-ddc-fqdns - Linux VDA には、Delivery Controller の登録に使用する Delivery Controller の完全修飾ドメイン名（FQDN）のスペース区切りの一覧が必要です。1 つまたは複数の完全修飾ドメイン名または CNAME を指定する必要があります。
- **CTX_XDL_VDA_PORT**=port-number - Linux VDA は、TCP/IP ポート経由で 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します。
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** - Linux Virtual Desktop サービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop 用に、システムのファイアウォールの必要なポート（デフォルトではポート 80 およびポート 1494）を自動で開放できます。
- **CTX_XDL_HDX_3D_PRO**=Y | N - Linux VDA では、HDX 3D Pro がサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連の GPU アクセラレーションテクノロジです。HDX 3D Pro を選択した場合、VDA は VDI デスクトップ（シングルセッション）モード用に構成されます（つまり、CTX_XDL_VDI_MODE=Y となります）。
- **CTX_XDL_VDI_MODE = Y | N** - 専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro 環境の場合は、値を Y に設定します。
- **CTX_XDL_SITE_NAME = dns-name** - Linux VDA は、DNS を使用して LDAP サーバーを検出します。DNS の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 を照会して LDAP サーバーを検出します。DNS が LDAP サービスレコードを提供できない場合は、LDAP の FQDN および LDAP ポートのスペース区切りの一覧を指定できます。たとえば、ad1.mycompany.com:389 となります。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（例：DC=mycompany,DC=com）に設定された検索ベースを使用して LDAP を照会します。検索のパフォ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ーマンスを改善するために、検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。不要な場合は、**<none>** に設定できます。

- **CTX_XDL_START_SERVICE** = Y | N - 構成の完了時に Linux VDA サービスが開始されるようにするかどうかを指定します。

設定されていないパラメーターがあるとインストールは対話モードにロールバックし、ユーザー入力が求められます。ctxinstall.sh スクリプトは、すべてのパラメーターが既に環境変数で提供されている場合は、回答の入力を求めません。

サイレントモードでは、次のコマンドを実行して環境変数を設定してから ctxinstall.sh スクリプト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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--NeedCopy-->
```

sudo コマンドに-E オプションを指定して実行し、作成する新しいシェルに既存の環境変数を渡します。最初の行として **#!/bin/bash** を記述し、前述のコマンドからなるシェルスクリプトファイルを作成することを Citrix ではお勧めします。

または、次のようにして、1 つのコマンドですべてのパラメーターを指定することができます。

```
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
<!--NeedCopy-->
```

注意事項

- ワークグループ名はデフォルトではドメイン名です。ご使用の環境内のワークグループをカスタマイズするには、以下の手順に従ってください。

  a. Linux VDA マシンで、/tmp/ctxinstall.conf ファイルを作成します。
  b.「workgroup=<your workgroup>」という行をこのファイルに追加します。ここで、「your workgroup」はワークグループ名です。

- Centrify ではピュア IPv6 DNS 構成をサポートしていません。`adclient`で AD サービスを適切に検索するためには、IPv4 を使用する DNS サーバーが/etc/resolv.conf に少なくとも 1 つ存在している必要があります。

- CentOS 上の Centrify では、Centrify の環境チェックツール「`adcheck`」で簡単インストールが失敗し、次のエラーが表示されることがあります。

  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.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3            : We guess you should be in the site Site1.
4   <!--NeedCopy-->
```

この問題は、Centrify の特定の設定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 の ［管理ツール］を開きます。
b.［**Active Directory** のサイトとサービス］を選択します。
c.［サブネット］の正しいサブネットアドレスを追加します。

- ドメインに参加させる方式として Centrify を選択する場合、ctxinstall.sh スクリプトでは Centrify パッケージが必要です。ctxinstall.sh で Centrify パッケージを取得する方法は 2 通りあります。

  - 簡単インストールは、インターネットから Centrify パッケージを自動でダウンロードするために役立ちます。ディストリビューションごとの URL は次のとおりです：

    RHEL：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：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

    SUSE：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

    Ubuntu：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取得します。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 サーバーで/tmp/ctxinstall.conf ファイルが存在していない場合は作成します。
    b.「centrifypkgpath=<path name>」という行をこのファイルに追加します。ここで、「path name」はパス名です。

    例：

```
1   cat /tmp/ctxinstall.conf
2   set  “centrifypkgpath=/home/mydir”
3   ls  -ls  /home/mydir
4                    9548 -r-xr-xr-x. 1 root root  9776688 May 13
        2016 adcheck-rhel4-x86_64
5                    4140 -r--r--r--. 1 root root  4236714 Apr 21
        2016 centrifyda-3.3.1-rhel4-x86_64.rpm
6                    33492 -r--r--r--. 1 root root 34292673 May
      13  2016 centrifydc-5.3.1-rhel4-x86_64.rpm
7                    4 -rw-rw-r--. 1 root root     1168 Dec  1
       2015 centrifydc-install.cfg
8                    756 -r--r--r--. 1 root root   770991 May 13
       2016 centrifydc-ldapproxy-5.3.1-rhel4-x86_64.rpm
9                    268 -r--r--r--. 1 root root   271296 May 13
       2016 centrifydc-nis-5.3.1-rhel4-x86_64.rpm
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                    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
<!--NeedCopy-->
```

トラブルシューティング

このセクションの情報を参照して、この機能を使用することで発生する可能性のある問題のトラブルシューティングを実行できます。

SSSD を使用してドメインに参加できない

ドメインに参加しようとすると、次のような出力のエラーが発生することがあります（画面印刷のログを確認する）:

```
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.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
- 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.
<!--NeedCopy-->
```

/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、次の手順に従います。

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 でマシンカタログおよび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 でマシンカタログおよびデリバリーグループを作成します。

Ubuntu のデスクトップセッションで灰色の画面が表示される

セッションを起動すると、空のデスクトップでブロックされる問題が発生します。また、サーバー OS マシンのコンソールでも、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灰色の画面が表示されます。

この問題を解決するには、次の手順に従います。

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. 次の行を/etc/lightdm/lightdm.conf に追加します:
   greeter-show-manual-login=true

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ubuntu のデスクトップセッションを起動しようとするとホームディレクトリがないため失敗する

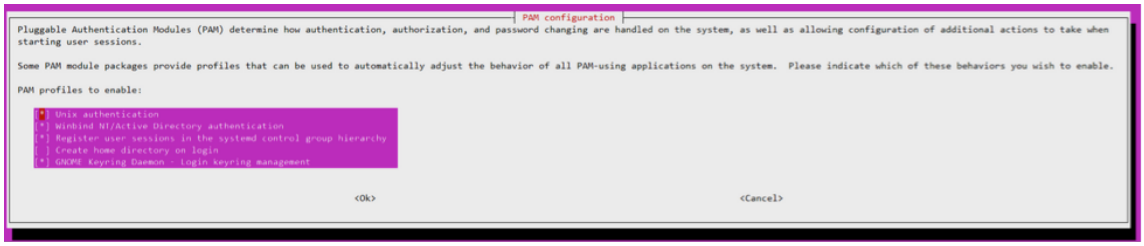
/var/log/xdl/hdx.log:

```
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.
<!--NeedCopy-->
```

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

この問題を解決するには、次の手順に従います。

1. コマンドラインで、**pam-auth-update** を入力します。
2. 表示されたポップアップウィンドウで、［ログイン時にホームディレクトリを作成する］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を起動または終了できない

/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...

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.
<!--NeedCopy-->
```

Ubuntu ディストリビューションの場合は、log /var/log/syslog を使用

```
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
<!--NeedCopy-->
```

再起動するまで機能しないグループまたはモジュールがあります。**dbus** エラーメッセージがログに表示される場合、システムを再起動してから再試行することを Citrix ではお勧めします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SELinux で **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
<!--NeedCopy-->
```

この問題を解決するには、次の手順に従います。

1. /etc/selinux/config に次の変更を加えることで、SELinux を無効にします。

   SELINUX=disabled

2. VDA を再起動します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 13, 2022

この記事の手順に従って手動でインストールするか、簡単インストールを使用して自動でインストールして構成するかを選択できます。簡単インストールは時間と労力を節約するだけでなく、手動のインストールよりもエラーを減らすことができます。

> 注
>
> ：新規のインストールでは、簡単インストールのみを使用します。既存インストールの更新には、簡単インストールを使用しないでください。

手順 **1**：**VDA** をインストールする **RHEL 7/CentOS 7**、**RHEL 6/CentOS 6** の準備

手順 **1a**：ネットワーク構成の確認

Citrix は、続行前にネットワークを接続し、適切に構成することをお勧めします。

手順 **1b**：ホスト名の設定

> 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 文字以内である必要があります。

マシンのホスト名が確実に正しく報告されるようにするには、**/etc/hostname** ファイルを変更してマシンのホスト名のみを記述します。

`HOSTNAME=`**hostname**

手順 **1c**：ホスト名へのループバックアドレスの割り当て

> 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 文字以内である必要があります。

マシンの DNS ドメイン名と完全修飾ドメイン名（FQDN）が確実に正しく報告されるようにするには、**/etc/hosts** ファイルの以下の行を変更し、最初の 2 つのエントリとして完全修飾ドメイン名とホスト名を記述します：

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

例：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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** に対するそ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使用しないでください。ホスト名を数字で開始したり、ハイフンで終了し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。

手順 **1d**：ホスト名の確認

次のコマンドで、ホスト名が正しく設定されていることを確認します：

```
hostname
<!--NeedCopy-->
```

このコマンドにより、そのマシンの完全修飾ドメイン名（FQDN）ではなく、そのホスト名のみが返されます。

次のコマンドで、完全修飾ドメイン名が正しく設定されていることを確認します：

```
hostname -f
<!--NeedCopy-->
```

このコマンドにより、そのマシンの完全修飾ドメイン名が返されます。

手順 **1e**：名前解決とサービス到達可能性の確認

次のコマンドで、完全修飾ドメイン名が解決できることと、ドメインコントローラーと Delivery Controller から ping に応答があ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
<!--NeedCopy-->
```

完全修飾ドメイン名を解決できない、またはこれらのマシンのいずれかから ping に応答がない場合は、手順を確認してから次に進んでください。

手順 **1f**：時刻同期の構成

VDA、Delivery Controller、ドメインコントローラーの間で正確な時刻同期を維持することは重要です。仮想マシンとして Linux VDA をホストすると、時刻が不正確になる問題が発生する可能性があります。したがって、リモート

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

のタイムサービスを使用して時刻を維持することをお勧めします。

RHEL 6.x 以前のリリースでは、時刻同期に NTP デーモン（ntpd）を使用しています。一方、RHEL 7.x のデフォルト環境では、新しい Chrony デーモン（chronyd）を代わりに使用しています。この 2 つのサービスの構成と操作手順は類似しています。

NTP サービスの構成（**RHEL 6/CentOS 6** のみ）　ルートユーザーとして **/etc/ntp.conf** を編集し、次のように各リモートタイムサーバーに対応する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
<!--NeedCopy-->
```

一般的な環境では、時間はローカルドメインコントローラーから同期します。公開 NTP プールサーバーから直接は同期しません。ドメインの各 Active Directory ドメインコントローラーに対応する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、パブリックサーバーの ***.pool.ntp.org** エントリなど、一覧にあるその他の **server** エントリを削除します。

変更を保存してから、次のコマンドで NTP デーモンを再起動します:

```
sudo /sbin/service ntpd restart
<!--NeedCopy-->
```

Chrony サービスの構成（**RHEL 7/CentOS 7** のみ）　ルートユーザーとして **/etc/chrony.conf** を編集し、次のように各リモートタイムサーバーに対応する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
<!--NeedCopy-->
```

一般的な環境では、時間はローカルドメインコントローラーから同期します。公開 NTP プールサーバーから直接は同期しません。ドメインの各 Active Directory ドメインコントローラーに対応する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、パブリックサーバーの ***.pool.ntp.org** エントリなど、一覧にあるその他の server エントリを削除します。

変更を保存してから、次のコマンドで Chrony デーモンを再起動します:

```
sudo /sbin/service chronyd restart
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 **1g**: **OpenJDK** のインストール

Linux VDA は OpenJDK に依存しています。通常、Runtime Environment は、オペレーティングシステムの一部としてインストールされています。

正しいバージョンを確認します。

- RHEL 7/CentOS 7:

```
sudo yum info java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum info java-1.7.0-openjdk
<!--NeedCopy-->
```

事前にパッケージされた 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、次のコマンドで最新バージョンに更新します:

- RHEL 7/CentOS 7:

```
sudo yum -y update java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum -y update java-1.7.0-openjdk
<!--NeedCopy-->
```

次の行を **~/.bashrc** ファイルに追加して、**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、次のコマンドで Java のバージョンを確認します:

```
java -version
<!--NeedCopy-->
```

> ヒント:
>
> 問題を回避するために、RHEL 6/CentOS 6 の場合は OpenJDK バージョン 1.7.0 または 1.8.0、RHEL 7/CentOS 7 の場合は OpenJDK バージョン 1.8.0 をインストールするようにしてください。その他のバージョンの Java は、システムからすべて削除します。

手順 **1h**: **PostgreSQL** のインストール

Linux VDA には、PostgreSQL 8.4 以降（RHEL 6 の場合）または PostgreSQL 9.2 以降（RHEL 7 の場合）のいずれかが必要です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
<!--NeedCopy-->
```

データベースを初期化し、マシンの起動時にサービスが確実に開始されるようにするには、次に示すインストール後の手順が必要です。この操作により、**/var/lib/pgsql/data** にデータベースファイルが作成されます。このコマンドは、PostgreSQL 8 と PostgreSQL 9 では異なります:

- RHEL 7 のみ: PostgreSQL 9

```
sudo postgresql-setup initdb
<!--NeedCopy-->
```

- RHEL 6 のみ: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
<!--NeedCopy-->
```

手順 **1i**: **PostgreSQL** の起動

マシンの起動時にサービスを開始し、直ち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
<!--NeedCopy-->
```

- RHEL 6 のみ: PostgreSQL 8

```
sudo /sbin/chkconfig postgresql on

sudo /sbin/service postgresql start
<!--NeedCopy-->
```

次のコマンドを使用して、PostgreSQL のバージョンを確認します。

```
psql --version
<!--NeedCopy-->
```

次のように **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'
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要:
>
> このリリースでは、gperftools-libs に新しい依存関係が追加されていますが、この依存関係は元のリポジトリには存在していません。`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ます。

手順 **2**: ハイパーバイザーの準備

サポートされるハイパーバイザー上で仮想マシンとして Linux VDA を実行する場合、いくつかの変更が必要です。使用するハイパーバイザーのプラットフォームに合わせて、次の変更を行います。ベアメタルハードウェアで Linux マシンを実行する場合、変更は必要ありません。

Citrix XenServer での時刻同期の修正

XenServer の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP と XenServer の両方がシステムの時間を管理しようとすることが原因となり問題が発生します。システムの時間と他のサーバーの時間との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時間が NTP と同期する必要があります。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、変更は必要ありません。

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、XenServer の時刻同期機能が存在するかどうかと、Linux 仮想マシン内で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
<!--NeedCopy-->
```

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いるため、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います。これ以上の操作は必要ありません。

/proc/sys/xen/indepent_wallclock ファイルが存在しない場合、以下の手順は必要ありません。

時刻同期機能が有効になっている場合は、ファイルに「1」と書き込んで無効にします:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

この変更を永続化し、再起動後も保持するには、**/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ため、次のようにしてシステムを再起動します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

このコマンドは 1 を返します。

Microsoft Hyper-V での時刻同期の修正

Hyper-V Linux 統合サービスがインストールされた Linux 仮想ホストでは、Hyper-V の時刻同期機能を適用してホストオペレーティングシステムの時間を利用できます。システムの時間を正確な状態で維持するには、NTP サービスとともに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で、次の操作を行います。

1. Hyper-V マネージャーを開きます。
2. Linux 仮想マシンの設定で、［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:
>
> この方法は VMware および XenServer の場合とは異なります。VMware および XenServer では、NTP との競合を避けるためにホストの時刻同期を無効にします。Hyper-V の時刻同期は、NTP と共存し、NTP の時刻同期を補完することができます。

ESX および **ESXi** での時刻同期の修正

VMware の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP とハイパーバイザーの両方がシステムの時間を同期しようとすることが原因となり問題が発生します。システムの時間と他のサーバーの時間との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時間が NTP と同期する必要があります。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 をインストールした状態で準仮想化 Linux カーネルを実行している場合は、次の操作を行います。

1. vSphere Client を開きます。
2. Linux 仮想マシンの設定を編集します。
3. ［仮想マシンのプロパティ］ダイアログボックスで、［オプション］タブをクリックします。
4. ［**VMware Tools**］を選択します。
5. ［詳細］ボックスで、［ホストとゲスト時刻を同期］チェックボックスをオフにします。

手順 **3**：**Linux** 仮想マシン（**VM**）を **Windows** ドメインに追加

Linux VDA は、Linux マシンを Active Directory（AD）ドメインに追加するさまざまな方法をサポートします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD

選択した方法の手順に従います。

> 注:
>
> Linux VDA のローカルアカウントと AD のアカウントで同じユーザー名を使用すると、セッションの起動に失敗することがあります。

Samba Winbind

次のようにして、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
<!--NeedCopy-->
```

マシンの起動時に **Winbind** デーモンを開始できるようにする　次のコマンドで、マシン起動時に Winbind デーモンが開始するように構成する必要があります:

```
sudo /sbin/chkconfig winbind on
<!--NeedCopy-->
```

Winbind 認証の構成　次のようにして、Winbind を使用した 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
<!--NeedCopy-->
```

ここで、**REALM** は大文字の Kerberos 領域名で、**domain** はドメインの NetBIOS 名です。

KDC サーバーおよび領域名を DNS ベースで参照する必要がある場合は、次の 2 つのオプションを前述のコマンドに追加します:

`--enablekrb5kdcdns --enablekrb5realmdns`

`authconfig`コマンドから返される、開始に失敗した`winbind`サービスに関するエラーは無視します。これらのエラーは、マシンがドメインにまだ参加していない状態で`authconfig`が`winbind`サービスを開始しようとすると発生することがあります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

/etc/samba/smb.conf を開いて、［Global］セクションに次のエントリを追加します。ただし、追加するのは、authconfigツールによって生成されたセクションの後です：

```
kerberos method = secrets and keytab
winbind refresh tickets = true
```

Delivery Controller に対する認証と登録には、Linux VDA にシステムの keytab ファイル/etc/krb5.keytab が必要です。前述の kerberos を使用した設定により、マシンが初めてドメインに参加するときに、Winbind によってシステムの keytab ファイルが強制的に作成されます。

Windows ドメインへの参加　ドメインコントローラーがアクセス可能で、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：

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

REALM は大文字の Kerberos 領域名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

Winbind 用の **PAM** の構成　デフォルトでは、Winbind PAM モジュール（pam_winbind）の構成で、Kerberos チケットキャッシュとホームディレクトリの作成が有効になっていません。/etc/security/pam_winbind.confを開いて、［Global］セクションで次のとおりにエントリを追加または変更します：

```
krb5_auth = yes
krb5_ccache_type = FILE
mkhomedir = yes
```

各設定の先頭のセミコロンは必ず削除します。これらを変更するには、次のようにして Winbind デーモンを再起動する必要があります：

```
1 sudo /sbin/service winbind restart
2 <!--NeedCopy-->
```

> ヒント：
>
> マシンがドメインに参加済みの場合にのみ、winbind デーモンは実行を続けます。

/etc/krb5.conf を開いて、［libdefaults］セクションで次の設定を 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 を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。

次のように、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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo net ads testjoin
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Kerberos 構成の確認　Linux VDA で使用できるように Kerberos が正しく構成されていることを確認するには、次のコマンドにより、システムの keytab ファイルが作成済みで keytab ファイルに有効なキーが含まれていることを確認します:

```
sudo klist -ke
<!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の`kinit`コマンドを実行し、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に対して認証します:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

マシン名と領域名は大文字で指定する必要があります。ドル記号（$）は、シェルによる置き換えを防ぐためにバックスラッシュ（\）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します:

```
sudo klist
<!--NeedCopy-->
```

次のコマンドを使用して、マシンアカウントの詳細を調査します:

```
sudo net ads status
<!--NeedCopy-->
```

ユーザー認証の確認　次のように、**wbinfo** ツールを使用して、ドメインユーザーがドメインに対して認証できることを確認します:

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

ここで指定するドメインは AD ドメイン名で、Kerberos 領域名ではありません。bash シェルの場合、バックスラッシュ文字（\）は、もう 1 つバックスラッシュ文字を指定してエスケープする必要があります。このコマンドにより、成功または失敗を示すメッセージが返されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

次のコマンドで、Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します:

```
klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します:

```
exit
<!--NeedCopy-->
```

Gnome コンソールまたは KDE コンソールに直接ログオンすると、同様のテストを実行できます。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。

Quest Authentication Service

ドメインコントローラーでの **Quest** の構成　次の操作は、Quest ソフトウェアを Active Directory ドメインコントローラーにインストールし、構成していることと、管理者特権が付与され、Active Directory にコンピューターオブジェクトを作成できることを前提としています。

Linux VDA マシンにドメインユーザーがログオンできるようにする　Linux VDA マシンで HDX セッションを確立する必要がある各ドメインユーザーに対して、次の操作を行います。

1. ［Active Directory ユーザーとコンピューター］管理コンソールで、目的のユーザーアカウントの Active Directory ユーザーの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］チェックボックスをオンにします。
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:
>
> この手順は、ドメインユーザーがコンソール、RDP、SSH、またはその他のリモート処理プロトコルを使用してログオンできるように設定する場合も同じです。

Linux VDA での **Quest** の構成

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SELinux ポリシー適用の回避策　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 ドメインソケットの IPC のメカニズムに干渉し、ドメインユーザーのログオンを妨げます。

この問題を回避するための便利な方法は、SELinux の無効化です。ルートユーザーとして、**/etc/selinux/config** を編集し、**SELinux** 設定を次のとおりに変更します:

```
SELINUX=permissive
```

この変更にはマシンの再起動が必要です:

```
reboot
<!--NeedCopy-->
```

> 重要:
>
> この設定は注意して使用してください。SELinux ポリシーの適用を無効にした後に再度有効にすると、ルートユーザーやその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てしまう可能性があります。

VAS デーモンの構成　次のように Kerberos チケットの自動更新を有効にして、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
<!--NeedCopy-->
```

このコマンドにより、更新間隔が 9 時間（32,400 秒）に設定されます。すなわち、チケットのデフォルトの有効期間である 10 時間よりも 1 時間短くなります。チケットの有効期間がさらに短いシステムでは、より小さい値をこのパラメーターに設定します。

PAM および **NSS** の構成　HDX や、su、ssh、RDP などのその他のサービスを介したドメインユーザーのログオンを有効にするには、次のコマンドを実行して PAM と NSS を手動で構成します:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

user は、コンピューターを Active Directory ドメインに追加する権限を持つ任意のドメインユーザーです。**domain-name** は、ドメインの DNS 名（example.com など）です。

ドメインメンバーシップの確認　Delivery Controller を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。Quest によって追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

マシンがドメインに参加している場合は、ドメイン名が返されます。マシンがドメインに追加していない場合、以下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　PAM を使用した Quest のドメインユーザーの認証が可能かどうかを確認するには、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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

次のコマンドで、**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
<!--NeedCopy-->
```

次のコマンドで、Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します:

```
exit
<!--NeedCopy-->
```

Gnome コンソールまたは KDE コンソールに直接ログオンすると、同様のテストを実行できます。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Centrify DirectControl

Windows ドメインへの参加　Centrify DirectControl Agent がインストールされている場合、次のように Centrify の`adjoin`コマンドを使用して、Linux マシンを Active Directory ドメインに追加します:

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

user パラメーターは、コンピューターを Active Directory ドメインに追加する権限を持つ任意の Active Directory ドメインユーザーです。**domain-name** は、Linux マシンを追加す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 を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。Centrify により追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
su -

adinfo
<!--NeedCopy-->
```

Joined to domain が有効であることと、CentrifyDC mode に connected が返されることを確認します。CentrifyDC mode が starting のまま変化しない場合は、Centrify クライアントにサーバーとの接続の問題、または認証の問題が発生しています。

次を使用すると、より包括的なシステム情報と診断情報を取得できます。

```
adinfo --sysinfo all

adinfo -diag
<!--NeedCopy-->
```

さまざまな Active Directory および Kerberos サービスとの接続をテストします。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。

```
adinfo --test
<!--NeedCopy-->
```

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。このセクションでは、Linux VDA マシンの Windows ドメインへの参加手順、および Kerberos 認証の構成について説明します。

SSSD を RHEL および CentOS でセットアップするには、次の作業を行います。

1. ドメインに参加し、Samba を使用してホストの keytab を作成する

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. SSSD のセットアップ
3. NSS/PAM の構成
4. Kerberos 構成の確認
5. ユーザー認証の確認

必要なソフトウェア　Active Directory プロバイダーは、SSSD Version 1.9.0 で初めて導入されました。古いバージョンを使用している場合は、Configuring the LDAP provider with Active Directoryの指示に従ってください。

次の環境については、このドキュメントに記載した指示を使用したテストおよび検証を行っています。

- RHEL 7.3 以降/CentOS 7.3 以降
- Linux VDA Version 1.3 以降

ドメインに参加し、**Samba** を使用してホストの **keytab** を作成する　SSSD では、ドメイン参加とシステムの keytab ファイルの管理に関する Active Directory のクライアント機能が提供されていません。代わりに`adcli`、`realmd`、`Winbind`または`Samba`を使用できます。

このセクションでは、`Samba`によるアプローチについてのみ説明します。`realmd`に関しては、RHEL または CentOS のドキュメントを参照してください。SSSD を構成する前に、以下の手順に従う必要があります。

Linux クライアントで、適切に構成されたファイルを使用します。

- /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
<!--NeedCopy-->
```

ここで、**REALM** は大文字の Kerberos 領域名で、**domain** は Active Directory ドメインの短い NetBIOS 名です。

KDC サーバーおよび領域名を DNS ベースで参照する必要がある場合は、次の 2 つのオプションを前述のコマンドに追加します:

`--enablekrb5kdcdns --enablekrb5realmdns`

/etc/samba/smb.conf を開いて、[**Global**] セクションに次のエントリを追加します。ただし、追加するのは、**authconfig** ツールによって生成されたセクションの後です:

`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できることと、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ます:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM は大文字の Kerberos 領域名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

SSSD のセットアップ　SSSD のセットアップは、以下の手順で構成されています:

- 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に設定の変更を行います（sssd.conf など）。
- **sssd** サービスを開始します。

sssd.conf の設定の例（必要に応じて追加の設定を行うことができます）:

```
[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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ad.example.com と **server.ad.example.com** を対応する値で置き換えます。詳しくは、『sssd-ad(5) - Linux man page』を参照してください。

ファイルの所有権およびアクセス権限を sssd.conf で設定します:

```
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、このホームディレクトリの作成機能が SELinux に対応していることを確認します:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir - -update
2
3 sudo service sssd start
4
5 sudo chkconfig sssd on
6 <!--NeedCopy-->
```

Kerberos 構成の確認　システムの **keytab** ファイルが作成され、このファイルに有効なキーが含まれていることを確認します:

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の **kinit** コマンドを実行し、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に対して認証します:

```
1 sudo kinit - k MACHINE$@REALM
2 <!--NeedCopy-->
```

マシン名と領域名は大文字で指定する必要があります。ドル記号（**$**）は、シェルによる置き換えを防ぐためにバックスラッシュ（****）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します:

```
1 sudo klist
2 <!--NeedCopy-->
```

ユーザー認証の確認　**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こと、および NSS が機能するかを確認します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

DOMAIN パラメーターは短い形式のドメイン名です。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ます。

サポートされているログオン形式は次の通りです:

- 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。以前はドメインユーザーアカウントは使用されていませんでした。

```
sudo ssh localhost  - l DOMAIN\username

id -u
<!--NeedCopy-->
```

次の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 }

<!--NeedCopy-->
```

次のコマンドで、ユーザーの Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します: 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。

```
klist
<!--NeedCopy-->
```

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

以前のバージョンの Linux VDA がインストールされている場合は、それをアンインストールしてから新しいバージョンをインストールする必要があります。

1. 次のコマンドで、Linux VDA サービスを停止します:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 次のコマンドで、パッケージをアンインストールします:

```
sudo rpm -e XenDesktopVDA
<!--NeedCopy-->
```

> 注:
>
> 最新の 2 バージョンからのアップグレードがサポートされます。
>
> 注:
>
> バージョン 1.3 以降、インストールパスが変更されます。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/** に配置されていました。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。代わりに、システムパスに**/opt/Citrix/VDA/sbin** および**/opt/Citrix/VDA/bin** を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、環境の 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
<!--NeedCopy-->
```

RHEL 6.9 の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6 の場合:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

RPM Package Manager 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、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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

RHEL 6.9 の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6 の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

RPM 依存関係一覧（**RHEL 7** の場合）:

```
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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

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
<!--NeedCopy-->
```

RPM 依存関係一覧（**RHEL 6.9** の場合）:

```
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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

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
<!--NeedCopy-->
```

RPM 依存関係一覧（**RHEL 6.6/CentOS 6.6** の場合）:

```
postgresql-jdbc >= 8.4
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
<!--NeedCopy-->
```

手順 **4d**：**Linux VDA** のアップグレード（オプション）

Yumコマンドで Linux VDA ソフトウェアをバージョン 7.14 や 7.13 に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
<!--NeedCopy-->
```

RHEL 6.9 の場合：

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6 の場合：

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

次のように、RPM Package Manager 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
<!--NeedCopy-->
```

RHEL 6.9 の場合：

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6 の場合：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

> 重要:
>
> ソフトウェアをアップグレードした後、Linux VDA マシンを再起動してください。

手順 5: NVIDIA GRID ドライバーのインストール

HDX 3D Pro を有効にするには、ハイパーバイザーと VDA マシンに必要なグラフィックドライバーをインストールするために、追加のインストール手順が必要です。

次のオプションを構成します:

1. Citrix XenServer
2. VMware ESX

選択したハイパーバイザーに対応する手順に従います。

Citrix XenServer:

この詳しいセクションでは、Citrix XenServer上での NVIDIA GRID ドライバーのインストールおよび構成の概略について説明します。

VMware ESX:

このガイドに掲載されている情報に従って、VMware ESX用の NVIDIA GRID ドライバーをインストールし、構成します。

VDA マシン:

以下の手順に従って、Linux 仮想マシンゲストのそれぞれに対してドライバーをインストールし、構成します:

1. 開始する前に、Linux 仮想マシンがシャットダウンされていることを確認します。
2. XenCenter で、GPU パススルーモードの GPU を仮想マシンに追加します。
3. RHEL 仮想マシンを起動します。

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
<!--NeedCopy-->
```

Red Hat Enterprise Linux のドキュメントの手順に従って、NVIDIA GRID ドライバーをインストールします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> GPU ドライバーのインストール時は、すべての質問でデフォルト（「いいえ」）を選択してください。
>
> 重要:
>
> GPU パススルーを有効にすると、XenCenter を利用して Linux 仮想マシンにアクセスできなくなります。SSH を使用して接続します。

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

次のコマンドで、カードに適切な構成を設定します:

```
etc/X11/ctx-nvidia.sh
```

高い解像度や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。この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の指示に従ってください。

手順 6: 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。このスクリプトは、変更を行う前に環境を確認し、すべての依存コンポーネントがインストールされていることが確認されます。必要に応じて、いつでもこのスクリプトを再実行して設定を変更できます。

このスクリプトは、手動で質問に回答しながら、または事前に構成した回答を使用して自動で実行できます。続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

質問に回答する構成

次のようにして、質問に回答する手動構成を実行します:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

自動化された構成

インストールを自動化するために、環境変数を使用して、セットアップスクリプトで必要となるオプションを指定できます。必要な変数がすべて指定されていると、スクリプトによってユーザーに情報の入力を求めるメッセージが表示されることがなくなります。

サポートされる環境変数には次のようなものがあります:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME** = **Y | N** - Linux VDA では、DNS CNAME レコードを使用して、Delivery Controller 名を指定できます。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 には、Delivery Controller の登録に使用する Delivery Controller の完全修飾ドメイン名（FQDN）のスペース区切りの一覧が必要です。1 つまたは複数の完全修飾ドメイン名または CNAME エイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT** = **port-number** - Linux VDA は、TCP/IP ポート（デフォルトではポート 80）を使用して、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します。デフォルトでは値は Y に設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES** = **Y | N** - Linux Virtual Desktop サービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop 用に、システムのファイアウォールの必要なポート（デフォルトではポート 80 およびポート 1494）を自動で開放できます。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 には、Delivery Controller に対して認証するために Kerberos 構成設定が必要です。Kerberos 構成は、システムにインストールおよび構成済みの Active Directory 統合ツールから指定します。次に示す、サポートされている Active Directory 統合方法のうち、使用するものを指定します:
  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 - Centrify DirectControl
  - 4 - SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** - Linux VDA では、HDX 3D Pro がサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連のグラフィックアクセラレーションテクノロジです。HDX 3D Pro を選択した場合、Virtual Delivery Agent は VDI デスクトップ（シングルセッション）モード用に構成されます（すなわち、CTX_XDL_VDI_MODE=Y となります）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_VDI_MODE** = **Y | N** - 専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro 環境では、この変数を Y に設定します。デフォルトでは N に設定されています。
- **CTX_XDL_SITE_NAME** = **dns-name** - Linux VDA は、DNS を使用して LDAP サーバーを検出します。DNS の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、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_LDAP_LIST** = **list-ldap-servers** - Linux VDA は、DNS を照会して LDAP サーバーを検出します。DNS が LDAP サービスレコードを提供できない場合は、LDAP の FQDN および LDAP ポートのスペース区切りの一覧を指定できます。たとえば、ad1.mycompany.com:389 となります。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_SEARCH_BASE** = **search-base-set** - Linux VDA は、Active Directory ドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを使用して LDAP を照会します。検索のパフォーマンスを改善するために、検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_START_SERVICE** = **Y | N** - Linux VDA 構成の完了時に Linux VDA サービスが開始されるようにするかどうかを指定します。デフォルトでは Y に設定されています。

次のようにして、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
<!--NeedCopy-->
```

sudo コマンドに**-E** オプションを指定して実行し、作成する新しいシェルに既存の環境変数を渡します。最初の行として **#!/bin/bash** を記述し、前述のコマンドからなるシェルスクリプトファイルを作成することを Citrix ではお勧

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

めします。

または、次のようにして、1 つのコマンドですべてのパラメーターを指定することができます。

```
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
<!--NeedCopy-->
```

構成変更の削除

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しないで、**ctxsetup.sh** スクリプトによって行われた構成変更を削除することが必要となる場合があります。

続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

構成変更を削除するには:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--NeedCopy-->
```

> 重要:
>
> このスクリプトにより、すべての構成データがデータベースから削除され、Linux VDA を操作できなくなります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

構成ログ

ctxsetup.sh および **ctxcleanup.sh** スクリプトでは、コンソールにエラーが表示され、構成ログファイル **/tmp/xdl.configure.log** に追加情報が書き込まれます。

Linux VDA サービスを再起動し、変更を反映させます。

手順 7：Linux VDA の実行

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 の起動：

Linux VDA サービスを起動するには、次のコマンドを実行します：

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Linux VDA の停止：

Linux VDA サービスを停止するには、次のコマンドを実行します：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

Linux VDA の再起動：

Linux VDA サービスを再起動するには、次のコマンドを実行します：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Linux VDA の状態の確認：

Linux VDA サービスの実行状態を確認するには、次のコマンドを実行します。

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 8：XenApp または XenDesktop でマシンカタログを作成

マシンカタログを作成し、Linux VDA マシンを追加する手順は、従来の Windows VDA での方法と似ています。このタスクを完了する方法の説明について詳しくは、「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。

次のように、Linux VDA マシンを含むマシンカタログの作成にはいくつかの制約があるため、Windows VDA マシンのマシンカタログの作成手順と異なる点があります：

- オペレーティングシステムには、次を選択します：
  - ホストされる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場合、［デスクトップ OS］オプション
- マシンが電源管理を行わない設定になっていることを確認します。
- MCS は Linux VDA ではサポートされないため、PVSまたは他のサービスまたはテクノロジ（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 の以前のバージョンは、「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 サーバー OS］オプションまたは［サーバー OS］オプションを選択すると、同等のホストされる共有デスクトップ配信モデルが暗黙的に選択されます。［Windows デスクトップ OS］オプションまたは［デスクトップ 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暗黙的に選択されます。
>
> ヒント：
>
> マシンが Active Directory ドメインから削除された後に再度追加された場合は、そのマシンをマシンカタログから削除してから再度追加する必要があります。

手順 9：XenApp または XenDesktop でデリバリーグループを作成

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手順は、Windows VDA マシンの場合とほとんど同じです。このタスクを完了する方法の説明について詳しくは、「デリバリーグループの作成」を参照してください。

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は、次の制約があります：

- 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。
- 選択する AD ユーザーおよびグループを、Linux VDA マシンにログオンするように適切に構成しておきます。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- Windows マシンを含むマシンカタログをデリバリーグループで混在させないでください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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、同一マシンへのデスクトップおよびアプリの配信は、Linux VDA でサポートされていません。

Linux Virtual Delivery Agent for SUSE のインストール

February 9, 2024

この記事の手順に従って手動でインストールするか、簡単インストールを使用して自動でインストールして構成するかを選択できます。簡単インストールは時間と労力を節約するだけでなく、手動のインストールよりもエラーを減らすことができます。

> 注
>
> : 新規のインストールでは、簡単インストールのみを使用します。既存インストールの更新には、簡単インストールを使用しないでください。

手順 **1**: インストールの準備

手順 **1a**: **YaST** ツールの起動

SUSE Linux Enterprise YaST ツールを使用して、オペレーティングシステムのすべての要素を構成します。

テキストベースの YaST ツールを起動する方法

```
su -

yast
<!--NeedCopy-->
```

代わりに、UI ベースの YaST ツールを起動する方法

```
su -

yast2 &
<!--NeedCopy-->
```

手順 **1b**: ネットワークの構成

以降のセクションでは、Linux VDA で使用するさまざまなネットワーク設定およびサービスの構成方法に関する情報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 ツールで実行する必要があります。次の手順は、UI ベースの YaST ツールを使用することが前提となっています。テキストベースの YaST ツールも使用できますが、ナビゲーション方法が異なり、ここでは説明していません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ホスト名と **DNS** の構成

1. YaST の［ネットワーク設定］を開きます。
2. SLED 12 のみ：［グローバルオプション］タブで、［ネットワークのセットアップ方法］を ［**Wicked** サービス］に変更します。
3. ［ホスト名/**DNS**］タブを開きます。
4. ［**DHCP** でホスト名を変更する］チェックボックスをオフにします。
5. ［ホスト名をループバック **IP** に割り当てる］チェックボックスをオンにします。
6. 以下を編集してネットワーク設定に反映させます。

   - 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］一覧–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。したがって、ホスト名は 15 文字以内である必要があります。
> ヒント：
>
> a～z、A～Z、0～9、およびハイフン（-）の文字のみ使用してください。アンダースコア（_）、スペース、およびその他の記号は使用しないでください。ホスト名を数字で開始したり、ハイフンで終了し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。

マルチキャスト **DNS** の無効化　SLED でのみ、デフォルトの設定でマルチキャスト DNS（mDNS）が有効であるため、名前解決の結果に不整合が発生する場合があります。SLES の場合、mDNS はデフォルトでは有効化されていないため、特に操作を行う必要はありません。

mDNS を無効にするには、**/etc/nsswitch.conf** を編集して、以下を含む行を変更します：

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

変更後：

```
hosts: files dns
```

ホスト名の確認　次のコマンドで、ホスト名が正しく設定されていることを確認します：

```
hostname
<!--NeedCopy-->
```

このコマンドにより、そのマシンの完全修飾ドメイン名（FQDN）ではなく、そのホスト名のみが返されます。

次のコマンドで、完全修飾ドメイン名が正しく設定されていることを確認します：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
hostname -f
<!--NeedCopy-->
```

このコマンドにより、そのマシンの完全修飾ドメイン名が返されます。

名前解決とサービス到達可能性の確認　次のコマンドで、完全修飾ドメイン名が解決できることと、ドメインコントローラーと Delivery Controller から ping に応答があ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
<!--NeedCopy-->
```

完全修飾ドメイン名を解決できない、またはこれらのマシンのいずれかから ping に応答がない場合は、手順を確認してから次に進んでください。

手順 **1c**: **NTP** サービスの構成

VDA、Delivery Controller、ドメインコントローラーの間で正確な時刻同期を維持することが重要です。仮想マシンとして Linux VDA をホストすると、時刻が不正確になる問題が発生する可能性があります。したがって、リモート NTP サービスを使用して時刻を維持することをお勧めします。次のように、デフォルト NTP 設定にいくつかの変更が必要な場合があります。

1. YaST の［NTP 環境設定］を開いて、［一般的な設定］タブをクリックします。
2. ［NTP デーモンを起動する］セクションで、［今すぐ開始し、システム起動時に開始するよう設定］をクリックします。
3. 表示されている場合は、［規律に従わないローカル時計（**LOCAL**）］項目を選択し、［削除］をクリックします。
4. ［追加］をクリックして、NTP サーバーのエントリを追加します。
5. ［サーバーの種類］を選択して、［次へ］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. ［オプション］フィールドは変更しません。
8. ［テスト］をクリックして、NTP サービスに到達できるかどうかを確認します。
9. 一連のウィンドウで ［**OK**］をクリックして、変更を保存します。

> 注:
>
> SLES 12 の実装では、AppArmor ポリシーに関する SUSE の既知の問題が原因で、NTP デーモンが起動に失敗することがあります。詳しくは、解決方法に従ってください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 **1d**：**Linux VDA** に依存するパッケージのインストール

SUSE Linux Enterprise 用の Linux VDA ソフトウェアは、次のパッケージに依存しています：

- 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 Runtime Environment 2.3.1 以降
- CUPS
  - 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

リポジトリの追加　次のように、必要なパッケージの中には、一部の SUSE Linux Enterprise リポジトリでは入手できないものがあります。

- SLED 11：PostgreSQL は、SLES 11 では入手できますが、SLED 11 では入手できません。
- SLES 11：OpenJDK と OpenMotif は、SLED 11 では入手できますが、SLES 11 では入手できません。
- SLED 12：PostgreSQL は、SLES 12 では入手できますが、SLED 12 では入手できません。ImageMagick は、SLE 12 SDK ISO またはオンラインリポジトリから入手できます。
- 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から入手できます。

この問題を解決するには、インストール元となる 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取得します。すなわち、SLED で不足しているパッケージを SLES メディアからインストールし、SLES で不足しているパッケージを SLED メディアからインストールします。次の方法では、SLED および SLES の ISO メディアファイルを両方ともマウントして、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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

sudo zypper ar -f /mnt/sles sles
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

Kerberos クライアントのインストール　次のコマンドで、Linux VDA と Delivery Controller 間の相互認証用に Kerberos クライアントをインストールします。

```
sudo zypper install krb5-client
<!--NeedCopy-->
```

Kerberos クライアントの構成は、使用する Active Directory 統合の方法によって異なります。以下の説明を参照してください。

OpenJDK のインストール　OpenJDK 1.7.0 に依存する Linux VDA

> ヒント:
>
> 問題を回避するには、必ず OpenJDK バージョン 1.7.0 のみをインストールしておきます。その他のバージョ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ンの Java は、システムからすべて削除します。

- **SLED**:

1. SLED では、Java Runtime Environment 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ています。次のコマンドで、インストールされているか確認してください。

```
sudo zypper info java-1_7_0-openjdk
<!--NeedCopy-->
```

2. ステータスが out-of-date であると報告された場合は、次のようにして最新バージョンに更新します:

```
sudo zypper update java-1_7_0-openjdk
<!--NeedCopy-->
```

3. 次のコマンドで、Java のバージョンを確認します。

```
java -version
<!--NeedCopy-->
```

- **SLES**:

1. SLES では、次のようにして Java Runtime Environment をインストールします。

```
sudo zypper install java-1_7_0-openjdk
<!--NeedCopy-->
```

2. 次のコマンドで、Java のバージョンを確認します。

```
java -version
<!--NeedCopy-->
```

PostgreSQL のインストール

- SLED/SLES 11 で、次のようにして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
 <!--NeedCopy-->
```

データベースサービスを初期化し、マシンの起動時に PostgreSQL が確実に開始されるようにするには、次に示すインストール後の手順が必要です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /sbin/insserv postgresql

sudo /etc/init.d/postgresql restart
<!--NeedCopy-->
```

- SLED/SLES 12 で、次のようにして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
<!--NeedCopy-->
```

データベースサービスを初期化し、マシンの起動時に PostgreSQL が確実に開始されるようにするには、次に示すインストール後の手順が必要です。

```
sudo systemctl enable postgresql

sudo systemctl restart postgresql
<!--NeedCopy-->
```

データベースファイルは/var/lib/pgsql/data にあります。

リポジトリの削除　依存するパッケージがインストールされると、以前にセットアップした代替エディションのリポジトリを削除し、メディアをマウント解除することができます。

- SLED 11 で、次のコマンドを実行してパッケージを削除します:

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- SLES 11 で、次のコマンドを実行してパッケージを削除します:

```
sudo zypper rr sled

sudo umount /mnt/sled

sudo rmdir /mnt/sled
<!--NeedCopy-->
```

- SLED 12 で、次のコマンドを実行してパッケージを削除します:

```
sudo zypper rr sles

sudo umount /mnt/sles
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- SLED/SLES 12 で、次のコマンドを実行してパッケージを削除します:

```
sudo zypper rr sdk

sudo umount /mnt/sdk

sudo rmdir /mnt/sd
<!--NeedCopy-->
```

手順 **2**: ハイパーバイザー用 **Linux** 仮想マシンの準備

サポートされるハイパーバイザー上で仮想マシンとして Linux VDA を実行する場合、いくつかの変更が必要です。使用するハイパーバイザーのプラットフォームに合わせて、次の変更を行います。ベアメタルハードウェアで Linux マシンを実行する場合、変更は必要ありません。

Citrix XenServer での時刻同期の修正

XenServer の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP と XenServer の両方がシステムの時刻を管理しようとすることが原因で問題が発生します。システムの時刻と他のサーバーの時刻との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時刻が NTP と同期する必要があります。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、変更は必要ありません。

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、XenServer の時刻同期機能が存在するかどうかと、Linux 仮想マシン内で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
<!--NeedCopy-->
```

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いるため、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います。これ以上の操作は必要ありません。

/proc/sys/xen/indepent_wallclock ファイルが存在しない場合、以下の手順は必要ありません。

時刻同期機能が有効になっている場合は、ファイルに「**1**」と書き込んで無効にします:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

この変更を永続化し、再起動後も保持するには、**/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ため、次のようにしてシステムを再起動します:

```
reboot
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

このコマンドは 1 を返します。

Microsoft Hyper-V での時刻同期の修正

Hyper-V Linux 統合サービスがインストールされた Linux 仮想マシンでは、Hyper-V の時刻同期機能を適用してホストオペレーティングシステムの時間を利用できます。システムの時間を正確な状態で維持するには、NTP サービスとともにこの機能を有効にします。

管理オペレーティングシステムで、次の操作を行います。

1. Hyper-V マネージャーを開きます。
2. Linux 仮想マシンの設定で、［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:
>
> この方法は VMware および XenServer の場合とは異なります。VMware および XenServer では、NTP との競合を避けるためにホストの時刻同期を無効にします。Hyper-V の時刻同期は、NTP と共存し、NTP の時刻同期を補完することができます。

ESX および **ESXi** での時刻同期の修正

VMware の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP とハイパーバイザーの両方がシステムの時間を同期しようとすることが原因で問題が発生します。システムの時刻と他のサーバーの時刻との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時刻が NTP と同期する必要があります。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 をインストールした状態で準仮想化 Linux カーネルを実行している場合は、次の操作を行います。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. vSphere Client を開きます。
2. Linux 仮想マシンの設定を編集します。
3. ［仮想マシンのプロパティ］ダイアログボックスで、［オプション］タブをクリックします。
4. ［**VMware Tools**］を選択します。
5. ［詳細］ボックスで、［ホストとゲスト時刻を同期］チェックボックスをオフにします。

手順 **3**：**Linux** 仮想マシン（**VM**）を **Windows** ドメインに追加

Linux VDA は、Linux マシンを Active Directory（AD）ドメインに追加するさまざまな方法をサポートします。

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

選択した方法の手順に従います。

Samba Winbind

Windows ドメインへの参加　ドメインコントローラーがアクセス可能で、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。

1. YaST の［Windows ドメインメンバーシップ］を開きます。
2. 以下の変更を行います。
   - ［ドメイン**/**ワークグループ］に 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 アドレスを設定します。ドメイン名は必ず大文字にします。
   - ［**Linux** の認証にも **SMB** の情報を使用する］チェックボックスをオンにします。
   - ［**Create Home Directory on Login**］チェックボックスをオンにします。
   - ［**SSH** 向けのシングルサインオン］チェックボックスをオンにします。
   - ［オフライン認証］チェックボックスがオフになっていることを確認します。Linux VDA は、このオプションに対応していません。
3. ［**OK**］をクリックします。いくつかのパッケージのインストールを促すメッセージが表示された場合は、［インストール］をクリックします。
4. ドメインコントローラーが見つかると、ドメインに参加するかどうかを確認するメッセージが表示されます。［はい］をクリックします。
5. メッセージが表示されたら、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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. いくつかの Samba および krb5 パッケージのインストールを促すメッセージが表示されたら、［インストール］をクリックします。

YaST により、これらの変更には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が示される場合があります。マシンを再起動することをお勧めします:

```
su -

reboot
<!--NeedCopy-->
```

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 は、デフォルトの Kerberos 資格情報キャッシュ名指定が通常の **FILE:/tmp/krb5cc_%{uid}** から **DIR:/run/user/%{uid}/krb5cc** に変更されました。Linux VDA はこの新しい DIR によるキャッシュ方法に対応していないため、手動で変更する必要があります。次の設定がない場合は、ルートユーザーとして **/etc/krb5.conf** を編集して、［**libdefaults**］セクションに追加します:

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

ドメインメンバーシップの確認　Delivery Controller を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。

次のように、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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Kerberos 構成の確認　Linux VDA で使用できるように Kerberos が正しく構成されていることを確認するには、次のコマンドにより、システムの keytab ファイルが作成済みで keytab ファイルに有効なキーが含まれていることを確認します:

```
sudo klist  - ke
<!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の`kinit`コマンドを実行し、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に対して認証します:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

マシン名と領域名は大文字で指定する必要があります。ドル記号（$）は、シェルによる置き換えを防ぐためにバックスラッシュ（\）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します：

```
sudo klist
<!--NeedCopy-->
```

次のコマンドを使用して、マシンアカウントの詳細を調査します。

```
sudo net ads status
<!--NeedCopy-->
```

ユーザー認証の確認　次のように、`wbinfo`ツールを使用して、ドメインユーザーがドメインに対して認証できることを確認します：

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

ここで指定するドメインは AD ドメイン名で、Kerberos 領域名ではありません。bash シェルの場合、バックスラッシュ文字（\）は、もう 1 つバックスラッシュ文字を指定してエスケープする必要があります。このコマンドにより、成功または失敗を示すメッセージが返されます。

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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

次のコマンドで、**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
<!--NeedCopy-->
```

次のコマンドで、ユーザーの Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します：

```
klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します

```
exit
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gnome コンソールまたは KDE コンソールに直接ログオンすると、同様のテストを実行できます。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。

Quest Authentication Service

ドメインコントローラーでの **Quest** の構成　次の操作は、Quest ソフトウェアを Active Directory ドメインコントローラーにインストールし、構成していることと、管理者特権が付与され、Active Directory にコンピューターオブジェクトを作成できることを前提としています。

Linux VDA マシンにドメインユーザーがログオンできるようにする　Linux VDA マシンで HDX セッションを確立する必要がある各ドメインユーザーに対して、次の操作を行います。

1. ［Active Directory ユーザーとコンピューター］管理コンソールで、目的のユーザーアカウントの Active Directory ユーザーの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］チェックボックスをオンにします。
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:
>
> この手順は、ドメインユーザーがコンソール、RDP、SSH、またはその他のリモート処理プロトコルを使用してログオンできるように設定する場合も同じです。

Linux VDA での Quest の構成

VAS デーモンの構成　次のように Kerberos チケットの自動更新を有効にして、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
<!--NeedCopy-->
```

このコマンドにより、更新間隔が 9 時間（32,400 秒）に設定されます。すなわち、チケットのデフォルトの有効期間である 10 時間よりも 1 時間短くなります。チケットの有効期間がさらに短いシステムでは、より小さい値をこのパラメーターに設定します。

PAM および **NSS** の構成　HDX や、su、ssh、RDP などのその他のサービスを介したドメインユーザーのログオンを有効にするには、次のコマンドを実行して PAM と NSS を手動で構成します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

user は、コンピューターを Active Directory ドメインに追加する権限を持つ任意のドメインユーザーです。**domain-name** は、ドメインの DNS 名（example.com など）です。

ドメインメンバーシップの確認　Delivery Controller を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。Quest によって追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

マシンがドメインに参加している場合は、ドメイン名が返されます。マシンがドメインに追加していない場合、以下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　PAM を使用した Quest のドメインユーザーの認証が可能かどうかを確認するには、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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

次のコマンドで、**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
<!--NeedCopy-->
```

次のコマンドで、Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します。

```
exit
<!--NeedCopy-->
```

Gnome コンソールまたは KDE コンソールに直接ログオンすると、同様のテストを実行できます。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。

Centrify DirectControl

Windows ドメインへの参加　Centrify DirectControl Agent がインストールされている場合、次のように Centrify の **adjoin** コマンドを使用して、Linux マシンを Active Directory ドメインに追加します:

```
su -

adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

user は、コンピューターを Active Directory ドメインに追加する権限を持つ任意の Active Directory ドメインユーザーです。**domain-name** は、Linux マシンを追加す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 を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。Centrify により追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
su -

adinfo
<!--NeedCopy-->
```

Joined to domain が有効であることと、**CentrifyDC mode** に **connected** が返されることを確認します。CentrifyDC mode が starting のまま変化しない場合は、Centrify クライアントにサーバーとの接続の問題、または認証の問題が発生しています。

次を使用すると、より包括的なシステム情報と診断情報を取得できます。

```
adinfo --sysinfo all

adinfo - diag
<!--NeedCopy-->
```

さまざまな Active Directory および Kerberos サービスとの接続をテストします。

```
adinfo --test
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

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。

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

最新の 2 バージョンおよび LTSR リリース以外の古いバージョンの Linux VDA がインストールされている場合は、それをアンインストールしてから新しいバージョンをインストールする必要があります。

1. 次のコマンドで、Linux VDA サービスを停止します:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

2. 次のコマンドで、パッケージをアンインストールします:

```
sudo rpm -e XenDesktopVDA
<!--NeedCopy-->
```

> 重要:
>
> 最新の 2 バージョンからのアップグレードがサポートされます。
>
> 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。代わりに、システムパスに**/opt/Citrix/VDA/sbin** および**/opt/Citrix/VDA/bin** を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、使用している Linux ディストリビューションに応じた適切な 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

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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SUSE 11 の場合:

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

RPM Package Manager 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、次の依存関係を解決します。

SUSE 12 の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

SUSE 11 の場合:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

手順 **4d**: **Linux VDA** のアップグレード（オプション）

RPM Package Manager を使用して、Linux VDA ソフトウェアをバージョン 7.14 や 7.13 に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
<!--NeedCopy-->
```

SUSE 11 の場合:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

RPM 依存関係一覧（**SUSE 12** の場合）:

```
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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
<!--NeedCopy-->
```

RPM 依存関係一覧（**SUSE 11** の場合）:

```
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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要:
>
> アップグレードした後、Linux VDA マシンを再起動してください。

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。このスクリプトは、変更を行う前に環境を確認し、すべての依存コンポーネントがインストールされていることが確認されます。必要に応じて、いつでもこのスクリプトを再実行して設定を変更できます。

このスクリプトは、手動で質問に回答しながら、または事前に構成した回答を使用して自動で実行できます。続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh -help
<!--NeedCopy-->
```

質問に回答する構成

次のようにして、質問に回答する手動構成を実行します:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

自動化された構成

インストールを自動化するために、環境変数を使用して、セットアップスクリプトで必要となるオプションを指定できます。必要な変数がすべて指定されていると、スクリプトによってユーザーに情報の入力を求めるメッセージが表示されることがなくなります。

サポートされる環境変数には次のようなものがあります:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** –Linux VDA では、DNS CNAME レコードを使用して、Delivery Controller 名を指定することができます。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 には、Delivery Controller の登録に使用する Delivery Controller の完全修飾ドメイン名（FQDN）のスペース区切りの一覧が必要です。1 つまたは複数の完全修飾ドメイン名または CNAME エイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT = port-number** –Linux VDA は、TCP/IP ポート（デフォルトではポート 80）を使用して、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します。デフォルトでは値は Y に設定されています。
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** –Linux Virtual Desktop サービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop 用に、

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

システムのファイアウォールの必要なポート（デフォルトではポート 80 およびポート 1494）を自動で開放できます。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 には、Delivery Controller に対して認証するために Kerberos 構成設定が必要です。Kerberos 構成は、システムにインストールおよび構成済みの Active Directory 統合ツールから指定します。次に示す、サポートされている Active Directory 統合方法のうち、使用するものを指定します：
  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 - Centrify DirectControl
  - 4 - SSSD
- **CTX_XDL_HDX_3D_PRO= Y | N** - Linux VDA では、HDX 3D Pro がサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連のグラフィックアクセラレーションテクノロジです。HDX 3D Pro を選択した場合、Virtual Delivery Agent は VDI デスクトップ（シングルセッション）モード用に構成されます（すなわち、CTX_XDL_VDI_MODE=Y となります）。
- **CTX_XDL_VDI_MODE = Y | N** –専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro 環境では、この変数を Y に設定します。デフォルトでは N に設定されています。
- **CTX_XDL_SITE_NAME = dns-name** –Linux VDA は、DNS を使用して LDAP サーバーを検出します。DNS の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、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_LDAP_LIST = list-ldap-servers** –Linux VDA は、DNS を照会して LDAP サーバーを検出します。DNS が LDAP サービスレコードを提供できない場合は、LDAP の FQDN および LDAP ポートのスペース区切りの一覧を指定できます。たとえば、ad1.mycompany.com:389 となります。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_SEARCH_BASE = search-base-set** –Linux VDA は、Active Directory ドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを使用して LDAP を照会します。検索のパフォーマンスを改善するために、検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_START_SERVICE = Y | N** –Linux VDA 構成の完了時に Linux VDA サービスが開始されるようにするかどうかを指定します。デフォルトでは Y に設定されています。

次のようにして、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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
<!--NeedCopy-->
```

sudo コマンドに**-E** オプションを指定して実行し、作成する新しいシェルに既存の環境変数を渡します。最初の行として **#!/bin/bash** を記述し、前述のコマンドからなるシェルスクリプトファイルを作成することを Citrix ではお勧めします。

または、次のようにして、1 つのコマンドですべてのパラメーターを指定することができます:

```
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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

構成変更の削除

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しないで、**ctxsetup.sh** スクリプトによって行われた構成変更を削除することが必要となる場合があります。

続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します:

```
sudo /usr/local/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

構成変更を削除するには:

```
sudo /usr/local/sbin/ctxcleanup.sh
<!--NeedCopy-->
```

> 重要:
>
> このスクリプトにより、すべての構成データがデータベースから削除され、Linux VDA を操作できなくなります。

構成ログ

ctxsetup.sh および **ctxcleanup.sh** スクリプトでは、コンソールにエラーが表示され、次の構成ログファイルに追加情報が書き込まれます:

`/tmp/xdl.configure.log`

Linux VDA サービスを再起動し、変更を反映させます。

手順 6: Linux VDA の実行

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 の起動:

Linux VDA サービスを起動するには、次のコマンドを実行します:

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Linux VDA の停止:

Linux VDA サービスを停止するには、次のコマンドを実行します:

```
sudo /sbin/service ctxvda stop

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

Linux VDA の再起動:

Linux VDA サービスを再起動するには、次のコマンドを実行します:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Linux VDA の状態の確認:

Linux VDA サービスの実行状態を確認するには、次のコマンドを実行します:

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

手順 7: XenApp または XenDesktop でマシンカタログを作成

マシンカタログを作成し、Linux VDA マシンを追加する手順は、従来の Windows VDA での方法と似ています。このタスクを完了する方法の説明について詳しくは、「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。

次のように、Linux VDA マシンを含むマシンカタログの作成にはいくつかの制約があるため、Windows VDA マシンのマシンカタログの作成手順と異なる点があります:

- オペレーティングシステムには、次を選択します:
  - ホストされる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場合、[デスクトップ OS] オプション
- マシンが電源管理を行わない設定になっていることを確認します。
- MCS は Linux VDA ではサポートされないため、PVSまたは他のサービスまたはテクノロジ (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 の以前のバージョンは、「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 サーバー OS] オプションまたは [サーバー OS] オプションを選択すると、同等のホストされる共有デスクトップ配信モデルが暗黙的に選択されます。[Windows デスクトップ OS] オプションまたは [デスクトップ 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暗黙的に選択されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ヒント：
>
> マシンが Active Directory ドメインから削除された後に再度追加された場合は、そのマシンをマシンカタログから削除してから再度追加する必要があります。

手順 **8**：**XenApp** または **XenDesktop** でデリバリーグループを作成

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手順は、Windows VDA マシンの場合とほとんど同じです。このタスクを完了する方法の説明について詳しくは、「デリバリーグループの作成」を参照してください。

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は、次の制約があります：

- 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。
- 選択する AD ユーザーおよびグループを、Linux VDA マシンにログオンするように適切に構成しておきます。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- Windows マシンを含むマシンカタログをデリバリーグループで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、同一マシンへのデスクトップおよびアプリの配信は、Linux VDA でサポートされていません。

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

December 13, 2022

この記事の手順に従って手動でインストールするか、簡単インストールを使用して自動でインストールして構成するかを選択できます。簡単インストールは時間と労力を節約するだけでなく、手動のインストールよりもエラーを減らすことができます。

> 注
>
> ：新規のインストールでは、簡単インストールのみを使用します。既存インストールの更新には、簡単インストールを使用しないでください。

手順 **1**：**Ubuntu for VDA** をインストールする準備

手順 **1a**：ネットワーク構成の確認

続行前にネットワークの接続と、適切に構成されていることを確認します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 **1b**：ホスト名の設定

マシンのホスト名が確実に正しく報告されるようにするには、**/etc/hostname** ファイルを変更してマシンのホスト名のみを記述します。

```
hostname
```

手順 **1c**：ホスト名へのループバックアドレスの割り当て

マシンの DNS ドメイン名と完全修飾ドメイン名（FQDN）が確実に正しく報告されるようにするには、**/etc/hosts** ファイルの以下の行を変更し、最初の 2 つのエントリとして完全修飾ドメイン名とホスト名を記述します：

```
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** に対するその他の参照を削除します。

> 注：
>
> Linux VDA は現在、NetBIOS 名の切り捨てをサポートしていません。したがって、ホスト名は 15 文字以内である必要があります。
>
> ヒント：
>
> a～z、A～Z、0～9、およびハイフン（-）の文字のみ使用してください。アンダースコア（_）、スペース、およびその他の記号は使用しないでください。ホスト名を数字で開始したり、ハイフンで終了し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。

手順 **1d**：ホスト名の確認

次のコマンドで、ホスト名が正しく設定されていることを確認します：

```
hostname
<!--NeedCopy-->
```

このコマンドによって、そのマシンの完全修飾ドメイン名（FQDN）ではなく、そのホスト名のみが返されます。

次のコマンドで、完全修飾ドメイン名が正しく設定されていることを確認します：

```
hostname -f
<!--NeedCopy-->
```

このコマンドにより、そのマシンの完全修飾ドメイン名が返されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 **1e**：マルチキャスト **DNS** の無効化

デフォルトの設定でマルチキャスト DNS（**mDNS**）が有効であるため、名前解決の結果に不整合が発生する場合があります。

mDNS を無効にするには、**/etc/nsswitch.conf** を編集して、以下を含む行を変更します：

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

変更後：

```
hosts: files dns
```

手順 **1f**：名前解決とサービス到達可能性の確認

次のコマンドで、完全修飾ドメイン名が解決できることと、ドメインコントローラーと Delivery Controller から ping に応答があ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
<!--NeedCopy-->
```

完全修飾ドメイン名を解決できない、またはこれらのマシンのいずれかから ping に応答がない場合は、手順を確認してから次に進んでください。

手順 **1g**：時刻同期の構成（**chrony**）

VDA、Delivery Controller、ドメインコントローラーの間で正確な時刻同期を維持することは重要です。仮想マシンとして Linux VDA をホストすると、時刻が不正確になる問題が発生する可能性があります。したがって、リモートのタイムサービスを使用して時刻を維持することをお勧めします。

chrony のインストール：

```
apt-get install chrony
<!--NeedCopy-->
```

ルートユーザーとして **/etc/chrony/chrony.conf** を編集し、次のように各リモートタイムサーバーに対応する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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

一般的な環境では、時間はローカルドメインコントローラーから同期します。公開 NTP プールサーバーから直接は同期しません。ドメインの各 Active Directory ドメインコントローラーに対応する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、パブリックサーバーの ***.pool.ntp.org** エントリなど、一覧にあるその他のサーバーまたはプールエントリを削除します。

変更を保存してから、次のコマンドで Chrony デーモンを再起動します:

```
sudo systemctl restart chrony
<!--NeedCopy-->
```

手順 **1h**: **OpenJDK** のインストール

Linux VDA は OpenJDK に依存しています。通常、Runtime Environment は、オペレーティングシステムの一部としてインストールされています。次のコマンドで、インストールされているか確認してください。

```
sudo apt-get install -y default-jdk
<!--NeedCopy-->
```

手順 **1i**: **PostgreSQL** のインストール

Linux VDA には、Ubuntu 16.04 に PostgreSQL バージョン 9.x が必要です。

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```

手順 **1j**: **Motif** のインストール

```
sudo apt-get install -y libxm4
<!--NeedCopy-->
```

手順 **1k**: 他のパッケージのインストール

```
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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

手順 2：ハイパーバイザーの準備

サポートされるハイパーバイザー上で仮想マシンとして Linux VDA を実行する場合、いくつかの変更が必要です。使用するハイパーバイザーのプラットフォームに合わせて、次の変更を行います。ベアメタルハードウェアで Linux マシンを実行する場合、変更は必要ありません。

Citrix XenServer での時刻同期の修正

XenServer の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP と XenServer の両方がシステムの時間を管理しようとすることが原因となり問題が発生します。システムの時間と他のサーバーの時間との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時間が NTP と同期する必要があります。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、変更は必要ありません。

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、XenServer の時刻同期機能が存在するかどうかと、Linux 仮想マシン内で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
<!--NeedCopy-->
```

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いるため、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います。これ以上の操作は必要ありません。

/proc/sys/xen/indepent_wallclock ファイルが存在しない場合、以下の手順は必要ありません。

時刻同期機能が有効になっている場合は、ファイルに「1」と書き込んで無効にします：

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

この変更を永続化し、再起動後も保持するには、**/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ため、次のようにしてシステムを再起動します：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

このコマンドは 1 を返します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Hyper-V での時刻同期の修正

Hyper-V Linux 統合サービスがインストールされた Linux 仮想マシンでは、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間を利用できます。システムの時間を正確な状態で維持するには、NTP サービスとともに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で、次の操作を行います。

1. Hyper-V マネージャーを開きます。
2. Linux 仮想マシンの設定で、［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：
>
> この方法は VMware および XenServer の場合とは異なります。VMware および XenServer では、NTP との競合を避けるためにホストの時刻同期を無効にします。Hyper-V の時刻同期は、NTP と共存し、NTP の時刻同期を補完することができます。

ESX および **ESXi** での時刻同期の修正

VMware の時刻同期機能が有効な場合、それぞれの準仮想化 Linux 仮想マシンで、NTP とハイパーバイザーの両方がシステムの時間を同期しようとすることが原因となり問題が発生します。システムの時間と他のサーバーの時間との同期が失われるのを防ぐには、各 Linux ゲストのシステムの時間が NTP と同期する必要があります。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 をインストールした状態で準仮想化 Linux カーネルを実行している場合は、次の操作を行います。

1. vSphere Client を開きます。
2. Linux 仮想マシンの設定を編集します。
3. ［仮想マシンのプロパティ］ダイアログボックスで、［オプション］タブをクリックします。
4. ［**VMware Tools**］を選択します。
5. ［詳細］ボックスで、［ホストとゲスト時刻を同期］チェックボックスをオフにします。

手順 **3**：**Linux** 仮想マシン（**VM**）を **Windows** ドメインに追加

Linux VDA は、Linux マシンを Active Directory（AD）ドメインに追加するさまざまな方法をサポートします。

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD

選択した方法の手順に従います。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Samba Winbind

必要なパッケージのインストールまたは更新

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-
    config krb5-locales krb5-user
<!--NeedCopy-->
```

マシンの起動時に **Winbind** デーモンを開始できるようにする　次のコマンドで、マシン起動時に Winbind デーモンが開始するように構成する必要があります。

```
sudo systemctl enable winbind
<!--NeedCopy-->
```

Kerberos の構成　ルートユーザーとして`/etc/krb5.conf`を開き、以下を設定します。

```
[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
<!--NeedCopy-->
```

ここで **domain-dns-name** プロパティは、DNS ドメイン名（**example.com** など）です。**REALM** は、大文字の Kerberos 領域名（**EXAMPLE.COM** など）です。

Winbind 認証の構成　RHEL の`authconfig`や、SUSE の yast2 のようなツールが Ubuntu にないため、手動で Winbind を構成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ルートユーザーとして/etc/samba/smb.confを開き、以下を設定します:

```
[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
<!--NeedCopy-->
```

WORKGROUP は、**REALM** の最初のフィールドです。REALM は大文字の Kerberos 領域名です。

nsswitch の構成　/etc/nsswitch.confを開き、winbindを次の行に追加します:

```
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がアクセス可能で、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
<!--NeedCopy-->
```

ここで、**REALM** は大文字の Kerberos 領域名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

winbind の再起動

```
sudo systemctl restart winbind
<!--NeedCopy-->
```

Winbind 用の **PAM** の構成　次のコマンドを実行して、[**Winbind NT/Active Directory authentication**] オプションと [**Create home directory on login**] オプションが選択されているようにします:

```
sudo pam-auth-update
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ヒント：
>
> マシンがドメインに参加済みの場合にのみ、winbind デーモンは実行を続けます。

ドメインメンバーシップの確認　Delivery Controller を使用するには、Windows または Linux に関係なく、すべての VDA マシンで Active Directory にコンピューターオブジェクトが必要です。

次のように、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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Kerberos 構成の確認　Linux VDA で使用できるように Kerberos が正しく構成されていることを確認するには、次のコマンドによって、システムの **keytab** ファイルが作成済みで keytab ファイルに有効なキーが含まれていることを確認します：

```
sudo klist -ke
<!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の`kinit`コマンドを実行し、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に対して認証します：

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

マシン名と領域名は大文字で指定する必要があります。ドル記号（$）は、シェルによる置き換えを防ぐためにバックスラッシュ（\）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します：

```
sudo klist
<!--NeedCopy-->
```

次のコマンドを使用して、マシンアカウントの詳細を調査します：

```
sudo net ads status
<!--NeedCopy-->
```

ユーザー認証の確認　次のように、**wbinfo** ツールを使用して、ドメインユーザーがドメインに対して認証できることを確認します：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

ここで指定するドメインは AD ドメイン名で、Kerberos 領域名ではありません。bash シェルの場合、バックスラッシュ文字（\）は、もう 1 つバックスラッシュ文字を指定してエスケープする必要があります。このコマンドにより、成功または失敗を示すメッセージが返されます。

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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

次のコマンドで、**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
<!--NeedCopy-->
```

次のコマンドで、ユーザーの Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します：

```
klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します。

```
exit
<!--NeedCopy-->
```

Gnome コンソールまたは KDE コンソールに直接ログオンすると、同様のテストを実行できます。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。

> 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を表示できない場合、マシンを再起動して再試行します。

Quest Authentication Service

ドメインコントローラーでの **Quest** の構成　次の操作は、Quest ソフトウェアを Active Directory ドメインコントローラーにインストールし、構成していることと、管理者特権が付与され、Active Directory にコンピューターオブジェクトを作成できることを前提としています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA マシンにドメインユーザーがログオンできるようにする　Linux VDA マシンで HDX セッションを確立する必要がある各ドメインユーザーに対して、次の操作を行います。

1. ［Active Directory ユーザーとコンピューター］管理コンソールで、目的のユーザーアカウントの Active Directory ユーザーの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］チェックボックスをオンにします。
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:
>
> この手順は、ドメインユーザーがコンソール、RDP、SSH、またはその他のリモート処理プロトコルを使用してログオンできるように設定する場合も同じです。

Linux VDA での **Quest** の構成

SELinux ポリシー適用の回避策　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 ドメインソケットの IPC のメカニズムに干渉し、ドメインユーザーのログオンを妨げます。

この問題を回避するための便利な方法は、SELinux の無効化です。ルートユーザーとして、**/etc/selinux/config** を編集し、**SELinux** 設定を次のとおりに変更します:

```
SELINUX=disabled
```

この変更にはマシンの再起動が必要です:

```
reboot
<!--NeedCopy-->
```

> 重要:
>
> この設定は注意して使用してください。SELinux ポリシーの適用を無効にした後に再度有効にすると、ルートユーザーやその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てしまう可能性があります。

VAS デーモンの構成　次のように Kerberos チケットの自動更新を有効にして、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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

このコマンドにより、更新間隔が 9 時間（32,400 秒）に設定されます。すなわち、チケットのデフォルトの有効期間である 10 時間よりも 1 時間短くなります。チケットの有効期間がさらに短いシステムでは、より小さい値をこのパラメーターに設定します。

PAM および **NSS** の構成　HDX や、su、ssh、RDP などのその他のサービスを介したドメインユーザーのログオンを有効にするには、次のコマンドを実行して PAM と NSS を手動で構成します:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

user は、コンピューターを Active Directory ドメインに追加する権限を持つ任意のドメインユーザーです。domain-name は、ドメインの DNS 名（example.com など）です。

ドメインメンバーシップの確認　Delivery Controller を使用するには、Windows または Linux に関係なく、すべての VDA マシンで Active Directory にコンピューターオブジェクトが必要です。Quest によって追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

マシンがドメインに参加している場合は、ドメイン名が返されます。マシンがドメインに追加していない場合、以下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　PAM を使用した Quest のドメインユーザーの認証が可能かどうかを確認するには、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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

次のコマンドで、**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
<!--NeedCopy-->
```

次のコマンドで、Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

次のコマンドで、セッションを終了します。

```
exit
<!--NeedCopy-->
```

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。

Centrify DirectControl

Windows ドメインへの参加　Centrify DirectControl Agent がインストールされている場合、次のように Centrify の`adjoin`コマンドを使用して、Linux マシンを Active Directory ドメインに追加します:

```
su -

adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

user パラメーターは、コンピューターを Active Directory ドメインに追加する権限を持つ任意の Active Directory ドメインユーザーです。**domain-name** パラメーターは、Linux マシンを追加す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 を使用するには、Windows または Linux に関係なく、すべての VDA マシンで Active Directory にコンピューターオブジェクトが必要です。Centrify により追加された Linux マシンがドメインに存在することを確認するには、次のコマンドを実行します:

```
su -

adinfo
<!--NeedCopy-->
```

Joined to domain が有効であることと、**CentrifyDC mode** に **connected** が返されることを確認します。CentrifyDC mode が starting のまま変化しない場合は、Centrify クライアントにサーバーとの接続の問題、または認証の問題が発生しています。

次を使用すると、より包括的なシステム情報と診断情報を取得できます。

```
adinfo --sysinfo all

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
adinfo --diag
<!--NeedCopy-->
```

さまざまな Active Directory および Kerberos サービスとの接続をテストします。

```
adinfo --test
<!--NeedCopy-->
```

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。

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
<!--NeedCopy-->
```

Kerberos を構成するには、`/etc/krb5.conf`をルートとして開き、次を設定します:

```
[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
<!--NeedCopy-->
```

ここで`domain-dns-name`プロパティは、DNS ドメイン名（`example.com`など）です。`REALM`は大文字の Kerberos 領域名で、`EXAMPLE.COM`などです。

ドメインに参加する　SSSD を構成して、Active Directory を ID プロバイダーおよび認証の Kerberos として使用します。ただし、SSSD では、ドメイン参加とシステムの keytab ファイルの管理に関する AD のクライアント機

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

能が提供されていません。代わりにadcli、realmdまたはSambaを使用できます。

> 注:
>
> このセクションでは、adcliとSambaに関する情報のみを提供します。

adcli を使用してドメインに参加させる:

adcli のインストール:

必要なパッケージをインストールします。

```
sudo apt-get install adcli
<!--NeedCopy-->
```

adcli でドメインに参加させる:

次を使用して古いシステム keytab ファイルを削除し、ドメインに参加させます。

```
su -

rm -rf /etc/krb5.keytab

adcli join domain-dns-name -U user -H hostname-fqdn
<!--NeedCopy-->
```

user は、ドメインにマシンを追加する権限があるドメインユーザーです。**hostname-fqdn** は、完全修飾ドメイン名形式のマシンのホスト名です。

-H オプションは、adcli が、Linux VDA で必要な host/hostname-fqdn@REALM という形式で SPN を生成するのに必要です。

システムの **Keytab** の確認:

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。システムの 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方法:

```
sudo klist -ket
<!--NeedCopy-->
```

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かを検証します。

samba を使用してドメインに参加させる:

パッケージのインストール:

```
sudo apt-get install samba
<!--NeedCopy-->
```

samba の構成:

ルートユーザーとして/etc/samba/smb.confを開き、以下を設定します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[global]

   workgroup = WORKGROUP

   security = ADS

   realm = REALM

   client signing = yes

   client use spnego = yes

   kerberos method = secrets and keytab
<!--NeedCopy-->
```

WORKGROUP は、**REALM** の最初のフィールドです。REALM は大文字の Kerberos 領域名です。

samba でドメインに参加させる:

ドメインコントローラーがアクセス可能で、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
<!--NeedCopy-->
```

ここで、**REALM** は大文字の Kerberos 領域名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

SSSD 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インストールされていない場合、インストールします。

```
sudo apt-get install sssd
<!--NeedCopy-->
```

パッケージが既にインストールされている場合、更新することをお勧めします。

```
sudo apt-get update sssd
<!--NeedCopy-->
```

> 注:
>
> Ubuntu のインストールプロセスは、デフォルトで自動的に **nsswitch.conf** および PAM ログインモジュールを構成します。

SSSD の構成　SSSD デーモンを起動する前に、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ないため、手動で作成する必要があります。root として **/etc/sssd/sssd.conf** を作成するか開いて、次を設定します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[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
<!--NeedCopy-->
```

> 注:
>
> ldap_id_mapping は **true** に設定されるため、SSSD 自体が Windows SID を Unix UID にマッピングします。設定しない場合、Active Directory が POSIX 拡張を提供できるようにする必要があります。PAM サービス（`ctxhdx`）は、ad_gpo_map_remote_interactive に追加されます。

ここで **domain-dns-name** プロパティは、DNS ドメイン名（example.com など）です。**REALM** は、大文字の Kerberos 領域名（EXAMPLE.COM など）です。NetBIOS ドメイン名を構成するための要件はありません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ヒント：
>
> この構成設定について詳しくは、sssd.conf および sssd-ad に関する man ページを参照してください。

SSSD デーモンでは、構成ファイルに所有者読み取り権限のみが設定されている必要があります。

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--NeedCopy-->
```

SSSD デーモンの起動　次のコマンドを実行して、SSSD デーモンを起動し、マシンの起動時にもデーモンを起動できるようにします。

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

PAM 構成　次のコマンドを実行して、［**SSS authentication**］オプションと ［**Create home directory on login**］オプションが選択されているようにします：

```
sudo pam-auth-update
<!--NeedCopy-->
```

ドメインメンバーシップの確認　Delivery Controller を使用するには、すべての VDA マシン（Windows と Linux VDA）で Active Directory にコンピューターオブジェクトが必要です。

adcli を使用したドメインメンバーシップの確認：

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
<!--NeedCopy-->
```

samba を使用したドメインメンバーシップの確認：

次のように、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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Kerberos 構成の確認　Linux VDA で使用できるように Kerberos が正しく構成されていることを確認するには、次のコマンドによって、システムの keytab ファイルが作成済みで keytab ファイルに有効なキーが含まれていることを確認します:

```
sudo klist -ke
<!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の`kinit`コマンドを実行し、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に対して認証します:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

マシン名と領域名は大文字で指定する必要があります。ドル記号（$）は、シェルによる置き換えを防ぐためにバックスラッシュ（\）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します。

```
sudo klist
<!--NeedCopy-->
```

ユーザー認証の確認　SSSD は、デーモンで直接認証をテストするコマンドラインツールを提供しません。PAM 経由でのみ完了できます。

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。以前はドメインユーザーアカウントは使用されていませんでした。

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

ユーザーの **klist** コマンドで返される Kerberos チケットが正しく、期限切れではないことを確認します。

ルートユーザーとして、前述の **id -u** コマンドで返された 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
<!--NeedCopy-->
```

KDE または Gnome Display Manager に直接ログオンすると、同様のテストを実行できます。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Web サイトにアクセスし、環境の 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

次のように、Debian Package Manager 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
<!--NeedCopy-->
```

Ubuntu の Debian 依存関係一覧：

```
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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
libgoogle-perftools4 >= 2.4~
<!--NeedCopy-->
```

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。このスクリプトは、変更を行う前に環境を確認し、すべての依存コンポーネントがインストールされていることが確認されます。必要に応じて、いつでもこのスクリプトを再実行して設定を変更できます。

このスクリプトは、手動で質問に回答しながら、または事前に構成した回答を使用して自動で実行できます。続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh -help
<!--NeedCopy-->
```

質問に回答する構成　次のようにして、質問に回答する手動構成を実行します：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

自動化された構成　インストールを自動化するために、環境変数を使用して、セットアップスクリプトで必要となるオプションを指定できます。必要な変数がすべて指定されていると、スクリプトによってユーザーに情報の入力を求めるメッセージが表示されることがなくなり、インストール処理をスクリプト化できます。

サポートされる環境変数には次のようなものがあります：

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** - Linux VDA では、DNS CNAME レコードを使用して、Delivery Controller 名を指定できます。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 には、Delivery Controller の登録に使用する Delivery Controller の完全修飾ドメイン名（FQDN）のスペース区切りの一覧が必要です。1 つまたは複数の完全修飾ドメイン名または CNAME エイリアスを指定する必要があります。
- **CTX_XDL_VDA_PORT = port-number** - Linux VDA は、TCP/IP ポート（デフォルトではポート 80）を使用して、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します。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 サービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop 用に、システムのファイアウォールの必要なポート（デフォルトではポート 80 およびポート 1494）を自動で開放できます。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 には、Delivery Controller に対して認証するために Kerberos 構成設定が必要です。Kerberos 構成は、システムにインストールおよび構成済みの Active

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directory 統合ツールから指定します。次に示す、サポートされている Active Directory 統合方法のうち、使用するものを指定します：

  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 - Centrify DirectControl
  - 4 - SSSD

- **CTX_XDL_HDX_3D_PRO = Y | N** - Linux VDA では、HDX 3D Pro がサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連のグラフィックアクセラレーションテクノロジです。HDX 3D Pro を選択した場合、Virtual Delivery Agent は VDI デスクトップ（シングルセッション）モード用に構成されます（すなわち、CTX_XDL_VDI_MODE=Y となります）。
- **CTX_XDL_VDI_MODE = Y | N** - 専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro 環境では、この変数を Y に設定します。デフォルトでは N に設定されています。
- **CTX_XDL_SITE_NAME = dns-name** - Linux VDA は、DNS を使用して LDAP サーバーを検出します。DNS の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、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_LDAP_LIST = list-ldap-servers** - Linux VDA は、DNS を照会して LDAP サーバーを検出します。DNS が LDAP サービスレコードを提供できない場合は、LDAP の FQDN および LDAP ポートのスペース区切りの一覧を指定できます。たとえば、ad1.mycompany.com:389 となります。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_SEARCH_BASE = search-base-set** - Linux VDA は、Active Directory ドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを使用して LDAP を照会します。ただし、検索のパフォーマンスを改善するために、検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。この変数は、デフォルトでは **<none>** に設定されています。
- **CTX_XDL_START_SERVICE = Y | N** - Linux VDA 構成の完了時に Linux VDA サービスが開始されるようにするかどうかを指定します。デフォルトでは Y に設定されています。

次のようにして、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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

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
<!--NeedCopy-->
```

sudo コマンドに**-E** オプションを指定して実行し、作成する新しいシェルに既存の環境変数を渡します。最初の行として **#!/bin/bash** を記述し、前述のコマンドからなるシェルスクリプトファイルを作成することを Citrix ではお勧めします。

または、次のようにして、1 つのコマンドですべてのパラメーターを指定することができます。

```
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
<!--NeedCopy-->
```

構成変更の削除　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しないで、**ctxsetup.sh** スクリプトによって行われた構成変更を削除することが必要となる場合があります。

続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

構成変更を削除するには:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--NeedCopy-->
```

> 重要:
>
> このスクリプトにより、すべての構成データがデータベースから削除され、Linux VDA を操作できなくなります。

構成ログ　**ctxsetup.sh** および **ctxcleanup.sh** スクリプトでは、コンソールにエラーが表示され、構成ログファイル **/tmp/xdl.configure.log** に追加情報が書き込まれます。

Linux VDA サービスを再起動し、変更を反映させます。

Linux VDA ソフトウェアのアンインストール　Linux VDA がインストールされているかどうかを確認したり、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、次のコマンドを実行します。

```
dpkg -l xendesktopvda
<!--NeedCopy-->
```

詳細を表示するには、次のコマンドを実行します。

```
apt-cache show xendesktopvda
<!--NeedCopy-->
```

Linux VDA ソフトウェアをアンインストールには、次のコマンドを実行します:

```
dpkg -r xendesktopvda
<!--NeedCopy-->
```

> 注:
>
> Linux VDA ソフトウェアをアンインストールすると、関連付けられた 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 のインストールより前にセットアップされた、PostgreSQL パッケージおよびその他の依存するパッケージは削除されません。
>
> ヒント:
>
> このセクションでは、PostgreSQL など、依存するパッケージの削除方法については説明していません。

手順 5: Linux VDA の実行

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA の起動:

Linux VDA サービスを起動するには、次のコマンドを実行します:

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Linux VDA の停止:

Linux VDA サービスを停止するには、次のコマンドを実行します:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

Linux VDA の再起動:

Linux VDA サービスを再起動するには、次のコマンドを実行します:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

Linux VDA の状態の確認:

Linux VDA サービスの実行状態を確認するには、次のコマンドを実行します。

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

手順 6: **XenApp** または **XenDesktop** でマシンカタログを作成

マシンカタログを作成し、Linux VDA マシンを追加する手順は、従来の Windows VDA での方法と似ています。このタスクを完了する方法の説明について詳しくは、「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。

次のように、Linux VDA マシンを含むマシンカタログの作成にはいくつかの制約があるため、Windows VDA マシンのマシンカタログの作成手順と異なる点があります:

- オペレーティングシステムには、次を選択します:
  - ホストされる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場合、[デスクトップ OS] オプション

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- マシンが電源管理を行わない設定になっていることを確認します。
- MCS は Linux VDA ではサポートされないため、PVSまたは他のサービスまたはテクノロジ（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 の以前のバージョンは、「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 サーバー OS] オプションまたは [サーバー OS] オプションを選択すると、同等のホストされる共有デスクトップ配信モデルが暗黙的に選択されます。[Windows デスクトップ OS] オプションまたは [デスクトップ 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暗黙的に選択されます。
>
> ヒント：
>
> マシンが Active Directory ドメインから削除された後に再度追加された場合は、そのマシンをマシンカタログから削除してから再度追加する必要があります。

手順 **7**：**XenApp** または **XenDesktop** でデリバリーグループを作成

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手順は、Windows VDA マシンの場合とほとんど同じです。このタスクを完了する方法の説明について詳しくは、「デリバリーグループの作成」を参照してください。

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は、次の制約があります：

- 配信の種類には、[デスクトップ] を選択します。Linux VDA for Ubuntu では、アプリケーション配信はサポートされていません。
- 選択する AD ユーザーおよびグループを、Linux VDA マシンにログオンするように適切に構成しておきます。
- 認証されていない（匿名）ユーザーのログオンを許可しないでください。
- Windows マシンを含むマシンカタログをデリバリーグループで混在させないでください。

Linux VDA の構成

November 21, 2020

このセクションでは、機能の説明、構成、トラブルシューティングなど、Linux VDA の機能について詳しく説明します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NIS の Active Directory との統合

November 30, 2022

このトピックでは、SSSD を使用して、NIS を Linux VDA の 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 および XenDesktop のコンポーネントと考えられています。そのため Linux VDA は、Windows AD 環境に密接に結びついています。

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には、AD と NIS でユーザー名とパスワードの組み合わせのアカウント情報を同一にする必要があります。

> 注:
>
> NIS を使用した場合も、認証は AD サーバーにより行われます。NIS+ はサポートされません。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 属性は使用されません。
>
> ヒント:
>
> これは、Linux VDA を展開する方法として廃止済みであるため、特定のユースケースでのみ使用してください。RHEL/CentOS ディストリビューションの場合は、「Linux Virtual Delivery Agent for RHEL/CentOS のインストール」の指示に従ってください。Ubuntu ディストリビューションの場合は、「Linux Virtual Delivery Agent for Ubuntu のインストール」の指示に従ってください。

SSSD:

SSSD はシステムデーモンです。SSSD 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する共通フレームワークを通じて、リモートリソースの識別および認証のアクセスを提供することです。PAM や NSS モジュールを提供しており、将来的には D-BUS ベースのインターフェイスもサポートして、拡張ユーザー情報に対応する予定です。また、ローカルユーザーアカウントと拡張ユーザー情報を保存するための優れたデータベースを提供します。

必要なソフトウェア

AD プロバイダーは、SSSD Version 1.9.0 で初めて導入されました。

次の環境については、このドキュメントに記載した指示を使用したテストおよび検証を行っています。

- RHEL 7.3 以降/CentOS 7.3 以降
- Linux VDA Version 1.3 以降

NIS と AD の統合

NIS と AD を統合するには、次の手順を実行します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Linux VDA を NIS クライアントとして追加
2. ドメインに参加し、Samba を使用してホストの keytab を作成
3. SSSD のセットアップ
4. NSS/PAM の構成
5. Kerberos 構成の確認
6. ユーザー認証の確認

Linux VDA を **NIS** クライアントとして追加

NIS クライアントを構成します。

```
yum -y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```

NIS ドメインを設定します。

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

nis.domain は、NIS サーバーのドメイン名です。**server.nis.domain** は、NIS サーバーのホスト名であり、NIS サーバーの IP アドレスにもできます。

NIS のサービスを設定します。

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

NIS の構成が正しいことを確認します。

```
ypwhich
<!--NeedCopy-->
```

NIS サーバーからアカウント情報が使用できることを確認します。

```
getent passwd nisaccount
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> **nisaccount** は、NIS サーバーの実際の NIS アカウントです。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設定されていることを確認します。

ドメインに参加し、**Samba** を使用してホストの **keytab** を作成

SSSD では、ドメイン参加とシステムの keytab ファイルの管理に関する AD のクライアント機能が提供されていません。この機能を取得するには次のような方法があります:

- adcli
- realmd
- Winbind
- Samba

このセクションでは、Samba によるアプローチについてのみ説明します。**realmd** については、RHEL または CentOS のベンダーのドキュメントを参照してください。SSSD を構成する前に、以下の手順に従う必要があります。

ドメインに参加し、**Samba** を使用してホストの **keytab** を作成する:

Linux クライアントで、適切に構成されたファイルを使用します。

- /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
<!--NeedCopy-->
```

ここで、**REALM** は大文字の Kerberos 領域名で、**domain** はドメインの NetBIOS 名です。

KDC サーバーおよび領域名を DNS ベースで参照する必要がある場合は、次の 2 つのオプションを前述のコマンドに追加します:

```
--enablekrb5kdcdns --enablekrb5realmdns
```

/etc/samba/smb.conf を開いて、[**Global**] セクションに次のエントリを追加します。ただし、追加するのは、**authconfig** ツールによって生成されたセクションの後です:

```
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できることと、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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

REALM は大文字の Kerberos 領域名で、**user** はコンピューターをドメインに追加する権限を持つドメインユーザーです。

SSSD のセットアップ

SSSD のセットアップは、以下の手順で構成されています:

- Linux クライアントマシンに **sssd-ad** パッケージおよび **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に設定の変更を行います（**sssd.conf** など）。
- **sssd** サービスを開始します。

/etc/sssd/sssd.conf　**sssd.conf** の設定の例（必要に応じて追加の設定を行うことができます）:

```
[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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ad.domain.com と **server.ad.example.com** を対応する値で置き換えます。詳しくは、「sssd-ad(5) - Linux man page」を参照してください。

ファイルの所有権およびアクセス権を **sssd.conf** で設定します:

```
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、このホームディレクトリの作成機能が SELinux に対応していることを確認します:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
6 <!--NeedCopy-->
```

> ヒント:
>
> Linux VDA の設定を行うときは、SSSD では Linux VDA クライアントの特別な設定がないことを考慮します。**ctxsetup.sh** スクリプトでのその他の解決方法としては、デフォルト値を使用します。

Kerberos 構成の確認

Linux VDA で使用できるように Kerberos が正しく構成されていることを確認するには、次のコマンドにより、システムの **keytab** ファイルが作成済みで keytab ファイルに有効なキーが含まれていることを確認します:

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

このコマンドにより、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に対して使用できるキーの一覧が表示されます。Kerberos の **kinit** コマンドを実行し、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に対して認証します:

```
1 sudo kinit  - k MACHINE$@REALM
2 <!--NeedCopy-->
```

マシン名と領域名は大文字で指定する必要があります。ドル記号（$）は、シェルによる置き換えを防ぐためにバックスラッシュ（\）でエスケープする必要があります。環境によっては、DNS ドメイン名が Kerberos 領域名と異なります。したがって、必ず領域名を使用します。このコマンドが成功すると、出力は表示されません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

次のコマンドを使用して、マシンアカウントの TGT チケットがキャッシュされたことを確認します:

```
sudo klist -ke
<!--NeedCopy-->
```

ユーザー認証の確認

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こと、および NSS が機能するかどうかを確認します:

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

DOMAIN パラメーターは短い形式のドメイン名です。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ます。

サポートされているログオン形式は次の通りです:

- 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。以前はドメインユーザーアカウントは使用されていませんでした。

```
sudo localhost  - l DOMAIN\username

id -u
<!--NeedCopy-->
```

次の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 }

<!--NeedCopy-->
```

次のコマンドで、ユーザーの Kerberos 資格情報キャッシュのチケットが有効で、期限切れではないことを確認します:

```
klist
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

公開アプリケーション

July 8, 2022

Linux VDA バージョン 7.13 では、Citrix でシームレスアプリケーション機能がサポート対象のすべての Linux プラットフォームに追加されました。この機能を使用するのに特別なインストール手順は不要です。

> ヒント：
>
> Linux VDA Version 1.4 では、非シームレスな公開アプリケーションとセッションの共有のサポートが Citrix で追加されました。

Citrix Studio を使ってアプリケーションを公開する

デリバリーグループを作成したり、既存のデリバリーグループにアプリケーションを追加したりすると、Linux VDA にインストールしたアプリケーションを公開することができます。このプロセスは、Windows VDA にインストールしたアプリケーションを公開する場合と同様です。詳しくは、Citrix Virtual Apps and Desktops ドキュメント（使用中の Citrix Virtual Apps and Desktops のバージョン）を参照してください。

> ヒント：
>
> デリバリーグループの構成では、デリバリーの種類を ［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］ に設定します。
>
> 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、同一マシンへのデスクトップおよびアプリの配信は、Linux VDA でサポートされていません。この問題に対処するには、アプリおよびデスクトップの配信で個別のデリバリーグループを作成することを Citrix ではお勧めします。
>
> 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。既に「TWIMode=Off」を設定して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。削除しない場合は、公開デスクトップを起動できないことがあります。

トラブルシューティング

公開アプリケーションの起動に 3 分以上かかり、シームレスモードでウィンドウを表示できない場合があります。問題が発生した場合は、シームレスモードが Linux VDA と StoreFront の両方で有効になっていることを確認します。

Linux VDA でシームレスモードが有効になっているかどうかを確認するコマンドは次のとおりです。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

「SeamlessEnabled = 0x00000000」と表示される場合、シームレスモードは無効です。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 "0
    x00000001"
<!--NeedCopy-->
```

既知の問題

アプリケーション公開時の既知の問題は次のとおりです:

- シームレスモードが StoreFront で無効になっている一方で、Linux VDA では有効なままの場合は、非シームレスな公開アプリケーションを起動できません。Linux VDA および 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ます。
- 非矩形のウィンドウはサポートされません。ウィンドウの隅にサーバー側の背景が表示されることがあります。
- ウィンドウの内容を公開アプリケーションからプレビューすることはサポートされていません。
- 現在、シームレスモードでは次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\SUSE 12.2）、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。ウィンドウマネージャーが、サポートされているモードに設定されていることを確認してください。
- 複数の LibreOffice アプリケーションによってプロセスが共有されるため、Citrix Studio には最初に起動したもののみが表示されます。
- 「Dolphin」などの公開された Qt5 ベースのアプリケーションについてはアイコンが表示されないことがあります。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 セッション内で実行されている公開アプリケーションのすべてのタスクバーボタンが同じグループに結合されます。この問題を解決するには、タスクバーボタンを結合しないようにタスクバーのプロパティを設定します。

印刷

July 31, 2021

ここでは、印刷のベストプラクティスについて説明します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

インストール

Linux VDA では、**cups** フィルターと **foomatic** フィルターの両方が必要です。Linux ディストリビューションに基づき、次のコマンドを実行します:

RHEL 7 印刷のサポート:

```
sudo yum -y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

RHEL 6 印刷のサポート:

```
sudo yum -y install cups

sudo yum -y install foomatic
<!--NeedCopy-->
```

用途

公開デスクトップおよび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 セッションに割り当てられます。デスクトップとアプリケーションとで異なるプリンター名にする必要があります。以下に注意してください:

- 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:
>
> 同一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は、どちらのプリンターもセッションで使用できます。公開アプリケーションのセッション内でのデスクトッププリンターへの印刷、または公開デスクトップでのアプリケーションプリンターへの印刷は失敗します。

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に確認する項目にはいろいろあります。印刷デーモンはセッションごとのプロセスで、実行されるのはセッションの期間中です。印刷デーモンが実行中であることを確認します。

```
ps -ef | grep ctxlpmngt
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ctxlpmngt プロセスが実行中でない場合は、コマンドラインから手動で **ctxlpmngt** を起動します。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ます。**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。これはマシンごとの単一プロセスとなっていて、次のコマンドで確認できます。

```
service ctxcups status
<!--NeedCopy-->
```

CUPS 印刷時の余分なログ

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の取得方法はその他のコンポーネントと同様です。

RHEL の場合、CUPS サービスファイルの構成には追加の手順が必要です。追加の手順を実行しないと、一部のログが **hdx.lo** で記録されません:

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--NeedCopy-->
```

> 注:
>
> この構成は、問題が発生した場合に完全な印刷ログを収集することのみを目的としています。通常は、CUPS のセキュリティが破られるため、この構成はお勧めしません。

印刷出力が文字化けする

対応していないプリンタードライバーを使用していることが、出力の文字化けの原因になっている可能性があります。ユーザーごとのドライバー構成を使用できるため、**~/.CtxlpProfile$CLIENT_NAME** 構成ファイルを編集して構成できます:

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

> 重要:
>
> **printername** は、現在のクライアント側の通常使うプリンターの名前が指定されているフィールドです。これは読み取り専用の値です。編集しないでください。
>
> **ppdpath**、**model**、**drivertype** の各フィールドは、マップされたプリンターに対していずれか 1 つのフィールドしか有効にならないため、同時には設定できません。

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に対応していない場合、**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表示できます:

```
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
<!--NeedCopy-->
```

次のようにして、プリンターに一致するようにモデルを設定できます。

```
Model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

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に対応していない場合、ネイティブプリンタードライバーの PPD ファイルのパスを構成します。**ppdpath** の値は、ネイティブプリンタードライバーファイルの絶対パスです。

たとえば、**ppd** ドライバーが/home/tester/NATIVE_PRINTER_DRIVER.ppd にある場合は、次のようになります:

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

Citrix が提供するユニバーサルプリンタードライバーは 3 種類（Postscript、pcl5、pcl6）です。ネイティブプリンタードライバーが使用できない場合は、ドライバーの種類を設定できます。

たとえば、クライアントが通常使うプリンターのドライバーの種類が PCL5 である場合は、次のようになります。

```
drivertype=pcl5
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

出力サイズがゼロ

別の種類のプリンターを試します。また、CutePDF や PDFCreator などの仮想プリンターを使用してみて、この問題がプリンタードライバーに関連するものかどうかを確認します。

印刷ジョブは、クライアントが通常使用するプリンターのドライバーによって異なります。現在適用されているドライバーの種類を特定することが重要です。クライアントのプリンターが PCL5 ドライバーを使用している一方で、Linux VDA が PostScript ドライバーを選択していると、問題が発生する場合があります。

プリンタードライバーの種類が正しい場合は、次の手順に従って問題を特定します。

問題を特定する方法:

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

```
deletespoolfile=no
<!--NeedCopy-->
```

4. いったんログオフしてからログオンし直して、構成の変更を読み込みます。
5. ドキュメントを印刷して問題を再現します。印刷が完了すると、**/var/spool/cups-ctx/$logon_user/$spool_file** にスプールファイルが保存されます。
6. スプールファイルが空であるかどうかを確認します。スプールファイルのサイズが 0 の場合は、これが問題になります。Citrix サポートに印刷ログを提供して、ガイダンスに従ってください。
7. スプールファイルのサイズが 0 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、クライアントが通常使用する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の（ネイティブ）ドライバーが PostScript である場合、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 の場合は、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。この手順の完了後に、別のプリンタードライバーを使用してテスト印刷します。
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、たとえば PostScript クライアントプリンターを使用します。

   a) アクティブセッションにログオンして、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
   <!--NeedCopy-->
   ```

   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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d) CUPS と CTX 間の接続を保持したまま［続行］をクリックし、プリンタードライバーを変更します。

e)［製造元とモデル］ページで、Citrix UPD ドライバーの代わりに他の PostScript ドライバー（Citrix Universal Driver PostScript など）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、［汎用 CUPS-PDF プリンター］を選択します。変更を保存します。

f) このプロセスが正常に完了した場合は、ドライバーの PPD ファイルパスを**.CtxlpProfile$CLIENT_NAME** で設定し、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します。

既知の問題

Linux VDA での印刷について、次の問題が確認されています。

CTXPS ドライバーが一部の **PLC** プリンターに対応しない

印刷出力が適切でない場合は、プリンタードライバーを、製造元から提供されたネイティブプリンタードライバーに設定してください。

サイズの大きな文書の印刷が遅い

ローカルのクライアントプリンターでサイズの大きなドキュメントを印刷すると、そのドキュメントはサーバーとの接続を介して転送されます。遅い接続では、この転送に時間がかかることがあります。

別のセッションからプリンター通知と印刷ジョブ通知が表示される

Linux でのセッションの考え方は、Windows オペレーティングシステムとは異なります。したがって、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。次の CUPS 構成ファイルを変更して、これらの通知を無効にできます：**/etc/cups/cupsd.conf**。

次のように、構成されている現在のポリシー名がこのファイルに記述されています。

```
DefaultPolicy default
```

ポリシー名が *default* である場合は、次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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
11        SubscriptionPrivateValues default
12
13        … …
14
15        <Limit Create-Printer-Subscription>
16
17             Require user @OWNER
18
19             Order deny,allow
20
21        </Limit>
22
23        <Limit All>
24
25             Order deny,allow
26
27        </Limit>
28
29   </Policy>
30   <!--NeedCopy-->
```

PDF 印刷

August 10, 2021

PDF 印刷に対応したバージョンの Citrix Workspace アプリを使用すると、Linux VDA セッションから変換された PDF を印刷できます。セッション印刷ジョブは、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 ビューアーを使用して PDF を開き、選択したプリンターで印刷することができます。

Linux VDA は以下のバージョンの Citrix Workspace アプリで PDF 印刷をサポートします:

- Citrix Receiver for HTML5 バージョン 2.4～2.6.9、HTML5 向け Citrix Workspace アプリ 1808 以降
- Citrix Receiver for Chrome バージョン 2.4～2.6.9、Chrome 向け Citrix Workspace アプリ 1808 以降
- Windows 向け Citrix Workspace アプリ 1905 以降

構成

PDF 印刷機能に対応した Citrix Workspace アプリを使用し、Citrix Studio で以下のポリシーを有効にします:

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

これらのポリシーが有効になっている場合、起動されたセッションで ［印刷］ をクリックすると、ローカルマシンの印刷プレビューに表示され、プリンターを選択できます。デフォルトプリンターの設定について詳しくは、Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

November 30, 2022

ここでは、Linux VDA のグラフィックの構成と微調整について説明します。

詳しくは、「システム要件」および「インストールの概要」を参照してください。

構成パラメーター

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は **HKEY_LOCAL_MACHINE\System\CurrentCo** にいくつかあります。

Thinwire Plus を有効にする方法

Thinwire Plus は、標準の VDA および 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

H.264 は、オペレーティングシステムの要件のほか、Citrix Workspace アプリ（Citrix Receiver の新名称）のバージョンにも最低条件があります。クライアントが要件を満たさない場合は、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 の最低条件
Windows	3.4 以降
Mac OS X	11.8 以降
Linux	13.0 以降
Android	3.5
iOS	5.9
Chrome OS	1.4

最新の Citrix Workspace アプリ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を参照してください。

次のコマンドを実行して、H.264 エンコーディングを VDA でアドバタイズします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

HDX 3D Pro の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 **AdvertiseH264** 設定では、ソフトウェアの H.264 エンコーディングのみが有効になります。次のコマンドを実行してハードウェアエンコーディングを有効にします:

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

> 注:
>
> 「`ctxreg command can't be found`」というエラーが表示された場合は、フルパスを指定して`ctxreg`コマンドを使用します。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。

Thinwire Plus を低帯域幅用に調整する方法

- MaxColorDepth

  ```
  Default 0x20, type DWORD
  <!--NeedCopy-->
  ```

  このオプションは、Thinwire プロトコルによりクライアントに転送されるグラフィックの色数を指定します。

  帯域幅を節約するには、色数を 0x10（シンプルなグラフィック用の優先色数）または 0x8（実験的な低帯域幅モード）に設定します。

- 品質

  表示品質

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- その他のパラメーター
  - TargetFPS

    ターゲットフレーム数

    ```
    Default: 0x1e (30), Type: DWORD
    <!--NeedCopy-->
    ```

  - MinFPS

    保持する最低フレーム数

    ```
    Default: 0xa (10), Type: DWORD
    <!--NeedCopy-->
    ```

  - MaxScreenNum

    1 人のユーザーが所有できるモニターの最大数

    ```
    Default: 0x2, Type: DWORD
    <!--NeedCopy-->
    ```

    標準 VDA の場合、最大値には 10 までの値を設定できます。3D Pro で許可される最大値は 4 です。

トラブルシューティング

どのエンコーディングが使用中かの確認

次のコマンドを実行して、H.264 エンコーディングが使用中であるかどうかを確認します。「**1**」は H.264、「**0**」は TW+ の意味です:

```
sudo ctxreg dump | grep H264
<!--NeedCopy-->
```

次の内容に類似した結果が出力されます。

```
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 のハードウェアエンコーディングが使用中であるかどうかの確認

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、**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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

次の内容に類似した結果が出力されます。

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

これ以外にも **nvidia-smi** コマンドを使用する方法があります。ハードウェアエンコーディングが使用中の場合は、次の内容に類似した結果が出力されます:

```
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 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

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します

NVIDIA GRID グラフィックスドライバーが正しくインストールされているかどうかを確認するには、**nvidia-smi** を実行します。次の内容に類似した結果が出力されます。

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70         |
|-------------------------------+----------------------+----------------------+
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
| 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
                                 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

次のコマンドで、カードに適切な構成を設定します:

```
etc/X11/ctx-nvidia.sh
```

HDX 3D Pro マルチモニターでの再描画の問題

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 のエラーログを確認する

Xorg のログファイルは、**Xorg.{DISPLAY}.log** に類似した名前で **/var/log/** フォルダー内にあります。

既知の問題と制限事項

vGPU で、**XenServer** のローカルコンソールに **ICA** デスクトップの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、仮想マシンのローカル 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"
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NVENC API が、**8Q** 以外の **vGPU** プロファイルでサポートされない

NVIDIA Tesla M60 カードの 8Q を除く vGPU プロファイルでは CUDA がサポートされていないため、NVENC API および Citrix 3D Pro のハードウェアエンコーディングを利用することはできません。

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ない

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くなる

これは Gnome 3 デスクトップのセッション開始時の機能的制限です。

一部の **OpenGL** および **WebGL** アプリケーションが、**Citrix Receiver** ウィンドウのサイズ変更時に適切に表示されない

Citrix Receiver のウィンドウサイズを変更すると、画面の解像度も変更されます。NVIDIA の独自ドライバーにより内部状態が一部変更されるため、それに応じた対応がアプリケーションに求められる場合があります。たとえば、WebGL ライブラリ要素の **lightgl.js** によって「`Rendering to this texture is not supported (incomplete frame buffer)`」というエラーメッセージが生成されることがあります。

GRID 以外の 3D グラフィック

March 11, 2024

概要

Linux VDA で NVIDIA GRID 3D カードだけでなく、GRID 以外の 3D カードもサポートするように機能が拡張されました。

インストール

GRID 以外の 3D グラフィックスの機能を使用するには、以下を実行する必要があります:

- 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ています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Linux VDA をインストールする場合は、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: Runtime Environment をセットアップしてインストールを完了する」を参照してください。

構成

Xorg の構成ファイル

ご使用の 3D カードドライバーが NVIDIA の場合、構成ファイルは自動でインストールおよび設定されます。

他の種類の **3D** カード

ご使用の 3D カードドライバーが NVIDIA 以外の場合は、/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 を例として使用しながら、以下の手順に従ってテンプレート構成ファイルを変更します:

1. ***driver_name*** は、実際のドライバー名で置き換えてください。

   たとえば、ドライバー名がintelの場合は、構成ファイル名をctx-intel-1に変更できます。

2. ビデオドライバー情報を追加します。

   各テンプレート構成ファイルには、「Device」という名前のセクションがあり、コメントアウトされています。このセクションでは、ビデオドライバー情報を記述します。ビデオドライバー情報を追加する前に、このセクションを有効にします。このセクションを有効にするには:

   a) 製造元から提供されている 3D カードガイドを参照して構成情報を確認します。ネイティブ構成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、ネイティブ構成ファイルを使用して、ローカル環境で 3D カードが動作可能であることを確認します。

   b) ネイティブ構成ファイルの［Device］セクションを **ctx-driver_name-1.conf** にコピーします。

3. 次のコマンドを実行して、手順 1 で設定した構成ファイル名を Linux VDA が認識できるように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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

GRID 以外の **3D** グラフィック機能を有効にする

GRID 以外の 3D グラフィック機能はデフォルトで無効です。次のコマンドを実行して XDamageEnabled を 1 に設定することで有効にできます。

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

トラブルシューティング

グラフィック出力がないか文字化けする

ローカルで 3D アプリケーションを実行でき、すべてを適切に構成しているのにグラフィック出力がないまたは不明瞭であるとすると、原因はバグです。/opt/Citrix/VDA/bin/setlog を使用して GFX_X11 を verbose に設定することでデバッグ用にトレース情報を収集します。

ハードウェアエンコーディングが機能しない

この機能で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。

ポリシーの設定

November 11, 2021

インストール

Linux VDA の準備についてはインストールのトピックを参照してください。

依存関係

Linux VDA パッケージのインストール前に、次の依存関係をインストールします。

RHEL/CentOS:

```
sudo yum -y install openldap

sudo yum -y install libxml2

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo yum -y install cyrus-sasl

sudo yum -y install cyrus-sasl-gssapi
<!--NeedCopy-->
```

SLES/SELD:

```
sudo zypper install openldap2

sudo zypper install libxml2

sudo zypper install cyrus-sasl

sudo zypper install cyrus-sasl-gssapi
<!--NeedCopy-->
```

Ubuntu:

```
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
<!--NeedCopy-->
```

構成

Citrix Studio のポリシー設定

Citrix Studio のポリシー設定は、次の操作を行います。

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. 「ポリシーサポート一覧」に沿ってポリシーを設定します。

VDA での **LDAP** サーバーの設定

Linux VDA での LDAP サーバーの設定は、単一ドメインの環境では必須ではありませんが、複数ドメインおよび複数フォレストの環境では必須です。これらの環境で LDAP 検索を実行するには、ポリシーサービスに LDAP サーバーの設定が必要です。

Linux VDA パッケージのインストール後に、次のコマンドを実行します。

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

すべての LDAP サーバーを、推奨される形式である LDAP の完全修飾ドメイン名（FQDN）および LDAP ポートのスペース区切りの一覧（例：ad1.mycompany.com:389 ad2.mycomany.com:389）で入力します。

```
Checking CTX_XDL_LDAP_LIST... value not set.
The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide
LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with
LDAP port (e.g. ad1.mycompany.com:389).
If required, please provide the FQDN:port of at least one LDAP server. [<none>]:
```

また、**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
<!--NeedCopy-->
```

次のポリシーは Linux VDA のみに適用され、Citrix Studio Version 7.12 以降でのみ構成できます：

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

ポリシーについての説明は、「ポリシーサポート一覧」にまとめられています。Citrix Studio Version 7.11 以前を使用している場合は、**ctxreg** コマンドを使用して Linux VDA 上でこれらのポリシーをローカルに構成する必要があります。

> 注：
>
> 値は一定範囲に制限されています。詳しくは、「ポリシーサポート一覧」を参照してください。

ポリシーサポート一覧

November 11, 2021

Linux VDA ポリシーサポート一覧

Studio ポリシー	キー名	種類	モジュール	デフォルト値
ICA Keep-Alive	SendICAKeepAlives	コンピューター	ICA\Keep Alive	ICA Keep-Alive メッセージ (0) を送信しない
ICA Keep-Alive タイムアウト	ICAKeepAliveTimeout	コンピューター	ICA\Keep Alive	60 秒

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio ポリシー	キー名	種類	モジュール	デフォルト値
ICA リスナーポートの番号	IcaListenerPortNumber	コンピューター	ICA	1494
オーディオリダイレクトの最大帯域幅 (Kbps)	LimitAudioBw	ユーザー	オーディオ	0Kbps
クライアントオーディオリダイレクト	AllowAudioRedirection	ユーザー	オーディオ	許可 (1)
クライアントプリンターリダイレクト	AllowPrinterRedir	ユーザー	印刷	許可 (1)
クライアントクリップボードリダイレクト	AllowClipboardRedir	ユーザー	クリップボード	許可 (1)
クライアント USB デバイスリダイレクト	AllowUSBRedir	ユーザー	USB	禁止 (0)
クライアント USB デバイスリダイレクト規則	USBDeviceRules	ユーザー	USB	“\0”
動画圧縮	MovingImageCompressionConfiguration	ユーザー	Thinwire	有効 (1)
保持する最低フレーム数	TargetedMinimumFramesPerSecond	ユーザー	Thinwire	10fps
ターゲットフレーム数	FramesPerSecond	ユーザー	Thinwire	30fps
表示品質	VisualQuality	ユーザー	Thinwire	中 (3)
圧縮にビデオコーデックを使用する	VideoCodec	ユーザー	Thinwire	選択された場合使用する (3)
ビデオ コーデックにハードウェアエンコーディングを使用します	UseHardwareEncodingForVideoCodec	ユーザー	Thinwire	有効 (1)
単純なグラフィックスの優先色深度	PreferredColorDepth	ユーザー	Thinwire	24 ビット/ピクセル (1)
音質	SoundQuality	ユーザー	オーディオ	高 - 高品位オーディオ (2)
クライアントマイクリダイレクト	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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio ポリシー	キー名	種類	モジュール	デフォルト値
同時ログオントレランス	ConcurrentLogonsTolerance	レジストリ	負荷管理	2
Controller の自動更新を有効にする	EnableAutoUpdateOfController	Controller	Virtual Delivery Agent 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
Speex 最大品質	MaxSpeexQuality	ユーザー	オーディオ	5
クライアントドライブに自動接続する	AutoConnectDrives	ユーザー	ICA\ファイルリダイレクト	有効 (1)
クライアント側光学式ドライブ	AllowCdromDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアント側固定ドライブ	AllowFixedDrives	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアント側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)
クライアント側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)
クライアント側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)
クライアントドライブリダイレクト	AllowDriveRedir	ユーザー	ICA\ファイルリダイレクト	許可 (1)
クライアント側ドライブへの読み取り専用アクセス	ReadOnlyMappedDrive	ユーザー	ICA\ファイルリダイレクト	無効 (0)

次のポリシーは、Citrix Studio バージョン 7.12 以降で構成できます。

- MaxSpeexQuality

  値（整数）：[0～10]

  デフォルト値：5

  詳細：

  オーディオリダイレクトで、音質が中または低の場合、オーディオデータを Speex でエンコードします（音質のポリシーを参照）。Speex は劣化を伴うコーデックであり、入力音声信号の品質を犠牲にして圧縮します。その他の音声コーデックと違い、品質とビットレートのバランスを制御できます。Speex のエンコーディング

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

プロセスは、ほとんどの場合、0 から 10 の範囲の品質パラメーターで制御します。品質が高いほど、ビットレートも高くなります。

Speex 最大品質は、最高の Speex 品質を選択して音声品質と帯域幅制限に従ってオーディオデータをエンコードします（オーディオリダイレクトおよび帯域幅制限のポリシー参照）。音声品質が中の場合、エンコーダーは広帯域モードの、より高いサンプルレートになります。音声品質が低の場合、エンコーダーは狭帯域モードで、より低いサンプルレートになります。同じ Speex 品質でも、モードとビットレートは異なります。最高の Speex 品質は、以下の条件を満たす最大の値です。

- 品質が Speex 最大品質以下
- ビットレートが帯域幅制限以下

関連設定：音質、オーディオリダイレクトの最大帯域幅

- PrimarySelectionUpdateMode

値（列挙）：[[0, 1, 2, 3]]

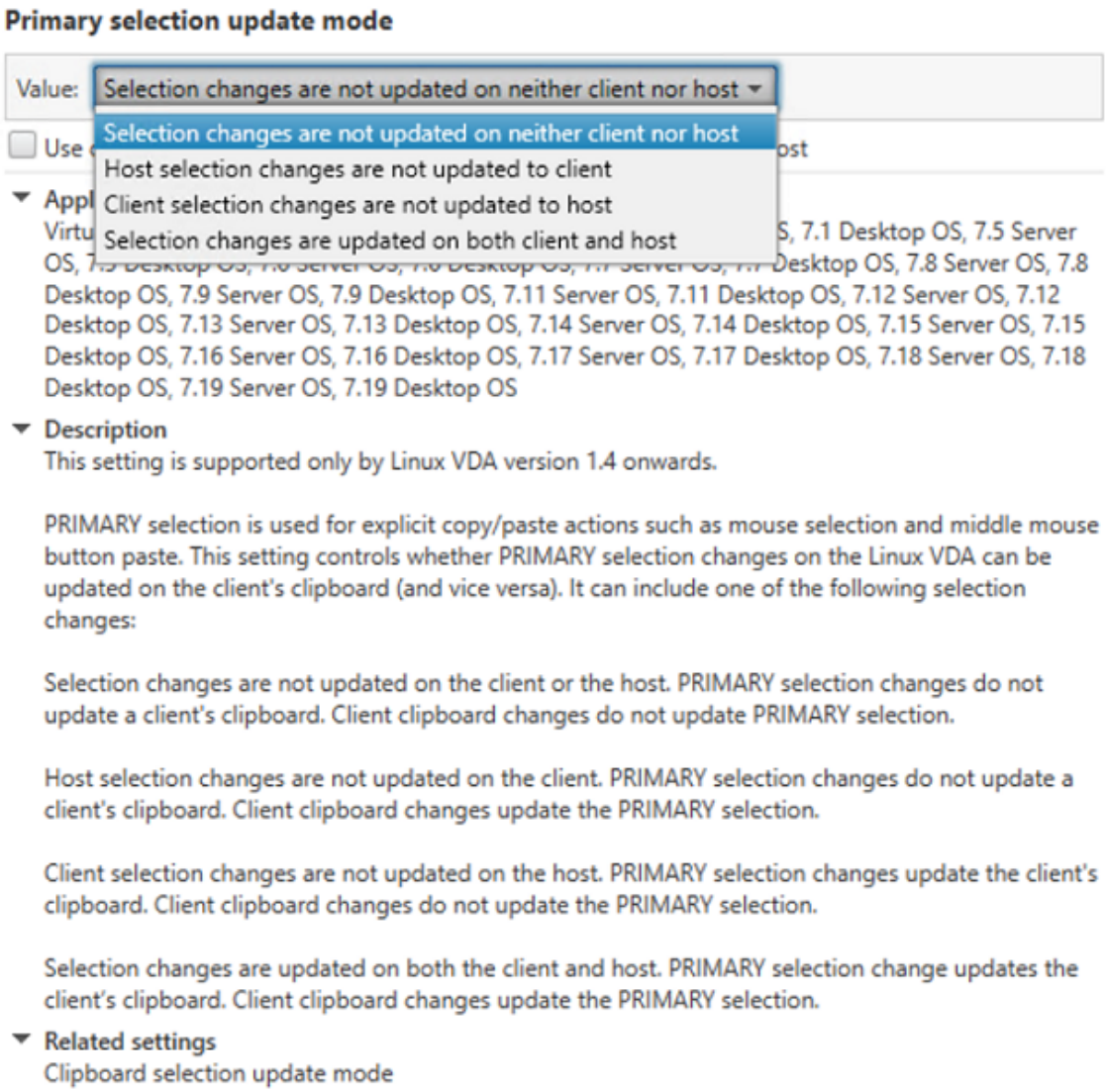
デフォルト値：3

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場合に使用されます。

この設定は、Linux VDA でのプライマリ選択の変更がクライアントのクリップボードで更新されるかどうかを制御します（逆の場合も同様）。値には、次の 4 つのオプションがあります：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 選択の変更はクライアントでもホストでも更新されません
  Linux VDA でのプライマリ選択の変更によって、クライアント上のクリップボードは更新されません。クライアントのプライマリ選択の変更により、Linux VDA のクリップボードが更新されることはありません。
- ホスト選択の変更はクライアントで更新されません
  Linux VDA でのプライマリ選択の変更によって、クライアント上のクリップボードは更新されません。クライアントのプライマリ選択の変更により、Linux VDA のクリップボードが更新されます。
- クライアント選択の変更はホストで更新されません
  Linux VDA でのプライマリ選択の変更によって、クライアント上のクリップボードが更新されます。クライアントのプライマリ選択の変更により、Linux VDA のクリップボードが更新されることはありません。
- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA でのプライマリ選択の変更によって、クライアント上のクリップボードが更新されます。クライアントのプライマリ選択の変更により、Linux VDA のクリップボードが更新されます。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

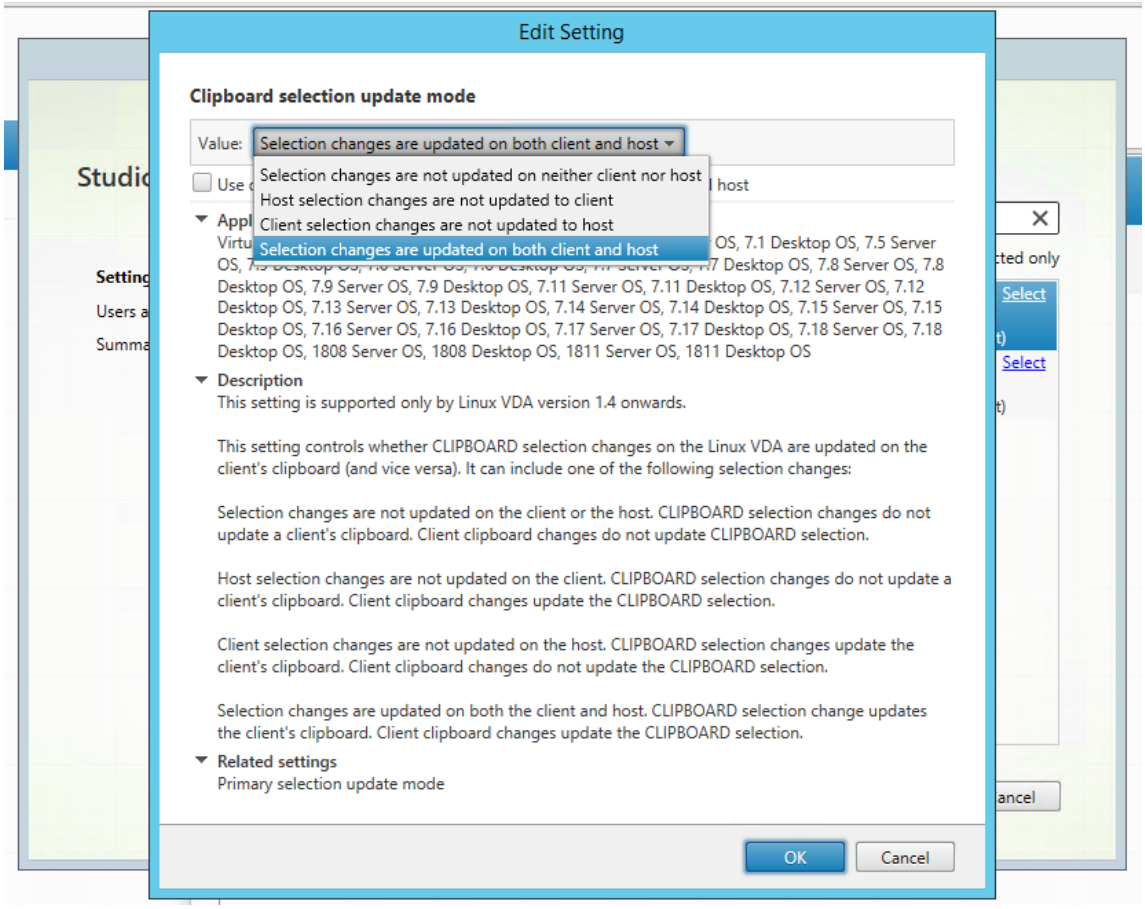
値（列挙）：[[0, 1, 2, 3]]

デフォルト値：3

詳細：

クリップボード選択は、いくつかのデータを選択し、ショートカットメニューの「コピー」を選択するなど、クリップボードに「コピー」することを明示的に要求する場合に使用します。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、プライマリ選択は Linux 特有の操作です。

このポリシーは、Linux VDA でのクリップボード選択の変更がクライアントのクリップボードで更新されるかどうかを制御します（逆の場合も同様）。値には、次の 4 つのオプションがあります：



  - 選択の変更はクライアントでもホストでも更新されません
    Linux VDA でのクリップボード選択の変更によって、クライアント上のクリップボードは更新されませ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ん。クライアントのクリップボード選択の変更により、Linux VDA のクリップボードが更新されることはありません。

- ホスト選択の変更はクライアントで更新されません
  Linux VDA でのクリップボード選択の変更によって、クライアント上のクリップボードは更新されません。クライアントのクリップボード選択の変更により、Linux VDA のクリップボードが更新されます。
- クライアント選択の変更は、ホストで更新されません
  Linux VDA でのクリップボード選択の変更によって、クライアント上のクリップボードが更新されます。クライアントのクリップボード選択の変更により、Linux VDA のクリップボードが更新されることはありません。
- 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によって、クライアント上のクリップボードが更新されます。クライアントのクリップボード選択の変更により、Linux VDA のクリップボードが更新されます。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 では、クリップボード選択とプライマリ選択の両方がサポートされています。Linux VDA とクライアント間のコピーおよび貼り付けの動作を制御するには、クリップボード選択更新モードとプライマリ選択更新モードの両方を同じ値に設定することをお勧めします。

IPv6 の構成

August 10, 2021

Linux VDA は、XenApp および XenDesktop に対応した IPv6 をサポートしています。この機能を使用するときは、次の点に注意してください。

- デュアルスタック環境で、IPv6 が明示的に有効になっていない場合、IPv4 が使用されます。
- IPv4 環境で IPv6 を有効にすると、Linux VDA は機能しません。

> 重要：
>
> - Linux VDA だけではなく、ネットワーク環境全体が IPv6 である必要があります。
> - Centrify ではピュア IPv6 をサポートしていません。

Linux VDA をインストールしている場合、IPv6 の特別なセットアップタスクは必要ありません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA で IPv6 を構成する

Linux VDA の構成を変更する前に、以前 IPv6 ネットワークで Linux 仮想マシンが機能していたかを確認する必要があります。IPv6 の構成に関連する 2 つのレジストリキーがあります。

```
1  “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
     -v “OnlyUseIPv6ControllerRegistration”
2
3  “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
     -v “ControllerRegistrationIPv6Netmask”
4  <!--NeedCopy-->
```

OnlyUseIPv6ControllerRegistration を 1 に設定して、Linux VDA で IPv6 を有効にします:

```
1  sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
     Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
     OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
2  <!--NeedCopy-->
```

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** で Linux VDA の登録に使用するネットワークインターフェイスを指定できます:

```
1  sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
     Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
     ControllerRegistrationIPv6Netmask " -d "{
2   IPv6 netmask }
3   " --force
4  <!--NeedCopy-->
```

{IPv6 netmask} を実際のネットマスク（2000::/64 など）に置き換えます。

XenApp および XenDesktop での IPv6 展開について詳しくは、「IPv4/IPv6 サポート」を参照してください。

トラブルシューティング

基本の IPv6 ネットワーク環境をチェックしてから、ping6 を使用して AD および Delivery Controller に接続できるかを確認します。

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

February 11, 2021

CEIP に参加すると、匿名の統計および使用状況情報が、Citrix 製品の品質およびパフォーマンスを向上させる目的で送信されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

レジストリ設定

デフォルトでは、ユーザーは Linux VDA のインストール時に CEIP に自動で参加します。Linux VDA のインストールからおよそ 7 日後に、初回データアップロードが行われます。このデフォルト設定はレジストリで変更できます。

- **CEIPSwitch**

CEIP を有効または無効にするレジストリ設定（デフォルトは 0）:

場所：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名前：CEIPSwitch

値のデータ：1 = 無効、0 = 有効

未指定の場合、CEIP は有効です。

クライアント上で次のコマンドを実行して CEIP を無効にできます:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "CEIPSwitch" -d "1"
<!--NeedCopy-->
```

- **DataPersistPath**

データ永続パス（デフォルトは/var/xdl/ceip）を制御するレジストリ設定:

場所：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名前：DataPersistPath

値のデータ：文字列

次のコマンドを実行してこのパスを設定できます。

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "DataPersistPath" -d "your_path"
<!--NeedCopy-->
```

構成したパスが存在しないかアクセスできない場合、データはデフォルトパスに保存されます。

Linux VDA から収集された CEIP データ

次の表では、収集される匿名の情報の種類の例を紹介します。データでは、お客様を特定するすべての詳細は含まれません。

データポイント	キー名	説明
マシンのグローバル一意識別子	machine_guid	データの発生元のマシンを識別

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

データポイント	キー名	説明
AD ソリューション	ad_solution	マシンのドメイン参加方式を示すテキスト文字列
Linux カーネルのバージョン	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 の更新または新規のインストール	update_or_fresh_install	現在の Linux VDA パッケージが新規インストールであるのか更新であるの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、簡単インストール、または手動インストールのいずれかでインストールされたかを示すテキスト文字列
HDX 3D Pro が有効かどうか	hdx_3d_pro	マシンで HDX 3D Pro が有効かどうかを示すテキスト文字列
VDI モードが有効化かどうか	vdi_mode	VDI モードが有効かどうかを示すテキスト文字列
LVDA キーサービスの前回再起動時間	ctxhdx ctxvda	dd-hh:mm:ss 形式（例: 10-17:22:19）による`ctxhdx`および`ctxvda`サービスの前回再起動時間
GPU の種類	gpu_type	マシンの GPU の種類
CPU コア	cpu_cores	マシンの CPU コア数を示す整数
CPU 周波数	cpu_frequency	CPU の周波数（MHz）を示す浮動小数点数
物理メモリサイズ	memory_size	物理メモリのサイズ（KB）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マシン上にあったアクティブなセッションの数を示す整数
Linux OS の名前およびバージョン	os_name_version	マシンの Linux OS の名前とバージョンを示すテキスト文字列
セッションキー	session_key	データの発生元のセッションを識別

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

データポイント	キー名	説明
再接続のタイムコスト	econnect_time_cost	セッションの再接続タイムコストの保存に使用。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、総和、更新回数が追跡されます。
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の保存に使用。セッションは切断や再接続がありえるため、単一のセッションのアクティブ時間が複数になることがあります。
セッション継続時間	session_duration_time	ログオンからログオフまでのセッションの継続時間の保存に使用
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	セッションで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	セッションで USB デバイスを使用した回数を示す整数

USB リダイレクトの設定

November 11, 2021

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、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することができます。

USB リダイレクトの主な機能として、次の 3 つが挙げられます。

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

オープンソース **VHCI**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB リダイレクトのこの機能により、IP ネットワーク上でシステムを共有する汎用 USB デバイスを開発します。この機能は Linux カーネルドライバーおよびユーザーモードのライブラリで構成されており、ユーザーはカーネルドライバーと通信してすべての USB データを取得することができます。Linux VDA の導入では、VHCI のカーネルドライバーが Citrix で再利用されます。ただし、Linux VDA と Citrix Receiver 間の USB データ転送はすべて Citrix ICA プロトコルパッケージに格納されます。

VHCI サービス:

VHCI サービスは、Citrix が提供する、VHCI カーネルモジュールとの通信のためのオープンソースサービスです。このサービスは VHCI と Citrix USB サービスの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 デバイスでの仮想化およびデータ転送をすべて管理する Citrix モジュールです。

USB リダイレクトのしくみ

通常、Linux VDA への USB デバイスのリダイレクトが正常に行われると、デバイスノードがシステムの/dev パスに作成されます。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 デバイスが正常に機能するかどうかはドライバーによって決まり、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 セッションにアクセスできません。確実に USB デバイスを接続するには、正しくドライバーをインストールしてシステムを設定してください。

Linux VDA は、クライアントとの間でリダイレクトが正常に行われた USB デバイスの一覧をサポートしています。また、デバイス、特に USB ディスクが適切にマウントされるため、ユーザーは追加の設定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

次のデバイスは、Linux VDA のこのバージョンをサポートしていることが確認されています。他のデバイスを使用すると、予期せぬ結果が生じる場合があります。

> 注:
>
> Linux VDA では、USB 2.0 プロトコルのみがサポートされます。

USB マスストレージデバイス	VID:PID	ファイルシステム
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston DataTraveler 101 II	0951:1625	FAT32
Kingston DataTraveler GT101 G2	1567:8902	FAT32

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB マスストレージデバイス	VID:PID	ファイルシステム
SanDisk SDCZ80 Flash Drive	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

USB 3D マウス	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

USB スキャナー	VID:PID
Epson Perfection V330 photo	04B8: 0142

USB リダイレクトの設定

USB デバイスのリダイレクトの有効化および無効化は、Citrix ポリシーにより制御されます。また、Delivery Controller ポリシーを使用してデバイスの種類を指定することもできます。USB リダイレクトを Linux VDA に設定するには、次のポリシーと規則を設定します。

- 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

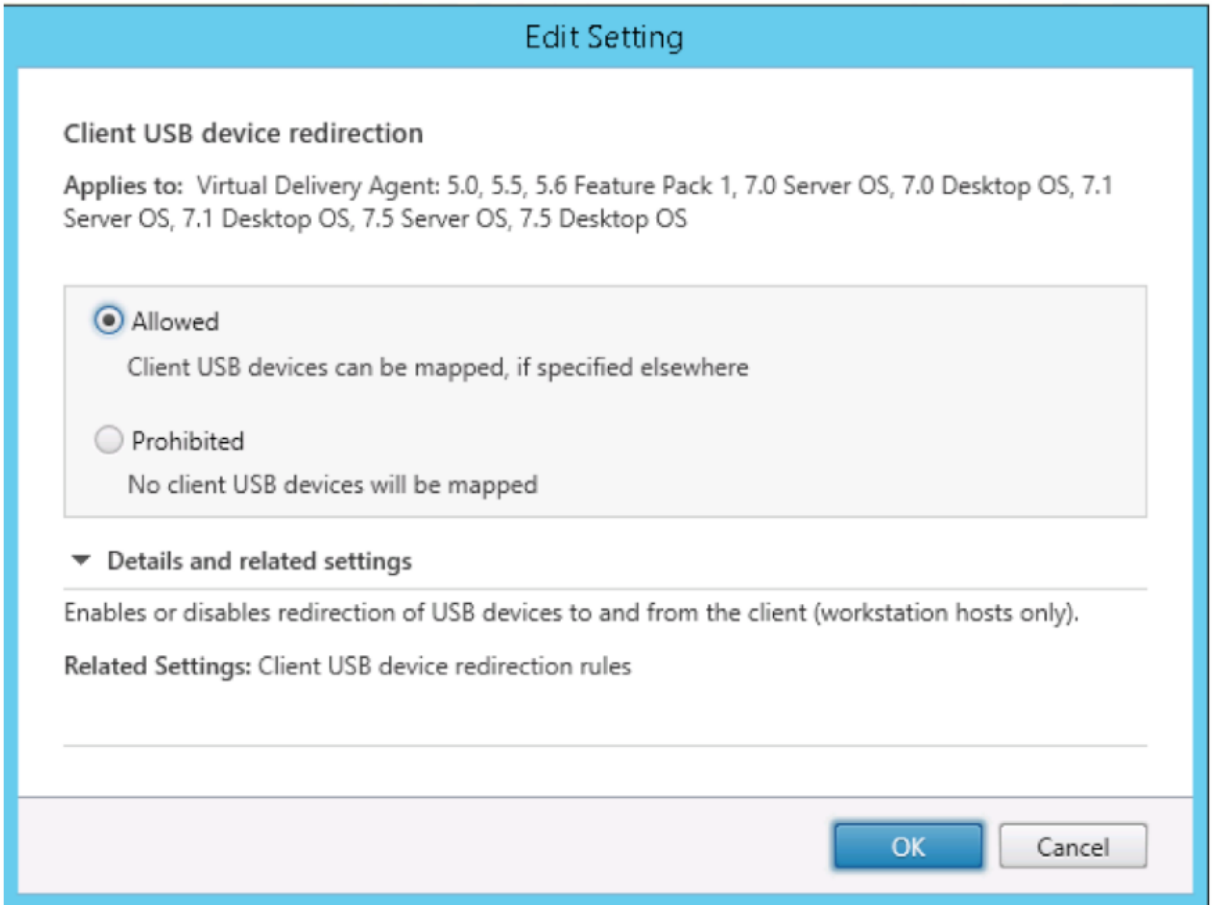
USB リダイレクトポリシーを有効にする

Citrix Studio で、クライアントと USB デバイス間の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のホストの場合のみ）。

［設定の編集］ダイアログボックスで、以下の設定を行います。

1. ［許可］を選択します。
2. ［**OK**］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



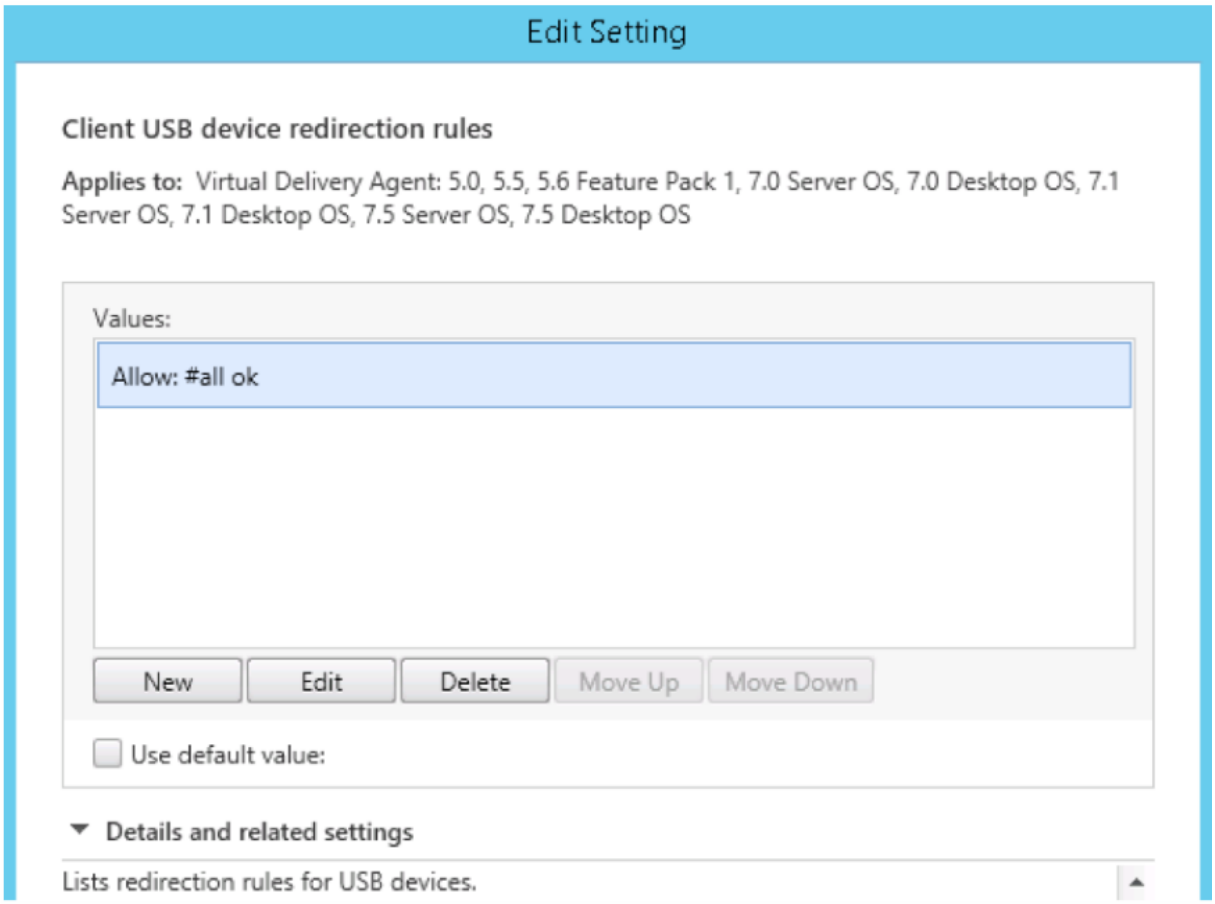
USB リダイレクト規則の設定

USB リダイレクトポリシーを有効にしたら、Citrix Studio を使用して、Linux VDA での使用を許可または禁止するデバイスを指定して、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］ダイアログボックスで、

1. ［新規］をクリックしてリダイレクト規則を追加するか、［編集］をクリックして既存の規則を確認します。
2. 規則の作成または編集後、［**OK**］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



汎用 USB リダイレクトの設定について詳しくは、「Citrix の汎用 USB リダイレクトの設定ガイド」を参照してください。

VHCI カーネルモジュールを構築します

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**）によって異なります。これらのモジュールは、RPM パッケージの一部として Linux VDA ディストリビューションに含まれます。これらは、Linux 公式ディストリビューションのカーネルをベースにコンパイルされたもので、次の表にまとめられています。

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-default
SUSE 11.4	3.0.101-0.47.55-default
Ubuntu 16.04	4.4.0-45-generic

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要:
>
> 使用するマシンのカーネルが、Linux VDA 用に Citrix の作成したドライバーに対応していない場合は、USB サービスの起動が失敗することがあります。この場合は、VHCI カーネルモジュールを構築している場合のみ、USB リダイレクト機能を使用できます。

使用するカーネルが **Citrix** の構築したモジュールに対応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、カーネルが対応しているかを確認します:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--NeedCopy-->
```

コマンドが正常に実行される場合は、カーネルモジュールのロードに成功し、バージョンが Citrix によりインストールされたものに対応しています。

コマンドの実行でエラーが生じた場合、カーネルは Citrix のモジュールに対応していないため、再構築の必要があります。

VHCI カーネルモジュールの再構築

カーネルモジュールが Citrix のバージョンに対応していない場合は、次の手順に従います。

1. Citrix の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。セクション ［**Linux Virtual Delivery Agent**（ソース)］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。**linux-vda-souces/vhci-hcd-1.15.tar.bz2** で VHCI ソースファイルを取得できます。**tar xvf vhci-hcd-1.15.tar.bz2** を使用して VHCI ファイルを復元できます。
3. ヘッダーファイルおよび **Module.symvers** ファイルに基づいて、カーネルモジュールを構築します。適切な Linux ディストリビューションに基づき、次の手順に従って、カーネルヘッダーファイルをインストールして **Module.symvers** を作成します:

   RHEL 7.3/RHEL 6.9/RHEL 6.6:

   ```
   yum install kernel-devel
   <!--NeedCopy-->
   ```

   SUSE 12.2:

   ```
   zypper install kernel-devel

   zypper install kernel-source
   <!--NeedCopy-->
   ```

   SUSE 11.4:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
zypper install kernel-source
<!--NeedCopy-->
```

Ubuntu 16.04:

```
apt-get install linux-headers
<!--NeedCopy-->
```

> ヒント:
>
> インストールが正常に完了すると、以下に類似した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 フォルダー内に **Module.symvers** ファイルがあることを確認します。フォルダーにこのファイルがない場合は、カーネルを構築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.*** からファイルをコピーします。
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
<!--NeedCopy-->
```

6. **vhci-hcd-1.15/** フォルダーで、**make** コマンドを実行して VHCI カーネルを構築します。

> 注:
>
> 構築に成功すると、**usb-vhci-hcd.ko** および **usb-vhci-iocifc.ko** が **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構築したモジュールに置き換えます: **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. ログオフして再びセッションに戻ります。USB リダイレクトが機能しているかを確認します。

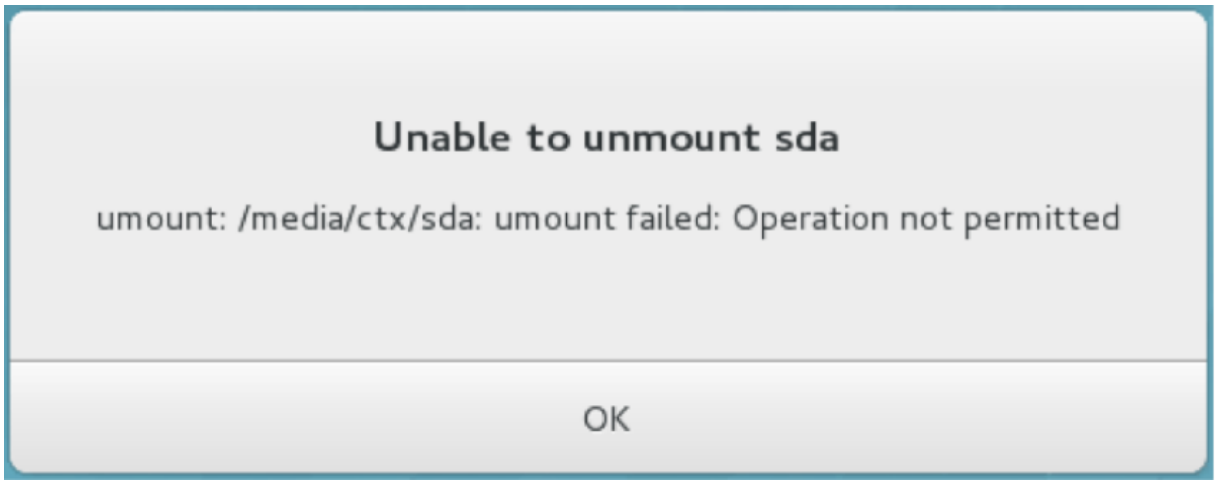
USB リダイレクト問題のトラブルシューティング

このセクションでは、Linux VDA の使用におけるさまざまな問題のトラブルシューティングについて説明します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

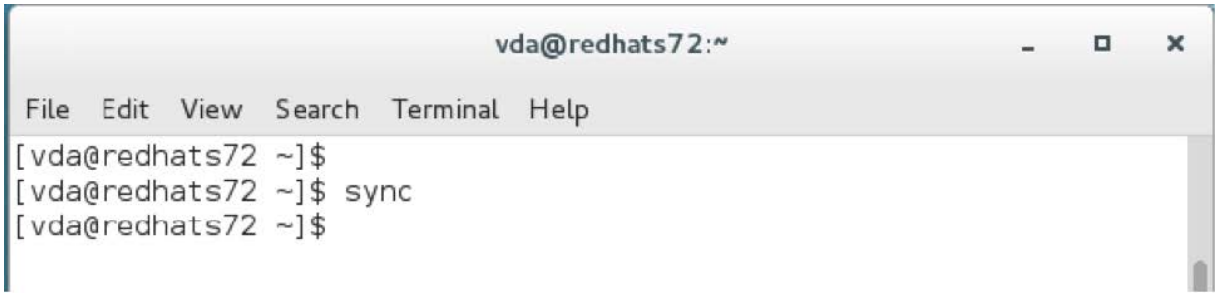
リダイレクトされた **USB** ディスクをマウント解除できない

Linux VDA では、Citrix Receiver からリダイレクトされたすべての USB ディスクのアクセスを制御するため、これらのデバイスをすべて管理者権限で管理し、リダイレクトされたデバイスに所有者のみがアクセスできるようにしています。そのため、管理者権限を持たないユーザーはデバイスをマウント解除できません。



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て、ディスク上でのファイルの作成などでディスクを変更した後に、Citrix Receiver のツールバーを使用して直ち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ことがあります。この問題は、ファイルシステムにデータを書き込むとメモリキャッシュがファイルシステムにマウントされることが原因で発生します。データはディスクそのもの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した場合、データがディスクにフラッシュされる時間が残っていないため、データが失われます。この問題を解決するには、ターミナルの 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てから USB リダイレクトを停止します。

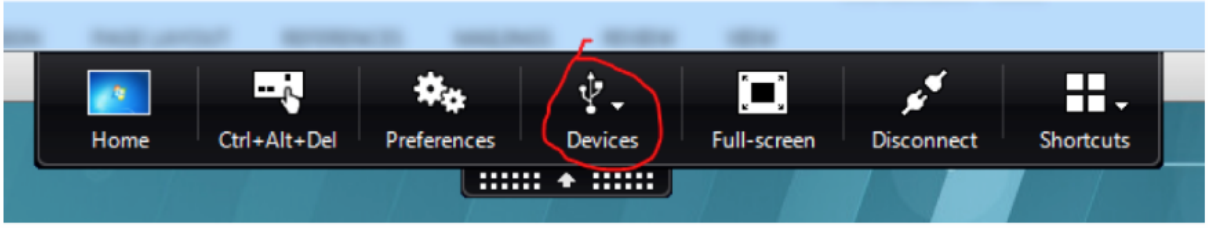


Citrix Receiver のツールバーにデバイスが表示されない

Citrix Receiver のツールバーにデバイスが表示されなくなることがありますが、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。問題が発生した場合は、次の点を確認してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ポリシーが、USB リダイレクトを許可する設定になっている
- カーネルモジュールが、使用するカーネルに対応している



> 注:
>
> ［デバイス］タブは Citrix Receiver for Linux で使用できません。

Citrix Receiver のツールバーに **USB** デバイスが表示されるが ［ポリシーの制限］と表記されリダイレクトが失敗する

この問題はデバイスのポリシー設定が原因で発生します。このような場合は、次を実行します:

- Linux VDA ポリシーを、リダイレクトを有効にする設定にします。
- Citrix Receiver のレジストリに、追加のポリシー制限が設定されているかどうかを確認します。Citrix Receiver のレジストリ設定によりデバイスが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** をチェックして、この設定でデバイスのアクセスが禁止されていないことを確認します:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

詳しくは、Citrix サポートサイトの「USB デバイスの自動リダイレクトの設定」を参照してください。

USB デバイスのリダイレクトは正常に行われるが、セッションでデバイスを使用できない

通常、リダイレクトできるのはサポートされている USB デバイスのみとなります。ただし、一覧に掲載されていないデバイスでも Linux VDA のアクティブなセッションにリダイレクトできる場合があります。このような場合は、リダイレクトしたデバイスごとに、ユーザーの所有するノードがシステムの **/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定されます。所有（プラグイン）しているもののアクセスできないデバイスを見つけた場合は、そのデバイスを制限されていないポリシーに追加します。

> 注:
>
> USB ドライバーの場合は、Linux VDA がディスクの設定とマウントを行います。ユーザー（およびデバイスをインストールした所有者のみ）は追加の設定なしでディスクにアクセスできます。「サポートされているデバイス一覧」に掲載されていないデバイスについては、これが適用されないことがあります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

クライアント入力システム（**IME**）

November 21, 2020

概要

2 バイト文字（日本語、中国語、韓国語などの文字）は、IME から入力する必要があります。Windows ネイティブの CJK IME など、クライアント側で Citrix Workspace アプリと互換性がある任意の IME を使用して、これらの文字を入力します。

インストール

この機能は、Linux VDA をインストールするときに自動でインストールされます。

用途

通常どおりに XenDesktop または XenApp のセッションを開きます。

クライアント側 IME の使用を開始するには、クライアント側での必要に応じて入力方式を変更します。

既知の問題

- クライアント側 IME 機能を使用して Google スプレッドシートのセルに文字を入力するには、スプレッドシート内のセルをダブルクリックする必要があります。
- クライアント側 IME は［パスワード］フィールドで自動で無効になりません。
- IME ユーザーインターフェイスは、入力領域ではカーソルに追従しません。
- クライアント側 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 Insight

February 9, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

概要

HDX Insight は、Citrix Application Delivery Management（ADM）の一部であり、一般的な業界標準の AppFlow をベースにしています。この機能は NetScaler または Citrix SD-WAN アプリケーションネットワークファブリックを経由する Citrix ICA トラフィックに対して、エンドツーエンドの優れた可視性を実現し、IT を通じて優れたユーザーエクスペリエンスを提供できるようにします。

このリリースの Linux VDA では、HDX Insight 機能の一部をサポートしています。EUEM（End User Experience Monitoring：エンドユーザー状況監視）機能は実装されていないため、期間に関連するデータポイントは使用できません。

インストール

インストールする必要のある依存関係パッケージはありません。

使用状況

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 を含む NetScaler Insight Center 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。NetScaler Insight Center の展開を、既存の構成や設定、データを失うことなく、Citrix ADM に移行できます。詳しくは、「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

データポイントがまったく表示されない

2 通りの原因が考えられます。

- HDX Insight が正しく構成されていません。

  NetScaler で AppFlow が有効になっていないか、Insight Center で構成されている NetScaler のインスタンスが正しくないなどです。

- Linux VDA で ICA コントロール仮想チャネル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、Citrix にバグをレポートするよう管理者に連絡します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

アプリケーションデータポイントがまったく表示されない

シームレス仮想チャネルが有効になっていることおよびシームレスアプリケーションが起動されてしばらく経過していることを確認します。

既知の問題

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

トレースオン

November 11, 2021

概要

ログの収集および問題の再現によって、診断速度やユーザーエクスペリエンスが低下します。トレースオン機能は、こうした事態に対応します。トレースは、Linux VDA でデフォルトで有効になっています。

構成

Linux VDA パッケージに、`ctxlogd`デーモンおよび setlog ユーティリティが追加されました。`ctxlogd`デーモンは、Linux VDA をインストールして構成すると、デフォルトで開始されます。

ctxlogd デーモン

トレースされた他のサービスはすべて`ctxlogd`デーモンに依存しています。Linux VDA をトレースしない場合は、`ctxlogd`デーモンを停止できます。

setlog ユーティリティ

トレースオン機能は、`setlog`ユーティリティ（パス：**/opt/Citrix/VDA/bin/**）で構成されます。このユーティリティを実行する権限があるのは、ルートユーザーのみです。GUI を使用するかコマンドを実行して、構成を表示したり変更したりできます。`setlog`ユーティリティのヘルプを表示するには、次のコマンドを実行します：

```
setlog help
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

値　デフォルトでは、［ログ出力パス］は **/var/log/xdl/hdx.log**、［最大ログサイズ］は 200MB に設定されています。［ログ出力パス］には、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
<!--NeedCopy-->
```

単一の`setlog`値を表示または設定します:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

例:

```
setlog value log_size 100
<!--NeedCopy-->
```

レベル　デフォルトで、ログレベルは **Warnings** に設定されています。

次のコマンドで、異なるコンポーネントに設定されたログレベルを表示します。

```
setlog levels
<!--NeedCopy-->
```

次のコマンドで、すべてのログレベル（Disable、Inherited、Verbose、Information、Warnings、Errors、Fatal Errors）を設定できます:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

`<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カバーするには、all に設定します:

```
setlog level all error

Setting log class ALL to ERROR.
<!--NeedCopy-->
```

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

現在のフラグを表示します:

```
setlog flags
<!--NeedCopy-->
```

1 つのログフラグを表示または設定します:

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

デフォルトに戻す　すべてのレベル、フラグ、値をデフォルト設定に戻します:

```
setlog default
<!--NeedCopy-->
```

> 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。このファイルは、ルートユーザーのみが作成できます。他のユーザーは、このファイルへの書き込み権限がありません。ルートユーザーが他のユーザーに書き込み権限を許可しないことを Citrix ではお勧めします。許可すると、`ctxlogd`が恣意的に、または悪意をもって構成される危険性があります。これによってサーバーのパフォーマンスが影響を受け、ユーザーエクスペリエンスにも影響を与える可能性があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

トラブルシューティング

/var/xdl/.ctxlog ファイルがない場合（過失による削除など）、`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.
<!--NeedCopy-->
```

この問題を解決するには、ルートユーザーとして`setlog`を実行して、**/var/xdl/.ctxlog** ファイルを再度作成します。次に、他のサービスが依存する`ctxlogd`サービスを再起動します。

認証が不要なセッションの構成

September 25, 2023

この記事の情報を使用して、認証が不要なセッションを構成します。Linux VDA をインストールしてこの機能を使用するために特別な設定は一切必要ありません。

> 注:
>
> 認証が不要なセッションを構成する場合は、セッションの事前起動がサポートされないことを考慮してください。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。

認証が不要なストアの作成

Linux VDA で認証が不要なセッションをサポートするには、StoreFront を使用して認証が不要なストアを作成します。

デリバリーグループで認証が不要なユーザーのアクセスを有効にする

認証が不要なストアを作成したら、デリバリーグループで認証が不要なユーザーのアクセスを有効にして、認証が不要な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 のドキュメントの指示に従います。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

認証が不要なセッションのアイドル時間を設定する

認証が不要なセッションのアイドル状態のタイムアウト値は、デフォルトで 10 分です。この値の設定は、レジストリ設定 **AnonymousUserIdleTime** で行います。**ctxreg** ツールを使ってこの値を変更します。たとえば、このレジストリ設定を 5 分にするには、次のコマンドを実行します。

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

認証が不要な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人数を設定するには、レジストリキー **MaxAnonymousUserNumber** を使用します。この設定により、単一の Linux VDA で同時に実行される認証が不要なセッション数が制限されます。このレジストリ設定を構成するには、**ctxreg** ツールを使用します。たとえば、値を 32 に設定するには、次のコマンドを実行します。

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

> 重要:
>
> 認証が不要なセッション数を制限します。同時に起動されるセッション数が非常に多い場合、VDA で使用できるメモリの不足などの問題を引き起こすことがあります。

トラブルシューティング

認証が不要なセッションを構成するときは、次の点を考慮してください。

- 認証が不要なセッションにログオンできませんでした。

レジストリが次を含むように更新されたことを確認します（0 に設定）。

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

ncsd サービスが実行中で、**passwd** キャッシュを有効にするように設定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'
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。設定の変更後に、Linux VDA の再インストールが必要となる場合があります。

- **KDE** でロック画面のボタンが認証不要のセッション中に表示されます。

デフォルトでは、ロック画面のボタンとメニューは、認証が不要なセッションでは無効になっています。ただし、KDE でなお表示されることがあります。KDE でロック画面のボタンとメニューを特定のユーザーに対して無効にするには、構成ファイル **$Home/.kde/share/config/kdeglobals** に次の行を加えます。例:

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

ただし、**KDE** アクション制限事項パラメーターがグローバルワイドな **kdeglobals** ファイル（**/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals** など）で不変に設定されている場合、ユーザー設定は効果がありません。

この問題を解決するには、システムワイドな **kdeglobals** ファイルを変更して ［**KDE** アクション制限事項］セクションの **\$i]** タグを削除するか、システムワイドな構成を直接使用して、ロック画面のボタンとメニューを無効にします。KDE 構成について詳しくは、「KDE System Administration/Kiosk/Keys」ページを参照してください。

LDAPS の構成

November 11, 2021

セキュリティで保護された LDAP（LDAPS）によって、Active Directory 管理対象ドメインに SSL（Secure Socket Layer）/TLS（Transport Layer Security）経由のセキュリティ保護された Lightweight Directory Access Protocol の通信を提供できます。

デフォルトで、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 を使用した LDAP（LDAPS）で、Linux VDA および LDAP サーバー間の LDAP クエリコンテンツを保護できます。

次の Linux VDA コンポーネントは、LDAPS との依存関係があります。

- ブローカーエージェント：Delivery Controller に Linux VDA を登録
- ポリシーサービス：ポリシー評価

以下は、LDAPS の構成に必要です。

- Active Directory（AD）/LDAP サーバーで LDAPS を有効化
- クライアントで使用するルート CA をエクスポート
- Linux VDA で LDAPS を有効化または無効化
- サードパーティのプラットフォームで LDAPS の構成
- SSSD の構成

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Winbind の構成
- Centrify の構成
- Quest の構成

AD/LDAP サーバーで LDAPS の有効化

Microsoft 証明機関（CA）または非 Microsoft CA のどちらかから適切な形式の証明書をインストールして、SSL 経由の LDAP（LDAPS）を有効にできます。

> ヒント：
>
> SSL/TLS 経由の LDAP（LDAPS）は、ドメインコントローラーで会社のルート CA をインストールすると、自動的に有効になります。

証明書をインストールして、LDAPS 接続を確認する方法について詳しくは、Microsoft Knowledgebase のサポート技術情報で「How to enable LDAP over SSL with a third-party certification authority」を参照してください。

証明機関の階層に複数の層（2 層または 3 層）がある場合、ドメインコントローラーで LDAPS 認証の適切な証明書を自動的に取得できません。

複数の証明機関の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詳しくは、Microsoft TechNet Web サイトで「LDAP over SSL (LDAPS) Certificate」を参照してください。

クライアントで使用するルート証明書（CA）の有効化

クライアントは、LDAP サーバーが信頼する CA 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 証明書をインポートしてキーストアを信頼します。

ルート CA をエクスポートする方法について詳しくは、Microsoft Support Web サイトで「How to export Root Certification Authority Certificate」を参照してください。

Linux VDA マシンで LDAPS を有効化または無効化

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

このコマンドの構文には次が含まれます。

- 指定されたルート CA 証明書で SSL/TLS 経由で LDAP を有効にします。

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- SSL/TLS を使用せずに LDAP にフォールバックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
<!--NeedCopy-->
```

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には、次が含まれます。

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
<!--NeedCopy-->
```

サードパーティのプラットフォームで **LDAPS** の構成

Linux VDA コンポーネントに加えて、VDA のさまざまなサードパーティのソフトウェアコンポーネントでは、SSSD、Winbind、Centrify、Quest などのセキュリティで保護された LDAP が必要な場合もあります。以下のセクションでは、LDAPS、STARTTLS または SASL（署名とシール）によるセキュリティで保護された LDAP を構成する方法について説明します。

> ヒント：
>
> これらすべてのソフトウェアコンポーネントで、SSL ポート 636 を使用し、セキュリティで保護された LDAP にすることが望ましいわけではありません。また、ほとんどの場合、LDAPS（ポート 636 での SSL 経由の LDAP）はポート 389 の STARTTLS と共存できません。

SSSD

オプションごとに、ポート 636 またはポート 389 のセキュリティで保護された SSSD LDAP トラフィックを構成します。詳しくは、SSSD LDAP Linux の man ページを参照してください。

Winbind

Winbind LDAP クエリは、ADS メソッドを使用します。Winbind は、ポート 389 で 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** および **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:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```

ldap ssl = start tls

ldap ssl ads = yes

client ldap sasl wrapping = plain
<!--NeedCopy-->
```

また、セキュリティで保護された LDAP は、SASL GSSAPI（署名およびシール）で構成されますが、TLS/SSL と共存することはできません。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
<!--NeedCopy-->
```

Centrify

Centrify ではポート 636 の LDAPS をサポートしていません。一方、ポート 389 上のセキュリティで保護された暗号化は提供しています。詳しくは、Centrify サイトを参照してください。

Quest

Quest 認証サービスはポート 636 の LDAPS をサポートしませんが、別の方法でポート 389 のセキュリティで保護された暗号化を提供します。

トラブルシューティング

この機能を使用すると、以下の問題が発生することがあります。

- **LDAPS** サービスの可用性

  AD/LDAP サーバーで LDAPS 接続が使用可能であることを確認します。デフォルトでは、このポートは 636 です。

- **LDAPS** を有効にすると **Linux VDA** の登録が失敗する

  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。最初にルート CA 証明書をチェックして、AD/LDAP サーバーと一致することを確認します。

- 誤ったレジストリ変更

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

LDAPS 関連のキーが誤って **enable_ldaps.sh** を使用せずに更新されると、LDAPS コンポーネントの依存関係を損なう可能性があります。

- **LDAP** トラフィックは、**Wireshark** やその他のネットワーク監視ツールから **SSL/TLS** で暗号化されません

  デフォルトでは、LDAPS は無効になっています。それを強制するには、**/opt/Citrix/VDA/sbin/enable_ldaps.sh** を実行します。

- **Wireshark** やその他のネットワーク監視ツールからの **LDAPS** トラフィックが存在しない

  LDAP/LDAPS トラフィックは、Linux VDA の登録やグループポリシーの評価を行う際に発生します。

- **AD** サーバーで **LDP** 接続を実行して **LDAPS** の可用性を確認できない

  IP アドレスの代わりに、AD FQDN を使用します。

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

  CA 証明書のフルパスを指定して、ルート CA 証明書の種類が正しいことを確認します。通常は、サポートされている Java Keytool の種類の大半で対応しています。サポート一覧にない場合は、最初に種類を変更してください。証明書の形式の問題が発生した場合は、Citrix では Base64 で暗号化された PEM 形式の使用をお勧めします。

- ルート **CA** 証明書を **Keytool** 一覧に表示できない

  /opt/Citrix/VDA/sbin/enable_ldaps.sh を実行して LDAPS を有効にすると、証明書が/etc/xdl/.keystore にインポートされ、キーストアを保護するパスワードが設定されます。パスワードを忘れた場合は、スクリプトを再度実行して新しいキーストアを作成します。

Xauthority の構成

November 11, 2021

Linux VDA は、対話型のリモート制御で X11 ディスプレイ機能（`xterm`と`gvim`を含む）を使用する環境をサポートしています。この機能は、XClient と XServer 間のセキュリティで保護された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。

このセキュリティで保護された通信の権限を保護するには、以下の 2 つの方法があります。

- **Xhost**。デフォルトでは、Xhost コマンドはローカルホスト XClient と XServer の通信のみを許可します。リモート XClient の XServer へのアクセスを許可すると、特定のマシンで権限を付与するために Xhost コマンドが実行される必要があります。あるいは、**xhost +** を使用して XClient に XServer への接続を許可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。このファイルは、XServer の認証の際に 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

インスタンス（Xorg）が起動されるときに、特定のディスプレイへの接続を認証するためにこの Cookie が使用されます。

機能

Xorg が起動されると、`.Xauthority`ファイルは Xorg に渡されます。この`.Xauthority`ファイルには次の要素が含まれます:

- 表示番号
- 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
<!--NeedCopy-->
```

XClient がリモートで Xorg に接続する場合、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 で Cookie 番号の 1 つを含む`.Xauthority`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 上で Xauthority を有効にするには、次の 2 個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
<!--NeedCopy-->
```

Xauthority に有効にしてから、手動によるか共有ホームディレクトリをマウントすることで`.Xauthority`ファイルを XClient に渡します。

- `.Xauthority`ファイルを XClient に手動で渡す

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ICA セッションを起動した後、Linux VDA は XClient 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ファイルを保存します。この `.Xauthority`ファイルをリモート 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`ファイルに保存した表示番号で、XAUTHORITY は Xauthority のファイルパスです。たとえば、次のコマンドを表示します:

```
export DISPLAY={
Display number stored in the Xauthority file }


export XAUTHORITY={
the file path of .Xauthority }

<!--NeedCopy-->
```

> 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することにより `.Xauthority`ファイルを XClient に渡す

  簡単な方法は、ログオンユーザーの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 セッションを起動すると、ログオンユーザーのホームディレクトリで `.Xauthority`ファイルが作成されます。このホームディレクトリが XClient と共有される場合、ユーザーがこの `.Xauthority`ファイルを手動で XClient に転送する必要はありません。DISPLAY および XAUTHORITY 環境変数を正しく設定した後、XServer で GUI が自動的に表示されます。

トラブルシューティング

Xauthority が機能しない場合は、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 特権を持つ管理者として、すべての Xorg Cookie を取得します:

   ```
   ps aux | grep -i xorg
   <!--NeedCopy-->
   ```

   このコマンドは、起動中 Xorg に渡される Xorg プロセスとパラメーターを表示します。もう 1 つのパラメーターは、どの `.Xauthority`ファイルが使用されるかを表示します。例:

   ```
   /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

   Xauth コマンドを使用して、Cookie を表示します:

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. **Xauth** コマンドを使用して、`~/.Xauthority`に含まれる Cookie を表示します。同じ表示番号の場合、表示される Cookie は Xorg および XClient の`.Xauthority`ファイルで同じである必要があります。
3. Cookie が同じあれば、リモートディスプレイポートが Linux VDA の IP アドレス（例：10.158.11.11）と公開デスクトップの表示番号（例：160）を使用してアクセスできるかを確認します。

   XClient マシンで次のコマンドを実行します。

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

   ポート番号は、6000 + 表示番号の合計です。

   telnet の操作が失敗すると、ファイアウォールが要求をブロックすることがあります。

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).