XenAppおよびXenDesktop 7.15 LTSR

Apr 18, 2018

XenAppおよびXenDesktop の長期サービスリリース（LTSR）プログラムは、XenApp/XenDesktop リリースに安定性と長期サポートを提供します。

XenAppおよびXenDesktopのLTSRは現在、バージョン7.6および7.15で使用できます。累積更新プログラム2（CU2）は、7.15 LTSRの最新の更新プログラムです。初めてLTSRプログラムに参加し、7.6または7.15のLTSRの初期リリースを展開していない場合は、どちらも今すぐインストールする必要はありません。その代わりに、7.15 LTSR CU2から始めることをお勧めします。

また、Citrix Receiverおよびその他のコンポーネントは、指定のバージョンを使用することをお勧めします。LTSRに適合する上では必須ではありませんが、こうしたコンポーネントを推奨バージョンにアップグレードすることで、展開環境のメンテナンスが容易になり、最新の修正を利用できるようになります。

7.6 LTSRのリリース以降に追加された7.15 LTSRの機能の概要については、『XenAppとXenDesktopの機能概要の比較』の表を参照してください。

ダウンロード

7.15 LTSR XenAppおよびXenDesktop累積更新プログラム2（CU2）

7.15 LTSR XenAppおよびXenDesktop

便利なリンク

- Citrix Supportability Pack

  Supportability Packは、XenDesktop/XenApp製品の診断とトラブルシューティングを支援するためにCitrixエンジニアが作成した、一般的なツールのコレクションです。ツールは、簡単に見つけて使用できるように、機能およびコンポーネントごとにカタログ化されています。このパックの以前のバージョンは...

- LTSRについてよく寄せられる質問

  Citrix Windowsアプリ配信チームは、速いテンポで（2015年は四半期ベースで新しい製品リリースを提供）XenAppおよびXenDesktop製品ラインのためのイノベーションと拡張機能をリリースしてきました。このように速いペースでイノベーションをリリースすることで...

- XenAppおよびXenDesktopのメンテナンスオプション

  柔軟なサービスオプションにより、受けられるサポート内容が明確です。CitrixはXenAppおよびXenDesktopに新しい機能を短い間隔で提供することで、ビジネスの競争力を維持し、ITの運用を合理化し、データセキュリティを強化するとともに、従業員がどこからでもビジネスリソースにアクセスできるようにしています。...

- 製品のライフサイクル日程

  製品のライフサイクル日程は、次の表を参照してください。以下の製品マトリクス表には、製品ライフサイクルがライフサイクルフェーズにより規定されるCitrix製品の情報が記載されています。製品のライフサイクルマイルストーンには、ステータス変更のお知らせ（Notice of Status Change：NSC）、販売終了（End of Sales：EOS）、メンテナンス終了（End of Maintenance：EOM）、および製品終了（End of Life：EOL）が含まれます。...

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Receiver for Windows向けLTSRプログラム

  Citrix Receiver for Windows、Mac、Linux、HTML5、JavaまたはWinCEの各メジャーバージョン（v3.0など）で、ユーザーが利用できる最短ライフサイクルは4年間です。ライフサイクルは、最初に最低3年間のメインストリームメンテナンスフェーズがあり、その後、残りのメンテナンス期間で、延長メンテナンスフェーズへ移行...

© 1999-2017 Citrix Systems, Inc. All rights reserved.

新機能

Apr 18, 2018

このリリースについて

累積更新プログラム2（CU2）について

累積更新プログラム1（CU1）について

7.15 LTSR（初期リリース）について

© 1999-2017 Citrix Systems, Inc. All rights reserved.

累積更新プログラム2（CU2）

Apr 18, 2018

このリリースについて

XenAppおよびXenDesktop 7.15 LTSR累積更新プログラム2（CU2）では、7.15 LTSRリリース以降に報告された150を超える問題が修正されています。

7.15 LTSR（一般情報）

XenAppおよびXenDesktop 7.15 LTSR CU1以降の解決された問題

このリリースの既知の問題について

ダウンロード

7.15 LTSR CU2をダウンロード

新しい展開環境

新しくCU2を展開するには

CU2メタインストーラーを使用して、CU2に基づく新しいXenApp/XenDesktop環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

「XenAppおよびXenDesktop 7.15長期サービスリリース（初期リリース）」を熟読し、「製品の技術概要」、「インストールと構成」、および「セキュリティ」セクションの内容に注意して、展開の計画を開始してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開環境

更新対象について

CU2では、7.15 LTSRのベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべてのLTSRコンポーネントをCU2に更新することをお勧めします。例えば、Provisioning ServicesがLTSR展開環境に含まれる場合、Provisioning ServicesコンポーネントをCU2に更新します。Provisioning Servicesが展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenAppおよびXenDesktop 7.15 LTSR CU2のベースラインコンポーネント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Baseline Component	Version	Notes
VDA for Desktop OS	7.15.2000	
VDA for Server OS	7.15.2000	
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	
グループポリシー管理のエクスペリエンス	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
Universal Print Server	7.15.2000	
セッション レコーディング	7.15.2000	Platinum Editionのみ
Linux VDA	7.15.2000	サポートされるプラットフォームについては、Linux VDAのドキュメントを参照してください。
Profile Management	7.15.2000	
Federated認証サービス	7.15.2000	

Citrix XenAppおよびXenDesktop 7.15 LTSR CU2の互換性のあるコンポーネント

7.15 LTSR環境では、以下のコンポーネントの使用が推奨されます。これらのコンポーネントは、LTSRの特典（ライフサイクルの延長と修正のみの累積更新プログラム）の対象にはなりません。7.15 LTSR環境に含まれるこれらのコンポーネントを、。り新しいバージョンにアップグレードするようお願いする場合があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU2 Compatible Components and Platforms	Version
App Layering	4.10.0
Citrix SCOM Management Pack for License Server	1.2
Provisioning Services用Citrix SCOM Management Pack	1.19
StoreFront用Citrix SCOM Management Pack	1.13
XenAppおよびXenDesktop用Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4
ライセンスサーバー	11.14.0.1ビルド23101
セルフサービス パスワード リセット	1.1.10.0
Workspace Environment Management	4.6

Citrix Receiverの互換バージョン

メンテナンスの容易化とパフォーマンスの最適化のために、Citrix Receiverは、最新バージョンが利用可能になり次第そのバージョンにアップグレードすることをお勧めします。最新バージョンは、https://www.citrix.com/downloads/citrix-receiver.htmlからダウンロードできます。Citrix Receiverの新バージョンが利用可能になったときに通知を受けることができるように、Citrix ReceiverのRSSフィードに登録することをお勧めします。

Citrix Receiverは、XenAppおよびXenDesktopのLTSRの特典（ライフサイクルの延長と修正のみの累積更新プログラム）の対象にはならないことに注意してください。7.15 LSTR環境に含まれるCitrix Receiverを、より新しいバージョンにアップグレードするようお願いする場合があります。Citrix Receiver for Windowsについては、専用のLTSRプログラムが公開されました。このプログラムについて詳しくは、「Lifecycle Milestones for Citrix Receiver」ページを参照してください。

具体的には、7.15 LTSR CU2ではCitrix Receiverの以下のバージョンとそれ以降のすべてのバージョンがサポートされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU2 Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.13.5以降
Citrix Receiver for Chrome	2.6.5以降
Citrix Receiver for HTML	2.6.5以降
Citrix Receiver for iOS	7.5.3以降
Citrix Receiver for Linux	13.9.1以降
Citrix Receiver for Mac	12.9以降
Citrix Receiver for UWP（ユニバーサルWindowsプラットフォーム）	1.0.5以降
Citrix Receiver for Windows	4.9以降

XenAppおよびXenDesktop 7.15 LTSRの注意すべき除外対象

以下の機能、コンポーネント、プラットフォームは、7.15 LTSRのライフサイクルマイルストーンと特典の対象外です。すなわち、累積更新プログラムとライフサイクル延長の特典は適用されません。除外対象の機能とコンポーネントの更新は、通常の最新リリースで入手可能です。

Excluded Features
Framehawk
StoreFront Citrix Onlineの統合

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk： • Windows 10マシンでは除外されます。 • Windows 7マシンの場合、2020年1月14日までLTSRは限定的にサポートされます（CUの要件が適用されます）
AppDisk

Excluded Windows Platforms *
Windows 2008 32ビット（Universal Print Server用）

* Citrixは、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を有します。

インストールとアップグレード分析

全製品インストーラーを使用してXenAppまたはXenDesktopコンポーネントを展開またはアップグレードする場合、インストールプロセスに関する匿名の情報が、コンポーネントをインストール/アップグレードするマシンで収集および保存されます。このデータは、インストールに関するカスタマーエクスペリエンス向上のために使用されます。詳しくは、http://more.citrix.com/XD-INSTALLERを参照してください。

XenApp 6.5からの移行

XenApp 6.5の移行プロセスでは、XenApp 6.5ファームをXenApp 7.15 LTSR CU2のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションとCitrixグループポリシーを含む環境で、アプリケーションとCitrixグループポリシーを手動で移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU2のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します。

- 各XenApp 6.5ワーカー上でXenApp 7.15 CU2インストーラーを実行します。これにより、Virtual Delivery Agent for Server OSにアップグレードされます。
- いずれかのXenApp 6.5コントローラー上でPowerShellエクスポートコマンドレットを実行して、アプリケーション設定とCitrixポリシー設定をXMLファイルにエクスポートします。
- 必要に応じてXMLファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XMLファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的にXenApp 7.15 LTSR CU2サイトにインポートできます（一部を先にインポートしてから残りを後でインポートするなど）。
- 新しいXenApp 7.15 CU2 Controller上でPowerShellインポートコマンドレットを実行して、XMLファイルから新しいXenAppサイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.xからの移行」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

解決された問題

Apr 18, 2018

Citrix Director

- DNS名でマシンをフィルター処理すると、Citrix Directorがマシンを表示しなかったり、重複したエントリが表示されたりすることがあります。この問題は、最初にマシンがMonitorデータベースに追加されたものの、2つの異なるDelivery Controllerから同時に追加された場合に発生します。その結果、2つのマシンエントリが作成されます。[#LC4905]
- カスタム管理者として、マシンカタログからリモートPC設定を取得できない場合、例外が発生することがあります。この問題は、マシンカタログを管理する権限があるにもかかわらず、スコープに特定のカタログが含まれていない場合に発生します。[#LC8170]
- Citrix Directorで **[フィルター]** > **[セッション]** の順に移動してWebブラウザーのサイズを変更しようとするときに、テーブル全体が正しく配置されないことがあります。 [#LC8624]
- Citrix Directorからデータをエクスポートすると、CSVファイルが使用できなくなります。英語以外のバージョンのMicrosoft WindowsをDirectorの表示言語として設定すると、カンマが値の区切り文字と小数点記号の両方として使用される可能性があるため、この問題が発生することがあります。 [#LC8625]
- Citrix Directorを起動すると、 **[インフラストラクチャ]** タブに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。Web サーバーとのネットワーク接続が無効になりました。ネットワーク接続を確認して再試行してください。」[#LC8752]
- 複数のCitrix Directorサイトを構成するとサイト名の一部が削除されることがありました。[#LC9258]

Citrixポリシー

- グループポリシーエディター（gpedit.msc）の2番目のインスタンスを開くと、Citrixポリシーノードが開かず、次のエラーメッセージが表示されることがあります。

  「Managed Codeスナップインでの未処理の例外。」[#LC7600]
- グループポリシー管理コンソール（GPMC）を使用してCitrixポリシーを適用すると、GPMCポリシー設定でポリシーが表示されないことがあります。ただし、グループポリシーオブジェクト（GPO）の編集で、ポリシーと設定が有効であることが表示されます。[#LC8282]
- Citrixグループポリシー管理3.1を使用してActive Directoryの **[ユーザー ポリシー]** に **[プリンター割り当て]** 設定を追加すると、ウィンドウのサイズが変更されるという問題が発生することがあります。ウィンドウを開いた後、ウィンドウのサイズが、画面の角に達するまで自動的に横方向に拡大されることがあります。その結果、すべての列にはアクセスできないため、ポリシーの編集が難しくなる場合があります。[#LC8684]
- ローカルポリシーキャッシュフォルダー（%ProgramData%/CitrixCseCache）内のファイルが「読み取り専用」に設定されていると、ポリシー設定が正常に適用されないことがあります。[#LC8750]
- VDAからシングルユーザー管理モードでApp-V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。この問題は、**ApplicationStartDetails**レジストリキーの値が空の場合、またはアプリケーションの詳細がレジストリキーに存在

© 1999-2017 Citrix Systems, Inc. All rights reserved.

しない場合に発生します。[#LC8798]

- ユーザーの関連付けにNETBIOS名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC9393]

Citrix Studio

- Linux VDAからアプリケーションを手動で追加しようとすると、次のエラーメッセージが表示されることがあります。

  「Value cannot be null while publishing the application.」

  ただし、表示されたエラーメッセージで［OK］をクリックすると、アプリケーションは正常に追加されます。 [#LC7910]

- アプリケーションがCitrix Studioの**Application**ノードのサブフォルダーにある場合、デリバリーグループからアプリケーションを削除しようとすると失敗することがあります。[#LC8705]

- ユーザーの関連付けにNETBIOS名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC9393]

コントローラー

- 日本語OS上にインストールされたCitrixサービスの「サービス表示名」と「サービスの説明」の末尾に、不必要な文字が表示される場合があります。[#LC5208]

- Citrix Directorからセッションのデータを取得しようとすると、nullエントリが監視データベースに表示されます。その結果、特定のデータがCitrix Directorに表示されず、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でした」[#LC6273]

- Linux VDAからアプリケーションを手動で追加しようとすると、次のエラーメッセージが表示されることがあります。

  「Value cannot be null while publishing the application.」

  ただし、表示されたエラーメッセージで［OK］をクリックすると、アプリケーションは正常に追加されます。 [#LC7910]

- Citrix Broker Service（Brokerservice.exe）が突然終了することがあります。この問題は、LicPolEng.dllモジュールに障害がある場合に発生します。[#LC8638]

- Machine Creation Servicesを使用して最小限必要なVMware権限で仮想マシン（VM）をプロビジョニングすると、VMの削除が失敗することがあります。このエラーは、最小限許可されているVMware権限でも発生する可能性があります。[#LC8868]

- ゾーン基本設定が割り当てられているActive Directoryユーザーが削除されると、セカンダリブローカーへのブローカー構成のインポートが失敗することがあります。XenDesktopを最新のバージョンにアップグレード後、インポート操作が失敗することがあります。[#LC9269]

- ユーザーの関連付けにNETBIOS名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生しま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。[#LC9393]

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトが有効な場合、VDAセッションをQumu.comに再接続すると、Flashコンテンツが Microsoft Internet Explorerに読み込まれないことがあります。[#LC9193]

インストーラー

- Delivery Controllerのインストールディレクトリのパスを変更しようとすると、**XaXdProxy.msi**で機能しないことがあります。[#LC8691]

Linux VDA

- 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]
- 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]

Profile Management

- Profile Managementサービスを再起動すると、Citrix Directorがユーザーのログオン情報および個人設定情報を表示しないことがあります。[#LC6942]

Provisioning Services

StoreFront

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 「デスクトップを自動的に起動する」設定を有効にすると、「複数起動を防止する」オプションが機能しないことがありま す。その結果、それ以降のデスクトップの同じインスタンスを起動する要求が失敗します。[#LC7430]
- デフォルト以外のドライブにインストールされているStoreFront 2.6をアップグレードすると、ユーザーのアプリケーショ ンサブスクリプションデータが保持されないことがあります。[#LC8046]
- StoreFront MMCコンソールを再起動すると、**[デスクトップビューアーを表示する]**チェックボックスの値が誤って表示されることがあります。[#LC8520]
- StoreFrontをカスタマイズするためのPNGファイル（透過性がサポートされている）で**Set-STFWebReceiverSiteStyle**コマンドを実行すると、PNGファイルはJPEGファイルに変換されます。このJPEGファイル形式で、透過性がサポートされないことがあります。[#LC8677]
- **Set-STFWebReceiverApplicationShortcuts**コマンドを実行してCitrix Receiver for Webサイトのアプリケーションショートカットに信頼されるURLを設定すると、URLの最後にスラッシュ（/）が追加されることがあります。[#LC8761]
- **Set-STFWebReceiverSiteStyle**コマンドを使用してStoreFrontをカスタマイズすると、style.cssがCustomフォルダーで正しく変更されないことがあります。その結果、StoreFrontコンソールはカスタマイズ内容を読み取ることができません。[#LC8776]
- StoreFrontサーバーで認証エラーが発生することがあります。この問題は、TCP動的ポートを使い果たすことによって発生します。[#LC8795]
- **Set-STFWebReceiverSiteStyle**コマンドを使用してStoreFrontロゴを変更しようとすると、失敗することがあります。[#LC8994]
- Citrix Receiver for Webサイトのカスタムファイルディレクトリ内に読み取り専用ファイルが存在する場合、StoreFrontをアップグレードしようとすると失敗することがあります。[#LC9252]

VDA for Desktop OS

HDX 3D Pro

- Microsoft Windows 10で実行されているVDAでHDX 3D Proとカスタム解像度を有効にすると、ログオン時に灰色の画面が断続的に表示されることがあります。 [#LC8417]

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトが有効な場合、VDAセッションをQumu.comに再接続すると、Flashコンテンツが Microsoft Internet Explorerに読み込まれないことがあります。[#LC9193]

HDX MediaStream Windows Mediaリダイレクト

- HDX MediaStream Windows Mediaリダイレクトが無効な場合、Windows Media Playerで特定のビデオファイル形式を開こうとすると、再生中のビデオが垂直方向に反転することがあります。[#LC9194]

HDX RealTime

- RealTime Connectorがインストールされています。Skype for Businessのようなリダイレクトされ たWebカメラを使用するアプリケーションを使用していると、初期セッションの開始時にVDA for Desktop OS上のWebカメラがリダイレクトされて検出されることがあります。ただし、ユーザーセッションに再接続すると、Webカメラは検出されなくなります。この

© 1999-2017 Citrix Systems, Inc. All rights reserved.

問題は、RealTime Media Engineがユーザーデバイスにインストールされていない場合に発生します。[#LC8793]

キーボード

- Androidデバイスでアプリケーションを起動しテキストフィールドに入力しようとすると、キーボードが自動的に表示されないことがあります。また、開始や終了は常にキーボードボタンを使用する必要があります。[#LC8936]

印刷

- Microsoft Wordを使用してプリンター設定で用紙の両面に印刷しようとすると、失敗することがあります。[#LC7501]
- 公開されたMicrosoft Internet Explorerインスタンスから文書を印刷しようとすると、失敗することがあります。[#LC8093]
- 表示言語としてフランス語がVDAにインストールされている場合、文書を印刷しようとすると失敗することがあります。[#LC8209]
- ユーザーデバイスからリダイレクトされるプリンターは、セッションに再接続するとリダイレクトされないことがあります。[#LC8762]
- 最初のセッションの開始中に印刷スプーラサービスを停止すると、Citrix Print Manager Service（cpsvc.exe）を再起動できないことがあります。[#LC9192]

セッション/接続

- マップされたクライアントドライブからファイルを読み取るとき、ファイルの長さがクライアントセッションの外部で変更されていると、古いキャッシュ済みのファイルの長さが返されることがあります。また、削除された文字の代わりにNu文字が挿入されます。

  この修正を有効にするには、以下のレジストリ値を「0」に設定します。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名前：CacheTimeout
  種類：REG_DWORD
  値：デフォルト値は60秒です。CacheTimeOutが「0」に設定されている場合、ファイルの長さは直ちに再読み込みされます。「0」に設定されていない場合は、定義されたタイムアウトが経過した後に読み込まれます。[#LC6314]

- 従来のグラフィックモードを使用している場合、VDA for Desktop OSで実行されているセッションが応答しなくなることがあります。問題が発生すると、Desktop Viewerで更新操作ができなくなる場合がありますが、Desktop Viewerは応答します。また、30〜60分後には応答していなかったセッションも回復します。[#LC7777]
- 残留セッション機能を有効にしてアプリケーションを起動すると、アプリケーションが表示された後にセッションがログオフすることがあります。 [#LC8245]
- VDA for Desktop OSを起動しようとすると、デスクトップが起動されてから数秒後に消えることがあります。[#LC8373]
- 以下のいずれかの場合、Windowsエクスプローラーは予期せずに閉じてしまうことがあります。
  - 名前に260文字を越える文字が含まれているファイルを大量に選択して、［送る］>［FAX受信者］オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDFを使用して、ファイルを結合しようとした場合。[#LC8423]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在のVDA for Desktop OSセッションには適用されても、それ以

© 1999-2017 Citrix Systems, Inc. All rights reserved.

降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定してください。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
名前：EnableVisualEffect
種類：DWORD
値：1 [#LC8049, #LC8658]

- セッションを切断すると、次のローカルログオン時にmonitor1がプライマリモニターとして誤って表示されることがあります。この現象は、マルチモニター環境でリモートPCアクセスVDAにローカルでログオンし、monitor2をプライマリモニターとして構成してからユーザーデバイス経由で接続し、Desktop Viewerを使用してセッションを切断する時に発生することがあります。[#LC8675]
- Microsoft Windows Server 2012または2016で実行されている公開アプリケーションを開始しようとすると、ロックアウトされる可能性があります。[#LC8681]
- マルチモニター環境でアプリケーションを起動すると、両方のモニターにわたってログオンバナーが表示されることがあります。1台のモニターを使用する場合、ログオンバナーウィンドウは全画面で表示されます。[#LC8741]
- ローカルアプリケーションアクセスが有効な場合、Microsoft Windows 10で実行されている公開デスクトップでアプリケーションを開こうとすると、アプリケーションを最小化できません。[#LC8813]
- DLPソフトウェアがUNCリンクでファイルをスキャンできないことがあります。[#LC8893]
- 公開アプリケーションを起動すると、NumLockキーが機能しません。この問題は、NumLockキーのLEDがユーザーデバイス上で表示されているにもかかわらず、ユーザーセッション内で数字が機能していない場合に発生します。新しく作成されたリモートデスクトップがLED状態を初期化するよりも早くクライアントがLEDの更新を要求した場合に発生します。この場合、WinStationはLED状態を更新せず、LED状態がエンドポイントとVDA間で同期していない可能性があります。[#LC8921]
- アプリケーションやデスクトップを起動しようとしても失敗することがあります。VDA for Server OSが応答しなくなると、この問題が発生することがあります。

  この修正を有効にするには、以下のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  名前：EnableSCardHookVcResponseTimeout
  種類：DWORD
  値：1 [#LC8969]
- VM Hosted Appsを開こうとして失敗することがあります。[#LC9001]
- セッションに再接続できないことがあります。[#LC9040]
- セッションでWFAPI SDK **WFQuerySessionInformation**コマンドを使用して、インストールされているVDAのバージョン情報を取得するときに、コマンドが機能しないことがあります。[#LC9041]
- XenAppおよびXenDesktopをバージョン7.14から7.15にアップグレードした後、公開アプリケーションのタブを切り替えると、アプリケーションが応答しなくなる可能性があります。また、シームレスウィンドウのサイズを小さなサイズに変更してからウィンドウを広げると、ウィンドウ内のすべての要素を描画するのに時間がかかります。[#LC9078]
- 公開アプリケーションは、アプリケーションの起動直後に断続的に終了することがあります。[#LC9167]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 初期接続とは異なる画面解像度でMillenniumスイート内のシームレスなアプリケーションに再接続すると、アプリケーションが誤ったサイズに変更されることがあります。その結果、ウィンドウが切り捨てられることがあります。[#LC9214]
- ユーザーデバイス経由でWindows 10バージョン1709の公開デスクトップに接続しようとすると、灰色の画面が表示されることがあります。ハイパーバイザーのコンソールから公開デスクトップに接続しようとすると、黒い画面に回転ホイールが表示されます。ただし、RDP経由で公開デスクトップに接続すると正常に機能します。[#LC9215]
- Citrix Receiver for Macからアプリケーションを起動できないことがあります。この問題は、クライアントライセンス（LicenseRequestClientLicense）を取得できない場合に発生します。[#LC9286]
- HDX 3D Proが有効な場合、XenDesktopを起動しようとすると断続的に失敗することがあります。この問題は、GPUに障害が発生した場合に発生します。[#LC9343]
- スムースローミングで、ユーザーセッションから管理対象外リモートデスクトップセッションにセッションが正しく表示されない可能性があります。[#LC9471]

スマートカード

- スマートカードを使用すると、特定のサードパーティアプリケーションが、PINプロンプトを表示するのでなく応答しなくなることがあります。[#LC8805]

システムの例外

- サーバーにおいて、バグチェックコード0x22の重大な例外がpicadm.sysで発生し、ブルースクリーンが表示されることがあります。[#LC6177]
- サーバーの致命的な例外が発生し、picadm.sysのバグチェックコード0x00000050（PAGE_FAULT_IN_NONPAGED_AREA）によるブルースクリーンが表示されことがあります。 [#LC6985]
- サーバーで致命的な例外が発生し、picadm.sysのバグチェックコード0x22によるブルースクリーンが表示されることがあります。[#LC7574]
- サーバーでvdtw30.dllの致命的な例外が発生し、停止コードSYSTEM_SERVICE_EXCEPTION（3b）によるブルースクリーンが表示されることがあります。[#LC8087]
- サーバーにおいて、バグチェックコード0x3Bの重大な例外がpdcrypt2.sysで発生し、ブルースクリーンが表示されることがあります。この問題は、VDAを起動するときに発生します。[#LC8328]
- HDX 3D ProおよびGPUハードウェアエンコーディングが有効になっている場合に、NVIDIA GPUを使用すると、Citrixソフトウェアグラフィックスプロセス（Ctxgfx.exe）が予期せず終了することがあります。この問題は、高解像度の画面を使用する場合に発生します。[#LC8435]
- VDA for Server OSのpicadm.sysでブルースクリーンエラーが発生することがあります。[#LC8708]
- VDAでpicadm.sysの致命的な例外が発生し、バグチェックコード0x22によるブルースクリーンが表示されることがあります。[#LC8749]
- VDAを再起動して初めてログオンすると、予期しないアクセス違反の例外が発生することがあります。Citrixソフトウェアグラフィックプロセス（Ctxgfx.exe）が予期せず終了します。その結果、VDAに表示される画像やテキストの品質が低下する可能性があります。[#LC9005]
- 以下のいずれかの場合、Windowsエクスプローラーは予期せずに閉じてしまうことがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 260文字を超える名前のファイルを大量に選択して、**[Send to]** > **[Fax recipient]** オプションを選択した場合。
- サードパーティのアプリケーションを開こうとした場合。
- Nitro PDFを使用して、ファイルを結合しようとした場合。[#LC9076]

ユーザーエクスペリエンス

- クライアント上で実行されているアプリケーションからコンテンツをコピーして、ユーザーセッションでアプリケーションに貼り付けるときに、そのコンテンツが貼り付けられないことがあります。また、**[貼り付け]** が無効になっていることがあります。[#LC8516]
- 以前ロックされたセッションにログオンしようとすると、ログオン画面が表示されないことがあります。[#LC8774]

ユーザーインターフェイス

- デスクトップの壁紙が、「デスクトップの壁紙」ポリシーを［禁止］に設定した後にも表示されます。 [#LC8398]
- 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]

その他

- この修正では、Enlightened Data Transport（EDT）のパフォーマンスおよび品質のマイナーな強化に対応しています。[#LC9278]

VDA for Server OS

HDX MediaStream Windows Mediaリダイレクト

- HDX MediaStream Windows Mediaリダイレクトが無効な場合、Windows Media Playerで特定のビデオファイル形式を開こうとすると、再生中のビデオが垂直方向に反転することがあります。[#LC9194]

HDX RealTime

- RealTime Connectorがインストールされています。Skype for BusinessのようなリダイレクトされたWebカメラを使用するアプリケーションを使用していると、初期セッションの開始時にVDA for Desktop OS上のWebカメラがリダイレクトされて検出されることがあります。ただし、ユーザーセッションに再接続すると、Webカメラは検出されなくなります。この問題は、RealTime Media Engineがユーザーデバイスにインストールされていない場合に発生します。[#LC8793]

キーボード

- Androidデバイスでアプリケーションを起動しテキストフィールドに入力しようとすると、キーボードが自動的に表示されないことがあります。また、開始や終了は常にキーボードボタンを使用する必要があります。[#LC8936]

印刷

- Microsoft Wordを使用してプリンター設定で用紙の両面に印刷しようとすると、失敗することがあります。[#LC7501]
- 公開されたMicrosoft Internet Explorerインスタンスから文書を印刷しようとすると、失敗することがあります。[#LC8093]
- 表示言語としてフランス語がVDAにインストールされている場合、文書を印刷しようとすると失敗することがあります。[#LC8209]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 最初のセッションの開始中に印刷スプーラサービスを停止すると、Citrix Print Manager Service（cpsvc.exe）を再起動できないことがあります。[#LC9192]

サーバー/サイトの管理

- 複数のドメインに同じ名前のグループが2つ以上ある場合、VDAがユーザーのグループメンバーシップをチェックしたときに、Citrix Stack Control Service（SCService64.exe）が予期せず終了することがあります。この問題は、DS_DOMAIN_TRUSTSW構造体の文字列 「DnsDomainName」が空の場合に発生します。 [#LC8484]

セッション/接続

- XenApp 7.6 LTSR CU2 VDA for Server OSまたは以前のバージョンを起動すると、システムイベントログで次の警告メッセージが表示されることがあります。

  「SemsServiceへの接続に失敗しました。エラーコード0x2。」[#LC6311]

- マップされたクライアントドライブからファイルを読み取るとき、ファイルの長さがクライアントセッションの外部で変更されていると、古いキャッシュ済みのファイルの長さが返されることがあります。また、削除された文字の代わりにNu文字が挿入されます。

  この修正を有効にするには、以下のレジストリ値を「0」に設定します。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名前：CacheTimeout
  種類：REG_DWORD
  値：デフォルト値は60秒です。CacheTimeOutが「0」に設定されている場合、ファイルの長さは直ちに再読み込みされます。「0」に設定されていない場合は、定義されたタイムアウトが経過した後に読み込まれます。[#LC6314]

- ラップトップを切り離した後に、セッション共有が失敗することがあります。この問題は、自動クライアント再接続中に障害通知がトリガーされているときに、VDAがDelivery Controllerに再登録すると発生します。 [#LC7450]

- 従来のグラフィックモードを使用している場合、VDA for Desktop OSで実行されているセッションが応答しなくなることがあります。問題が発生すると、Desktop Viewerで更新操作ができなくなる場合がありますが、Desktop Viewerは応答します。また、30〜60分後には応答していなかったセッションも回復します。[#LC7777]

- VDAにインストールされたApp-Vクライアントを使用して公開アプリケーションを閉じ、セッションで構成設定「EnablePubilishingRefreshUI」と ［セッションの残留］ が有効になっていると、iOSデバイスで黒いウィンドウが開いたままになることがあります。この問題は、セッションがアクティブな残留状態にある時に発生します。[#LC8080]

- 残留セッション機能を有効にしてアプリケーションを起動すると、アプリケーションが表示された後にセッションがログオフすることがあります。 [#LC8245]

- RPM.dllでサーバーが応答しなくなり、次のエラーメッセージが表示されることがあります。

  「Event ID 1009, picadm: Timeout waiting for response message from client」 [#LC8339]

- 以下のいずれかの場合、Windowsエクスプローラーは予期せずに閉じてしまうことがあります。

  - 名前に260文字を越える文字が含まれているファイルを大量に選択して、［送る］>［FAX受信者］オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDFを使用して、ファイルを結合しようとした場合。[#LC8423]
- Citrix Directorで、複数の接続障害が報告されることがあります。この問題は、アプリケーションの表示制限を制御するた

© 1999-2017 Citrix Systems, Inc. All rights reserved.

めに割り当てられたグループの拡張が、ユーザーごとに使用されている場合に発生します。この拡張プロセスは完了までに時間がかかり、複数のドメインにまたがる多数のグループがある大規模なネットワークで発生することがあります。[#LC8652]

- COMポートは、バージョン7.15のVDAにマップできないことがあります。[#LC8656]
- Microsoft Windows Server 2012または2016で実行されている公開アプリケーションを開始しようとすると、ロックアウトされる可能性があります。[#LC8681]
- マルチモニター環境でアプリケーションを起動すると、両方のモニターにわたってログオンバナーが表示されることがあります。1台のモニターを使用する場合、ログオンバナーウィンドウは全画面で表示されます。[#LC8741]
- ローカルアプリケーションアクセスが有効な場合、Microsoft Windows 10で実行されている公開デスクトップでアプリケーションを開こうとすると、アプリケーションを最小化できません。[#LC8813]
- ユーザーデバイスをVDAに接続すると、デスクトップが表示されないことがあります。代わりに、灰色の画面がデスクトップに表示されます。[#LC8821]
- DLPソフトウェアがUNCリンクでファイルをスキャンできないことがあります。[#LC8893]
- 公開アプリケーションを起動すると、NumLockキーが機能しません。この問題は、NumLockキーのLEDがユーザーデバイス上で表示されているにもかかわらず、ユーザーセッション内で数字が機能していない場合に発生します。新しく作成されたリモートデスクトップがLED状態を初期化するよりも早くクライアントがLEDの更新を要求した場合に発生します。この場合、WinStationはLED状態を更新せず、LED状態がエンドポイントとVDA間で同期していない可能性があります。[#LC8921]
- アプリケーションやデスクトップを起動しようとしても失敗することがあります。VDA for Server OSが応答しなくなると、この問題が発生することがあります。

  この修正を有効にするには、以下のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  名前：EnableSCardHookVcResponseTimeout
  種類：DWORD
  値：1 [#LC8969]
- VM Hosted Appsを開こうとして失敗することがあります。[#LC9001]
- セッションでWFAPI SDK **WFQuerySessionInformation**コマンドを使用して、インストールされているVDAのバージョン情報を取得するときに、コマンドが機能しないことがあります。[#LC9041]
- XenAppおよびXenDesktopをバージョン7.14から7.15にアップグレードした後、公開アプリケーションのタブを切り替えると、アプリケーションが応答しなくなる可能性があります。また、シームレスウィンドウのサイズを小さなサイズに変更してからウィンドウを広げると、ウィンドウ内のすべての要素を描画するのに時間がかかります。[#LC9078]
- 公開アプリケーションは、アプリケーションの起動直後に断続的に終了することがあります。[#LC9167]
- 初期接続とは異なる画面解像度でMillenniumスイート内のシームレスなアプリケーションに再接続すると、アプリケーションが誤ったサイズに変更されることがあります。その結果、ウィンドウが切り捨てられることがあります。[#LC9214]
- Citrix Receiver for Macからアプリケーションを起動できないことがあります。この問題は、クライアントライセンス（LicenseRequestClientLicense）を取得できない場合に発生します。[#LC9286]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スマートカード

- スマートカードを使用すると、特定のサードパーティアプリケーションが、PINプロンプトを表示するのでなく応答しなくなることがあります。[#LC8805]

システムの例外

- サーバーにおいて、バグチェックコード0x22の重大な例外がpicadm.sysで発生し、ブルースクリーンが表示されることがあります。[#LC6177]
- サーバーの致命的な例外が発生し、picadm.sysのバグチェックコード0x00000050（PAGE_FAULT_IN_NONPAGED_AREA）によるブルースクリーンが表示されことがあります。 [#LC6985]
- サーバーで致命的な例外が発生し、picadm.sysのバグチェックコード0x22によるブルースクリーンが表示されることがあります。[#LC7574]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、icaendpoint.dllモジュールに障害がある場合に発生します。[#LC7694]
- サーバーでvdtw30.dllの致命的な例外が発生し、停止コードSYSTEM_SERVICE_EXCEPTION（3b）によるブルースクリーンが表示されることがあります。[#LC8087]
- サーバーにおいて、バグチェックコード0x3Bの重大な例外がpdcrypt2.sysで発生し、ブルースクリーンが表示されることがあります。この問題は、VDAを起動するときに発生します。[#LC8328]
- HDX 3D ProおよびGPUハードウェアエンコーディングが有効になっている場合に、NVIDIA GPUを使用すると、Citrixソフトウェアグラフィックスプロセス（Ctxgfx.exe）が予期せず終了することがあります。この問題は、高解像度の画面を使用する場合に発生します。[#LC8435]
- サーバーで致命的な例外が発生し、icardd.dllのバグチェックコード0x0000003Bによるブルースクリーンが表示されることがあります。[#LC8492]
- VDA for Server OSのpicadm.sysでブルースクリーンエラーが発生することがあります。[#LC8708]
- サーバーで致命的な例外が発生し、icardd.dllのバグチェックコード0x0000003Bによるブルースクリーンが表示されることがあります。[#LC8732]
- VDAでpicadm.sysの致命的な例外が発生し、バグチェックコード0x22によるブルースクリーンが表示されることがあります。[#LC8749]
- VDAを再起動して初めてログオンすると、予期しないアクセス違反の例外が発生することがあります。Citrixソフトウェアグラフィックプロセス（Ctxgfx.exe）が予期せず終了します。その結果、VDAに表示される画像やテキストの品質が低下する可能性があります。[#LC9005]
- 以下のいずれかの場合、Windowsエクスプローラーは予期せずに閉じてしまうことがあります。
  - 260文字を超える名前のファイルを大量に選択して、**[Send to]** > **[Fax recipient]** オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDFを使用して、ファイルを結合しようとした場合。[#LC9076]

ユーザーエクスペリエンス

- クライアント上で実行されているアプリケーションからコンテンツをコピーして、ユーザーセッションでアプリケーショ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンに貼り付けるときに、そのコンテンツが貼り付けられないことがあります。また、 **[貼り付け]** が無効になっているこ
があります。[#LC8516]

- VDA for Server OSでは、マウスカーソルがセッションから消えることがあります。この問題は、カーソルが**テキスト選択**カーソルに変更され、背景色が**テキスト選択**カーソルの色と同じである場合に発生します。Microsoft Windowsの編集可能領域のデフォルトの背景色は白で、デフォルトの**テキスト選択**カーソルの色も常に白です。その結果、カーソルが表示されなくなる可能性があります。[#LC8807]
- Microsoft Windowsで、正しい資格情報を送信した後でも、セッションログオン中にパスワードフィールドが編集可能のままになることがあります。[#LC9407]

ユーザーインターフェイス

- デスクトップの壁紙が、「デスクトップの壁紙」ポリシーを［禁止］に設定した後にも表示されます。 [#LC8398]
- 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]

その他

- この修正では、Enlightened Data Transport（EDT）のパフォーマンスおよび品質のマイナーな強化に対応しています。[#LC9278]

その他

Citrix Telemetry Serviceが無効になっているか停止している場合、メタインストーラーを使用してXenAppおよびXenDesktop 7.15 LTSRを累積更新プログラム1（CU1）にアップグレードすると、次の警告メッセージが表示されることがあります。「Ca Homeに登録するためのCitrixサービスを開始できません。

詳しくは、CTX218094を参照してください。」[#LCM-3642]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cumulative Update 1（CU1）

Apr 18, 2018
リリース日：2017年12月5日

このリリースについて

XenAppおよびXenDesktop 7.15 LTSR Cumulative Update 1（CU1）では、初期リリース以降に報告された80を超える問題が修正されています。

7.15 LTSR（一般情報）

XenAppおよびXenDesktop 7.15 LTSR以降の解決された問題（初期リリース）

このリリースの既知の問題について

7.6 LTSR CU5からアップグレードする前に...

7.6 LTSR CU5から7.15 LTSR CU1へのアップグレードする主な利点は、基本の7.15 LTSRには、基本の7.6 LTSRよりも多くの機能が含まれていることです。ただし、アップグレードを検討している場合、7.6 LTSR CU5に含まれている修正プログラムの一部は、7.15 LTSR CU1には存在しないことに注意してください。これは、7.6 LTSR CU5より前に7.15 LTSR CU1がリリースされたためです。7.15には存在するものの、7.15 LTSR CU1には含まれない修正プログラムの一覧については、「7.6 LTSR CU5に含まれるが7.15 LTSR CU1には含まれない修正プログラムの一覧」を参照してください。展開が7.6 LTSR CU5に含まれている特定の修正プログラムに依存している場合は、アップグレードする前にこの一覧を確認することをお勧めします。

新しい展開環境

新しくCU1を展開するには

CU1メタインストーラーを使用して、CU1に基づく真新しいXenApp/XenDesktop環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

「XenAppおよびXenDesktop 7.15長期サービスリリース（初期リリース）」を熟読し、「製品の技術概要」、「インストールと構成」、および「セキュリティ」セクションの内容に注意して、展開の計画を開始してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開環境

更新対象について

CU1では、7.15 LTSRの未定のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべてのLTSRコンポーネントをCU1に更新することをお勧めします。たとえば、Provisioning ServicesがLTSR展開環境に含まれる場合、Provisioning ServicesコンポーネントをCU1に更新します。Provisioning Servicesが展開環境に含まれない場合は、インストールや更新を行う必要はありません。

Citrix XenAppおよびXenDesktop 7.15 LTSR CU1のベースラインコンポーネント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU1 Baseline Component	Version	Notes
VDA for Desktop OS	7.15.1000	
VDA for Server OS	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	
グループポリシー管理のエクスペリエンス	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	
Universal Print Server	7.15.1000	
セッション レコーディング	7.15.1000	Platinum Editionのみ
Linux VDA	7.15.1000	サポートされるプラットフォームについては、Linux VDAのドキュメントを参照してください。
Profile Management	7.15.1000	
Federated 認証サービス	7.15.1000	

Citrix XenAppおよびXenDesktop 7.15 LTSR CU1の互換性のあるコンポーネント

7.15 LTSR CU1環境では、以下のコンポーネントの使用が推奨されます。これらのコンポーネントは、LTSRの特典（ライフサイクルの延長と修正のみのCumulative Update）の対象にはなりません。7.15 LTSR CU1環境に含まれるこれらのコンポーネントを、より新しいバージョンにアップグレードするようお願いする場合があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.16
ライセンスサーバー用Citrix SCOM Management Pack	1.2
Citrix SCOM Management Pack for Provisioning Services	1.19
Citrix SCOM Management Pack for StoreFront	1.13
XenAppおよびXenDesktop向けCitrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.2.100
ライセンスサーバー	11.14.0.1ビルド22103
ワークスペース環境管理	4.4
App Layering	4.6
セルフサービス パスワード リセット	1.1

Citrix Receiverの互換バージョン

メンテナンスの容易化とパフォーマンスの最適化のために、Citrix Receiverは、最新バージョンが利用可能になり次第そのバージョンにアップグレードすることをお勧めします。最新バージョンは、https://www.citrix.com/downloads/citrix-receiver.htmlからダウンロードできます。Citrix Receiverの新バージョンが利用可能になったときに通知を受けることができるように、Citrix ReceiverのRSSフィードに登録することをお勧めします。

Citrix Receiverは、XenAppおよびXenDesktopのLTSRの特典（ライフサイクルの延長と修正のみのCumulative Update）の対象にはならないことに注意してください。7.15 LSTR CU1環境に含まれるCitrix Receiverを、より新しいバージョンにアップグレードするようお願いする場合があります。Citrix Receiver for Windowsについては、専用のLTSRプログラムが公開されました。このプログラムについて詳しくは、「Lifecycle Milestones for Citrix Receiver」ページを参照してください。

具体的には、7.15 LTSR CU1ではCitrix Receiverの以下のバージョンとそれ以降のすべてのバージョンがサポートされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.12.3以降
Citrix Receiver for Chrome	2.5.2以降
Citrix Receiver for HTML	2.5.2以降
Citrix Receiver for iOS	7.3.1以降
Citrix Receiver for Linux	13.7以降
Citrix Receiver for Mac	12.7以降
Citrix Receiver for UWP（ユニバーサル Windows プラットフォーム）	1.0.5以降
Citrix Receiver for Windows	4.9以降

XenAppおよびXenDesktop 7.15 LTSRの注意すべき除外対象

以下の機能、コンポーネント、プラットフォームは、7.15 LTSRのライフサイクルマイルストーンと特典の対象外です。すなわち、Cumulative Updateとライフサイクル延長の特典は適用されません。除外対象の機能とコンポーネントの更新は、通常の最新リリースで入手可能です。

Excluded Features
Framehawk
StoreFront Citrix Onlineの統合

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk： • Windows 10マシンでは除外されます。 • Windows 7マシンの場合、2020年1月14日までLTSRは限定的にサポートされます（CUの要件が適用されます）
AppDisk

Excluded Windows Platforms *
Windows 2008 32ビット（Universal Print Server用）

* Citrixは、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を有します。

インストールとアップグレード分析

全製品インストーラーを使用してXenAppまたはXenDesktopコンポーネントを展開またはアップグレードする場合、インストールプロセスに関する匿名の情報が、コンポーネントをインストール/アップグレードするマシンで収集および保存されます。このデータは、インストールに関するカスタマーエクスペリエンス向上のために使用されます。詳しくは、http://more.citrix.com/XD-INSTALLERを参照してください。

XenApp 6.5からの移行

XenApp 6.5の移行プロセスでは、XenApp 6.5ファームをXenApp 7.15 LTSR CU1のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションとCitrixグループポリシーを含む環境で、アプリケーションとCitrixグループポリシーを手動で移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU1のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します。

- 各XenApp 6.5ワーカー上でXenApp 7.15 CU1インストーラーを実行します。これにより、Virtual Delivery Agent for Server OSにアップグレードされます。
- いずれかのXenApp 6.5コントローラー上でPowerShellエクスポートコマンドレットを実行して、アプリケーション設定とCitrixポリシー設定をXMLファイルにエクスポートします。
- 必要に応じてXMLファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XMLファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的にXenApp 7.15 LTSR CU1サイトにインポートできます（一部を先にインポートしてから残りを後でインポートするなど）。
- 新しいXenApp 7.15 CU1 Controller上でPowerShellインポートコマンドレットを実行して、XMLファイルから新しいXenAppサイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.xからの移行」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.6 LTSR CU5に含まれるが7.15 LTSR CU1には含まれない修正プログラムの一覧

7.6 LTSR CU5から7.15 LTSR CU1へのアップグレードを検討している場合、7.6 LTSR CU5に含まれている修正プログラムの一部は、7.15 LTSR CU1には存在しないことに注意してください。展開が7.6 LTSR CU5に含まれている特定の修正プログラムに依存している場合は、アップグレードする前にこの一覧を確認することをお勧めします。

LC6311
LC6985
LC7430
LC7450
LC7574
LC7600
LC7777
LC7911
LC8046
LC8080
LC8130
LC8170
LC8281
LC8339
LC8492
LC8732
LC8750
LC8774

© 1999-2017 Citrix Systems, Inc. All rights reserved.

解決された問題

Apr 18, 2018
XenAppおよびXenDesktop 7.15 LTSR累積更新プログラム1（CU1）では、初期リリース以降に報告された80を超える問題が修正されています。

Citrix Director

- Directorコンソールを開いて最初にユーザーを検索したときに、読み込みを示すバーが表示されません。その後の検索では、バーは期待通りに表示されます。 [#LC8190]

Citrixポリシー

- Active Directoryでユーザーポリシーに新しいUSBリダイレクト規則を追加しようとすると、失敗することがあります。この問題は、スクロールバーが利用できない場合に発生します。[#LC8112]
- 「プリンター割り当て」ポリシーを管理しようとすると、以下の問題が発生することがあります。
  - プリンター割り当てポリシーを追加または編集しようとすると、例外「InvalidCastException」が発生します。
  - 新しいセッションプリンターを追加しようとすると、例外「InvalidOperationException」が発生します。
  - プリンター割り当てポリシーからセッションプリンターを削除しようとすると失敗します。この問題は、［Remove］オプションを無効にすると発生します。
  - 「プリンター割り当て」ポリシーの検索ボックスで入力をやめると、検索処理が開始されません。
  - セッションプリンターの上書き設定チェックボックス（PrintQuality、PaperSize、Scale、TrueTypeOption）は、前回無効にした場合でも、常に有効になっています。[#LC8146]

Citrix Studio

- ユーザーが割り当てたマシンをデリバリーグループに追加しようとすると、未割り当てのマシンが［マシン割り当て］ページに表示されることがあります。[#LC6755]
- Citrix Studioのマシンカタログにアクセスしようとすると、Citrix Studioが予期せず終了して次の例外が発生することがあります。

  「エラーID：XDDS:ABB14FD9」[#LC7961]
- 英語以外のWindowsオペレーティングシステムで実行されている場合、［接続およびリソースの追加］ウィザードの［Us storage local to the hypervisor］オプションのテキストが省略されることがあります。[#LC8041]
- Citrix Studioをバージョン7.14.1にアップグレードした後、既存のApp-Vパッケージの［使用者］列（アプリケーションが使用されるデリバリーグループを指す）が空白になることがあります。 [#LC8075]
- Citrix Studioでデリバリーグループリンクをクリックすると、選択したデリバリーグループノードに移動しないことがあります。[#LC8095]
- 「プリンター割り当て」ポリシーを管理しようとすると、以下の問題が発生することがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- プリンター割り当てポリシーを追加または編集しようとすると、例外「InvalidCastException」が発生します。
- 新しいセッションプリンターを追加しようとすると、例外「InvalidOperationException」が発生します。
- プリンター割り当てポリシーからセッションプリンターを削除しようとすると失敗します。この問題は、［Remove］オプションを無効にすると発生します。
- 「プリンター割り当て」ポリシーの検索ボックスで入力をやめると、検索処理が開始されません。
- セッションプリンターの上書き設定チェックボックス（PrintQuality、PaperSize、Scale、TrueTypeOption）は、前回無効にした場合でも、常に有効になっています。[#LC8146]

- Delivery Controllerをバージョン7.15にアップグレードすると、Delivery ControllerでのCitrix Studioの起動に失敗することがあり、次のエラーメッセージが表示されます。

  「MissingMandatoryParameter、Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand」
  [#LC8396]

- Citrix Studioでデリバリーグループノードを選択し、［アプリケーション］タブを選択すると、［アプリケーション］タブのリンクが機能しなくなることがあります。[#LC8555]

コントローラー

- デリバリーグループに保守モードのもう1つのVDAが含まれる場合、公開アプリケーションを起動するデリバリーグループを選択できないことがあります。[#LC6943]

- Machine Creation Services（MCS）を使用して作成されたマシンカタログを更新すると、vSAN 6以降のバージョンでホストされている仮想マシンが起動に失敗することがあります。VMwareコンソールに次のエラーメッセージが表示されます。

  「一般的なシステムエラーが発生しました：PreProcessReconfigureSpec中にPBMエラーが発生しました：pbm.fault.PBMFault;プリプロビジョニングの検証を実行しようとしたときにエラーが発生しました。」[#LC7860]

- Citrix Studioのマシンカタログにアクセスしようとすると、Citrix Studioが予期せず終了して次の例外が発生することがあります。

  「エラーID：XDDS:ABB14FD9」[#LC7961]

- Citrix Directorは1時間ごとに間違った切断されたセッション数を表示することがあります。[#LC8006]

- サーバーOSでセッションの「AllowRestart」ポリシーによって、ユーザーが切断されたセッションからログオフできません。切断されたセッションを再起動すると、新しいセッションが開始されず、前回のセッションに再接続されます。[#LC8090]

- 「プリンター割り当て」ポリシーを管理しようとすると、以下の問題が発生することがあります。

  - プリンター割り当てポリシーを追加または編集しようとすると、例外「InvalidCastException」が発生します。
  - 新しいセッションプリンターを追加しようとすると、例外「InvalidOperationException」が発生します。
  - プリンター割り当てポリシーからセッションプリンターを削除しようとすると失敗します。この問題は、［Remove］オプションを無効にすると発生します。
  - 「プリンター割り当て」ポリシーの検索ボックスで入力をやめると、検索処理が開始されません。
  - セッションプリンターの上書き設定チェックボックス（PrintQuality、PaperSize、Scale、TrueTypeOption）は、前回無効にした場合でも、常に有効になっています。[#LC8146]
- Monitoring Serviceが、監視データベースへの新しいセッションデータの挿入に失敗することがあります。[#LC8191]

- **［Director］** > **［傾向］** > **［ログオンパフォーマンス］** の下の［ユーザーセッションごとのログオン期間］パネルに、一部

© 1999-2017 Citrix Systems, Inc. All rights reserved.

のログオンレコードしか表示されないことがあります。 [#LC8265]

- Delivery Controllerをバージョン7.15にアップグレードすると、Delivery ControllerでのCitrix Studioの起動に失敗することがあり、次のエラーメッセージが表示されます。

  「MissingMandatoryParameter、Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand」
  [#LC8396]

- 大規模なXenAppおよびXenDesktop環境では、Monitorデータベースのサイズが大きい場合、Monitorデータベースのグルーミングのストアドプロシージャが正しく動作しません。[#C8770]

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトを有効にしているときに、MSN.comおよびNews.comでFlashビデオの再生に失敗することがあります。[#LC6823]

Linux VDA

- 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]

Profile Management

- Microsoft Windows 10のセッションの起動時に、Profile Managementにより黒い画面が表示されることがあります。この修正では、「同期するディレクトリ」ポリシーを構成し、フォルダー「*AppData\Local\Microsoft\Windows\Caches*」を追加する必要があります。[#LC7596]
- Microsoft Windows 10上で動作しているVDAからログオフすると、ntuser.datファイルが使用中になり、Profile Managementストアにコピーされないことがあります。その結果、「HKEY_CURRENT_USER」レジストリキーでの変更が失われます。[#LC8068]
- ［ログオフ時にローカルでキャッシュしたプロファイルの削除］ポリシーを有効にし、［キャッシュしたプロファイルを削除する前の待ち時間］を2分に設定した場合、同じユーザーアカウントを使用して2分以内にセッションからログオフしてログオンしようとすると、新しいローカルプロファイルが作成されることがあります。[#LC8388]

Provisioning Services

StoreFront

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 一部のアプリケーションで「TWIMode」が「Off」に設定されている場合、Citrix Receiver for Chromeを使用すると、すべてのアプリケーションがウィンドウモードで起動されます。[#LC7558]
- StoreFrontに複数のストアがある場合、最初のストアまたは2番目のストアで［リモートアクセス設定の構成］をクリックすると、そのストア名が最近追加されたストアに複製されることがあります。 [#LC8089]
- StoreFrontで共有認証を使用してストアを構成した場合、新しいNetScalerアプライアンスをストアにリンクしようとすると、既にリンクされている既存のNetScaler Gatewayアプライアンスが削除されることがあります。ストアにログオンしようとすると、次のエラーメッセージが表示されます。

  「ログオンの有効期限が切れました。続行するには、もう一度ログオンしてください。」

  さらに、StoreFrontコンソールには重複したストア名が表示されます。[#LC8219]
- 「Import-STFConfiguration」PowerShellコマンドを使用してHTML5構成のストアをインポートすると、インポートが正常に完了することがあります。ただし、Citrix Receiver for HTML5を使用してアプリケーションを起動しようとすると失敗します。[#LC8290]
- StoreFrontサーバーは、コンソールのReceiver for WebサイトでNULLエントリを表示することがあります。この問題は、URLのストア名が「discovery」で始まる場合に発生します。[#LC8320]
- W3Cログサービスを有効にすると、StoreFront構成に変更を加えることができず、次のエラーメッセージが表示されることがあります。

  「変更の保存時にエラーが発生しました。」[#LC8370]
- ソケットプールを有効にした状態で、サイトデータベースの接続が一貫していない場合、継続的にログオンしてログオフすると、StoreFrontのソケットが過度に消費されることがあります。[#LC8514]

VDA for Desktop OS

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトを有効にしているときに、MSN.comおよびNews.comでFlashビデオの再生に失敗することがあります。[#LC6823]
- HDXシームレスアプリが有効なセッションで実行されているMicrosoft Officeファイル（Microsoft Excelスプレッドシートなど）を保存しようとすると、ファイルが予期せず終了する場合があります。［＃LC8572］

HDX Plug-n-Play

- 複数のデバイスで同じシリアル番号があるUSBデバイス（Syn-Tech ProKee V2など）がVDAセッションにリダイレクトされないことがあります。以下のCDFトレースが表示されます。

  「Failed to assign the instance ID, error 0xc000000d.」[#LC8264]

印刷

- アプリケーションがCitrix Print Manager Service（cpsvc.exe）のミューテックスオブジェクトを待機しているときに、公開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。[#LC6829]
- Citrix Print Manager Service（cpsvc.exe）が断続的に終了することがあります。[#LC7535]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- クライアント間でセッションを移動すると、セッションプリンターを削除できません。たとえば、「プリンター割り当て」ポリシーを構成して、クライアントAからクライアントBに移動すると、プリンターA（クライアントAのプリンター）を削除できないことがあります。[#LC8077]

サーバー/サイトの管理

- VDA 7.12以降のバージョンのレジストリキー HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWIでシームレスフラグを"0x00040000"（言語バーエージェントの無効化）に設定してシームレスセッションの言語バーを非表示にしようとすると、言語バーが非表示にならなくなります。[#LC8349]

セッション/接続

- ローカルアプリケーションアクセスが有効な場合、インタラクティブなログオン時の免責事項ポリシーを使用すると、黒または灰色の画面が45秒間表示されることがあります。[#LC6518]
- アプリケーションに再接続しようとすると、失敗することがあります。この問題は、セッションが最初に切断されたときに切断されたアプリケーションのいずれかが応答しなくなった場合に発生します。 [#LC6550]
- HDX 3D Proを使用してデュアルモニターセッションをロックすると、プライマリモニターだけがロックされます。[#LC7767]
- Skype for Businessのビデオ通話を確立すると、サードパーティアプリケーションのウィンドウと交差した後、青色のウィンドウ枠が表示されることがあります。 [＃LC7773]
- ローカルアプリケーションアクセスが有効な場合、インタラクティブなログオン時の免責事項ポリシーを使用すると、黒または灰色の画面が表示されることがあります。[#LC7798]
- 一部の公開アプリケーションが、最大化されたときに画面全体が表示されないことがあります。 [#LC7854]
- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィンドウが応答しなくなることがあります。[#LC7912]
- 特定のシナリオでは、シームレスモードでシームレスアプリケーションが表示されない、または一部の機能が動作しないことがあります。 [#LC8030]
- VDAでHDX 3D Proを有効にし、ログオン画面が表示されたときの「ログオンしようとしているユーザー向けのメッセージテキスト」のポリシーを有効にすると、公開されたデスクトップの起動に失敗し、灰色の画面が表示されることがあります。

  この修正を有効にするには、以下のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig
  名前：HKLM_DisableMontereyFBCOnInit
  値：DWORD
  種類：有効にする場合は1[#LC8082]
- ローカルアプリケーションアクセスを有効にした状態で、対話型のログオン免責事項ポリシーを使用すると、VDAに接続したときにDesktop Viewerに灰色の画面が表示されることがあります。 [#LC8136]
- Skype for BusinessやVLCメディアプレーヤーなど、リダイレクトされたWebカメラを使用するアプリケーションを使用していると、初期セッションの開始時にWebカメラがリダイレクトされて検出される場合があります。ただし、ユーザーセッションに再接続すると、Webカメラは検出されなくなります。代わりに、ビデオプレビューの代わりに灰色の画面が

© 1999-2017 Citrix Systems, Inc. All rights reserved.

表示されます。 [＃LC8588]

スマートカード

- スマートカードを使用してセッションにログオンすると、セッションを切断して再接続するまで、セッションが応答しなくなることがあります。 [#LC8036]

システムの例外

- wfshell.exeプロセスが予期せず終了し、タスクバーのグループ化モジュールを指すことがあります。 [＃LC6968]
- USBリダイレクトポリシーを有効にすると、VDAに致命的な例外が発生し、バグチェックコードSYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）のブルースクリーンが表示されることがあります。 [＃LC7999]
- バグチェックコード0x7Eによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。この問題は、しばらくの間VDAセッションをアイドル状態のままにした場合に発生します。 [＃LC8045]
- サーバーに致命的な例外が発生し、picavc.sysのバグチェックコードSYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）によるブルースクリーンが表示されることがあります。 [＃LC8063]

ユーザーエクスペリエンス

- シームレスアプリケーションセッションに再接続したときに、アプリケーションウィンドウがクライアント側で正しく表示されないことがあります。代わりに、クライアント側の小さな四角形内にセッショングラフィックが描画されます。 [#LC7857]
- Windows Media Playerで、Microsoft AVI（.avi）ファイル形式が垂直方向に反転されて表示されることがあります。 [#LC8308]
- 公開されたアプリケーションが3番目のモニターの画面で最大化されると、アプリケーションが画面全体をカバーしないことがあります。代わりに、黒い線が表示されます。 [＃LC8472]
- VDA 7.15でホストされているシームレスアプリケーションでは、アプリケーションウィンドウの移動時に、背景に灰色または黒色のフレームが表示されることがあります。 [＃LC8551]

ユーザーインターフェイス

- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。 [#LC7557]

VDA for Server OS

HDX MediaStream Flashリダイレクト

- HDXシームレスアプリが有効なセッションで実行されているMicrosoft Officeファイル（Microsoft Excelスプレッドシートなど）を保存しようとすると、ファイルが予期せず終了する場合があります。[#LC8572]

HDX Plug-n-Play

- 複数のデバイスで同じシリアル番号があるUSBデバイス（Syn-Tech ProKee V2など）がVDAセッションにリダイレクトされないことがあります。以下のCDFトレースが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「Failed to assign the instance ID, error 0xc000000d.」[#LC8264]

印刷

- アプリケーションがCitrix Print Manager Service（cpsvc.exe）のミューテックスオブジェクトを待機しているときに、公開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。[#LC6829]
- Citrix Print Manager Service（cpsvc.exe）が断続的に終了することがあります。[#LC7535]
- クライアント間でセッションを移動すると、セッションプリンターを削除できません。たとえば、「プリンター割り当て」ポリシーを構成して、クライアントAからクライアントBに移動すると、プリンターA（クライアントAのプリンター）を削除できないことがあります。[#LC8077]

サーバー/サイトの管理

- VDA 7.12以降のバージョンのレジストリキーHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWIでシームレスフラグを"0x40000"（言語バーエージェントの無効化）に設定してシームレスセッションの言語バーを非表示にしようとすると、言語バーが非表示にならなくなります。[#LC8349]

セッション/接続

- アプリケーションに再接続しようとすると、失敗することがあります。この問題は、セッションが最初に切断されたときに切断されたアプリケーションのいずれかが応答しなくなった場合に発生します。 [#LC6550]
- セッション開始の進行状況バーで［キャンセル］をクリックしたときに、間違ったセッション情報がDelivery Controllerに残る可能性があります。その結果、実際のセッションがVDAで作成されず、新しいセッションを開始できないことがあります。 [#LC6779]
- ［クライアントマイクリダイレクト］ポリシーの値を［禁止］に設定した後にも、ユーザーセッションでマイクが断続的にリダイレクトされることがあります。

  この修正によりこの問題が解決されます。ただし、問題が解決されない場合は、マイク搭載デバイスに次のレジストリキーを適用してください。

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名前：MaxPolicyAge
    種類：DWORD
    値：最後のポリシー評価とエンドポイントでのライセンス認証の間で許容される最長時間（秒単位）。デフォルトは30秒です。
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名前：PolicyTimeout
    種類：DWORD
    値：ポリシーが最新ではないと判断した後、システムがポリシーを待機する最長時間（ミリ秒単位）。デフォルトは4,000ミリ秒です。タイムアウトが発生すると、システムはポリシーを読み取り、初期化を続行します。この値を（0）に設定すると、Active Directoryポリシーチェックは行われず、ポリシーがすぐに処理されます。 [#LC7495]
- Skype for Businessのビデオ通話を確立すると、サードパーティアプリケーションのウィンドウと交差した後、青色のウィンドウ枠が表示されることがあります。[#LC7773]
- 一部の公開アプリケーションが、最大化されたときに画面全体が表示されないことがあります。 [#LC7854]
- vGPUを使用しているときにVDAのバージョン7.13、7.14、または7.15にアップグレードすると、Microsoft Windows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Serverオペレーティングシステムで実行されている公開アプリケーションまたはデスクトップに黒い領域が表示されるこ
があります。[#LC7875]

- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィンドウが応答しなくなることがあります。[#LC7912]
- 特定のシナリオでは、シームレスモードでシームレスアプリケーションが表示されない、または一部の機能が動作しないことがあります。 [#LC8030]
- ローカルアプリケーションアクセスを有効にした状態で、対話型のログオン免責事項ポリシーを使用すると、VDAに接続したときにDesktop Viewerに灰色の画面が表示されることがあります。 [#LC8136]
- 障害通知がDelivery Controllerに送信されると、サーバーOSのVDAが断続的に再登録されることがあります。 [#LC8228]
- Skype for BusinessやVLCメディアプレーヤーなど、リダイレクトされたWebカメラを使用するアプリケーションを使用していると、初期セッションの開始時にWebカメラがリダイレクトされて検出される場合があります。ただし、ユーザーセッションに再接続すると、Webカメラは検出されなくなります。代わりに、ビデオプレビューの代わりに灰色の画面が表示されます。[#LC8588]

スマートカード

- スマートカードを使用してセッションにログオンすると、セッションを切断して再接続するまで、セッションが応答しなくなることがあります。 [#LC8036]

システムの例外

- wfshell.exeプロセスが予期せず終了し、タスクバーのグループ化モジュールを指すことがあります。[#LC6968]
- タスクバーのボリュームコントロールをクリックすると、Windowsシェルエクスペリエンスホストが突然終了することがあります。 [#LC7000]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、icaendpoint.dllモジュールに障害がある場合に発生します。[#LC7900]
- USBリダイレクトポリシーを有効にすると、VDAに致命的な例外が発生し、バグチェックコードSYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）のブルースクリーンが表示されることがあります。[#LC7999]
- サーバーに致命的な例外が発生し、picavc.sysのバグチェックコードSYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）によるブルースクリーンが表示されることがあります。[#LC8063]

ユーザーエクスペリエンス

- シームレスアプリケーションセッションに再接続したときに、アプリケーションウィンドウがクライアント側で正しく表示されないことがあります。代わりに、クライアント側の小さな四角形内にセッショングラフィックが描画されます。[#LC7857]
- Windows Media Playerで、Microsoft AVI（.avi）ファイル形式が垂直方向に反転されて表示されることがあります。[#LC8308]
- 公開されたアプリケーションが3番目のモニターの画面で最大化されると、アプリケーションが画面全体をカバーしないことがあります。代わりに、黒い線が表示されます。[#LC8472]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- VDA 7.15でホストされているシームレスアプリケーションでは、アプリケーションウィンドウの移動時に、背景に灰色または黒色のフレームが表示されることがあります。[#LC8551]

ユーザーインターフェイス

- コネクションセンターを使用して、データを保存せずにシームレスなセッションからログオフすると、画面が黒くなり、以下のようなメッセージが表示されます。

  「プログラムを閉じる必要があります」。2つのオプション［ログオフを強制する］または［キャンセル］から選択してください。この時に、［キャンセル］オプションが動作しません。

  この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。[#LC6075]

- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。[#LC7557]

- Microsoft Windows Server 2008 R2デスクトップセッションからログオフしようとすると、ログオフ画面が表示されないことがあります。セッションからログオフできたとしても、セッションが予期せずに切断されたように見えます。[#LC8016]

仮想デスクトップコンポーネント - その他

- Citrix Directorは1時間ごとに間違った切断されたセッション数を表示することがあります。[#LC8006]

- Monitoring Serviceが、監視データベースへの新しいセッションデータの挿入に失敗することがあります。[#LC8191]

- **[Director]** > **[傾向]** > **[ログオンパフォーマンス]** の下の［ユーザーセッションごとのログオン期間］パネルに、一部のログオンレコードしか表示されないことがあります。 [#LC8265]

- VDAをインストールしたMicrosoft Windows 10をBuild 1511からBuild 1703にアップグレードした後、System Center Configuration Manager（SCCM）クライアントが突然終了することがあります。[#LC8632]

- Machine Creation Services（MCS）を使用している場合、Microsoft Office 2016のリセットがMicrosoft Windows 10で失敗する場合があります。[#LC8680]

- 大規模なXenAppおよびXenDesktop環境では、Monitorデータベースのサイズが大きい場合、Monitorデータベースのグルーミングのストアドプロシージャが正しく動作しません。[#LC8770]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR（初期リリース）

Apr 18, 2018

このリリースについて

XenAppおよびXenDesktopの7.15長期サービスリリース（LTSR）には、Windows VDAの新規バージョンと、複数のXenAppおよびXenDesktopコアコンポーネントの新規バージョンが含まれています。マシンの追加方法

- **XenAppまたはXenDesktopサイトのインストールまたはアップグレード**

  このリリースのISOを使用して、すべてのコアコンポーネントとVirtual Delivery Agent（VDA）をインストールまたはアップグレードします。最新のバージョンをインストールまたはアップグレードすることで、最新の機能を使用できます。

- **既存のサイトでのVDAのインストールまたはアップグレード**

  XenAppまたはXenDesktopの環境でコアコンポーネントをアップグレードする準備が整っていない場合でも、新しいVDAをインストール（またはアップグレード）することで、最新のHDX機能を使用できます。VDAのみをアップグレードすると、通常、強化された機能を実稼働環境以外の環境でテストするのに役立ちます。

手順については、「インストールの準備」または「展開のアップグレード」を参照してください。

このリリースのXenAppおよびXenDesktopのダウンロードページでは、以下のソフトウェアの更新版もダウンロードできます。機能とインストーラーの説明について詳しくは、各コンポーネントのドキュメントを参照してください。

StoreFront

AppDNA

XenAppおよびXenDesktop向けCitrix SCOM Management Pack

XenAppおよびXenDesktop 7.6 LTSRリリースから追加された機能の概要については、https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/xenapp-xendesktop-715-ltsr-feature-summary-comparison-to-76-ltsr.pdfを参照してください。

製品リリースには、XenAppおよびXenDesktop 7.14.1から以下の新しい、修正された、また強化された機能も含まれています。

Microsoft Media Foundationをインストールしていないマシンでの VDAのインストール

サポートされているほとんどのWindowsのエディションには、Microsoft Media Foundationが既にインストールされています。マシンにMedia Foundationがインストールされていない場合（Nエディション等）は、複数のマルチメディア機能がインストールされず、動作しません。その制限を認識するか、VDAのインストールを中止して、Media Foundationをインストール後に再開してください。グラフィカルユーザーインターフェイス上に、この選択がメッセージとして表示されます。制限を認識するには、コマンドラインで/no_mediafoundation_ackオプションを使用してください。

XenApp 6.5ワーカーから新しいVDAへのアップグレード

XenApp 6.5ファームに移行した後、XenApp 6.5ワーカーを新しいVDAにアップグレードできます。以前は、ワーカーサーバーでXenAppおよびXenDesktopインストーラーを実行すれば、自動的にXenApp 6.5ソフトウェアが削除され、新しいVDAがイン

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ストールされました。今回のリリースでは、最初にサーバーからHRP7とXenApp 6.5ソフトウェアを別プロセスで削除してください。その後に、新しいVDAをインストールしてください。詳しくは、「XenApp 6.5ワーカーから新しいVDAへのアップグレード」を参照してください。

MCSの第2世代VMのサポート

VMを使用するためにMicrosoft System Center Virtual Machine Managerを使う場合、Machine Creation Services（MCS）が第2世代VMのプロビジョニングに使えるようになりました。

ローカルホストキャッシュ

XenAppおよびXenDesktopの新規インストール時に、ローカルホストキャッシュはデフォルトで有効になっています。接続リース機能は、デフォルトで無効になっています。

アップグレード後、ローカルホストキャッシュ設定は変更されません。たとえば、ローカルホストキャッシュが以前のバージョンで有効にされていると、アップグレードされたバージョンでも引き続き有効になっています。以前のバージョンで無効な場合、またはサポートされていなかった場合、アップグレードされたバージョンでも無効のままです。

Director

アプリケーション障害の監視。Directorは **[アプリケーション障害]** タブで、公開アプリケーションに関連した障害履歴を表示するために、［傾向］ビューが拡張されています。選択されたアプリケーションまたはプロセスが、選択された期間中、起動時または実行中に発生した障害とエラーを確認することができます。この情報によって、アプリケーション特有の問題を理解して、トラブルシューティングすることができます。詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーション障害履歴の監視」を参照してください。

デフォルトでは、サーバーOSのVDAでホストされたアプリケーションの障害が監視されています。アプリケーション障害の監視の有効化、デスクトップOSのVDA上のアプリケーション障害の監視の有効化、および障害の監視から除外されるアプリケーションの一覧の設定は、監視グループポリシーで変更が可能です。詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

この機能の使用には、Delivery ControllerおよびVDAのバージョン7.15以降が必要です。Windows Vista以降のデスクトップOSのVDA、およびWindows Server 2008以降のサーバーOSのVDAがサポートされます。

Virtual Delivery Agent（VDA）7.15

VDAをバージョン7.9、7.11、7.12、7.13または7.14からアップグレードした後で、マシンカタログの機能レベルを更新する必要はありません。デフォルトの「7.9以降」が、なおも現在の機能レベルです。詳しくは、「VDAバージョンと機能レベル」を参照してください。

Session Recording 7.15

Session Recording 7.15の負荷分散：XenAppおよびXenDesktop 7.14で実験的に導入されていたこの機能は、このリリースには含まれていません。

新しい展開環境

新しく7.15 LTSRを展開するには

7.15 LTSRメタインストーラーを使用して、新しいXenAppまたはXenDesktop環境を設定できます。*設定前に、製品の使用に習熟してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「XenAppおよびXenDesktop 7.15長期サービスリリース」を熟読し、「製品の技術概要」、「インストールと構成」、および「セキュリティ」セクションの内容に注意して、展開の計画を開始してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。展開手順については、「インストールと構成」を参照してください。

*注：Provisioning ServicesとSession Recordingが別々のダウンロードおよびインストーラーとして利用可能

既存の展開環境

更新対象について

XenAppおよびXenDesktop 7.15 LTSRでは、7.6 LTSRのすべてのベースラインコンポーネントが更新されています。注意：展開環境のすべてのLTSRコンポーネントを7.15 LTSRに更新することをお勧めします。たとえば、Provisioning ServicesがLTSR展開環境に含まれる場合、Provisioning Servicesコンポーネントを更新します。Provisioning Servicesが展開環境に含まれない場合は、インストールや更新を行う必要はありません。

元の7.6 LTSRのリリース以降、統一インターフェイスでLTSR環境の既存のコンポーネントを更新できるメタインストーラーが追加されました。「アップグレード手順」に従い、メタインストーラーを使用して展開環境のLTSRコンポーネントを更新します。

Citrix XenAppおよびXenDesktop 7.15 LTSRのベースラインコンポーネント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Baseline Component	Version	Notes
VDA for Desktop OS	7.15	
VDA for Server OS	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
グループポリシー管理のエクスペリエンス	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
Universal Print Server	7.15	
セッション レコーディング	7.15	Platinum Editionのみ
Linux VDA	7.15	サポートされるプラットフォームについては、Linux VDAのドキュメントを参照してください。
Profile management	7.15	
Federated 認証サービス	7.15	

Citrix XenAppおよびXenDesktop 7.15 LTSRの互換性のあるコンポーネント

7.15 LTSR環境では、以下のコンポーネントの使用が推奨されます。これらのコンポーネントは、LTSRの特典（ライフサイクルの延長と修正のみのCumulative Update）の対象にはなりません。7.15 LTSR環境に含まれるこれらのコンポーネントを、より新しいバージョンにアップグレードするようお願いする場合があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.15
ライセンスサーバー用Citrix SCOM Management Pack	1.2
Citrix SCOM Management Pack for Provisioning Services	1.19
Citrix SCOM Management Pack for StoreFront	1.12
XenAppおよびXenDesktop向けCitrix SCOM Management Pack	3.13
HDX RealTime Optimization Pack	2.3
ライセンスサーバー	11.14.0ビルド21103
ワークスペース環境管理	4.4
App Layering	4.3
セルフサービス パスワード リセット	1.1

Citrix Receiverの互換バージョン

メンテナンスの容易化とパフォーマンスの最適化のために、Citrix Receiverは、最新バージョンが利用可能になり次第そのバージョンにアップグレードすることをお勧めします。最新バージョンは、https://www.citrix.com/downloads/citrix-receiver.htmlからダウンロードできます。Citrix Receiverの新バージョンが利用可能になったときに通知を受けることができるように、Citrix ReceiverのRSSフィードに登録することをお勧めします。

Citrix Receiverは、XenAppおよびXenDesktopのLTSRの特典（ライフサイクルの延長と修正のみのCumulative Update）の対象にはならないことに注意してください。7.15 LSTR環境に含まれるCitrix Receiverを、より新しいバージョンにアップグレードするようお願いする場合があります。Citrix Receiver for Windowsについては、専用のLTSRプログラムが公開されました。このプログラムについて詳しくは、「Lifecycle Milestones for Citrix Receiver」ページを参照してください。

具体的には、7.15 LTSRではCitrix Receiverの以下のバージョンとそれ以降のすべてのバージョンがサポートされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.11.1以降
Citrix Receiver for Chrome	2.4以降
Citrix Receiver for HTML5	2.4以降
Citrix Receiver for iOS	7.2以降
Citrix Receiver for Linux	13.5以降
Citrix Receiver for Mac	12.5以降
Citrix Receiver for UWP (ユニバーサル Windows プラットフォーム)	1.0.5以降
Citrix Receiver for Windows	4.9以降

XenAppおよびXenDesktop 7.15 LTSRの注意すべき除外対象

以下の機能、コンポーネント、プラットフォームは、7.15 LTSRのライフサイクルマイルストーンと特典の対象外です。すなわち、Cumulative Updateとライフサイクル延長の特典は適用されません。除外対象の機能とコンポーネントの更新は、通常の最新リリースで入手可能です。

Excluded Features
Framehawk
StoreFront Citrix Onlineの統合

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk： • Windows 10マシンでは除外されます。 • Windows 7マシンの場合、2020年1月14日までLTSRは限定的にサポートされます（CUの要件が適用されます）
AppDisk

Excluded Windows Platforms *
Windows 2008 32ビット（Universal Print Server用）

* Citrixは、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を有します。

全製品インストーラーを使用してXenAppまたはXenDesktopコンポーネントを展開またはアップグレードする場合、インストールプロセスに関する匿名の情報が、コンポーネントをインストール/アップグレードするマシンで収集および保存されます。このデータは、インストールに関するカスタマーエクスペリエンス向上のために使用されます。詳しくは、http://more.citrix.com/XD-INSTALLERを参照してください。

XenApp 6.5からの移行

XenApp 6.5の移行プロセスでは、XenApp 6.5ファームをXenApp 7.15 LTSR以降のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションとCitrixグループポリシーを含む環境で、アプリケーションとCitrixグループポリシーを手動で移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSRのコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します。

- 各XenApp 6.5ワーカー上でXenApp 7.15インストーラーを実行します。これにより、Virtual Delivery Agent for Server OSにアップグレードされます。
- いずれかのXenApp 6.5コントローラー上でPowerShellエクスポートコマンドレットを実行して、アプリケーション設定とCitrixポリシー設定をXMLファイルにエクスポートします。
- 必要に応じてXMLファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XMLファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的にXenApp 7.15 LTSRサイトにインポートできます（一部を先にインポートしてから残りを後でインポートするなど）。
- 新しいXenApp 7.15 Controller上でPowerShellインポートコマンドレットを実行して、XMLファイルから新しいXenAppサイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.xからの移行」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

解決された問題

Apr 18, 2018
バージョン7.14.1では、次の問題が解決されています。

7.14.1と比較して解決された問題

7.6 LTSR CU4と比較して解決された問題

7.14.1と比較して解決された問題

AppDNA

Citrix Director

- Citrix Directorの［**傾向**］>［**失敗**］>［**接続**］タブに移動すると、次のエラーメッセージが表示されることがあります。

  「予期しないエラーです。ネットワーク接続をチェックするか、詳細についてサーバーのイベントログを参照してください）」[#LC7755]

- Citrix Directorのセッションでポリシー情報を表示できず、次のエラーメッセージが表示されることがあります。

  「データを取得できません。」[#LC8207]

Citrixポリシー

- CitrixとMicrosoftの両方の設定を含むグループポリシーオブジェクトが適用されない場合があります。この問題は、一覧内の拡張ユニットが2つ以上のグローバル一意識別子を含む場合に発生します。[#LC7533]

Citrix Studio

- PowerShellコマンドを使う代わりにGUIモードを使う場合、新規または既存のマシンカタログにコンピューターアカウントを追加しようとすると、失敗することがあります。この問題は、NetBIOS名の検索時に、ディレクトリ検索ツールが正しいオブジェクトをバインドしなかった場合に発生します。

  たとえば、ドメイン名がxyz.ad.airxyz.aaで、NetBIOS名がxyz-Adである場合、GUIモードを使用すると、NetBIOS名はxyz-Adの代わりにxyzとして受け入れられます。結果として、マシンアカウントは既存および新規のコンピューターアカウントのどちらにも追加できません。[#LC6679]

- Citrix Delivery Controllerをバージョン7.12にアップグレードした後、マルチドメイン環境でマシンをCitrix Provisioning Services（PVS）からカタログに追加しようとすると、失敗する場合があります。この問題はPVSがデバイス名と一緒にドメイン名を返さなかった場合に発生します。Citrix Studioがローカルドメインでアカウント名を検索する場合は、アカウントが見つかりません。[#LC6818]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- App-Vアプリケーションを公開しようとすると、失敗する場合があります。[#LC7421]
- 管理者がApp-Vアプリケーションを分離グループからデリバリーグループに追加しようとするか、分離グループを作成しようとすると、Citrix Studioで以下のエラーメッセージが表示されることがあります。

  「不明なエラーが発生しました。」[#LC7594]
- ユーザーの関連付けに「NETBIOS」名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC7830]

コントローラー

- Citrix Delivery Controllerをバージョン7.12にアップグレードした後、マルチドメイン環境でマシンをCitrix Provisioning Services（PVS）からカタログに追加しようとすると、失敗する場合があります。この問題はPVSがデバイス名と一緒にドメイン名を返さなかった場合に発生します。Citrix Studioがローカルドメインでアカウント名を検索する場合は、アカウントが見つかりません。[#LC6818]
- マシンを既存のMachine Creation Serviceカタログに追加しようとすると、複数のストレージで新しいマシンを受け入れるためのラウンドロビン方式を使用しないことがあります。[#LC7456]
- カスタムの管理権限を持つ管理者が分離グループを作成しようとすると失敗して、次のエラーメッセージが表示されることがあります。

  「この要求を完了するために必要な権限がありません。詳しくは、XenDesktopサイト管理者に問い合わせてください。」[#LC7563]
- 管理者がApp-Vアプリケーションを分離グループからデリバリーグループに追加しようとするか、分離グループを作成しようとすると、Citrix Studioで以下のエラーメッセージが表示されることがあります。

  「不明なエラーが発生しました。」[#LC7594]
- Citrix Delivery Controller上でTLSv1.0を無効にしようとすると、VMware vCenterハイパーバイザーとの通信の損失が発生する場合があります。[#LC7686]
- ユーザーの関連付けに「NETBIOS」名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC7830]

HDX RealTime Optimization Pack

Profile management

- プロファイルストリーミングを有効にしてプロファイルでファイルを開こうとすると、ログオン後にファイルが空として表示されることがあります。[#LC6996]
- サーバーにおいて、バグチェックコード0x135の重大な例外がupmjit.sysで発生し、ブルースクリーンが表示されることがあります。 [#LC7841]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- VDAにログオンすると、UserProfileManager.exeが予期せず終了することがあります。[#LC7952]

StoreFront

- マルチサイト集約環境で切断されたセッションに再接続しようとすると、失敗することがあります。これによって、同じリソースの2つ目のインスタンスを受信することがあります。[#LC7453]
- 集約されたアプリケーションのソースのいずれかが無効になっている場合は、アプリケーションが予期せずエンドユーザーから非表示になることがあります。[#LC7675]
- StoreFrontで［アカウントセルフサービス］オプションを無効にしようとすると、無効と表示されていても無効にならないことがあります。[#LC7744]
- StoreFrontでストアから共有認証を削除しようとすると、変更の保存中、次のエラーメッセージが表示されることがあります。

  「変更の保存時にエラーが発生しました。」[#LC7781]

Universal Print Server

クライアント

- 印刷スプーラーサービスが応答しなくなり、ユニバーサル印刷が機能しなくなることがあります。この問題は、スプーラーサービスからの応答を待機中に、トランザクションがタイムアウトになった場合に発生します。[#LC5209]
- Profile managementを使用する環境で、あるサーバー上のCitrix Universal Printサーバープリンターを変更（追加、削除、名前の変更）しても、別のサーバー上での以降のセッションで変更が正しく反映されない場合があります。[#LC7645]

サーバー

- ドキュメントを印刷しようとすると失敗する場合があり、次のエラーメッセージが表示されます。

  「現在のプリンターの設定に問題があるため、Windowsは印刷できません。」[#LC6825]
- 特定のプリンターを使用している時に、Microsoftメモ帳が「ハンドルが無効です」のメッセージを表示し、印刷が失敗することがあります。この問題は、Citrixポリシーの「ユニバーサル印刷の使用」内で「プリンター固有のドライバーのみを使用する」が構成されており、Citrixポリシーの「Universal Print Serverの有効化」内で「有効。Windowsのリモート印刷機能にフォールバックしない」が構成されている場合に発生します。[#LC7623]

VDA for Desktop OS

インストール、アンインストール、アップグレード

- VDAをバージョン5.6.400からバージョン7.9にアップグレードした後、VDAを再起動させると以前のバージョンでインストールされたミラードライバーが残される場合があります。[#LC6295]
- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7555]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7587]

印刷

- 新しいユーザーがログオンした時に、Citrix Print Managerサービス（cpsvc.exe）が応答しなくなり、予期せず終了することがあります。[#LC6933]
- VDAをバージョン7.9からバージョン7.12以降にアップグレードした後に、Microsoft Internet ExplorerからCitrix Universal Print Driverを使って印刷しようとした時に、選択したトレイの代わりにトレイ1のみが印刷されることがあります。[#LC7463]

セッション/接続

- VDA for Desktop OS上に同じモデルの複数のWebカメラがインストールされている環境で、最新のWebカメラだけがセッションから認識されマップされることがあります。[#LC5008]
- リムーバブルクライアントドライブが、VDA for Desktop OS上のWFAPI SDKから返されないことがあります。[#LC6877]
- 複数のモニターを使用している時に公開デスクトップセッションを再接続すると、ウィンドウの配置が維持されないことがあります。[#LC7644]
- 従来のグラフィックモードを有効にし、Desktop Viewerを構成しない状態で、複数の全画面モードのモニター間でセッションを切り替えると、1つのモニターのみがセッションを実行しているように見えることがあります。[#LC7907]

スマートカード

- スマートカードの取り出しによってユーザーセッションをロックするよう構成されている場合でも、スマートカードリーダーの取り出しでユーザーセッションがロックされないことがあります。[#LC7411]

システムの例外

- vd3dk.sysでバグチェックコード0X00000050による重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC6833]
- セッションのシャットダウン中にpicadm.sysでバグチェックコード0x7Fによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7545]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、scardhook64.dllモジュールに障害がある場合に発生します。[#LC7580]
- サーバーにおいて、停止コード0xc0000006の重大な例外がvdtw30.dllで発生し、ブルースクリーンが表示されることがあります。[#LC7608]
- tdica.sysでバグチェックコードによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7632]
- この修正により、サーバーの予期しない終了を引き起こす、wdica.sysファイルのメモリの問題が対処されます。[#LC7666]

ユーザーエクスペリエンス

- この修正により、高品質なオーディオを使用して短時間再生されるサウンドのサポートが強化されます。

  注：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- この修正はWindows Server 2008 R2が実行されているセッションには影響しません。
- この修正を有効にするには、Citrix Receiver 4.4 for Windows Long Term Service Release（LTSR）CU5以降のバージョン、およびXenAppおよびXenDesktop 7.6 LTSR CU4以降のVDAバージョンを使う必要があります。

[#LC5842]

- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィンドウが応答しなくなることがあります。[#LC7481]

- マルチモニター環境では、外部モニターをWindowsの「メインディスプレイ」として定義し、コントロールパネルのディスプレイ設定でこれをノートブックまたはタブレットのセカンダリモニターの右に配置します。外部モニターに表示され公開アプリケーションを起動し、このアプリケーションを外部モニターに接続されたタブレットモニターまたはノートブックモニターに移動すると、タブレットやノートブックの開閉時に公開アプリケーション画面が黒く表示されることがあります。

  これを修正するには、VDAで次のレジストリキー値を設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  名前：EnableDrvTw2NotifyMonitorOrigin
  種類：REG_DWORD
  値：1（有効化）および0（無効化。デフォルト値）。デフォルトでは、レジストリ値は設定されていません。

  [#LC7760]

ユーザーインターフェイス

- タッチパネルでの操作に最適化されたデスクトップを使用すると、URLショートカットのアイコンが空白で表示されることがあります。[#LC6663]

- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。[#LC7557]

VDA for Server OS

インストール、アンインストール、アップグレード

- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7555]

- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7587]

印刷

- 新しいユーザーがログオンした時に、Citrix Print Managerサービス（cpsvc.exe）が応答しなくなり、予期せず終了することがあります。[#LC6933]

- VDAをバージョン7.9からバージョン7.12以降にアップグレードした後に、Microsoft Internet ExplorerからCitrix Universal Print Driverを使って印刷しようとした時に、選択したトレイの代わりにトレイ1のみが印刷されることがあります。[#LC7463]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サーバー/サイトの管理

- アプリケーションをWeb InterfaceまたはStoreFrontで起動する間に、子ドメインユーザーに対して次のエラーメッセージが表示されることがあります。

  「この公開アプリケーションへのアクセス権がありません。」[#LC7566]

セッション/接続

- VDA for Desktop OS上に同じモデルの複数のWebカメラがインストールされている環境で、最新のWebカメラだけがセッションから認識されマップされることがあります。[#LC5008]
- セッションに再接続しようとすると断続的に失敗し、VDA for Server OSが「初期化中」状態に移行します。この問題はVDAがDelivery Controllerに再度登録されると発生します。

  [#LC6647]

- Delivery Controllerの接続が切断されると、XenAppサーバーでアクティブなセッションが切断されることがあります。この問題は、VDAが「事前起動」から「アクティブ」へ正しく移行するセッションの状態を追跡できない時に発生します。そのため、Delivery Controllerが再起動されると、VDAのリソースをクリアしようとし、アプリケーションがアクティブにもかかわらず、事前起動状態のセッションが切断されるかログオフされます。[#LC6819]
- Microsoft Windows Server 2016で公開アプリケーションを起動すると、アプリケーションが表示されるまでしばらく黒い画面が表示されることがあります。[#LC7947]

システムの例外

- セッションのシャットダウン中にpicadm.sysでバグチェックコード0x7Fによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7545]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、scardhook64.dllモジュールに障害がある場合に発生します。[#LC7580]
- サーバーにおいて、停止コード0xc0000006の重大な例外がvdtw30.dllで発生し、ブルースクリーンが表示されることがあります。[#LC7608]
- tdica.sysでバグチェックコードによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7632]
- この修正により、サーバーの予期しない終了を引き起こす、wdica.sysファイルのメモリの問題が対処されます。[#LC7666]

ユーザーエクスペリエンス

- この修正により、高品質なオーディオを使用して短時間再生されるサウンドのサポートが強化されます。

  注：

  - この修正はWindows Server 2008 R2が実行されているセッションには影響しません。
  - この修正を有効にするには、Citrix Receiver 4.4 for Windows Long Term Service Release（LTSR）CU5以降のバージョン、およびXenAppおよびXenDesktop 7.6 LTSR CU4以降のVDAバージョンを使う必要があります。

  [#LC5842]

- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィン

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ドウが応答しなくなることがあります。[#LC7481]

- マルチモニター環境では、外部モニターをWindowsの「メインディスプレイ」として定義し、コントロールパネルのディスプレイ設定でこれをノートブックまたはタブレットのセカンダリモニターの右に配置します。外部モニターに表示され公開アプリケーションを起動し、このアプリケーションを外部モニターに接続されたタブレットモニターまたはノートブックモニターに移動すると、タブレットやノートブックの開閉時に公開アプリケーション画面が黒く表示されることがあります。

  これを修正するには、VDAで次のレジストリキー値を設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  名前：EnableDrvTw2NotifyMonitorOrigin
  種類：REG_DWORD
  値：1（有効化）および0（無効化。デフォルト値）。デフォルトでは、レジストリ値は設定されていません。

  [#LC7760]

ユーザーインターフェイス

- タッチパネルでの操作に最適化されたデスクトップを使用すると、URLショートカットのアイコンが空白で表示されることがあります。[#LC6663]
- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。[#LC7557]

仮想デスクトップコンポーネント - その他

- App-Vアプリケーションを公開しようとすると、失敗する場合があります。[#LC7421]
- シングル管理モードでApp-Vアプリケーションを起動しようとすると失敗する場合があります。この問題は、アプリケーション名に特殊文字が含まれている場合に発生します。[#LC7897]

7.6 LTSR CU4と比較して解決された問題

Citrix Director

- Windows統合認証（WIA）を使用したCitrix Directorが、Kerberosの制約付き委任のセットアップで機能しないことがあります。[#LC5196]
- Citrix Directorにログインした後に「システム利用不可」エラーが発生します。[#LC5385]
- Citrix Directorがセッション詳細を表示しないことがあります。この問題は、アプリケーションタイプとして公開コンテンツを使用する場合に発生します。[#LC6577]

Citrixポリシー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrixポリシー処理が応答しなくなることがあります。これにより、ユーザーセッションも応答しなくなります。この問題が発生すると、Citrix Receiverおよびリモートデスクトップ（RDP）への接続要求が失敗します。[#LA4969]

- システムに修正#LC1987（GPCSExt170W2K8R2X64006またはそれに代わるもの）がインストールされると、CitrixとMicrosoftの両方の設定を含むActive Directory（AD）ポリシーが適用されないことがあります。

  注：この修正は、この更新をインストールした後に作成したADポリシーの問題に対応します。また、Citrixの設定がMicrosoftの設定より前に構成された*既存*のポリシーの問題にも対応します。Microsoftの設定がCitrixの設定より*前に*構成された既存のADポリシーの問題には対応しません。これらのADポリシーについては、影響されるポリシーを開いて、Citrの設定を保存する必要があります。[#LC2121]

- この機能強化により、Citrix Group Policy Engineは、Citrixポリシーの処理時に追加のイベントログメッセージを生成します。[#LC3664]

- 7.6からバージョン7.8または7.9にアップグレードすると、Citrix Studioの一部の配色で、テキストが適切に表示されないほど表示が暗くなることがあります。[#LC5690]

- Citrix Federated Authenticationサービスをインストールした後、StoreFrontサーバー上の［ユーザー規則］の下に［Securityアクセス制御一覧］を構成しようとすると、構成ウィンドウが応答しなくなる場合があります。[#LC5788]

- マクロを含む、XLSMファイル拡張子のファイルを開く間に、Microsoft ExcelのCPUとメモリの消費が急増することがあります。結果として、ファイルを開こうとすると失敗します。[#LC6142]

- CitrixとMicrosoftの両方の設定を含むグループポリシーオブジェクトが適用されない場合があります。この問題は、一覧内の拡張ユニットが2つ以上のグローバル一意識別子を含む場合に発生します。[#LC7533]

Citrix Studio

- 複数のユーザーが複数のStudioセッションでポリシーを作成すると、Citrix Studioが更新された時に、一番新しく作成されたポリシーによって、それ以前のポリシーが上書きされます。[#LA5533]

- Citrix StudioによってXenDesktop App Editionライセンスが認識されず、次のエラーメッセージが表示されることがありました。

  「有効なライセンスが見つかりません
  使用できる適切なライセンスがありません。ライセンスサーバーのアドレス、製品エディション、およびモデルを確認してください。」[#LC0822]

- クロスドメインユーザーをDelivery Groupに追加しようとすると、Citrix Studioによってこれらのユーザーの実際のドメインがローカルドメインアカウントとして解決されるという問題がありました。[#LC1886]

- 引用符（"）を含むコマンドライン引数を使用してCitrix Studio 7.7でアプリケーションを公開しようとすると、エラーメッセージが表示されることがあります。[#LC4525]

- カタログの更新が実行されていない場合、Citrix Studioがカタログロールバックオプションを提供することがあります。ロールバックを選択すると、例外が発生します。[#LC4791]

- Citrix StudioからマシンをMachine Catalogに追加しようとすると、次のエラーメッセージが表示されることがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この問題は、XenDesktopセットアップウィザードを使用した場合は発生しません。[#LC5030]

- 2つのアプリケーションが同じApplicationIDを持つ場合、App-Vアプリケーションを更新すると、Citrix StudioによるApp-Vパッケージ名の設定が不正確になることがあります。[#LC5261]
- Delivery Controllerがオフラインまたは使用不可になると、Citrix Studioの動作が遅くなることがありました。[#LC5335]
- XenAppまたはXenDesktopを7.6から7.7にアップグレードした後に、アップグレードを求めるメッセージがCitrix Studioに表示されることがありました。[#LC5478]
- 多くのパッケージを含むApp-Vサーバーとともに構成されているバージョン7.9のCitrix Studioインスタンスを閉じて、再度開こうとした時に、Studioが開いたままになり、開けなくなります。[#LC5643]
- Citrix Studioを使うと、サイトにApp-Vサーバーを1台しか追加できません。更にApp-Vサーバーをサイトに追加するには、PowerShellを使う必要があります。[#LC5767]
- Citrix Studioを7.8から7.9にアップグレードした後に、アップグレードの後に追加したアプリケーションが、パッケージ名またはバージョンなしで表示されます。[#LC5958]
- Citrix Studioの［アプリケーション］ノードを介してアプリケーションを追加すると、アプリケーションが追加されないエラーが発生することがあります。回避策として、［デリバリーグループ］ノードを使用してアプリケーションを追加します。[#LC5975]
- Citrix Studioを介して新しいXenDesktopサイトを作成し、SQL AlwaysOn Listenerを参照すると、次のエラーが表示されることがあります。

  「レプリカサーバーに接続できませんでした。SQL Serverでデータベースの状態をチェックしてください。データベースサーバーがリモート接続を実行でき、ファイヤーウォールが接続をブロックしていないか確認してください。」[#LC6010]
- 既存の公開されたApp-VパッケージをCitrix Studioから削除して、同じ名前と公開場所で同じApp-Vパッケージの異なるバージョンをデリバリーグループに追加しようとすると、そのパッケージに赤い感嘆符「!」が付いて、次のエラーメッセージが表示されます。

  「アプリケーション”アプリケーション名”のアプリケーションデータを読み込めませんでした」[#LC6254]
- Citrix StudioからControllerを追加するオプションとPowerShellコマンドの「Add-XDController」を使用して、ミラーリンクされたデータベースの設定にDelivery Controllerを追加しようとすると失敗する場合があります。[#LC6563]
- PowerShellコマンドを使う代わりにGUIモードを使う場合、新規または既存のマシンカタログにコンピューターアカウントを追加しようとすると、失敗することがあります。この問題は、NetBIOS名の検索時に、ディレクトリ検索ツールが正しいオブジェクトをバインドしなかった場合に発生します。

  たとえば、ドメイン名がxyz.ad.airxyz.aaで、NetBIOS名がxyz-Adである場合、GUIモードを使用すると、NetBIOS名はxyz-Adの代わりにxyzとして受け入れられます。結果として、マシンアカウントは既存および新規のコンピューターアカウントのどちらにも追加できません。[#LC6679]
- Citrix Delivery Controllerをバージョン7.12にアップグレードした後、マルチドメイン環境でマシンをCitrix Provisioning Services（PVS）からカタログに追加しようとすると、失敗する場合があります。この問題はPVSがデバイス名と一緒にドメイン名を返さなかった場合に発生します。Citrix Studioがローカルドメインでアカウント名を検索する場合は、アカウントが見つかりません。[#LC6818]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- XenAppサイトをアップグレードした時に、予期せずライセンスモデルがXenAppからXenDesktopに変更される場合があります。[#LC6981]
- PowerShell 5での実行時に、「Get-XDSite」およびその他のXenDesktopの高レベル管理PowerShellコマンドに対する「Start-Transcript」コマンドが失敗する場合があります。[#LC7006]
- 管理者がApp-Vアプリケーションを分離グループからデリバリーグループに追加しようとするか、分離グループを作成しようとすると、Citrix Studioで以下のエラーメッセージが表示されることがあります。

  「不明なエラーが発生しました。」[#LC7594]
- ユーザーの関連付けに「NETBIOS」名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC7830]

コントローラー

- Citrix StudioのMachine Creation Serviceを使って仮想マシンを展開すると、次のエラーメッセージが表示されます。

  「エラーId: XDDS:0F7CB924」 [#LC4930]
- XenServerで作成されたプールカタログを削除しようとしてから、カタログのアップデートを実行すると、ベースディスクがストレージから削除されず、ベースディスクの数が増えることがありました。[#LC0577]
- Active Directoryのグループポリシーオブジェクト（GPO）で、またはXenDesktop 5.6 Desktop Delivery Controller（DDC）を使用して開始されるVDA 7.x上のCitrix Studioセッションで、セッション画面の保持を無効にすることができないという問題がありました。[#LC0878]
- Machine Creation Serviceを使用して、カスタムVMXとnvram設定によるマスターイメージから新たにプールされたマシンを作成する時に、設定が新しい仮想マシンにコピーされないという問題がありました。[#LC0967]
- Broker Serviceで実行されるPrepareSessionタスクは、XenDesktop 5.6環境で使われるとタイムアウトを起こすことがあり、StoreFrontの失敗の原因になります。[#LC1055]
- この修正は、最初のマシンを作成する時にPersonal vDiskボリュームをフォーマットする間、ハイパーバイザーの混雑によって発生する可能性があるタイミングの問題に対応します。[#LC3275]
- VMware vSphere 6.0とvSAN 6ストレージを使った、Machine Creation Serviceでの仮想マシンの作成は、失敗することがあります。[#LC4563]
- WaitForTask応答により、マシンカタログの更新を許可しない例外VimApi.MissingPropertyが発生します。[#LC4573]
- Citrix StudioからマシンをMachine Catalogに追加しようとすると、次のエラーメッセージが表示されることがあります。この問題は、XenDesktopセットアップウィザードを使用した場合は発生しません。[#LC5030]
- VDAをバージョン7.8にアップグレードした後、インベントリの更新操作を実行しようとすると失敗する場合があり、次のエラーメッセージが表示されます。

  「内部エラーが発生しました。エラーコード0x2により、インベントリの更新に失敗しました。」[#LC5051]
- 日本語OS上にインストールされたCitrixサービスの「サービス表示名」と「サービスの説明」の末尾に、不必要な文字が表

© 1999-2017 Citrix Systems, Inc. All rights reserved.

示される場合があります。[#LC5208]

- 2つのアプリケーションが同じApplicationIDを持つ場合、App-Vアプリケーションを更新すると、Citrix StudioによるApp-Vパッケージ名の設定が不正確になることがあります。[#LC5261]
- XenAppまたはXenDesktopを7.6から7.7にアップグレードした後に、アップグレードを求めるメッセージがCitrix Studioに表示されることがありました。[#LC5478]
- アプリケーションのタイトルにアンパサンド（&）が含まれていると、StoreFront XMLが破損し、アプリケーションまたはアイコンが表示されなくなることがあります。[#LC5505]
- 多くのパッケージを含むApp-Vサーバーとともに構成されているバージョン7.9のCitrix Studioインスタンスを閉じて、再度開こうとした時に、Studioが開いたままになり、開けなくなります。[#LC5643]
- XenDesktop 7.9にアップグレードした後に、NetScalerブローカーが正しく資格情報を送信しないために、ログオンが失敗することがあります。[#LC5753]
- Citrix Studioを使うと、サイトにApp-Vサーバーを1台しか追加できません。更にApp-Vサーバーをサイトに追加するには、PowerShellを使う必要があります。[#LC5767]
- Citrix Federated Authenticationサービスをインストールした後、StoreFrontサーバー上の **[ユーザー規則]** の下に **[Securityアクセス制御一覧]** を構成しようとすると、構成ウィンドウが応答しなくなる場合があります。[#LC5788]
- 分析、ブローカー、ログなどのFlexcast Management ArchitectureサービスのSDKポートを変更すると、Citrix Studioが正しく接続されない原因になります。[#LC6005]
- Citrix Studioを介して新しいXenDesktopサイトを作成し、SQL AlwaysOn Listenerを参照すると、次のエラーが表示されることがあります。

  「レプリカサーバーに接続できませんでした。SQL Serverでデータベースの状態をチェックしてください。データベースサーバーがリモート接続を実行でき、ファイヤーウォールが接続をブロックしていないか確認してください。」[#LC6010]
- Citrix Directorによって傾向ページのレポートと一致しない未登録マシンがダッシュボードにいくつか表示されることがあります。[#LC6184]
- 監視サービスは、負荷評価基準インデックスポリシーが有効になると、監視データベースへの新しいセッションデータの挿入に失敗します。これによって、Citrix Directorがセッションの最新情報（ログオン処理時間、現在アクティブなセッション数など）を表示できなくなります。Citrix Directorで表示される問題は、Delivery Controllerでの問題が原因で発生します。Controllerの最新バージョンは、この問題に対応しています。[#LC6241]
- ホスティングユニットを削除しようとすると、他のすべてのホスティングユニットでのAppDisksのレプリケーションが失敗する場合があります。結果として、AppDisksを持つデリバリーグループのマシンの起動に失敗します。[#LC6433]
- Citrix Monitoring ServiceまたはCitrix Delivery Controllerの再起動後、イベントID 1013が表示される場合があります。

  「次の原因により、初期データベースハウスキーピングに失敗しました：System.NullReferenceException：オブジェクト参照がオブジェクトインスタンスに設定されていません。」

  この問題は、Citrix Monitor Serviceが停止している時に発生します。[#LC6438]
- Citrix Delivery Controller上で特定のサードパーティ製アプリケーション（RayStationなど）を使用しようとすると、失敗し

© 1999-2017 Citrix Systems, Inc. All rights reserved.

て次のエラーメッセージが表示されます。

「通信オブジェクトSystem.ServiceModel.Channels.ServiceChannelが破損しているため通信に使用できません。」[#LC6552]

- Citrix Studioから追加のControllerを追加するオプションとPowerShellコマンドの「Add-XDController」を使用して、ミラーリングされたデータベースの設定にDelivery Controllerを追加しようとすると失敗する場合があります。[#LC6563]
- VMware VSANのMCSカタログを削除しようとすると失敗する場合があります。[#LC6691]
- Monitoring Serviceのメモリ消費が急増する場合があり、これによりサーバーの反応が遅くなります。[#LC6705]
- Citrix Studioを以前のバージョンからアップグレードしたり、Citrix Studioバージョン7.12を新規インストールしたりした後で、Delivery Controllerが原因でCitrix Studioが必須のアップグレードループに陥る場合があります。[#LC6737]
- Machine Creation Serviceのバージョン7.12を使用して仮想マシンを作成すると、XenToolsのインストールが失敗し、仮想マシンを通常の方法でシャットダウンできません。[#LC6769]
- Citrix Delivery Controllerをバージョン7.12にアップグレードした後、マルチドメイン環境でマシンをCitrix Provisioning Services（PVS）からカタログに追加しようとすると、失敗する場合があります。この問題はPVSがデバイス名と一緒にドメイン名を返さなかった場合に発生します。Citrix Studioがローカルドメインでアカウント名を検索する場合は、アカウントが見つかりません。[#LC6818]
- App-Vパッケージの公開許可を、完全なアクセス権を持たない管理者に設定しようとすると、次の例外が発生して拒否される場合があります。

  「Citrix.Console.Models.Exceptions.PermissionDeniedException：この操作を実行する権限がありません。」[#LC6897]
- HighAvailabilityService.exeプロセスによってメモリの消費量が多くなることがあります。[#LC6918]
- XenAppサイトをアップグレードした時に、予期せずライセンスモデルがXenAppからXenDesktopに変更される場合があります。[#LC6981]
- PowerShell 5での実行時に、「Get-XDSite」およびその他のXenDesktopの高レベル管理PowerShellコマンドに対する「Start-Transcript」コマンドが失敗する場合があります。 [#LC7006]
- この修正によりCitrix Host Serviceのメモリの問題が解決されます。[#LC7516]
- カスタムの管理権限を持つ管理者が分離グループを作成しようとすると失敗して、次のエラーメッセージが表示されることがあります。

  「この要求を完了するために必要な権限がありません。詳しくは、XenDesktopサイト管理者に問い合わせてください。」[#LC7563]
- 管理者がApp-Vアプリケーションを分離グループからデリバリーグループに追加しようとするか、分離グループを作成しようとすると、Citrix Studioで以下のエラーメッセージが表示されることがあります。

  「不明なエラーが発生しました。」[#LC7594]
- Microsoftリモートデスクトップセッションホストの役割サービスが既にインストールされている時に、Microsoft Windowsサーバー上にVDAをインストールしようとすると、失敗することがあります。[#LC7680]
- Citrix Delivery Controller上でTLSv1.0を無効にしようとすると、VMware vCenterハイパーバイザーとの通信の損失が発生する場合があります。[#LC7686]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ユーザーの関連付けに「NETBIOS」名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題はNETBIOS名が間違ったURLを使った場合に発生します。[#LC7830]

ライセンス管理

- 「X-Frame-Options」ヘッダータイプが設定されていないため、ライセンスサーバーによる、クリックジャッキングに対するPayment Card Industry（PCI）コンプライアンススキャンが失敗します。[#LC1983]
- 名前が32文字より多いドメイングループを追加しようとすると、失敗することがあります。[#LC1986]
- NetBiosドメイン名にアンパサンド（&）が含まれている場合、Studioで［ライセンス］タブを開こうとすると失敗して次のエラーメッセージが表示されます。

  「Citrixライセンスサーバーを使用できません」[#LC2728]

Profile management

- ログオンまたはログオフ時に、一部のサードパーティ製アプリケーションによるファイル名の変更やファイルの移動に失敗することがありました。たとえば、ローカルプロファイル内にfile0、file1、およびfile2という名前のファイルがあった場合に、ログオフ時にfile2からfile3、file1からfile2、およびfile0からfile1への変更に失敗します。この問題は、待機領域またはユーザーストア内にfile2が既に存在する場合に発生します。[#LC0465]
- ユーザーのログオフ時に、Profile managementサービス（UserProfileManager.exe）が異常停止することがありました。[#LC0625]
- パフォーマンスモニター（Perfmon）の［ログオン期間］パネルに、Profile Managementによって管理されていないユーザーログオンのデータが記録される場合がありました。[#LC0779]
- Profile managementによるファイルとユーザーストアの同期が一定期間行われない場合がありました。[#LC1338]
- 次のログオプションを有効にすると、デバッグ情報が次のログファイルに記録されませんでした。
  - ポリシー：Active Directory操作
  - ポリシー：ログオンおよびログオフ時のポリシー値
  - ポリシー：ログオフ時のレジストリ差分

  [#LC2003]
- ユーザーがhttps://support.microsoft.com/ja-jp/kb/2890783で説明されているようにプロファイルのバージョンを有効にすると、Profile managementは次の理由で移行を行わない場合がありました。
  - Microsoft移動プロファイルが「V4」という拡張子で作成されている。
  - UPMプロファイルが「デフォルトユーザー」テンプレートから移行および作成されなかった。

  [#LC2427]
- ユーザープロファイルをDesktop Directorでリセットすると、ユーザーが初めてログオンする場合にフォルダーへのリダイレクトが動作しなくなっていました。フォルダーへのリダイレクトは、ユーザーが後でログオンする時には動作します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LC2602]

- Profile Management（UserProfileManager.exe）サービスが予期せずに閉じる場合がありました。[#LC2979]
- #LC0625の修正を適用すると、Profile Management（UserProfileManager.exe）サービスが予期せずに閉じる場合がありました。[#LC3058]
- Windows 8.1では、拡張保護モードが有効の場合、Internet Explorer 11を使用してファイルをダウンロードしようとしても失敗します。[#LC3464]
- Profile Managementでのログオフプロセスで、次のエラーメッセージとともにファイルのロックが発生する可能性があります。

  「The process cannot access the file because it is being locked by another process.」

  ロックが解除されるまで、Profile managementによってロックされたファイルを削除しようとしても失敗することがあります。[#LC3532]
- ユーザーデバイスがシャットダウンのプロセス中に、Profile managementが予期せずに終了することがありました。[#LC3626]
- 再起動されるまで、ファームのXenAppサーバーが応答しなくなることがあります。[#LC4318]
- RDPを使用してXenApp 7.7サーバーにログオンしようとすると、サーバーがようこそ画面のまま応答しなくなることがあります。[#LC5169]
- VDAをバージョン7.6.1000以前からバージョン7.7以降にアップグレードした後でProfile ManagementやVDAを削除、修復、または再インストールしようとすると、失敗することがあります。[#LC5207]
- ログオフ時に、Profile managementでサーバー上のファイル/フォルダーがロックされ、そのためにアプリケーションが起動に失敗することがあります。ローカルにキャッシュされたプロファイルも削除されません。[#LC5266]
- Profile managementで、ユーザープロファイル内のファイルがロックされることがあります。その場合、それらのプロファイルのロックが解除されるまで、ユーザーは再接続試行時に一時プロファイルを受け取ります。[#LC5278]
- ユーザーのログオフ時に、ローカルでキャッシュしたプロファイルが削除されません。[#LC5470]
- ライセンスサーバーがオフラインの時、サーバーでユーザーリダイレクトフォルダーを使用するファイルが失われます。[#LC5595]
- 更新しないままライセンスの試用期間が終了すると、ユーザーのファイルが失われます。[#LC5775]
- Profile managementにより、ネットワークが失われたことを示す「NetworkDetection」フラグが誤って発生することがあります。この修正には、ネットワークが一時的に使用できないかどうかに代わって、ネットワークが利用できないかを確認する追加のチェックが導入されています。[#LC5943]
- Windows Server 2012 R2で、ユーザーログオン画面が応答しなくなることがあります。 [#LC6149]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 移動プロファイルをProfile managementに移行しようとすると、失敗することがあります。この問題は、不正確なバージョン番号がプロファイルに追加された時に発生します。[#LC6150]

- WAN接続でProfile managementのユーザープロファイルストアからアプリケーションのアイコンをコピーしようとすると、アイコンが灰色表示されることがあります。[#LC6152]

- Microsoft Windows 10およびWindows Server 2016上で実行中のProfile Managementが有効なセッションで、ファイルの種類の関連付けがローミングできないことがあります。[#LC6736]

- Microsoft Windows 10またはWindows Server 2016でログオフ時にローカルキャッシュを削除するポリシーを有効にしていると、ログオフ時にNTUSER.DATファイルが削除されないことがあり、次回のログオン時に別のローカルプロファイルが作成されます。[#LC6765]

- Microsoft Windows Server 2016上でProfile Managementを使用し、usrclass.datが含まれていると、［スタート］メニューが動作しないことがあります。[#LC6914]

- プロファイルストリーミングを有効にしてプロファイルでファイルを開こうとすると、ログオン後にファイルが空として表示されることがあります。[#LC6996]

- Microsoft Windows 10のセッションの起動時に、Profile managementにより黒い画面が表示されることがあります。この修正では、「同期するディレクトリ」ポリシーを構成し、フォルダー「*AppData\Local\Microsoft\Windows\Caches*」を追加する必要があります。[#LC7596]

Provisioning Services

コンソールの問題

- この修正により、［次のvDisk更新をこの日に実行する］オプションおよび［vDisk更新を検出したらすぐに適用する］オプションはProvisioning Servicesで利用できなくなります。[#LA4166]

- XenDesktopセットアップウィザードを介して仮想マシンを作成しようとすると、英語版以外のMicrosoft System Center Virtual Machine Manager（SCVMM）環境で失敗することがあります。[#LC5451]

- New-BootDeviceManager PowerShellスクリプトでISOを作成しようとすると失敗し、次のエラーメッセージが表示されることがあります。「ISOFileNameは、作成する新しいISOファイルの名前にする必要があります。」[#LC5559]

- クラスターストレージボリュームを使用する場合は、ストリーム配信仮想マシンセットアップウィザードでボリュームを選択できませんが、ランダムボリュームにターゲットデバイスを作成できます。[#LC5890]

- XenDesktopセットアップウィザードまたはストリーム配信仮想マシンセットアップウィザードの実行後にProvisioning Servicesコンソールを閉じようとすると、例外が発生することがあります。[#LC6048]

- PVS 7.11をバージョン7.6からアップグレードすると、他のドメインのユーザーがコンソールにログオンできないことがあります。[#LC6216]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- サーバー通信のタイムアウト。ログイン処理時間が大幅に長くなる（2分を超えるなど）こともあり、これによって、PVSコンソールとSOAPサーバーの間でサーバータイムアウトが発生することがあります。デフォルトでは、こうした接続のタイムアウトは2分で発生します。タイムアウト時間を延長するには、次のレジストリ値を変更します。HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<秒単位のタイムアウト>。ログイン時間が約4分より長くなると、PVSコンソールを含むMicrosoft管理コンソール（MMC）からタイムアウトします（このタイムアウトは破棄することもできます）。

  この問題は、Active Directoryに到達不能ドメインがある場合にも発生します。Active Directoryの到達不能ドメインへの接続は、30秒でタイムアウトになります。到達不能ドメインが複数ある場合は、ログイン処理時間は合計で数分になります。通常、Active Directoryにテストドメインや試験的なドメインを追加し、後から削除すると、到達不能ドメインが作成されることになります。ドメインは削除されても、ドメインや認証グループを列挙したActive Directoryのレポートには残ります。

  また、ドメインコントローラーが一時的にシャットダウンされ、ネットワークから切断された時も、到達不能ドメインとなされます。そのため、すべての到達不能ドメインをブラックリストに登録すべきではありません。

  到達不能ドメインがあるかを判断する最良の方法は、PVS_DLL_ADSUPPORTモジュールのCitrix診断ファシリティ（CDF）トレースで「Unreachable Domain」および「Server Referral」エラーを見つけることです。どちらかが見つかった場合、それらのドメインがもう使用されていないことを確認します。使用されていない場合、ドメイン名をブラックリストに追加します。

  ブラックリストは「%ProgramData\Citrix\Provisioning Services\blacklist.json」というJSON形式のファイルです。例：
  {

  "Domains":

  [

  "sub.xs.local",

  "sb.xs.local"

  ]

  }

  ここで**sub.xs.local**および**sb.xs.local**という2つのドメインは、ドメインおよびグループの列挙から除外されます。JSONファイルの更新後、SOAPサーバーと実行中のすべてのコンソールを再起動して更新された値を読み込みます。[#LC6249]

- Provisioning Servicesコンソールの構成後、ターゲットデバイスプロパティのラベル名がない場合があります。[#LC6864]

サーバーの問題

- VMware ESX環境で、XenDesktopのセットアップウィザードで例外が発生し、テンプレートおよびマシンを正しくセットアップできなくなることがありました。[#LA2499]

- 2つのPVSサーバーで、相手サーバーのvDiskの複製状態は表示できませんが、自身のvDiskの状態は適切に表示できることがあります。#LC4317]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix PXEサービスが、BOOTPTABファイルのエントリを無視することがあります。[#LC4600]

- BDMパーティションを使用している場合、VMware上のターゲットデバイスは、リストの最上位に表示されているサーバーにアクセスできないと、リスト上のどのサーバーにもログオンを試みません。[#LC4736]

- XenDesktopセットアップウィザードを介して仮想マシンを作成しようとすると、英語版以外のMicrosoft System Center Virtual Machine Manager（SCVMM）環境で失敗することがあります。[#LC5451]

- ハードドライブのすべてのパーティションが複製されているのでなければ、最後のパーティションの複製が失敗する場合があります。[#LC5452]

- PVSコンソールで2つのPVSサーバーの複製状態を実行すると、どちらのサーバーの状態も不完全として表示されます。[#LC5700]

- クラスターストレージボリュームを使用する場合は、ストリーム配信仮想マシンセットアップウィザードでボリュームを選択できませんが、ランダムボリュームにターゲットデバイスを作成できます。[#LC5890]

- PVS 7.11をバージョン7.6からアップグレードすると、他のドメインのユーザーがコンソールにログオンできないことがあります。[#LC6216]

- サーバー通信のタイムアウト。ログイン処理時間が大幅に長くなる（2分を超えるなど）こともあり、これによって、PVSコンソールとSOAPサーバーの間でサーバータイムアウトが発生することがあります。デフォルトでは、こうした接続のタイムアウトは2分で発生します。タイムアウト時間を延長するには、次のレジストリ値を変更します。HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<秒単位のタイムアウト>。ログイン時間が約4分より長くなると、PVSコンソールを含むMicrosoft管理コンソール（MMC）からタイムアウトします（このタイムアウトは破棄することもできます）。

  この問題は、Active Directoryに到達不能ドメインがある場合にも発生します。Active Directoryの到達不能ドメインへの接続は、30秒でタイムアウトになります。到達不能ドメインが複数ある場合は、ログイン処理時間は合計で数分になります。通常、Active Directoryにテストドメインや試験的なドメインを追加し、後から削除すると、到達不能ドメインが作成されることになります。ドメインは削除されても、ドメインや認証グループを列挙したActive Directoryのレポートには残ります。

  また、ドメインコントローラーが一時的にシャットダウンされ、ネットワークから切断された時も、到達不能ドメインとみなされます。そのため、すべての到達不能ドメインをブラックリストに登録すべきではありません。

  到達不能ドメインがあるかを判断する最良の方法は、PVS_DLL_ADSUPPORTモジュールのCitrix診断ファシリティ（CDF）トレースで「Unreachable Domain」および「Server Referral」エラーを見つけることです。どちらかが見つかった場合、それらのドメインがもう使用されていないことを確認します。使用されていない場合、ドメイン名をブラックリストに追加します。

  ブラックリストは「%ProgramData\Citrix\Provisioning Services\blacklist.json」というJSON形式のファイルです。例：

  {

  "Domains":

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[

"sub.xs.local",

"sb.xs.local"

]

}

ここで**sub.xs.local**および**sb.xs.local**という2つのドメインは、ドメインおよびグループの列挙から除外されます。JSONファイルの更新後、SOAPサーバーと実行中のすべてのコンソールを再起動して更新された値を読み込みます。[#LC6249]

ターゲットの問題

- Provisioning Servicesターゲットデバイスの自動更新機能を使用している時に、更新が利用できない場合、ターゲットのイベントビューアーで次のアプリケーションエラーメッセージ（イベントID：0）が生成されるという問題がありました。「No update server found. Stopping client service.（更新サーバーが見つかりません。クライアントサービスが停止しています。）」[#LC0450]

- ターゲットデバイスのソフトウェアがAppDiskドライブを認識せず、AppDiskドライブを書き込みキャッシュ用に使用して、競合が引き起こされることがあります。[#LC5409]

- 「RAMの書き込みキャッシュ」を使用してvDiskを構成し、RAMキャッシュサイズを4,096MBまたは4,097MBに設定した場合に、Hyper-V第2世代仮想マシンから起動するとターゲットデバイスに重大な例外が発生しブルースクリーンが表示されることがあります。[#LC6707]

StoreFront

- 管理者がグループポリシー設定のMaxPasswordAgeの値を変更すると、StoreFrontのデフォルトのドメインサービスは新しい値を再読み込みしません。このため、ユーザーに誤った「パスワードの有効期限までの日数」が表示されます。

  注：この問題は解決されましたが、新しい値を読み込むには最大1時間を要することがあります。[#DNA-41380]

- StoreFront 3.5をインストールすると、カテゴリビューのフォルダーの色に、StoreFront管理コンソールで定義されたカスタム色が使用されなくなる可能性があります。フォルダーの色はデフォルト色に戻ります。[#LC5001]

- Citrix Receiver for Webサイトを管理している時に、StoreFrontが予期せず終了することがあります。この問題は、style.cssがCitrix Receiver for Web用にカスタマイズされると発生します。[#LC5589]

- StoreFrontでFederated Authentication Serviceを有効にすると、ログオンエラーが発生することがあります。[#LC5708]

- Citrix StoreFrontでCitrix Receiver for HTML5を有効にしている場合でも、StoreFrontコンソールにはHTMLバージョンが表示されず「未使用」と表示されることがあります。[#LC6626]

- XenDesktopのセットアップ中、構成されたサイトを選択すると、StoreFrontでデフォルトの認証サービスを使用するデ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フォルトのストアが作成されることがあります。このストアを削除すると、Citrix Receiver for Windowsユーザーはストアを追加できなくなり、次のエラーメッセージが表示されることがあります。

「認証サービスとの通信中にプロトコルエラーが発生しました。」[#LC6664]

- StoreFrontコンソールを使用して特定のストアでセルフサービスパスワードリセット（SSPR）を構成すると、この構成は選択された特定のストアだけではなくすべてのストアに適用されます。[#LC6987]
- マルチサイト集約環境で切断されたセッションに再接続しようとすると、失敗することがあります。これによって、同じリソースの2つ目のインスタンスを受信することがあります。[#LC7453]
- 集約されたアプリケーションのソースのいずれかが無効になっている場合は、アプリケーションが予期せずエンドユーザーから非表示になることがあります。[#LC7675]
- StoreFrontで［アカウントセルフサービス］オプションを無効にしようとすると、無効と表示されていても無効にならないことがあります。[#LC7744]
- StoreFrontでストアから共有認証を削除しようとすると、変更の保存中、次のメッセージが表示されることがあります。

  「変更の保存時にエラーが発生しました。」 [#LC7781]

Universal Print Server

クライアント

- Profile managementを使用する環境で、あるサーバー上のCitrix Universal Printサーバープリンターを変更（追加、削除、名前の変更）しても、別のサーバー上での以降のセッションで変更が正しく反映されない場合があります。[#LC7645]

サーバー

- Citrixユニバーサルプリンタードライバーを使用している時に、Microsoft Internet Explorerから印刷しようとすると、次のエラーメッセージが表示されて失敗することがありました。

  「内部エラーが発生しました。Internet Explorerはこのドキュメントを印刷できません。」[#LC4735]

- ドキュメントを印刷しようとすると失敗する場合があり、次のエラーメッセージが表示されます。

  「現在のプリンターの設定に問題があるため、Windowsは印刷できません。」 [#LC6825]

- 特定のプリンターを使用している時に、Microsoftメモ帳が「ハンドルが無効です」のメッセージを表示し、印刷が失敗することがあります。この問題は、Citrixポリシーの「ユニバーサル印刷の使用」内で「プリンター固有のドライバーのみを使用する」が構成されており、Citrixポリシーの「Universal Print Serverの有効化」内で「有効。Windowsのリモート印刷機能にフォールバックしない」が構成されている場合に発生します。 [#LC7623]

VDA for Desktop OS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コンテンツリダイレクト

- DirectShowを使用した画像のキャプチャが失敗し、アプリケーションが予期せず終了します。[#LC6667]

HDX Broadcast

- セッションを開始する時に、HDXオーディオデバイスがランダムに無効にされることがありました。[#LC5281]

インストール、アンインストール、アップグレード

- VDAをバージョン5.6.400からバージョン7.9にアップグレードした後、VDAを再起動させると以前のバージョンでインストールされたミラードライバーが残される場合があります。[#LC6295]
- VDAをバージョン5.6から7.xにアップグレードすると、誤った従来のビデオドライバーがインストールされることがあります。[#LC6363]
- Machine Creation Serviceのバージョン7.12を使用して仮想マシンを作成すると、XenToolsのインストールが失敗し、仮想マシンを通常の方法でシャットダウンできません。[#LC6769]
- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7555]
- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7587]

キーボード

- Citrix Receiver for LinuxがSpanish DNIeのIDカードをサポートしない場合があります。[#LC6547]
- VDAでHDX 3D Proが有効になっていると、キーボードショートカットの「Alt+p」と「Alt+s」が機能しない場合があります。[#LC6826]

印刷

- ドキュメントを2枚以上印刷しようとすると、1枚しか印刷されない場合があります。この問題は、Citrixポリシーの「ユニバーサル印刷の使用」内で「プリンター固有のドライバーのみを使用する」が構成されており、Citrixポリシーの「Universal Print Serverの有効化」内で「有効。Windowsのリモート印刷機能にフォールバックしない」が構成されている場合に発生します。 [#LC6023]
- 新しいユーザーがログオンした時に、Citrix Print Managerサービス（cpsvc.exe）が応答しなくなり、予期せず終了することがあります。[#LC6933]
- VDAをバージョン7.9からバージョン7.12以降にアップグレードした後に、Microsoft Internet ExplorerからCitrix Universal Print Driverを使って印刷しようとした時に、選択したトレイの代わりにトレイ1のみが印刷されることがあります。[#LC7463]

サーバー/サイトの管理

- ［視覚効果］の下の［システムの詳細設定］の変更が、現在のVDA for Desktop OSセッションには適用されても、それ以降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定してください。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前：EnableVisualEffect
種類：DWORD
値：1

[#LC8049]

セッション/接続

- クライアントUSBデバイスリダイレクト規則ポリシーを適用できないことがあります。この問題は、ユーザーがポリシーに入力した文字が1002文字を超過すると発生します。[#LC1144]
- ネットワーク中断後にVDAセッションへの再接続が失敗することがありました。この問題は、VDAのバージョン7.8へのアップグレード後に発生します。[#LC5040]
- Framehawkを有効にすると、XenDesktop 7.8のVDAセッションで、マウスのスクロールボタンによる操作が実行されないことがあります。XenDesktop 7.9で、対応するVDA側の修復を利用できます。[#LC5302]
- VDAでCitrixディスプレイドライバーvdodk.sysのタイプ0x50の致命的例外（Page_Fault_In_NonPaged_Area）が発生することがありました。[#LC5074]
- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上で実行中の仮想マシンにAppDiskが接続されている場合は、「［今すぐ再起動する］または［後で再起動する］」のプロンプトが表示されることがあります。この修正で、プロンプトは表示されなくなります。[#LC5403]
- 切断されたマルチモニターセッションに再接続後、表示画面が黒色になり、カスタム設定がデフォルトに戻ります。[#LC5556]
- VDAをVersion 7.6.300から7.8にアップグレードした後、クリップボード同期が機能しなくなることがあります。[#LC5699
- Framehawkを有効にすると、XenDesktop 7.9のVDAセッションで、マウスのスクロールボタンによる操作が実行されないことがあります。[#LC5779]
- Federated Authentication Services用に構成されたVDAが接続の受け入れを停止し、再起動するまで「ようこそ」画面で応答しなくなることがあります。[#LC5978]
- Citrix Receiverがアプリを起動する時、「接続が確立されました。機能をネゴシエートしています」から先に進まないことがあります。[#LC6021]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在のVDAセッションには適用されても、それ以降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect
  種類：DWORD
  値：0

  [#LC6163]

- タッチ操作可能なデバイス上で実行しているリモートPCセッションを切断しようとすると、黒い画面が表示されて回復できなくなる場合があります。[#LC6384]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix Receiver for LinuxがSpanish DNIeのIDカードをサポートしない場合があります。[#LC6547]
- リモートPCのセッションをWindows 10にインストールされたSecureDocでロックする場合、ロック画面の表示に最大2分かかります。その間、セッションは操作できません。[#LC6668]
- 再生中にCitrix Receiver for Macのセッションを何度も切断したり再接続したりすると、音声が機能しなくなる場合があります。[#LC6678]
- リムーバブルクライアントドライブが、VDA for Desktop OS上のWFAPI SDKから返されないことがあります。[#LC6877]
- XenDesktop 7.13 Windows 7 VDA上で従来のグラフィックモードを使用すると、灰色の画面が表示される場合があります。[#LC7477]
- 従来のグラフィックモードを有効にし、Desktop Viewerを構成しない状態で、複数の全画面モードのモニター間でセッションを切り替えると、1つのモニターのみがセッションを実行しているように見えることがあります。[#LC7907]

システムの例外

- VDA for Server OSのTDICA.sysでブルースクリーンエラーが発生することがあります。[#LC6898]
- サーバーにおいて、停止コード0xc0000006の重大な例外がvdtw30.dllで発生し、ブルースクリーンが表示されることがあります。 [#LC7608]
- tdica.sysでバグチェックコードによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7632]
- この修正により、サーバーの予期しない終了を引き起こす、wdica.sysファイルのメモリの問題が対処されます。[#LC7666

スマートカード

- ユーザーセッションとMicrosoft Remote Desktopセッションを切り替えると、Microsoft OutlookやMicrosoft Wordなどの、セッション中のスマートカード対応アプリケーションで、スマートカードを使用できないことがあります。結果として、さまざまなエラーメッセージが表示されます。また、コマンドウィンドウで「CertUtil/scinfo」によるセッション中スマートカードサポートをテストすると、次のエラーメッセージが表示されることがあります。

  「Microsoftスマートカードリソースマネージャーが実行されていません。」[#LC5839]
- スマートカードのパススルーが断続的に失敗することがあります。[#LC6147]

ユーザーエクスペリエンス

- Excel 2010のスプレッドシートで複数のブックを開いた場合、タスクバーに最新のブックしか表示されません。[#LC5370]
- XenDesktop 7.11 Windows 7 VDAで従来のグラフィックモードを使用すると画面の左上しか表示されません。[#LC6532]
- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィンドウが応答しなくなることがあります。[#LC7481]

ユーザーインターフェイス

- コネクションセンターを使用して、データを保存せずにシームレスなセッションからログオフすると、画面が黒くなり、以下のようなメッセージが表示されます。

  「プログラムを閉じる必要があります」。2つのオプション［ログオフを強制する］または［キャンセル］から選択してく

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ださい。この時に、［キャンセル］オプションが動作しません。

この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。[#LC6075]

- 「キーボードの自動表示」のポリシーを有効にし、「タッチパネルでの操作に最適化されたデスクトップ」のポリシーを無効に設定していると、iPadで公開デスクトップを起動した時にドキュメントビューアーが80%で表示される場合があります。デスクトップ上のアプリケーションを閉じると、ドキュメントビューアーは100%で表示されるようになります。[#LC6460]
- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。[#LC7557]

VDA for Server OS

コンテンツリダイレクト

- DirectShowを使用した画像のキャプチャが失敗し、アプリケーションが予期せず終了します。[#LC6667]

インストール、アンインストール、アップグレード

- VDA 7.11 for Desktop OSからVDA 7.12 for Desktop OSにアップグレードした後、特定のアプリケーションの起動中に次のエラーメッセージが表示される場合があります。

  「wfapi.dllがありません」[#LC6874]

- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7555]
- Microsoft Windowsオペレーティングシステムの英語以外のバージョン上でVDAのバージョン7.12または7.13をインストールした後に、特定のWMIクラスの名前が変更されることがあります。[#LC7587]

印刷

- CreateClientPrinterコマンドを使用してネットワークプリンターをマップすると、Citrix Print Managerが予期せず終了します。[#LC4685]
- ドキュメントを2枚以上印刷しようとすると、1枚しか印刷されない場合があります。この問題は、Citrixポリシーの「ユニバーサル印刷の使用」内で「プリンター固有のドライバーのみを使用する」が構成されており、Citrixポリシーの「Universal Print Serverの有効化」内で「有効。Windowsのリモート印刷機能にフォールバックしない」が構成されている場合に発生します。 [#LC6023]
- 新しいユーザーがログオンした時に、Citrix Print Managerサービス（cpsvc.exe）が応答しなくなり、予期せず終了することがあります。[#LC6933]
- VDAをバージョン7.9からバージョン7.12以降にアップグレードした後に、Microsoft Internet ExplorerからCitrix Universal Print Driverを使って印刷しようとした時に、選択したトレイの代わりにトレイ1のみが印刷されることがあります。[#LC7463]

サーバー/サイトの管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 異なるネットワークサブネット上のセッション間で移動すると、ユーザーが現在ログオンしているサブネットのプリンターではなく、両方のサブネットのプリンターがプリンター一覧に表示されるという問題がありました。#LC2308]
- アプリケーションをWeb Interfaceで起動する間に、子ドメインユーザーに対して次のエラーメッセージが表示されることがあります。

  「この公開アプリケーションへのアクセス権がありません。」[#LC7566]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在のVDA for Desktop OSセッションには適用されても、それ以降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定してください。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect
  種類：DWORD
  値：1

  [#LC8049]

セッション/接続

- （Hotfix Rollup Pack 6に含まれる）修正#LC2702が適用されているシステムで、クライアントがマップされたドライブへのアプリケーションの保存が失敗し、代わりに破損したファイルが生成されるという問題がありました。[#LC3976]
- Streaming ProfilerまたはOffline Plug-inがインストールされている場合、WinDbg.exeでのプロセスの起動に失敗することがありました。この問題は、RadeAPHookによってHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*プロセス名*>およびHKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*プロセス名*>の設定がフックされることによって発生します。

  この修正を有効にするには、以下のレジストリキーを作成します。

- *32ビットWindows：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
  名前：EnableReadImageFileExecOptionsExclusionList
  種類：Reg_SZ
  値のデータ：<*イメージファイル実行オプションの設定に関してフックから除外される実行可能ファイルの一覧（スペースなしのコンマ区切り）。例：windbg.exe,application_1.exe*>
- *64ビットWindows（32ビットアプリケーション）：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  名前：EnableReadImageFileExecOptionsExclusionList
  種類：Reg_SZ
  値のデータ：<*イメージファイル実行オプションの設定に関してフックから除外される実行可能ファイルの一覧（スペースなしのコンマ区切り）。例：windbg.exe,application_1.exe。*>

  [#LC4750]
- 新しいセッションを開始すると、Citrix Audio Redirection Serviceが無効な情報を含む仮想チャネルセッションに接続しよう

© 1999-2017 Citrix Systems, Inc. All rights reserved.

として失敗することがあります。[#LC5024]

- Framehawkを有効にすると、XenDesktop 7.8のVDAセッションで、マウスのスクロールボタンによる操作が実行されないことがあります。XenDesktop 7.9で、対応するVDA側の修復を利用できます。[#LC5302]
- VDAをVersion 7.6.300から7.8にアップグレードした後、クリップボード同期が機能しなくなることがあります。[#LC5699
- Framehawkを有効にすると、XenDesktop 7.9のVDAセッションで、マウスのスクロールボタンによる操作が実行されないことがあります。[#LC5779]
- Federated Authentication Services用に構成されたVDAが接続の受け入れを停止し、再起動するまで「ようこそ」画面で応答しなくなることがあります。[#LC5978]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在のVDAセッションには適用されても、それ以降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect
  種類：DWORD
  値：0

  [#LC6163]

- XenApp 7.6長期サービスリリースCumulative Update 2 VDA for Server OSまたは以前のバージョンを起動すると、システムイベントログで次の警告メッセージが表示されることがあります。

  「SemsServiceへの接続に失敗しました。エラー コード0x2。」[#LC6311]

- リモートデスクトップセッションがVDA for Server OSのコンソールセッションを引き継ぐ時に、動作しないXenAppセッションが作成される場合があります。[#LC6617]
- セッションに再接続しようとすると断続的に失敗し、VDA for Server OSが「初期化中」状態に移行します。この問題はVDAがDelivery Controllerに再度登録されると発生します。[#LC6647]
- リモートPCのセッションをWindows 10にインストールされたSecureDocでロックする場合、ロック画面の表示に最大2分かかります。その間、セッションは操作できません。[#LC6668]
- 再生中にCitrix Receiver for Macのセッションを何度も切断したり再接続したりすると、音声が機能しなくなる場合があります。[#LC6678]
- Microsoft Windows Server 2016で公開アプリケーションを起動すると、アプリケーションが表示されるまでしばらく黒い画面が表示されることがあります。 [#LC7947]

スマートカード

- ユーザーセッションとMicrosoft Remote Desktopセッションを切り替えると、Microsoft OutlookやMicrosoft Wordなどの、セッション中のスマートカード対応アプリケーションで、スマートカードを使用できないことがあります。結果として、さまざまなエラーメッセージが表示されます。また、コマンドウィンドウで「CertUtil/scinfo」によるセッション中スマートカードサポートをテストすると、次のエラーメッセージが表示されることがあります。

  「Microsoftスマートカードリソースマネージャーが実行されていません。」[#LC5839]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

システムの例外

- VDA for Server OSのTDICA.sysでブルースクリーンエラーが発生することがあります。[#LC6898]
- サーバーにおいて、停止コード0xc0000006の重大な例外がvdtw30.dllで発生し、ブルースクリーンが表示されることがあります。 [#LC7608]
- tdica.sysでバグチェックコードによる重大な例外エラーが発生し、VDAでブルースクリーンが表示されることがあります。[#LC7632]
- この修正により、サーバーの予期しない終了を引き起こす、wdica.sysファイルのメモリの問題が対処されます。[#LC7666

ユーザーエクスペリエンス

- Excel 2010のスプレッドシートで複数のブックを開いた場合、タスクバーに最新のブックしか表示されません。[#LC5370]
- VDAバージョン7.9上で実行される、2つのMicrosoft Excel 2010ワークシート間で挿入処理を実行する場合、Excelのウィンドウが応答しなくなることがあります。[#LC7481]

ユーザーインターフェイス

- コネクションセンターを使用して、データを保存せずにシームレスなセッションからログオフすると、画面が黒くなり、以下のようなメッセージが表示されます。

  「プログラムを閉じる必要があります」。2つのオプション［ログオフを強制する］または［キャンセル］から選択してください。この時に、［キャンセル］オプションが動作しません。

  この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。[#LC6075]
- 「キーボードの自動表示」のポリシーを有効にし、「タッチパネルでの操作に最適化されたデスクトップ」のポリシーを有効に設定していると、iPadで公開デスクトップを起動した時にドキュメントビューアーが80%で表示される場合があります。デスクトップ上のアプリケーションを閉じると、ドキュメントビューアーは100%で表示されるようになります。[#LC6460]
- Excel 2010で、複数のブックをスプレッドシートで開いた場合、タスクバーに最新のブックしか表示されません。[#LC7557]

仮想デスクトップコンポーネント - その他

- ユーザーのVMでホストされるアプリケーションセッションのセッションの種類が、「アプリケーション」から「デスクトップ」に予期せず変更されることがあります。結果として、アプリケーションに再接続しようとすると、失敗します。[#LC5461]
- XenDesktopと統合されたMicrosoft App-V 5.0インフラストラクチャを使用してApp-vパッケージを起動する場合、App-Vパッケージが同期に失敗し、次の例外が発生することがあります。

  「を開始できません」[#LC5483]
- ネットワークを介してApp-Vアプリケーションをロードしようとすると、次のエラーメッセージが表示されることがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「インデックスが範囲を超えています。負でない値で、コレクションのサイズよりも小さくなければなりません。」[#LC5828]

- XenAppをVersion 7.7からVersion 7.8にアップグレードした後で、App-Vアプリケーションの起動に失敗することがあります。この問題は、「TargetIn」ブール値の値が「1」でなく「0」と設定されている時に発生します。また、値を手動で設定しても、何も変わらないことがあります。アプリケーションを更新すると、値が元に戻ることがあります。[#LC5861]
- Citrix Studioに複数のアプリケーションを含むApp-Vパッケージを追加して、パッケージ内のすべてのアプリケーションを公開すると、ユーザーセッションで最初のアプリケーションだけが起動することがあります。[#LC5863]
- App-Vアプリケーションを起動できるのは単一ユーザーのみです。同じサーバー上で同じアプリケーションを別のユーザーが起動しようとすると失敗する場合があります。[#LC6414]
- シーケンスされたApp-Vアプリケーションが、パッケージ（InTarget=False）によって参照されている場合でも、実際のApp-Vパッケージに含まれない場合があります。その結果、アプリケーションを正常に機能させるために必要な、依存関係にある接続グループでアプリケーションを起動できません。[#LC6534]
- XenApp/XenDesktop 7.11から7.12にアップグレードすると、既存のデリバリーグループ再起動スケジュールが適用されません。[#LC6766]
- マップされたドライブからApp-Vアプリケーションを起動しようとすると失敗する場合があります。[#LC6961]
- App-Vアプリケーションを公開しようとすると、失敗する場合があります。

  [#LC7421]
- VDAマスターイメージにMicrosoft Message Queuingがインストールされている場合、マシンカタログを作成しようとすると失敗することがあり、次のメッセージがCitrix Studioに表示されます。

  「イメージの準備が完了していません。ステータス 'NotSet' [＃LC7528]
- シングル管理モードでApp-Vアプリケーションを起動しようとすると失敗する場合があります。この問題は、アプリケーション名に特殊文字が含まれている場合に発生します。 [#LC7897]

その他の解決された問題

- Delivery Controllerを7.11から7.14、7.12から7.14、または7.13から7.14にアップグレードする前に、［Profile Management］>［レジストリ］>［デフォルトの除外］の下にある ［UPM］-［Software\Microsoft\Speech_OneCore］ポリシーが構成されていた場合、Citrix Studioのグループポリシーが不明になります。[#UPM-538]
- XenAppとXenDesktopの全製品インストーラーを使用して、Windows Server 2008上でSession Recordingバージョン7.14をインストールまたはアップグレードしようとすると、インストールに失敗し、次のエラーメッセージが表示されます。「Microsoft Message Queuingに失敗しました。」[#SRT-1782]
- Controllersをアップグレードした後、VDAの電源の状態が「不明」と表示される場合があります。[#DNA-37756]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

既知の問題

Apr 18, 2018

このページの7.15基本製品およびCU1セクションで説明されている既知の問題は、 解決された問題」に記載されていない限りCU2でも引き続き存在します。

累積更新プログラム2の既知の問題

- W2k16 VDAでは、スマートカードを使用してログインするユーザーは、ログオン時に使用可能なすべてのユーザーを表示できないことがあります。この問題は、ログオンウィンドウのデフォルトのサイズ（600x520）によって発生します。回避策などを含め、詳しくはKnowledge CenterのCTX204070を参照してください。[LCM-3951]

- Windows 10 Redstone 4（Insider Previewビルド）の既知の問題の一覧については、Knowledge CenterのCTX231942を参照してください。

累積更新プログラム1の既知の問題

- StoreFront 3.12（XenAppおよびXenDesktop 7.15 LTSR）からStoreFront 3.12.1000（XenAppおよびXenDesktop 7.15 LTSR CU1）へのアップグレード後、またはStoreFront 3.12.1000のインストール後にStoreFront管理コンソールが開きません。StoreFront管理コンソールに「MMCがスナップインを作成できませんスナップインが正しくインストールされていない可能性があります。」というエラーが表示されます。この問題を解決するには、CTX233206の手順に従います。[#LC8935]

- Windows 7またはWindows Server 2008 R2マシンにSHA-256証明書で署名されたドライバーをインストールすると、Microsoft WHQL（Windows Hardware Quality Labs）のメッセージが表示されることがあります。この問題を解決するには、マシンに以下のマイクロソフトの修正プログラムをインストールします。
  - Windows 7（修正プログラムは1つ）：https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i
  - Windows Server 2008 R2（修正プログラムは2つ）：https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-iおよびhttps://support.microsoft.com/en-us/help/2837108/you-cannot-import-a-windows-8-signed-driver-on-a-windows-server-2008-r [#LCM-2836]
- Citrix Telemetry Serviceが無効になっているか停止している場合、メタインストーラーを使用してXenAppおよびXenDesktop 7.15 LTSRを累積更新プログラム1（CU1）にアップグレードすると、次の警告メッセージが表示されることがあります。
  「Call Homeに登録するためのCitrixサービスを開始できません。詳しくは、CTX218094を参照してください。」[#LCM-3642]

7.15 LTSR（初期リリース）の既知の問題

XenAppおよびXenDesktop 7.15 LTSRのリリースには、以下の問題が含まれます。

App-V

- Studioの［アプリケーション］ノードから、または選択したデリバリーグループから、1つまたは複数のApp-Vアプリケーションを削除した場合、「不明なエラーが発生しました」というメッセージが表示されます。このメッセージは無視して

© 1999-2017 Citrix Systems, Inc. All rights reserved.

も問題ありません。アプリケーションは削除されます。[#DNA-29702]

- App-Vアプリケーションの子プロセスが起動していると、デリバリーグループからそのアプリケーションを削除できないが、アプリケーションを終了させても子プロセスが終了できません。アプリケーションが使用中であるというエラーが表されます。プロセス名を確認するために、Get-AppVVirtualProcessを実行します。タスクマネージャーまたはStop-AppVClientPackageで、そのプロセスを終了させます。[#DNA-23624]

- App-Vパッケージをアプリケーションライブラリから削除しても、Studioの表示はなくなるがVDAから削除されません。この問題を回避するには、管理者権限を引き上げて以下のコマンドレットを実行します。

  ```
  Import-Module AppvClient
  Get-AppVClientPackage -all
  #削除するパッケージのPackageIdおよびVersionIdを特定します
  Remove-AppVClientPackage -PackageId <packageid> -VersionId <versionid>
  ```

  [#DNA-47379]

- Microsoft App-Vの動作によって、シングル管理またはデュアル管理方式で同じアプリの複数のシーケンスされたバージョンを公開すると、ユーザーごとに一度に1つのバージョンのアプリケーションしかVDAで起動できません。ユーザーが最初に起動するバージョンによって、その後に実行されるバージョンが決まります。同様の動作は、Citrixコンポーネントが含まれていなくても、それぞれ異なるパスのデスクトップショートカットからシーケンスされたアプリケーションを起動しても発生します。Mozilla FirefoxとGoogle Chromeブラウザーのさまざまなバージョンで、この現象が確認されています [#APPV-60]

インストールとアップグレード

- VDA 7.14をVDA 7.15にアップグレードすると、**管理用テンプレート**を使用して適用されるCitrixポリシー設定用のレジストリキーHKEY_LOCAL_MACHINE¥Software¥Policies¥Citrixで作成されたキーが、VDAから削除される可能性があります。[#LCM-3876]

- インストールメディア上のAutoSelectアプリケーションを使用してコンポーネントをインストールする時に、autorun.logファイルに、不十分な権限に関するエラーと例外が含まれる場合があります。インストールが成功していれば、これらのエラーは無視できます。ただし、これを避けるには、**[管理者として実行]**を使ってAutoSelectを起動してください。[#DNA-45937]

- XenDesktop 5.6環境をXenDesktop 7.15 LTSRにアップグレードした場合、グループポリシーが不明になります。この問題を回避するには、最初にXenDesktop 5.6をXenDesktop 7.13にアップグレードしてください。次に、7.13から7.15 LTSRにアップグレードしてください。[#DNA-44818]

- Controllerをインストールして、インストールウィザードの**[Smart Tools]**ページに表示される**[Smart ToolsとCall Homeに接続します]**を選択すると、Call Homeが有効にならない場合があります。この問題を回避するには、Citrix Scoutのスケジュール機能を使用するか、PowerShellでCall Homeを有効にしてください。[#CAM-9907]

- Windows Server 2012 R2またはWindows Server 2016にDelivery Controllerをインストールする場合、Smart Toolsへの接続を選択し、お使いのCitrix Cloudアカウントに1つまたは複数の組織をリンクさせると、Citrix Cloudの資格情報でログオンする時にログオン処理が完了しないことがあります。この問題を回避するには、次のいずれかを実行してください。
  - Windows ServerとInternet Exploreが最新のバージョンに更新されていることを確認します。
  - Internet Exploreブラウザーの設定で[インターネット オプション]>[セキュリティ]>[ローカル イントラネット]>[サイト]>[プロキシ サーバーを使用しないサイトをすべて含める]をオフにします。

  [#CAM-9816]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- StoreFrontがインストールメディアから実行可能ファイルを使用してインストールされている場合、以降のバージョンの全製品インストーラーを使用した時に、StoreFrontはアップグレードの対象とされません。この問題を回避するには、インストールメディアから実行可能ファイルを使用してStoreFrontをアップグレードしてください。[#DNA-47816]

- Delivery Controllerを7.13より前のバージョンから7.13以降のバージョンにアップグレードすると、「クライアントの自動再接続のタイムアウト」設定がいずれかのポリシーで設定されている場合に、エラー（例外）が発生することがあります。このエラーは、「クライアントの自動再接続のタイムアウト」の設定値が、バージョン7.13で初めて導入された許容範囲0～300を超えている場合に発生します。このエラーを回避するには、Citrix Group Policy PowerShell Providerを使用して設定を構成解除するか、指定された範囲内の値に設定します。例については、CTX22947を参照してください。[#DNA-52476]

- マシンを選択して既存のデリバリーグループに追加する場合、Studioを使用して互換性のないマシンカタログから同じデリバリーグループにマシンを追加できます。（最初にデリバリーグループを選択してそこにマシンを追加する場合、Studioは互換性のないマシンカタログからのマシンの追加を許可しません。） [#DNA-39589]

全般

- セッション中のFederated Authentication Serviceを使ってTLS 1.1（またはそれ以前）の接続を認証しようとすると、接続に失敗する場合があります。ハッシュIDがサポートされていないことを示す、イベントID 305がログに記録されます。Federated Authentication Serviceは、SHAMD5ハッシュをサポートしません。この問題を回避するには、TLS 1.2接続を使用します。この問題は、XenAppおよびXenDesktop 7.9から本バージョンまで影響があります。[#DNA-47628]

- プリンタードライバーマッピングと互換性ポリシーには、ポリシー設定が保存されません。この問題を回避するには、Citrix Group Policy PowerShellプロバイダーを使用して、この設定を編集してください。回避策について詳しくは、CTX226589を参照してください。[#DNA-47423]

- Windowsイベントログエラー：「WindowsはMfApHook64.dllファイルのイメージの整合性を検証できません」。詳しくは、CTX226397を参照してください。[HDX-9063]

- StoreFrontからアプリケーションを起動した時、アプリケーションがフォアグラウンドで起動されないか、フォアグラウンドではあるがフォーカスを持たないことがあります。この問題を回避するには、タスクバーのアイコンをクリックしてアプリケーションを前面に移動させるか、アプリケーション画面でフォーカスに移動させます。[#HDX-10126]

- 公開コンテンツは、Citrix Receiverから開始されると開始に失敗します。StoreFront Webクライアント（またはWebインターフェイス）で開始されたコンテンツは問題なく開始できます。[#LC6316, #RFWIN-4957]

- IDディスクが確実に取得されないため、VMware VSAN 6.xでMachine Creation Services（MCS）のイメージ更新処理が失敗し、仮想マシンに再度接続されることがあります。この場合、手動で仮想マシンを削除して再度作成するか、イメージ更新用の新しいカタログを作成します。詳しくは、CTX219670を参照してください。

- Azure Resource Managerマシンカタログを削除した時に、関連するマシンとリソースグループを保持するように指定しても、Azureから削除されます。[#DNA-37964]

- Citrix Receiver for Windowsバージョン4.6以降を使用すると、マルチキャストがビデオを表示しない場合があります。オーディオは再生されます。この問題を回避するには、エンドポイントに次のレジストリキーを追加します。

  HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream\
  名前：DisableVMRSupport
  種類：DWORD
  値：4

  [#HDX-10055]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷

- Citrix Print Managerサービスを停止または再起動した時に、CpSvc.exeプロセスが応答しなくなることがあります。この問題を回避するには、サービススナップインのサービスを停止または再起動する前に、CpsSvc.exeプロセスを終了させるか、VDAを再起動させます。[#HDX-10071]

- 仮想デスクトップで選択されたUniversal Print ServerプリンターがWindowsコントロールパネルの**[デバイスとプリンター]** に表示されない場合があります。この問題が発生しても、アプリケーションからこのプリンターを使って正しく印刷できます。この問題は、Windows Server 2012、Windows 10、およびWindows 8プラットフォームでのみ発生します。詳しくは、Knowledge CenterのCTX213540を参照してください。[#335153]

Profile Management

Microsoft Windows 10のセッションの起動時に、Profile Managementにより黒い画面が表示されることがあります。この修正では、「同期するディレクトリ」ポリシーを構成し、フォルダー「*AppData\Local\Microsoft\Windows\Caches*」を追加する必要があります。詳しい情報と回避策については、Knowledge CenterのCTX234144を参照してください。[#LC-9030]

セッション レコーディング

- Machine Creation Services（MCS）またはProvisioning Services（PVS）で、構成済みのマスターイメージとインストール済みのMicrosoft Message Queuing（MSMQ）を使用して複数のVDAを作成すると、一定の状況下において、これらのVDAのQMIdが同じになる可能性があります。これは、次のようなさまざまな問題が発生する原因となる場合があります。
  - 録画契約が承認されていても、セッションが録画されない場合があります。
  - セッションのログオフ信号がSession Recordingサーバーによって受信されず、セッションのステータスが常に［ライブ］になってしまう可能性があります。

  回避策については、Session Recordingのインストールの記事を参照してください。[#528678]

サードパーティの問題

- CitrixとMicrosoftは、Windows Server 2016を実行中のサーバーVDAからシームレスアプリケーションを起動した時に問題があることを確認しました。このVDAから公開されたアプリケーションが起動されると、アプリケーションが起動されるまに、Citrix Receiverはモニターのワークスペースが数秒間黒い画面で覆われます。詳しくは、https://support.citrix.com/article/CTX225819を参照してください。

  警告：Azure Active Directory（AAD）を使用している場合、CTX225819に記載されたようにレジストリに変更は加えないでください。このように変更すると、AADユーザーがセッションを起動できない可能性があります。[HDX-5000]

- 負荷テスト環境で20,000回のログオンを行ったときに、Microsoft WindowsのWinLogon.exeは0.001%未満の頻度で断続的にクラッシュすることがあります。 [#HDX-9938]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サードパーティ製品についての通知

Apr 18, 2018

XenAppおよびXenDesktopのこのリリースには、次のドキュメントで定義された条件の元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。

PDF XenAppおよびXenDesktopサードパーティ製品についての通知

PDF Non-Commercial Software Disclosures For FlexNet Publisher 2016 R1（11.14.0.0）

PDF FLEXnet Publisher Documentation Supplement： FlexNet Publisher 11.14.0で使用されるオープンソースソフトウェア

PDF Session Recordingサードパーティ製品についての通知

© 1999-2017 Citrix Systems, Inc. All rights reserved.

廃止

Apr 18, 2018

この文書の以下の告知は、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止されるプラットフォーム、Citrix製品、機能について前もってお知らせするためのものです。Citrixではお客様の使用状況とフィードバックをチェックして、各プラットフォーム、Citrix製品、機能を撤廃するかどうかを判断しています。このリストは以降のリリースでの変更に従っており、廃止される機能がすべて含まれるわけではありません。

以下のプラットフォーム、Citrix製品、機能が*廃止されます*。これらは即時削除されるというわけではありません。これらは、XenAppおよびXenDesktop 7.15の長期サービスリリース（Long Term Service Release：LTSR）では引き続きサポートされます。廃止される項目は、このLTSRに続く最新リリースで削除されます。可能な場合、廃止される項目の代替が提案されます。

製品ライフサイクルサポートについて詳しくは、 製品ライフサイクルサポートポリシー」の文書を参照してください。

項目	対象バージョン	代替
Citrix Receiver for Webクラシックエクスペリエンス（「緑色の泡」ユーザーインターフェイス）	7.15 LTSR（およびStoreFront 3.12）	Citrix Receiver for Web統合エクスペリエンス
Windows 10バージョン1511（Threshold 2）およびWindows8.xとWindows7を含む、以前のWindowsデスクトップOSリリース用VDA	7.15 LTSR（および7.12）	Windows 10バージョン1607（Redstone 1）以降の半期チャネル用デスクトップOS VDAをインストールします。1607 LTSBを使用している場合、7.15 VDAをお勧めします。
Windows Server 2008 R2およびWindows Server 2012上のVDA（Service Packを含む）。	7.15 LTSR（および7.12）	Windows Server 2012 R2またはWindows Server 2016など、サポートされているバージョンにサーバーOS VDAをインストールします。
Windows Server 2012および2008 R2上のDelivery Controller（Service Packを含む）。	7.15 LTSR	オペレーティングシステムをサポートする代替のDelivery Controllerをインストールします。
Windows 7上のStudio（Service Packを含む）。	7.15 LTSR	オペレーティングシステムをサポートする代替のStudioをインストールします。
Flashリダイレクト。	7.15 LTSR	HTML5 Videoを使用します。詳しくは、Flashリダイレクトの製品終了（EOL）に関する記述を参照してください。
DirectXコマンドリモート処理（DCR）。	7.15 LTSR	Thinwireを使用します。
StoreFrontを含むCitrix Online Integration（Goto製品）	7.14 （およびStoreFront	StoreFront 3.12からは、StoreFront管理コンソールでこの機能を構成することはできません。 StoreFront 3.12へのアップグレードの場合、引き続

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	3.11)	きこの機能を使用できます。構成を変更するには、PowerShellコマンドレットのUpdate-DSGenericApplicationsを使用します。詳しくは、「Citrix Onlineアプリケーションをストアに統合する」を参照してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード。	7.13	これらのバージョンは、以降のサポート対象バージョンにアップグレードしてから、XenAppおよびXenDesktop 7.13にアップグレードします。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード。	7.12	XenDesktop 5.6または5.6 FP1展開を、最新のXenDesktopバージョンに移行します。
Windows 8.1およびそれ以前のWindowsデスクトップリリース上のVDA。	7.12	Windows 10にデスクトップOS VDAをインストールします。
Windows Server 2008 R2上のVDA。	7.12	Windows Server 2012 R2または Windows Server 2016など、サポートされているバージョンにサーバーOS VDAをインストールします。
Windows XP上で使用されるXenDesktop 5.6。Windows XP上のVDAインストールはサポートされません。	7.12	サポートされているWindowsバージョンにVDAをインストールします。
CloudPlatform接続。	7.12	サポートされている各種ハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（別名Azure Service Management）接続。	7.12	Azure Resource Managerを使用します。
32ビットマシン上へのコアコンポーネント（Studio以外）のインストール：Delivery Controller、Director、StoreFront、およびLicense Server。	7.12	64ビットマシンを使用します。
接続リース。	7.12	ローカルホストキャッシュを使用します。
従来のThinwireモード	7.12	Thinwireを使用します。
HDXデスクトップコンポジションリダイレクト（DCR）	7.12	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDiskおよびPersonal vDisk

XenAppおよびXenDesktopのAppDisksとPersonal vDiskの機能は、現在のリリースで廃止されています*。この機能は、Unidesk社（Citrix App Layering）から最近獲得したテクノロジに置き換えられる予定です。この移行時期には、「XenAppおよびXenDesktopのメンテナンスオプション」で説明している通り現在のサポートレベルが引き続き維持されます。

*AppDisksとPersonal vDiskは長期サービスリリース（LTSR）サービスオプションではカバーされていません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Section 508 Voluntary Product Accessibility Template（VPAT）

Apr 18, 2018

PDF Citrix XenApp and XenDesktop 7.15 Director VPAT

PDF Citrix XenApp and XenDesktop 7.15 Installer VPAT

PDF Citrix XenApp and XenDesktop 7.15 Licensing Administration Console VPAT

PDF Citrix XenApp and XenDesktop 7.15 Licensing Manager VPAT

PDF Citrix XenApp and XenDesktop 7.15 Receiver for Web Classic Experience VPAT

PDF Citrix XenApp and XenDesktop 7.15 Receiver for Web Unified Experience VPAT

PDF Citrix XenApp and XenDesktop 7.15 StoreFront VPAT

PDF Citrix XenApp and XenDesktop 7.15 Studio VPAT

PDF Citrix Provisioning Services Boot Device Manager VPAT

PDF Citrix Provisioning Services BOOTPTAB Editor VPAT

PDF Citrix Provisioning Services Client Side Imaging Wizard VPAT

PDF Citrix Provisioning Services Configuration Wizard VPAT

PDF Citrix Provisioning Services Console VPAT

PDF Linux VDA VPAT

PDF Citrix Scout VPAT

PDF Citrix Session Recording Player VPAT

PDF Citrix Session Recording 承認コンソールVPAT

PDF Citrix Workspace Environment Management承認コンソールVPAT

PDF Citrix Workspace Environment Managementインフラストラクチャサービス構成VPAT

PDF Citrix Workspace Environment Management Agentログパーサー VPAT

PDF Citrix Workspace Environment Managementインストーラー VPAT

PDF Citrix Workspace Environment Management Profile Cleanser VPAT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PDF Citrix Workspace Environment Management Integrity Condition List Manager VPAT

PDF Citrix Workspace Environment Management Database Management Utility VPAT

PDF Citrixセルフサービスパスワードリセット VPAT

PDF Citrix SCOM Management Pack VPAT

PDF Citrix Receiver for macOS VPAT

PDF Citrix管理パック構成VPAT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

システム要件

Apr 25, 2018

ここでは次のことについて説明します。

- はじめに
- Delivery Controller
- データベース
- Citrix Studio
- Citrix Director
- Virtual Delivery Agent（VDA）for Desktop OS
- Virtual Delivery Agent（VDA）for Server OS
- ホスト/仮想化リソース
- Active Directoryの機能レベル
- HDX
- Session Recording
- Universal Print Server
- そのほか

はじめに

ここで説明するシステム要件は、この製品バージョンがリリースされた時点で確認済みのものです。更新は定期的に行われます。このトピックで説明されていないシステム要件コンポーネント（StoreFront、ホストシステム、ReceiverとPlug-in、Provisioning Services）については、各コンポーネントのドキュメントを参照してください。

重要： インストールの前に、「インストールの準備」の内容を確認してください。

特に明記されている場合を除き、コンポーネントの必須ソフトウェア（.NETやC++パッケージなど）のバージョンがインストールされていないことが検出された場合、インストーラーにより自動的にインストールされます。これらの必須ソフトウェアの一部は、製品のインストールメディアにも収録されています。

インストールメディアには複数のサードパーティ製コンポーネントが収録されています。Citrixソフトウェアを使用する前に、サードパーティからのセキュリティに関するアップデートを確認して、必要に応じてインストールしてください。

グローバリゼーション情報について詳しくは、CTX119253を参照してください。

Windowsサーバーにインストール可能なコンポーネントと機能に関しては、Server CoreのインストールおよびNano Serverのインストールは、特段の記載がない限りサポートされていません。

Windows 10マシンで使用できるコンポーネントおよび機能については、次のWindows 10のサービスオプションおよびエディションがサポートされます。

- 半期チャネル：Pro、Enterprise、Education、Mobile Enterprise（IoT Core Pro EditionはCitrix Receiverでのみサポートされます）
- Long-term Servicingチャネル（LTSC）：Enterprise LTSB Edition

  詳しくは、CTX224843を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ハードウェア要件

RAMおよびディスクスペースの値は、マシン上の製品イメージ、オペレーティングシステム、およびそのほかのソフトウェアの要件に追加されます。パフォーマンスは構成に応じて異なります。構成には、使用する機能やユーザーの数なども含まれます。最低限のみを使うとパフォーマンスが低下する可能性があります。

たとえば、接続リース機能（デフォルトで有効化）に必要なControllerのディスクスペースは、ユーザー、アプリケーション、およびモードの数によって異なります。100,000人のRDSユーザーが、最近使用された100個のアプリケーションで接続リース機能を利用するには、約3GBのスペースが必要です。実装するアプリケーションが増えれば、より多くのスペースが必要となる可能性があります。専用のVDIデスクトップでは、40,000台のデスクトップに対して少なくとも400～500MBが必要です。どのような場合も、数GB多めに確保しておくことが推奨されます。

次の表は、コアコンポーネントでの最小要件を示しています。

Component	Minimum
1つのサーバー上のすべてのコアコンポーネント、評価用のみ、非実稼働展開	5GBのRAM
1つのサーバー上のすべてのコアコンポーネント、テスト展開または小規模実稼働展開用	12GBのRAM
Delivery Controller（ローカルホストキャッシュを使用するには、さらに多くのディスクスペースが必要）	5GBのRAM、800MBのハードディスク、データベース：「サイジングガイダンス」参照
Studio	1GBのRAM、100MBのハードディスク
Director	2GBのRAM、200MBのハードディスク
StoreFront	2GBのRAM。ディスクの推奨事項については、StoreFrontのドキュメント参照
ライセンスサーバー	2GBのRAM。ディスクの推奨事項については、ライセンス管理のドキュメント参照

デスクトップやアプリケーションを配信する仮想マシンのサイジング

ハードウェアの提供は複雑かつ動的であり、XenAppおよびXenDesktopの展開にはそれぞれ一意のニーズがあるため、特定の推奨事項を示すことはできません。通常、XenApp仮想マシンのサイジングはユーザーのワークロードではなくハードウェアに基づきます（RAM以外。より多く消費するアプリケーションにはより多くのRAMが必要です）。「XenAppおよびXenDesktop 7.15 LTSRのCitrix VDIベストプラクティス」には、VDAのサイズ変更に関する最新のガイダンスが含まれています。

Delivery Controller

© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016、Standard、およびDatacenterエディション。
- Windows Server 2012 R2、Standard、およびDatacenterエディション。
- Windows Server 2012、Standard、およびDatacenterエディション。
- Windows Server 2008 R2 SP 1、Standard、Enterprise、およびDatacenterエディション。

要件：

- Microsoft .NET Framework 3.5.1（Windows Server 2008 R2のみ）。
- Microsoft .NET Framework 4.5.2（4.6～4.7もサポートされます）。
- Windows PowerShell 3.0以降。
- Microsoft Visual C++ 2015 Runtime（32および64ビット）

データベース

サイト構成データベース、構成ログデータベースおよび監視データベースでサポートされているMicrosoft SQL Serverのバージョン：

- SQL Server 2017のExpress、Standard、およびEnterprise Edition。
- SQL Server 2016のSP1までのExpress、Standard、Enterprise Edition。
- SQL Server 2014のSP2までのExpress、Standard、およびEnterprise Edition。 デフォルトでは、Controllerのインストール時に適切なバージョンのSQL Serverが検出されない場合、SQL Server 2014 SP2 Expressがインストールされます。
- SQL Server 2012のSP4までのExpress、Standard、Enterprise Edition。
- SQL Server 2008 R2 SP2およびSP3のExpress、Standard、Enterprise、およびDatacenter Edition。

以下のデータベース高可用性ソリューションがサポートされます（スタンドアロンモードのみをサポートするSQL Server Expressを除く）。

- SQL Server AlwaysOnフェールオーバークラスターインスタンス
- SQL ServerのAlwaysOn可用性グループ（基本な可用性グループを含む）
- SQL Serverデータベースミラーリング

ControllerとSQL Serverサイトデータベース間の接続にはWindows認証が必要です。

Controllerをインストールする時、ローカルホストキャッシュ機能と連携して使用するために、デフォルトでSQL Server Expressデータベースがインストールされます。このインストールは、サイトデータベースのデフォルトのSQL Server Expressインストールとは異なるものです。

詳しくは、次の記事を参照してください。

- データベース
- CTX114501
- データベースのサイジングガイダンス
- ローカルホストキャッシュ

Citrix Studio

以下のオペレーティングシステムがサポートされています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Windows 10（ *[はじめに]* セクションのエディションサポート参照）
- Windows 8.1、Professional、およびEnterprise Edition。
- Windows 7 Professional、Enterprise、およびUltimateエディション。
- Windows Server 2016、Standard、およびDatacenterエディション。
- Windows Server 2012 R2、Standard、およびDatacenterエディション。
- Windows Server 2012、Standard、およびDatacenterエディション。
- Windows Server 2008 R2 SP 1、Standard、Enterprise、およびDatacenterエディション。

要件：

- Microsoft .NET Framework 4.5.2（4.6～4.7もサポートされます）。
- Microsoft .NET Framework 3.5 SP1（Windows Server 2008 R2およびWindows 7の場合のみ）。
- Microsoft管理コンソール3.0（サポートされているすべてのオペレーティングシステムに付属）。
- Windows PowerShell 2.0

Citrix Director

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016、Standard、およびDatacenterエディション。
- Windows Server 2012 R2、Standard、およびDatacenterエディション。
- Windows Server 2012、Standard、およびDatacenterエディション。
- Windows Server 2008 R2 SP 1、Standard、Enterprise、およびDatacenterエディション。

要件：

- Microsoft .NET Framework 4.5.2（4.6～4.7もサポートされます）。
- Microsoft .NET Framework 3.5 SP1（Windows Server 2008 R2の場合のみ）。
- Microsoftインターネットインフォメーションサービス（IIS） 7.0およびASP.NET 2.0。IISと一緒に［静的コンテンツ］の役割サービスがインストールされていることを確認してください。これらがインストールされていない場合は、Windows Serverのインストールメディアを指定するためのメッセージが表示され、自動的にインストールされます。

System Center Operations Manager（SCOM）の統合要件は以下のとおりです。

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Directorを表示するための以下のWebブラウザー。

- Internet Explorer 11以降。（Internet Explorer 10は、Windows Server 2012 R2マシンでのみ使用できます。）互換モードはInternet Explorerではサポートされません。Directorを表示するには、Webブラウザーの推奨設定を使用する必要があります。Internet Explorerをインストールする時に、セキュリティおよび互換性に関するデフォルトの推奨設定を適用してください。インストール済みのInternet Explorerで推奨設定を使用していない場合は、［ツール］、［インターネットオプション］、［詳細設定］、［リセット］の順に選択し、表示される指示に従います。
- Microsoft Edge
- Firefox ESR（Extended Support Release）。
- Chrome。

Directorの表示に推奨される最適な画面解像度は1366 × 1024です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent（VDA）for Desktop OS

以下のオペレーティングシステムがサポートされています。

- Windows 10、（「*はじめに*」セクションのエディションサポート参照）。Windows 10では、デスクトップコンポジションのリダイレクトと従来のグラフィックモードはサポートされません。
- Windows 8.1、Professional、およびEnterprise Edition。
- Windows 7 SP1、Professional、Enterprise、およびUltimateエディション。

要件：

- Microsoft .NET Framework 4.5.2（4.6～4.7もサポートされます）
- Microsoft .NET Framework 3.5.1（Windows 7のみ）
- Microsoft Visual C++ 2013および2015 Runtime（32および64ビット）

リモートPCアクセスでは、このVDAを社内の物理PC上にインストールします。このVDAでは、Windows 10でのXenDesktopリモートPCアクセス向けのセキュアブートがサポートされます。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Mediaリダイレクトなど）では、VDAのインストール先マシンにMicrosoft Media Foundationをインストールする必要があります。マシンにMedia Foundationがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。サポートされているWindowsデスクトップOSのほとんどのエディションには、Media Foundationがあらかじめインストールされており、削除することはできません。ただし、Nエディションには一部のメディア関連機能が付属しません。これらのソフトウェアは、Microsoft社またはサードパーティから入手できます。詳しくは、「インストールの準備」を参照してください。

VDAをインストールする時に、VDA for Windows Desktop OSのHDX 3D Proモードを選択できます。このモードは、DirectXやOpenGL指向のアプリケーション、およびビデオなどのリッチメディアに特に適しています。追加のサポート情報について詳しくは、「HDX 3D Pro」セクションを参照してください。

Linux VDAについては、「Linux Virtual Delivery Agent」を参照してください。

サポートされているサーバーオペレーティングシステムでは、コマンドラインインターフェイスを使用してVDA for Windows Desktop OSをインストールしてサーバーVDI機能を使用できます。詳しくは、「サーバーVDI」を参照してください。

Virtual Delivery Agent（VDA）for Server OS

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016、Standard、およびDatacenterエディション。
- Windows Server 2012 R2、Standard、およびDatacenterエディション。
- Windows Server 2012、Standard、およびDatacenterエディション。
- Windows Server 2008 R2 SP 1、Standard、Enterprise、およびDatacenterエディション。

以下の必須ソフトウェアは、インストーラーにより自動的にインストールされます。これらのソフトウェアは、Citrixインストールメディアの*Support*フォルダーにも収録されています。

- Microsoft .NET Framework 4.5.2（4.6～4.7もサポートされます）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft .NET Framework 3.5.1（Windows Server 2008 R2のみ）
- Microsoft Visual C++ 2013および2015 Runtime（32および64ビット）

リモートデスクトップサービスの役割サービスが自動的にインストールされて有効になります。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Mediaリダイレクトなど）では、VDAのインストール先マシンにMicrosoft Media Foundationをインストールする必要があります。マシンにMedia Foundationがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。ほとんどのWindows Serverバージョン上には、サーバーマネージャー（Windows Server 2012以降はServerMediaFoundation、Windows Server 2008 R2の場合はDesktopExperience）を介してMedia Foundation機能がインストールされます。ただし、Nエディションには一部のメディア関連機能が付属しません。これらのソフトウェアは、Microsoft社またはサードパーティから入手できます。詳しくは、「インストールの準備」を参照してください。

VDAにMedia Foundationがない場合、これらのマルチメディア機能は機能しません。

- Flashリダイレクト
- Windowsメディアリダイレクト
- HTML5ビデオリダイレクション
- HDX Realtime Webカメラリダイレクト

Linux VDAについては、「Linux Virtual Delivery Agent」を参照してください。

ホスト/仮想化リソース

XenAppおよびXenDesktopの機能の中には、一部のホストプラットフォームまたは一部のホストプラットフォームのバージョンでのみサポートされるものもあります。たとえば、AppDiskはXenServer、VMware、およびSystem Center Virtual Machine Managerホストでサポートされています。詳しくは、各機能のドキュメントを参照してください。

リモートPCアクセスのWake on LAN機能を使用するには、Microsoft System Center Configuration Manager 2012以上が必要です。

サポートされるホストプラットフォームおよび仮想化環境

重要：以下の*major.minor*バージョン（およびこれらのバージョンの更新プログラム）がサポートされます。CTX131239には、最新のハイパーバイザーのバージョン情報と既知の問題へのリンクが記載されています。

XenServer

- XenServer 7.4
- XenServer 7.3
- XenServer 7.2
- XenServer 7.1 LTSR
- XenServer 7.0
- XenServer 6.5およびSP1
- XenServer 6.2 SP1にHotfixを適用したもの（Hotfixを適用できるようにするには、SP1を適用しておく必要があります）
- XenServer 6.1

VMware vSphere（vCenter + ESXi）。vSphere vCenterのリンクモードはサポートされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- VMware vSphere 5.1
- VMware vSphere 5.0
- VMware vCenter 5.5、6、6.5アプライアンス

System Center Virtual Machine Manager。 サポートされるSystem Center Virtual Machine Managerのバージョンに登録できるあらゆるHyper-Vのバージョンが含まれます。

- System Center Virtual Machine Manager 2016
- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5

Amazon Web Services（AWS）

- サポートされるWindowsサーバーOSで、アプリケーションやデスクトップをプロビジョニングできます。
- Amazon Relational Database Service（RDS）はサポートされません。
- 詳しくは、「Citrix XenDesktop on AWS」を参照してください。

CloudPlatform

- Hotfix 4.2.1～4を適用したVersion 4.2.1以降がサポートされます。
- ハイパーバイザーとして、XenServer 6.2（Service Pack 1とXS62ESP1003適用済み）およびvSphere 5.1での動作がテストされています。
- CloudPlatformでは、Hyper-Vハイパーバイザーはサポートされません。
- CloudPlatform 4.3.0.1では、VMware vSphere 5.5がサポートされます。
- 詳しくは、CloudPlatformのドキュメント（使用するバージョンのCloudPlatformのリリースノートを含む）を参照してください。

Microsoft Azure

Microsoft Azure Resource Manager

Active Directoryの機能レベル

Active Directoryフォレストとドメインの以下の機能レベルがサポートされています。

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000ネイティブ（ドメインコントローラーでサポートされない）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX

Receiver for WindowsおよびReceiver for Linux 13では、マルチストリームICAでのUDPオーディオがサポートされています。

Citrix Receiver for Windowsでは、エコーキャンセルがサポートされています。

該当するHDX機能のサポートおよび要件については、後述の説明を参照してください。

HDX - デスクトップコンポジションリダイレクト

Windowsベースのユーザーデバイスまたはシンクライアントでの要件は以下のとおりです。

- DirectX 9
- Pixel Shader 2.0（ハードウェアでのサポート）
- 32ビット/ピクセル
- 1.5GHz、32ビットまたは64ビットプロセッサ
- 1GBのRAM
- IGP（Integrated Graphics Processor）またはグラフィックカード上の128MBのビデオメモリ。

HDXにより、必要なGPU機能が使用可能かどうかがWindowsデバイスに照会され、使用できない場合は自動的にサーバー側のデスクトップコンポジションが使用されます。GPU機能が使用可能であってもプロセッサ速度やRAMの要件が満たされないデバイスは、デスクトップコンポジションリダイレクトの除外デバイスとしてGPOグループに追加してください。

最小使用可能帯域幅は1.5Mbpsです。推奨帯域幅は5Mbpsですこれらの値では、エンドツーエンドの遅延が考慮されています。

HDX - Windows Media配信

Windows Mediaのクライアント側でのコンテンツ取得、Windows Mediaリダイレクト、およびリアルタイムWindows Mediaマルチメディアトランスコードでは、Citrix Receiver for Windows、Citrix Receiver for iOS、Citrix Receiver for Linuxの各クライアントがサポートされています。

Windows MediaコンテンツをWindows 8デバイス側で取得するには、デフォルトプログラムとしてCitrix Multimedia Redirectorを設定します。これを行うには、**[コントロールパネル]**、**[プログラム]**、**[既定のプログラム]**、**[既定のプログラムの設定]**の順に選択し、**[Citrix Multimedia Redirector]**を選択して**[すべての項目に対し、既定のプログラムとして設定する]**または**[既定でこのプログラムで開く項目を選択する]**のいずれかをクリックします。GPUトランスコードでは、NVIDIA CUDAが有効なGPU（Compute Capability 1.1以上）が必要です。詳しくは、http://developer.nvidia.com/cuda/cuda-gpusを参照してください。

HDX Flashリダイレクト

以下のクライアントとAdobe Flash Playerがサポートされています。

- Citrix Receiver for Windows（第2世代のFlashリダイレクト機能用） - 第2世代Flashリダイレクト機能には、Adobe Flash Player for Other Browser（「NPAPI（Netscape Plugin Application Programming Interface）Flash Player」と呼ばれることもあります）が必要です。
- Citrix Receiver for Linux（第2世代のFlashリダイレクト機能用） - 第2世代Flashリダイレクト機能ではAdobe Flash Player for other LinuxまたはAdobe Flash Player for Ubuntu。
- Citrix Online Plug-in 12.1（従来のFlashリダイレクト機能） - 従来のFlashリダイレクト機能ではAdobe Flash Player for Windows Internet Explorer（「ActiveXプレーヤー」と呼ばれることもあります）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーデバイス上のFlash Playerのバージョン（メジャーバージョン番号）は、サーバー上のものと同じまたはそれ以降である必要があります。ユーザーデバイスに以前のバージョンのFlash Playerがインストールされている、またはユーザーデバイスにFlash Playerがインストールされていない場合、Flashコンテンツはサーバー上で処理されます。

VDAを実行するマシンでの要件は以下のとおりです。

- Adobe Flash Player for Windows Internet Explorer（ActiveXプレーヤー）
- Internet Explorer 11（非Modern UIモード）バージョン7～10のInternet Explorerを使用することもできますが、Microsoftはバージョン11をサポートしており、Citrixもバージョン11を使用することを推奨しています。Flashリダイレクトでは、サーバーにInternet Explorerが必要です。ほかのWebブラウザーを使用する場合、Flashコンテンツはサーバー側で処理されます。
- Internet Explorerの保護モードの無効化：（［ツール］>［インターネットオプション］>［セキュリティ］タブ>［保護モードを有効にする］チェックボックスをオフ）。変更を反映させるため、Internet Explorerを再起動します。

HDX 3D Pro

VDA for Windows Desktop OSをインストールする時に、HDX 3D Proバージョンのインストールを選択できます。

アプリケーションをホストする物理マシンまたは仮想マシンでは、GPUパススルーまたは仮想GPU（vGPU）を使用できます。

- GPUパススルーは、Citrix XenServer、Nutanix AHV、VMware vSphereおよびVMware ESX（仮想Direct Graphics Acceleration（vDGA））、Windows Server 2016のMicrosoft Hyper-V（Discrete Device Assignment（DDA））で使用できます。
- vGPU機能は、Citrix XenServer、Nutanix AHV、VMware vSphereで使用できます。https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.htmlを参照してください。

ホストコンピューターとして、4GB以上のRAMと2.3GHz以上の4つの仮想CPUを推奨します。

GPU（Graphical Processing Unit）：

- 無損失圧縮を含むCPUベース圧縮では、ホストコンピューター上のあらゆるディスプレイアダプター（配信するアプリケーションと互換性があるもの）がサポートされます。
- NVIDIA GRID APIを使用する仮想化グラフィックアクセラレーションでは、サポートされるNVIDIA GRIDカードとHDX 3D Proを併用できます（「NVIDIA GRID」参照）。NVIDIA GRIDでは高いフレームレートが配信されるため、ユーザーエクスペリエンスが向上します。
- 仮想化グラフィックアクセラレーションは、データセンターグラフィックプラットフォームのIntel Xeon Processor E3ファミリでサポートされます。詳しくは、http://www.citrix.com/intelおよびhttp://www.intel.com/content/www/us/en/servers/data-center-graphics.htmlを参照してください。
- 仮想化グラフィックアクセラレーションは、AMD FirePro SシリーズサーバーカードのAMD RapidFireでサポートされています（「AMD Virtualization Solution」を参照してください）。

ユーザーデバイス：

- HDX 3D Proでは、ホストコンピューター上のGPUでサポートされるすべてのモニターの解像度がサポートされます。ただし、推奨されている最低限のユーザーデバイスおよびGPU仕様でのパフォーマンスを最適化するには、最大モニター解像度を1920×1200ピクセル（LAN接続の場合）または1280×1024ピクセル（WAN接続の場合）にすることをお勧めします。
- ユーザーデバイスでは、1GB以上のRAMと1.6GHz以上のCPUを推奨します。低帯域幅接続で必要とされるデフォルトの深圧縮コーデックを使用する場合は、より強力なCPUが必要です（ハードウェアでデコードしない場合）。パフォーマンスを最適化するには、ユーザーデバイスに2GB以上のRAMおよび3GHz以上のデュアルコアCPUを推奨します。
- マルチモニター環境の場合は、クアッドコアCPUを推奨します。
- HDX 3D Proで配信されたデスクトップやアプリケーションにアクセスする場合、ユーザーのデバイスにGPUは必要ありま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

せん。
- Citrix Receiverのインストールが必要です。

詳しくは、「HDX 3D Pro」およびwww.citrix.com/xenapp/3dを参照してください。

HDX - Webカメラビデオ圧縮でのビデオ会議の要件

サポートされるクライアント：Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux

サポートされるビデオ会議アプリケーションは以下のとおりです。

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google+ハングアウト
- IBM Sametime
- Windows 8.x、Windows Server 2012、およびWindows Server 2012 R2上で動作するMedia Foundation形式のビデオアプリケーション
- Microsoft Lync 2010および2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

WindowsクライアントでSkypeを使用するには、クライアント側およびサーバー側のレジストリを編集する必要があります。

クライアントのレジストリキー：HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

値の名前：DefaultHeight、種類：REG_DWORD、値のデータ：240

値の名前：DefaultWidth、種類：REG_DWORD、値のデータ：320

サーバーのレジストリキー：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

値の名前：skype.exe、種類：REG_DWORD、値のデータ：0

そのほかのユーザーデバイス要件：

- サウンド再生のためのハードウェア
- DirectShow対応のWebカメラ（Webカメラのデフォルト設定を使用してください）。Webカメラ側のハードウェアエンコーディング機能を使用すると、クライアント側のCPU使用率が軽減されます。
- Webカメラの製造元から入手したドライバー（入手できる場合）

Session Recording

Session Recording Administrationコンポーネント

Session Recording Administrationコンポーネント（Session Recordingデータベース、Session Recording Server、Session Recording Policy Console）は、1台のサーバーにインストールすることも、異なるサーバーにインストールすることも可能です。

Session Recordingデータベース

以下のオペレーティングシステムがサポートされています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

サポートされているMicrosoft SQL Serverのバージョン：

- Microsoft SQL Server 2016 SP1 Enterprise、Express、およびStandard Edition
- Microsoft SQL Server 2014 SP2 Enterprise、Express、およびStandard Edition
- Microsoft SQL Server 2012 SP3 Enterprise、Express、およびStandard Edition
- Microsoft SQL Server 2008 R2 SP3 Enterprise、Express、およびStandard Edition

要件：.NET Framework 4.7、4.6.2または4.5.2

Session Recordingサーバー

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

そのほかの要件：

- インターネットインフォメーションサービス（IIS）10、8.5、8.0または7.5
- .NET Framework Version 4.7、4.6.2または4.5.2
- Session Recording Serverで、通信プロトコルとしてHTTPS、および有効な証明書を使用する場合。Session Recordingでは、デフォルトでCitrixの推奨プロトコルであるHTTPSが使用されます。
- Active Directory統合を無効にし、MSMQ HTTPサポートを有効にしたMicrosoft Message Queuing（MSMQ）。
- Administrator Loggingの場合：Chrome、Firefox、またはInternet Explorer 11の最新バージョン。

Session Recordingポリシーコンソール

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

要件：.NET Framework 4.7、4.6.2または4.5.2

Session Recording Agent

Session Recording Agentは、セッションを録画するXenAppおよびXenDesktopサーバーごとにインストールします。

以下のオペレーティングシステムがサポートされています。

- Windows Server 2016
- Windows Server 2012 R2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows 10
- Windows 8.1
- Windows 7 SP1

要件：

- PlatinumライセンスのXenApp/XenDesktop 7.15
- PlatinumライセンスのXenApp/XenDesktop 7.6.4000（VDA for Windows Server OSのみ。VDA for Windows Desktop OSはサポートされません）
- .NET Framework 4.7、4.6.2または4.5.2
- Active Directory統合を無効にし、MSMQ HTTPサポートを有効にしたMicrosoft Message Queuing（MSMQ）

Session Recording Player

以下のオペレーティングシステムがサポートされています。

- Windows 10
- Windows 8.1
- Windows 7 SP1

要件：.NET Framework 4.7、4.6.2または4.5.2

最適なパフォーマンスを得るには、Session Recording Playerを以下の条件のワークステーションにインストールします。

- 1024 X 768の画面解像度
- 32ビット以上の色数
- 2GB RAM（最小）。グラフィックが多用されている録画を再生する場合、特に録画にアニメーションが多く含まれる場合には、RAMおよびCPU/GPUリソースを追加すると、パフォーマンスが向上します。

シークの応答速度は、録画のサイズやマシンのハードウェア仕様によって異なります。

Universal Print Server

Universal Print Serverは、クライアント側およびサーバー側のコンポーネントで構成されています。UpsClientコンポーネントは、VDAと一緒にインストールされます。UpsServerコンポーネントは、ユーザーセッションでCitrixユニバーサルプリンタードライバーをプロビジョニングする共有プリンターがある各印刷サーバー上にインストールします。

UpsServerは以下でサポートされています。

- Windows Server 2016
- Windows Server 2012 R2および2012。
- Windows Server 2008 R2 SP1

要件：Microsoft Visual C++ 2013 Runtime（32および64ビット）

Windows Server OS対応VDAで、印刷操作間にユーザー認証を実行するには、Universal Print Serverは、VDAと同じドメインに参加する必要があります。

スタンドアロンクライアントとサーバーコンポーネントのパッケージはダウンロードして入手することもできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

詳しくは、「プリンターのプロビジョニング」を参照してください。

そのほか

この製品では、StoreFront 3.12.1000以降がサポートされます。ゾーンの優先度機能を使用するには、StoreFront 3.12.2000以降およびNetScaler Gateway 11.0-65.xを使用している必要があります。

Provisioning Servicesを併用する場合、Provisioning Services 7.15.3以降がサポートされます。

Citrix License Server 11.14のみサポートされます。

Citrixポリシー情報をサイト構成データベースではなくActive Directoryに格納する場合、Microsoftグループポリシー管理コンソール（GPMC）が必要です。CitrixGroupPolicyManagement_x64.msiを個別にインストールした場合（たとえば、マシンにXenAppまたはXenDesktopのコアコンポーネントがインストールされていない場合）、そのマシンにはVisual Studio 2015 Runtimeをインストールする必要があります。詳しくは、Microsoft社のドキュメントを参照してください。

複数のネットワークインターフェイスカードがサポートされます。

VDAをインストールすると、デフォルトでCitrix Receiver for Windowsもインストールされます。詳しくは、Citrix Receiver for Windowsのドキュメントを参照してください。

サポートされているMicrosoft App-Vのバージョンについては、「App-V」を参照してください。

この機能でサポートされているブラウザー情報について詳しくは、「ローカルアプリケーションアクセス」を参照してください。

サポートおよび要件の情報については、「セルフサービスパスワードリセット」ドキュメントを参照してください。

クライアントフォルダーのリダイレクト - サポートされるオペレーティングシステム：

- サーバー：Windows Server 2008 R2 SP1、Windows Server 2012、Windows Server 2012 R2
- クライアント（最新のCitrix Receiver for Windowsを使用する場合）：Windows 7、Windows 8、Windows 8.1

複数のモニターによるDPIの混在Citrix XenDesktopおよびxenApp環境では、モニター間で異なるDPIを使用することはサポートされていません。Windowsコントロールパネルの［ディスプレイ］オプションで、DPI（%スケール）を確認できます。Windows 8.1またはWindows 10クライアントデバイスを使用している場合は、Windowsコントロールパネルの［ディスプレイ］オプションで**［すべてのディスプレイで同じ拡大率を使用する］オプション**を有効にすると、モニターが適切に構成されます。詳しくは、CTX201696を参照してください。

このバージョンのXenAppおよびXenDesktopは、AppDNA 7.8およびAppDNA 7.9と互換性がありません。現在のAppDNAリリースを使用されることをお勧めします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

製品の技術概要

Dec 05, 2017

ここでは次のことについて説明します。

- 主要なXenAppおよびXenDesktopコンポーネント
- 一般的な展開環境のしくみ
- ユーザー接続を処理するしくみ
- データアクセスのしくみ
- デスクトップとアプリケーションの配信：マシンカタログ、デリバリーグループ、およびアプリケーショングループ

XenAppおよびXenDesktopによる 仮想化ソリューションにより、IT担当者は仮想マシン、 アプリケーション、ライセンス、およびセキュリティを完全に制御でき、あらゆる デバイスからのアクセスを提供できます。

XenAppおよびXenDesktopでは、以下の機能が提供されます。

- エンドユーザーは、デバイスで動作するオペレーティングシステムやインターフェイスに依存せずにアプリケーションやデスクトップを実行できます。
- 管理者はネットワークを管理して、特定のデバイスまたはすべてのデバイスにアクセスを制御できます。
- 管理者は、単一のデータセンターからネットワーク全体を管理できます。

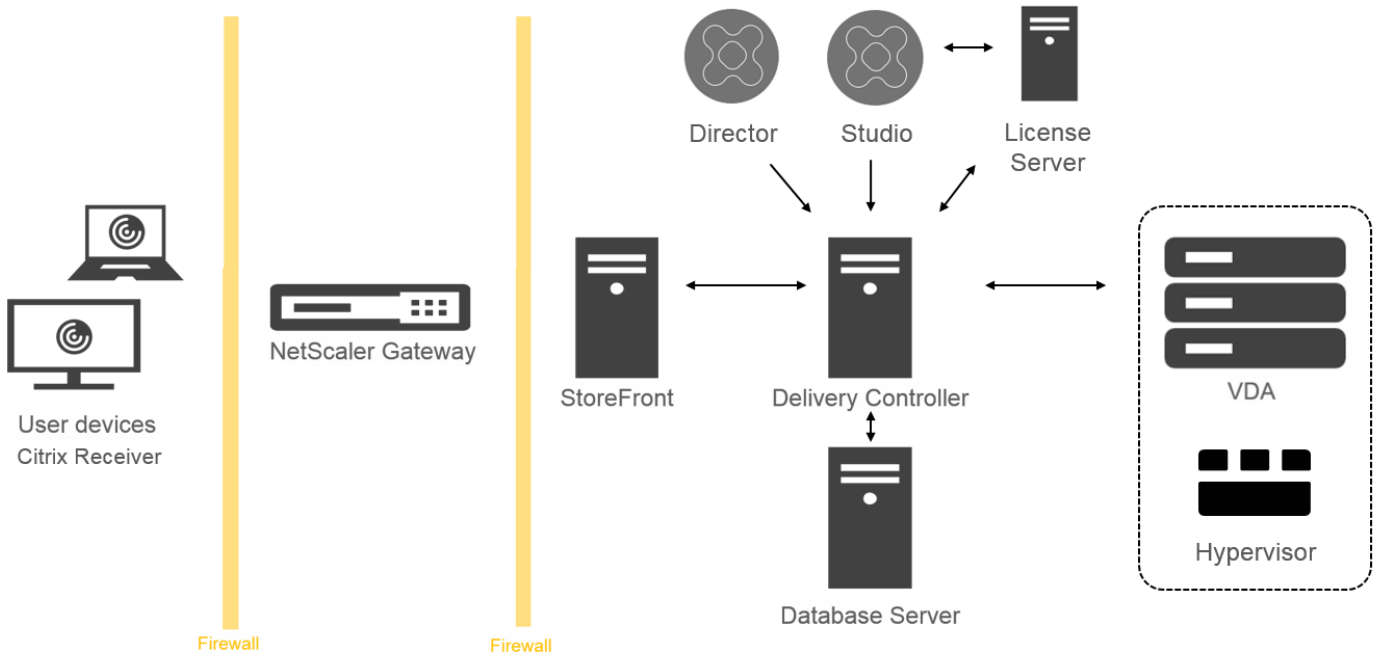
XenAppとXenDesktopでは「FlexCast Management Architecture（FMA）」と呼ばれる共通の統合アーキテクチャが使用されます。FMAにより、単一サイトで複数のバージョンのXenAppまたはXenDesktopを実行でき、プロビジョニング機能が統合されます。

主要なXenAppおよびXenDesktopコンポーネント

ヒント： XenAppまたはXenDesktopに詳しくない場合は、この記事が最も役立ちます。現時点で、6.x以前のXenAppファームまたはXenDesktop 5.6以前を使用している場合は、「7.xでの変更点」も参照してください。

この図は、一般的なXenApp/XenDesktop展開環境（「サイト」と呼ばれます）を構成する主要コンポーネントを示しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Delivery Controller

Delivery Controllerは、XenAppまたはXenDesktopサイトでの中心的な管理コンポーネントです。各サイトには1つ以上のDelivery Controllerが必要で、データセンター内で動作する1つ以上のサーバー上にインストールします。サイトの信頼性および可用性を向上させるには、複数のサーバー上にControllerをインストールします。展開にハイパーバイザー上またはクラウドサービス上でホストされる仮想マシンが含まれる場合、Controllerサービスがハイパーバイザーと通信してアプリケーションやデスクトップを配信したり、ユーザーアクセスを認証および管理したり、ユーザーと仮想デスクトップやアプリケーションとの接続を仲介したり、接続を最適化して負荷を分散させたりします。

ControllerのBroker Serviceは、ログオンしているユーザー、ログオン先、ユーザーのセッションリソース、既存のアプリケーションへの再接続が必要かどうかを追跡します。Broker Serviceは、PowerShellコマンドレットを実行し、VDA上のTCPポート80でBroker Agentと通信します。TCPポート443を使用するオプションはありません。

Monitor Serviceは履歴データを収集して監視データベースに配置します。このサービスはTCPポート80または443を使用します。

Controllerサービスからのデータはサイトデータベースに格納されます。

Controllerは、仮想デスクトップの状態を管理してユーザーからの要求や管理構成に基づいてそれらを起動および停止します。一部のエディションでは、仮想化または物理的なWindows環境でユーザーの個人用設定を管理するためのProfile managementをインストールできます。

データベース

XenAppまたはXenDesktopの各サイトでは、構成情報やセッション情報を格納するためのMicrosoft SQL Serverデータベースが少なくとも1つ必要です。このデータベースには、Controllerを構成する各サービスによって収集および管理されたデータが格納されます。データセンター内にデータベースをインストールして、Controllerと永続的に接続されるようにしてください。サイトは、構成ログデータベースおよび監視データベースも使用します。デフォルトでは、これらはサイトデータベースと同じ場所にインストールされますが、変更できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent（VDA）

VDAは、ユーザーに提供するサイトの各物理マシンおよび仮想マシン上にインストールされ、アプリケーションまたはデスクトップを配信できます。VDAにより、これらのマシンがControllerに登録され、ユーザーがこれらのマシンおよびマシン上でホストされるリソースを使用できるようになります。VDAは、マシンとユーザーデバイス間の接続を確立して、そのユーザーやセッションに必要なCitrixライセンスを検証して、適切なポリシーを適用します。

VDAは、VDAに含まれているBroker Agentを介してController上のBroker Serviceとセッションに関する情報を送受信します。Broker Agentは複数のプラグインをホストし、リアルタイムデータを収集します。Studioは、TCPポート80でControllerと通信します。

「VDA」という語は、それがインストールされているマシンだけでなく、エージェントを指すためにもしばしば使用されます。

VDAは、Windowsサーバーおよびデスクトップオペレーティングシステムで利用できます。VDA for Windows Server OSでは、同時に複数のユーザーがそのサーバーに接続できます。VDA for Windows Desktop OSでは、デスクトップへの単一ユーザー接続のみが許可されます。Linux VDAも使用できます。

Citrix StoreFront

StoreFrontは、リソースをホストするサイトにアクセスするユーザーを認証して、ユーザーのデスクトップやアプリケーションのストアを管理します。StoreFrontにより、デスクトップやアプリケーションへのセルフサービスアクセスをユーザーに提供する「エンタープライズアプリケーションストア」がホストされます。また、ユーザーのアプリケーションサブスクリプション、ショートカット名、およびそのほかのデータが維持・管理され、さまざまなユーザーデバイスを使用するユーザーに一貫したアクセス体験が提供されます。

Citrix Receiver

スマートフォン、タブレット、コンピューターなどのユーザーデバイスや仮想デスクトップなどのエンドポイント上にCitrix Receiverをインストールすると、アプリケーション、デスクトップ、および業務データへのすばやく安全なセルフサービスアクセスが提供されます。また、Windows、Web、およびSaaS（Software as a Service）アプリケーションへのオンデマンドアクセスも提供されます。Citrix Receiverソフトウェアをインストールできないデバイスでは、HTML5互換のWebブラウザーからCitrix Receiver for HTML5を使用してアクセスすることもできます。

Citrix Studio

Studioは、XenAppおよびXenDesktopの展開環境を構成して管理するための管理コンソールです。アプリケーション用とデスクトップ用に異なる管理コンソールを使用する必要はありません。Studioでは、環境のセットアップ、アプリケーションやデスクトップをホストするためのワークロードの作成、アプリケーションやデスクトップのユーザーへの割り当てなどを実行するさまざまなウィザードが提供されます。Studioでは、サイトのCitrixライセンスの割り当てや追跡も可能です。

Studioは、Controller上のBroker ServiceとTCPポート80経由で通信して、そこからの情報を表示します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Director

Directorは、ITサポート担当者やヘルプデスクのスタッフが環境の状態を監視して、重大な障害が生じる前にトラブルシューティングを講じたりエンドユーザーをサポートしたりするためのWebベースのツールです。Directorでは、複数のXenApp/XenDesktopサイトに接続して監視することができます。

Directorには次のものが表示されます。

Controller上のBroker Serviceからのリアルタイムセッションデータ。これには、VDA内のBroker AgentからBroker Serviceが収集したデータも含まれます。

Controller上のMonitor Serviceからのサイト履歴データ。

HDX Insightが収集したNetScalerからのHDXトラフィック（「ICAトラフィック」とも呼ばれます）に関するデータ。HDX Insightが付属するXenAppまたはXenDesktopのエディションおよびNetScalerを使用する環境に限られます。

また、Windowsリモートアシスタンスを使用すると、Directorを介してユーザーのセッションを表示したり制御したりすることもできます。

Citrixライセンスサーバー

ライセンスサーバーはCitrix製品のライセンスを管理します。Controllerと通信して各ユーザーセッションのライセンスを管理し、Studioと通信してライセンスファイルを割り当てます。少なくとも1台のライセンスサーバーを作成して、ライセンスファイルを格納および管理する必要があります。

ハイパーバイザーまたはクラウドサービス

ハイパーバイザーまたはクラウドサービスは、サイトの仮想マシンをホストします。これには、アプリケーションやデスクトップをホストする仮想マシンだけでなく、XenAppやXenDesktopのコンポーネントをホストする仮想マシンも含まれます。ハイパーバイザーは、仮想マシンをホストする専用のコンピューター上にインストールします。

XenAppおよびXenDesktopは、さまざまなハイパーバイザーおよびクラウドサービスをサポートします。

多くのXenApp/XenDesktop展開ではハイパーバイザーを併用しますが、リモートPCアクセスを提供する場合、または仮想マシンのプロビジョニングにMachine Creation Services（MCS）ではなくProvisioning Services（XenAppおよびXenDesktopの一部のエディションに付属）を使用する場合、ハイパーバイザーは不要です。

詳細情報の参照先：

- ポートについて詳しくは、「ネットワークポート」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- データベースについて詳しくは、「データベース」を参照してください。
- XenAppおよびXenDesktopコンポーネントのWindowsサービスについて詳しくは、「ユーザー権利の構成」を参照してください。
- サポートされるハイパーバイザーとクラウドサービスについて詳しくは、「システム要件」を参照してください。

追加のコンポーネント

XenAppまたはXenDesktop展開では、上図に示されていない以下の追加コンポーネントを使用することもできます。詳しくは、それぞれのドキュメントを参照してください。

Provisioning Services（PVS）

PVSは、XenAppおよびXenDesktopの一部のエディションに付属するオプションコンポーネントです。仮想マシンをプロビジョニングするMCSの代替として使用できます。MCSがマスターイメージのコピーを作成するのに対し、PVSはマスターイメージをユーザーデバイスにストリーム配信します。PVSではハイパーバイザーが不要なため、物理マシンをホストすることができます。サイト内のPVSは、Controllerと通信してユーザーにリソースを提供します。

NetScaler Gateway

ユーザーが組織のファイアウォールの外側から接続する場合、XenAppおよびXenDesktopでCitrix NetScaler Gateway（旧称「Access Gateway」）技術を使用して接続をTLSで保護できます。NetScaler GatewayやNetScaler VPX仮想アプライアンスは非武装地帯（DMZ）に配置するSSL VPNアプライアンスで、企業ファイアウォールを介した安全な単一アクセスポイントを提供します。

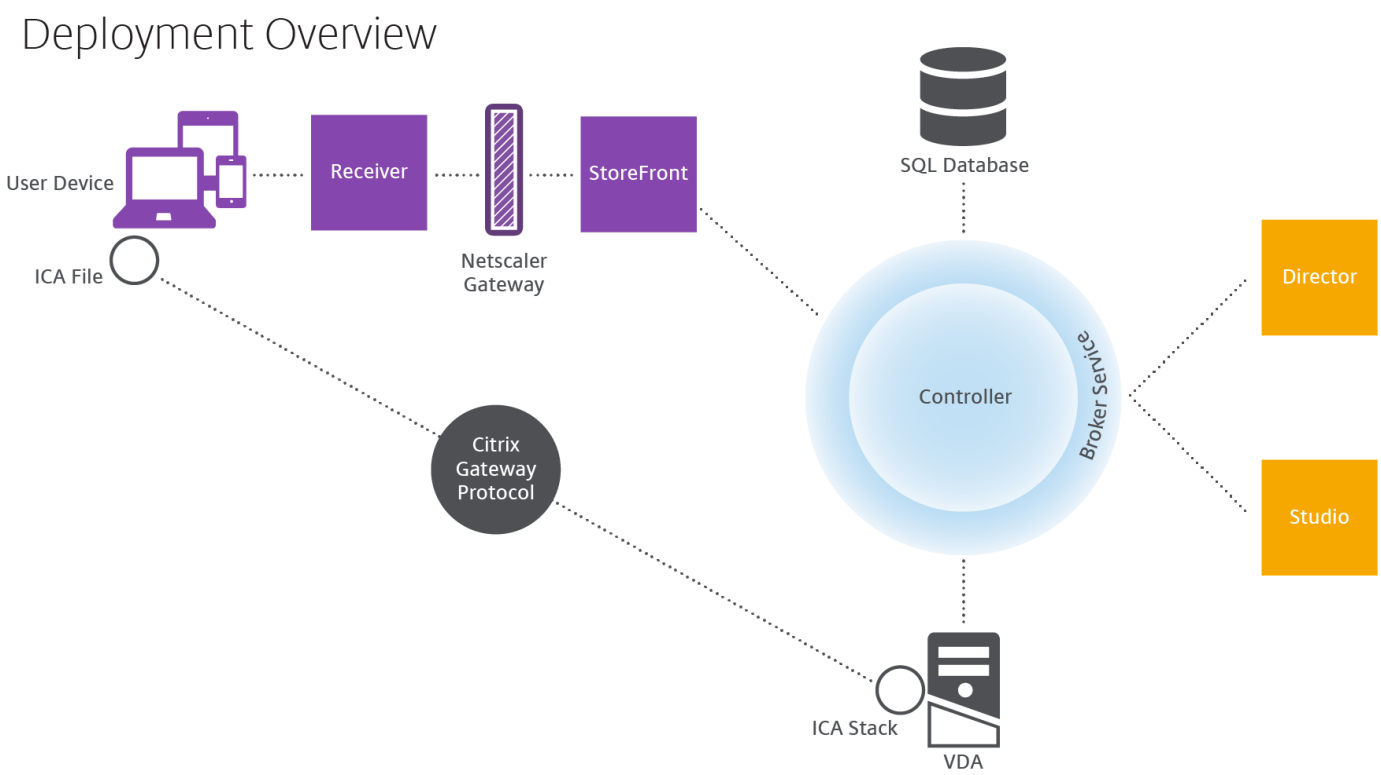
NetScaler SD-WAN

支店など遠隔地のユーザーがWANを介して仮想デスクトップに接続する環境では、Citrix NetScaler SD-WAN（旧称「Citrix CloudBridge」、「Branch Repeater」、または「WANScaler」）技術によりWAN接続のパフォーマンスを最適化できます。この製品によりWAN接続におけるパフォーマンスが向上するため、WAN接続でもLAN接続のようなユーザーエクスペリエンスが提供されます。NetScaler SD-WANでは、さまざまなユーザー操作に優先順位を割り当てることができます。たとえば、ネットワーク上で大きなファイルや印刷ジョブを送信する操作に高い優先度を割り当てて、遠隔地のユーザーがストレスなく作業できるようにします。HDX WANの最適化によりトークン化された圧縮およびデータ重複排除が提供され、帯域幅消費が減少してパフォーマンスが向上します。

一般的な展開環境のしくみ

XenAppおよびXenDesktopのサイトは、スケーラビリティ、高可用性、およびフェールオーバーを実現する特定の役割を持ついくつかのマシンで構成され、「セキュア・バイ・デザイン」なソリューションを提供します。XenApp/XenDesktopサイトは、VDAがインストールされたサーバーマシンとデスクトップマシン、およびアクセスを管理するDelivery Controllerで構成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



VDAは、ユーザーがデスクトップやアプリケーションにアクセスすることを可能にするエージェントソフトウェアです。多くの場合、このコンポーネントはデータセンター内のサーバーまたはデスクトップマシン上にインストールされますが、リモートPCアクセス展開では社内の物理PC上にインストールされます。

Controllerは、リソース、アプリケーション、およびデスクトップを管理したりユーザー接続を最適化および負荷分散したりする、独立したいくつかのWindowsサービスで構成されます。各サイトでは1つまたは複数のControllerが動作し、理想的にはそのすべてが同一LAN上に配置されている必要があります。これは、セッションが遅延、帯域幅、およびネットワークの信頼性に依存するためです。

ユーザーがControllerに直接アクセスすることはありません。ユーザーとController間の通信の中継点としてVDAが機能します。ユーザーがStoreFrontを使用してサイトにログオンすると、ユーザーの資格情報がController上のBroker Serviceに渡され、そこでそのユーザーに適用されるポリシーに基づいてプロファイルおよびリソースが取得されます。

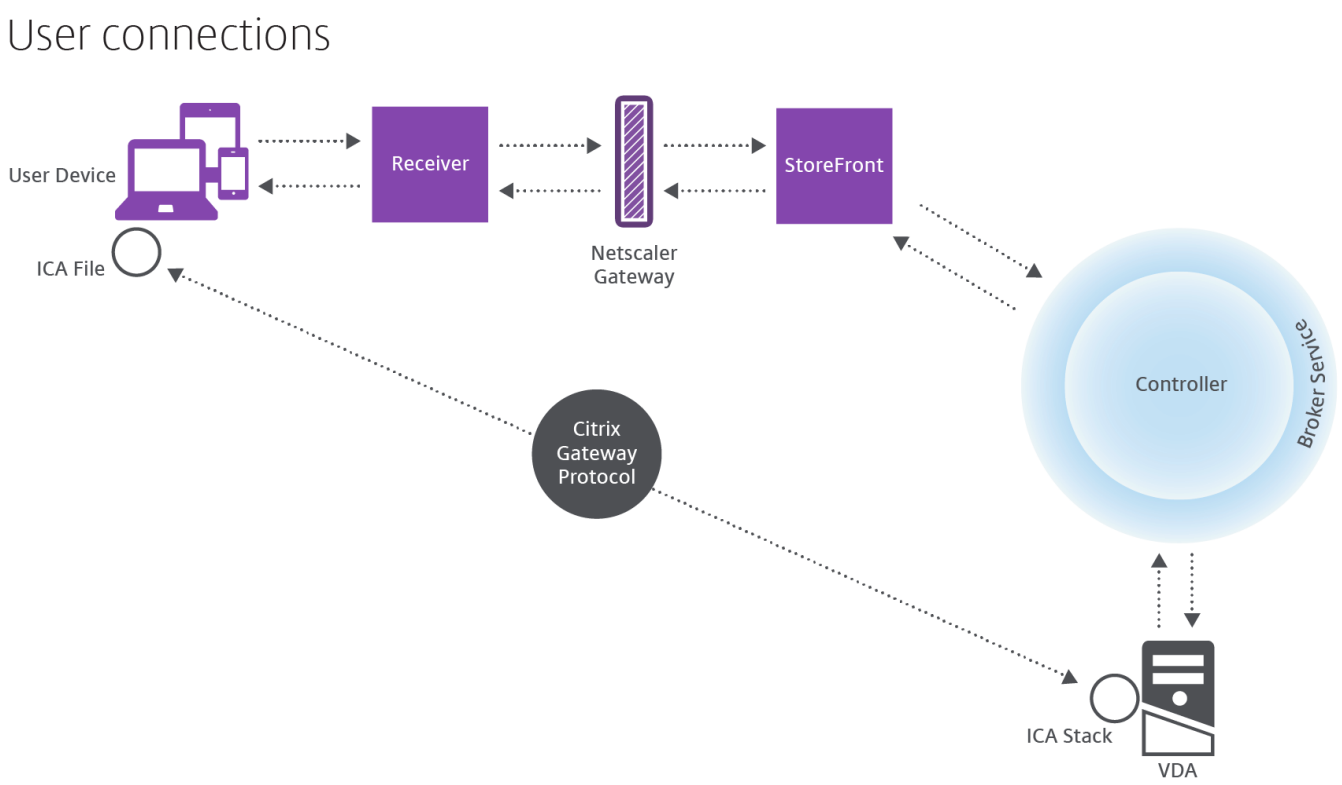
ユーザー接続を処理するしくみ

ユーザーがXenAppまたはXenDesktopのセッションを開始するには、ユーザーデバイス上にインストールされたCitrix ReceiverまたはStoreFront Citrix Receiver for Webサイトを使用します。

ユーザーは、使用する物理デスクトップまたは仮想デスクトップ、または仮想アプリケーションを選択します。

下図の経路で、Controllerにアクセスするためのユーザーの資格情報が転送されます。Controllerは、Broker Serviceと通信して必要なリソースを決定します。Citrix Receiverから送信される資格情報を暗号化で保護するために、StoreFront上にSSL証明書をインストールすることをお勧めします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Broker Serviceにより、ユーザーがアクセスできるデスクトップやアプリケーションが決定されます。

資格情報の検証後、アクセス可能なデスクトップやアプリケーションの情報がStoreFrontとCitrix Receiver経由でユーザー側に返送されます。ユーザーが一覧からアプリケーションまたはデスクトップを選択すると、その情報が同じ経路でControllerに送信され、そこでアプリケーションまたはデスクトップのホストとして適切なVDAが決定されます。

Controllerはユーザーの資格情報をメッセージとしてVDAに送信し、さらにユーザーと接続に関するすべてのデータをVDAに送信します。VDAが接続を受け入れて、同じ経路でCitrix Receiverに情報を返送します。必要なパラメーターのセットはStoreFrontで収集されます。収集されたパラメーターは、Receiver-StoreFront間でのプロトコル変換の一部として、またはIndependent Computing Architecture（ICA）ファイルに変換されダウンロードされて、Citrix Receiverに送信されます。サイトが正しく構成されている場合、ユーザーの資格情報はこれらの処理をとおして暗号化されたまま転送されます。

ICAファイルがユーザーデバイスにコピーされ、VDA上で実行されるICAスタックとの直接接続が確立されます。この接続により、管理インフラストラクチャ（Citrix Receiver、StoreFront、およびController）がバイパスされます。

Citrix ReceiverとVDA間の接続ではCitrix Gateway Protocol（CGP）が使用されます。接続が中断されても、セッション画面の保持機能により同じVDAに再接続されます。管理インフラストラクチャ経由でセッションを再起動する必要はありません。セッション画面の保持機能の有効または無効の設定はCitrixポリシーで行います。

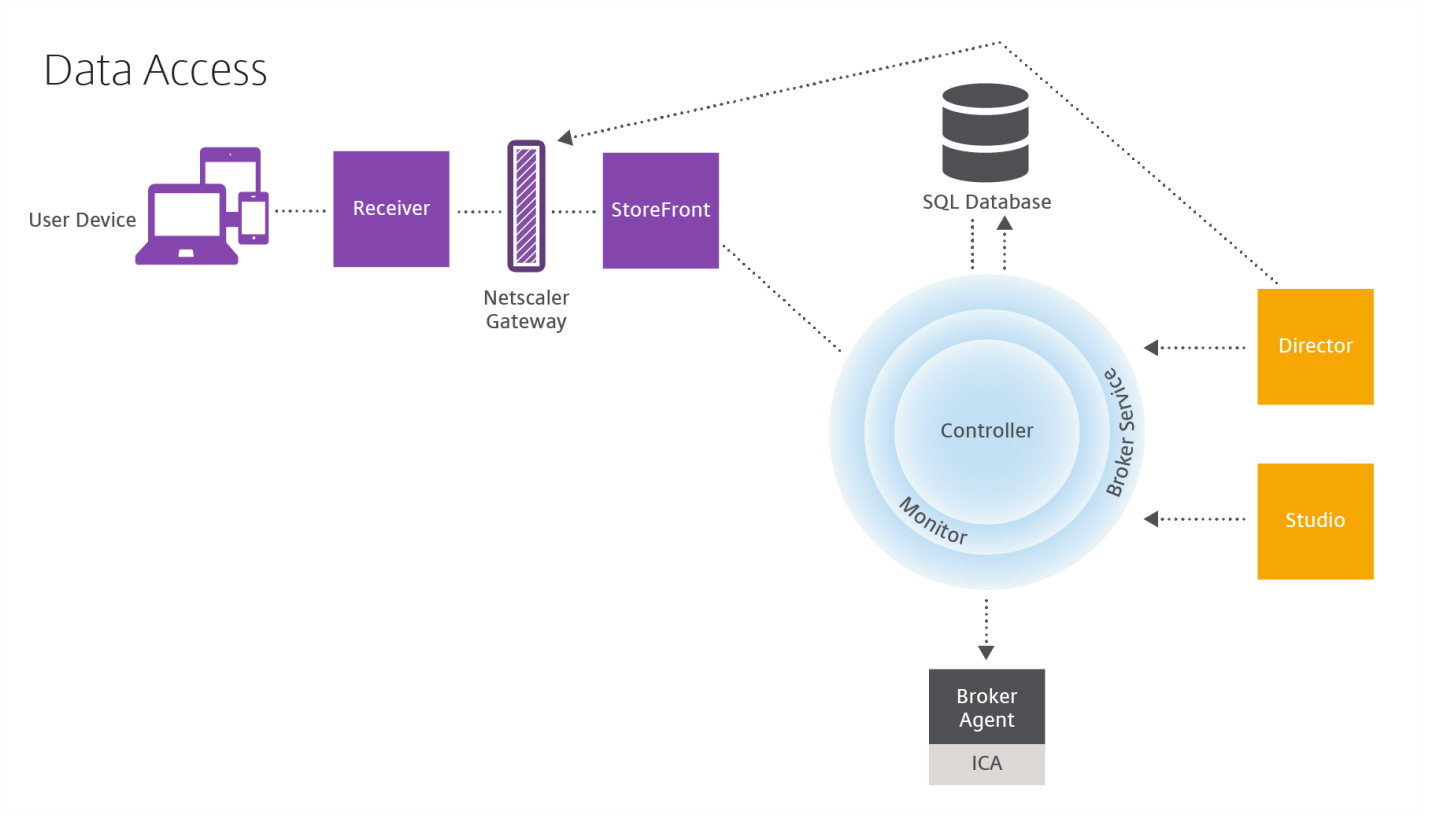
クライアントがVDAに接続すると、ユーザーがログオンしたことがVDAによりControllerに通知されます。Controllerは、この情報をサイトデータベースに送信し、監視データベース内でのデータ記録を開始します。

データアクセスのしくみ

IT担当者は、XenAppまたはXenDesktopの各セッションにより提供されるデータにStudioやDirectorでアクセスできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Studioを使用すると、Broker Agentからのリアルタイムデータにアクセスしてサイトを詳細に管理できます。Directorでは、Broker Agentからのリアルタイムデータに加えて、監視データベースに格納された履歴データやNetScaler Gatewayからの HDXデータにアクセスしてヘルプデスク業務やトラブルシューティングに役立てることができます。



Controller内では、Broker Serviceがリアルタイムデータを提供するマシン上の各セッションについてのセッションデータをレポートします。Monitor Serviceもこのリアルタイムデータを監視して、履歴データとして監視データベース内に格納します。

StudioはBroker Serviceとのみ通信するため、リアルタイムデータにのみアクセスします。Directorは、Broker Serviceと（Broker Agent内のプラグイン経由で）通信してサイトデータベースにアクセスします。

また、DirectorはNetScaler Gatewayにもアクセスして、HDXデータの情報を取得します。

デスクトップとアプリケーションの配信：マシンカタログ、デリバリーグループ、およびアプリケーショングループ

アプリケーションおよびデスクトップを提供するマシンをマシンカタログにセットアップします。次に、（カタログにあるマシンの一部またはすべてを使用して）利用可能になり、ユーザーがアクセスできるアプリケーションおよびデスクトップを指定するデリバリーグループを作成します。

マシンカタログ

マシンカタログとは、単一のエンティティとして管理される物理マシンまたは仮想マシンのグループを指します。これらのマ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

シンおよびそのアプリケーションや仮想デスクトップは、ユーザーに提供する「リソース」です。カタログ内のすべてのマシンには、同じオペレーティングシステムおよびVDAがインストールされている必要があります。また、同じアプリケーションまたは仮想デスクトップがある必要があります。

通常、管理者はマスターイメージを作成して、それを基にカタログ内に同一構成の仮想マシンを作成します。仮想マシンの場合、Citrixツール（PVSまたはMCS）または他のツールから、そのカタログにあるマシンのプロビジョニング方法を指定できます。または、独自の既存イメージを使用することもできます。その場合、管理者は、サードパーティ製のESD（Electronic Software Delivery：電子ソフトウェア配信）ツールを使用してターゲットデバイスを個別または集合的に管理します。

有効なマシンの種類は以下のとおりです。

- **サーバーOSマシン**：サーバーオペレーティングシステムが動作する仮想マシンまたは物理マシンで、XenApp公開アプリケーション（「サーバーでホストされるアプリケーション」とも呼ばれます）とXenApp公開デスクトップ（「サーバーでホストされるデスクトップ」とも呼ばれます）を配信します。これらのマシンには同時に複数のユーザーが接続できます。
- **デスクトップOSマシン**：デスクトップオペレーティングシステムが動作する仮想マシンまたは物理マシンで、「VDIデスクトップ」（デスクトップオペレーティングシステムのデスクトップ。ユーザーによるパーソナライズも許可できる）、「VM Hosted App」（デスクトップオペレーティングシステム上のアプリケーション）、および物理マシンでホストされるデスクトップを配信します。これらの各デスクトップにアクセスできるのは単一のユーザーのみです。
- **リモートPCアクセス**：リモートユーザーがCitrix Receiverが動作するあらゆるデバイスからオフィスの物理PCにアクセスできるようにします。オフィスのPCはXenDesktop環境を介して管理します。ユーザーデバイスはホワイトリストに指定する必要があります。

詳しくは、「マシンカタログの作成」を参照してください。

デリバリーグループ

デリバリーグループは、どのマシンのどのアプリケーションやデスクトップをどのユーザーが使用できるかを指定します。デリバリーグループには、マシンカタログのマシンと、サイトにアクセスできるActive Directoryユーザーが属しています。通常、デリバリーグループにユーザーを割り当てるにはActive Directoryグループを使用します。これは、Active Directoryのグループもデリバリーグループも同様の要件に基づいてユーザーをグループ化するためのものだからです。

1つのデリバリーグループに複数のマシンカタログのマシンを追加したり、1つのカタログのマシンを複数のデリバリーグループに追加したりすることができます。ただし、特定のマシンを同時に複数のデリバリーグループに追加することはできません。

管理者は、デリバリーグループ内のユーザーがどのリソースにアクセスできるのかを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信する場合、マシンカタログのマスターイメージ上にそれらのアプリケーションをすべてインストールしておき、複数のデリバリーグループに追加するための十分な数のマシンをそのカタログに作成できます。次に、それらのマシンから適切なアプリケーションが適切なユーザーに配信されるように各デリバリーグループを構成します。

詳しくは、「デリバリーグループの作成」を参照してください。

アプリケーション グループ

アプリケーショングループは、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします。タグ制約機能を使用すると、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制約は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。また、アプリケーショングループを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

詳しくは、「アプリケーショングループの作成」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Active Directoryの要件：

Dec 05, 2017

認証および承認にはActive Directoryが使用されます。Active DirectoryのKerberosインフラストラクチャにより、Delivery Controllerとの通信の機密性および整合性が保護されます。Kerberosについて詳しくは、Microsoft社のドキュメントを参照してください。

「システム要件」で、フォレストとドメインでサポートされる機能レベルについて確認してください。ポリシーモデル作成機能を使用するには、ドメインコントローラーがWindows Server 2003～Windows Server 2012 R2上で動作している必要があります（ドメインの機能レベルには影響しません）。

以下の環境がサポートされています。

- ユーザーアカウントおよびコンピューターアカウントが単一Active Directoryフォレスト内のドメインに属している。同一フォレスト内であれば、ユーザーアカウントとコンピューターアカウントが異なるドメインに属していても構いません。このような環境では、すべてのドメイン機能レベルおよびフォレスト機能レベルがサポートされます。
- ユーザーアカウントが、Controllerおよび仮想デスクトップのコンピューターアカウントと異なるActive Directoryフォレストに属している。このような環境では、Controllerおよび仮想デスクトップのコンピューターアカウントのドメインが、ユーザーアカウントのドメインを信頼している必要があります。フォレストの信頼または外部の信頼を使用できます。このような環境では、すべてのドメイン機能レベルおよびフォレスト機能レベルがサポートされます。
- Controllerのコンピューターアカウントが、仮想デスクトップのコンピューターアカウントが属している追加のActive Directoryフォレストと異なるフォレストに属している。このような環境では、Controllerのコンピューターアカウントのドメインと、仮想デスクトップのコンピューターアカウントのすべてのドメインとの間に相互信頼関係が必要です。このような環境では、Controllerまたは仮想デスクトップのコンピューターアカウントが属しているすべてのドメインが［Windows 2000ネイティブ］機能レベルまたはそれ以上である必要があります。すべてのフォレスト機能レベルがサポートされます。
- 書き込み可能なドメインコントローラー。読み取り専用のドメインコントローラーはサポートされません。

必要に応じて、Virtual Delivery Agent（VDA）で登録可能なControllerを検出するときに、Active Directoryの情報を使用することもできます。この機能は主に後方互換性を保持するためのもので、VDAとControllerが同じActive Directoryフォレストに属している場合のみ使用できます。この検出方法について詳しくは、「Delivery Controller」およびCTX118976を参照してください。

ヒント： サイトの構成後、コンピューター名やControllerのドメインメンバーシップを変更しないでください。

複数のActive Directoryフォレスト環境での展開

注： このトピックの内容は、XenDesktop 7.1以降およびXenApp 7.5以降に適用されます。これらの製品の以前のバージョンには適用されません。

複数のフォレストがあるActive Directory環境では、一方向または双方向の信頼関係が構成済みの場合にDNSフォワーダーによる名前参照や登録を使用できます。適切なActive Directoryユーザーがコンピューターアカウントを作成できるようにするには、オブジェクト制御の委任ウィザードを使用します。このウィザードについて詳しくは、Microsoft社のドキュメントを参照してください。

適切なDNSフォワーダーがフォレスト間に存在する場合、DNSインフラストラクチャにDNS逆引きゾーンは必要ありません。

VDAとControllerが別のフォレストにある場合、Active DirectoryとNetBIOSの名前が異なっているかどうかに関係なく、レジストリキーSupportMultipleForestが必要です。SupportMultipleForestキーは、VDA上でのみ必要です。以下のレジストリキーを追加してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - 値の名前：SupportMultipleForest
  - 種類：REG_DWORD
  - 値のデータ：0x00000001（1）

DNS名前空間がActive Directoryのそれと異なる場合、DNS逆引き構成が必要になることがあります。

セットアップ時に外部信頼が構成済みの場合は、レジストリキーListOfSIDsが必要になります。また、Active DirectoryのFQDNがDNS FQDNと異なる場合、またはドメインコントローラーのドメインがActive Directory FQDNとは異なるNetBIOS名を持っている場合も、レジストリキーListOfSIDsが必要です。以下のレジストリキーを追加します。

- 32ビットまたは64ビットのVDA：HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - 値の名前：ListOfSIDs
  - 種類：REG_SZ
  - 値のデータ：Controllerのセキュリティ識別子（SID）

適切な外部信頼が構成済みの場合、VDA上で以下の変更を行います。

1. \Citrix\Virtual Desktop Agent\brokeragentconfig.exe.configファイルを検索します。
2. ファイルのバックアップコピーを作成します。
3. メモ帳などのテキストエディターを使ってファイルを開きます。
4. 「allowNtlm="false"」を「allowNtlm="true"」に変更します。
5. ファイルを保存します。

ListOfSIDsレジストリキーを追加してbrokeragent.exe.configファイルを編集したら、Citrix Desktop Serviceを再起動して変更を適用します。

次の表は、サポートされる信頼の種類を示しています。

信頼の種類	推移性	方向	このリリースでのサポート
親および子	推移的	双方向	はい
ツリールート	推移的	双方向	はい
外部	非推移的	一方向または双方向	はい
フォレスト	推移的	一方向または双方向	はい
ショートカット	推移的	一方向または双方向	はい
領域	推移的または非推移的	一方向または双方向	なし

複雑なActive Directory環境での展開について詳しくは、CTX134971を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

データベース

Dec 05, 2017

XenAppまたはXenDesktopサイトは、以下の3種類のSQL Serverデータベースを使用しています。

- **サイト：**（別名：サイト構成）実行中のサイト構成に加えて、その時点でのセッションの状態と接続情報を格納します。
- **構成ログ：**（別名：ログ）サイト構成の変更や管理タスクに関する情報を格納します。このデータベースは、構成ログ機能が有効化（デフォルトは有効）されているときに使用されます。
- **モニター：**セッションや接続情報などのデータを格納するために、Directorにより使用されます。

各Delivery Controllerはサイトデータベースと通信します。Controllerとデータベース間の接続にはWindows認証が必要です。任意のControllerをシャットダウンしても、そのサイトのほかのControllerには影響しません。しかしながら、これはサイトデータベースが単一障害点になりうることを意味します。このデータベースサーバーで障害が発生しても、既存の接続は、ユーザーがログオフまたは切断するまでは機能し続けます。サイト構成データベースが利用可能な場合の接続動作について詳しくは、「ローカルホストキャッシュ」を参照してください。

データベースのバックアップを定期的に作成して、データベースサーバーに障害が発生してもバックアップから復元できるようにすることをお勧めします。各データベースを異なる方法でバックアップしなければならない場合があります。手順については、CTX135207を参照してください。

サイトに複数のゾーンが含まれている場合は、サイトベースは必ずプライマリゾーンに格納してください。すべてのゾーンのコントローラーは、このデータベースと通信します。

高可用性

自動フェールオーバーを確実にするために、数種類の高可用性ソリューションがあります。

- **AlwaysOn可用性グループ機能：**SQL Server 2012で導入されたエンタープライズレベルの高可用性および障害回復ソリューション。これにより、1つまたは複数のデータベースの可用性を最大化できます。AlwaysOn可用性グループ機能では、Windows Server Failover Clustering（WSFC）ノード上にSQL Serverインスタンスが存在する必要があります。詳しくは、http://msdn.microsoft.com/en-us/library/hh510230を参照してください。
- **SQL Serverデータベースのミラーリング：**データベースをミラーリングすると、アクティブなデータベースサーバーが停止しても自動フェールオーバー処理が実行され、ユーザーは通常、停止の影響を受けません。各データベースサーバー上に完全なSQL Serverライセンスが必要になるため、ほかのソリューションよりも費用が高くつきます。SQL Server Expressエディションを使用してデータベースをミラーリングすることはできません。
- **SQLクラスタリング：**MicrosoftのSQLクラスタリングテクノロジを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQLミラーリングなどほかのソリューションよりも自動フェールオーバー処理には一般的に時間がかかります。
- **ハイパーバイザーの高可用性機能の使用：**この方法では、仮想マシンとしてデータベースを展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションでは既存のハイパーバイザーソフトウェアを使用でき、またSQL Server Expressエディションも使用できるため、ミラーリングよりも費用が安いというメリットがあります。ただし、データベースの新しい仮想マシンの起動に時間がかかるため、自動フェールオーバー処理が遅くなり、ユーザーへのサービスが中断する可能性があります。

注： SQLクラスター化またはSQLミラー化インストールのおけるノード上へのControllerのインストールはサポートされていません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SQL Server高可用性ベストプラクティスを補完するローカルホストキャッシュ機能を使用すると、サイトデータベースが使用不可の場合でも、ユーザーがアプリケーションやデスクトップに接続および再接続できるようになります。詳しくは、「ローカルホストキャッシュ」を参照してください。

サイト内のすべてのControllerで障害が起きた場合、VDAが高可用性モードで動作するように構成できます。これにより、ユーザーは障害発生後もデスクトップやアプリケーションにアクセスして使用することができます。高可用性モードでは、Controllerを経由しない、VDAへの直接ICA接続が可能になります。この機能は、すべてのControllerとの通信に障害がある場合にのみ使用してください。ほかの高可用性ソリューションの代替策ではありません。詳しくは、CTX 127564を参照してください。

データベースソフトウェアのインストール

デフォルトでは、初めてDelivery Controllerをインストールしたときに、そのサーバーで他のSQL Serverインスタンスが検知されなかった場合に、SQL Server Expressエディションがインストールされます。通常、概念実証またはパイロット展開では、このデフォルトの動作で十分です。ただし、SQL Server ExpressはMicrosoftの高可用性機能をサポートしていません。

デフォルトのインストールでは、デフォルトのWindowsサービスアカウントおよび権限を使用します。Windowsサービスアカウントをsysadminロールに追加する方法など、デフォルトの設定について詳しくは、Microsoft社のドキュメントを参照してください。Controllerは、この構成でNetwork Serviceアカウントを使用します。SQL Serverに追加のロールまたは権限は必要ありません。

必要に応じて、データベースインスタンスで **[インスタンスの非表示]** を選択できます。Studioでデータベースのアドレスを構成する場合、インスタンス名ではなく、インスタンスの静的ポート番号を入力してください。SQL Serverデータベースエンジンのインスタンスを非表示にする方法について詳しくは、Microsoft社のドキュメントを参照してください。

大半の実稼働展開、およびMicrosoftの高可用性機能を利用しているすべての展開では、最初のControllerをインストールしたサーバー以外のマシンにインストールされており、なおかつExpress以外のサポート対象エディションのSQL Serverを使用してください。サポートされているSQL Serverのバージョンについては、「システム要件」の記事を参照してください。データベースは1つまたは複数のマシンに常駐できます。

サイトを作成する前に、SQL Serverソフトウェアをインストールしておく必要があります。データベースを作成する必要はありませんが、作成する場合は、必ず空にしておいてください。Microsoft高可用性テクノロジの構成も推奨されます。

Windows Updateを使用して、SQL Serverを最新の状態に保ってください。

サイトの作成ウィザードを使ったデータベースのセットアップ

サイトの作成ウィザードの **[データベース]** ページでデータベースの名前とアドレス（場所）を指定します。後述の「*データベースのアドレス形式*」を参照してください。DirectorがMonitor Serviceをクエリするときのエラーを回避するためには、監視データベースの名前にはスペースを使用しないでください。

[データベース] ページには、自動とスクリプト使用の2つのデータベース設定オプションがあります。Studioユーザーや Citrix管理者が、必要なデータベースアクセス権を持っている場合は、通常、自動オプションを使用します。データベースのセットアップに必要な権限については、後述の「権限」を参照してください。

データベースの場所は、サイトの作成後に変更できます。後述の「*データベースの場所の変更*」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ミラーデータベースを使用するようにサイトを構成するには、以下の手順を完了してから、自動またはスクリプトによるセットアップ手順に進みます。

1. SQL Serverソフトウェアをサーバー AおよびBにインストールします。
2. サーバーAに、プライマリとして使用するデータベースを作成します。サーバーAのデータベースをバックアップしてから、サーバーBにコピーします。
3. サーバーBで、バックアップファイルを復元します。
4. サーバーAでミラーリングを開始します。

ヒント：サイトの作成後にミラーリング設定を検証するには、PowerShellコマンドレット**get-configdbconnection**を実行して、ミラーに対する接続文字列でフェールオーバーパートナーが設定されていることを確認します。

ミラー化されたデータベース環境でDelivery Controllerを後から追加、移動、または削除する場合は、「Delivery Controller」の記事を参照してください。

自動セットアップ

必要なデータベース権限を持っている場合は、サイトの作成ウィザードの**[データベース]** ページにある「Studioでデータベースを作成および設定する」オプションを選択し、プリンシパルデータベースの名前とアドレスを指定します。

指定したアドレスにデータベースが存在する場合、そのデータベースは空でなければなりません。指定されたアドレスにデータベースが存在しない場合、データベースが見つからないというメッセージが表示され、データベースを作成するかどうかの確認を求められます。作成に同意すると、Studioにより自動的にデータベースが作成され、プリンシパルデータベースとレプリカデータベースに初期化スクリプトが適用されます。

スクリプトを使ったセットアップ

必要なデータベース権限がない場合は、データベース管理者など、権限を持っている人に支援を依頼する必要があります。その手順は以下のとおりです。

1. サイトの作成ウィザードで **[スクリプトを生成]** オプションを選択します。この操作により、合計6つのスクリプトが作成されます。3つのデータベースそれぞれに対して2つずつ（1つはプリンシパルデータベース、もう1つは各レプリカデータベース）が使用されます。スクリプトの格納先を指定します。
2. これらのスクリプトをデータベース管理者に渡します。この時点で、サイトの作成ウィザードは自動的に停止します。あとでサイトの作成を続行しに戻ってきたときに、プロンプトが表示されます。

その後、データベース管理者がデータベースを作成します。個々のデータベースには、次の特性が必要です。

- 「_CI_AS_KS」で終わる照合順序を使用します。Citrixは、「_100_CI_AS_KS」で終わる照合順序の使用を推奨しています。
- 最適なパフォーマンスを実現するには、SQL Server Read-Committed Snapshotを有効化します。詳しくは、CTX 137161を参照してください。
- 必要に応じて、高可用性機能を構成します。
- ミラーリングを構成するには、まず、完全復旧モデルを使用するようにデータベースを設定します（デフォルトは簡易モデル）。プリンシパルデータベースをファイルにバックアップして、それをミラーサーバーにコピーします。ミラーデータベースで、バックアップファイルをミラーサーバーに復元します。その後、プリンシパルサーバーでミラーリングを開始します。

データベース管理者は、SQLCMDコマンドラインユーティリティ、またはSQL Server Management StudioをSQLCMDモードで使用し、高可用性SQL Serverデータベースインスタンスで各xxx_Replica.sqlスクリプトを実行します（高可用性機能が構成されている場合）。その後、プリンシパルSQL Serverデータベースインスタンスで各xxx_Principal.sqlスクリプトを実行しま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。SQLCMDについて詳しくは、Microsoftのドキュメントを参照してください。

すべてのスクリプトが正常に終了したら、データベース管理者は、Citrix管理者に3種類のプリンシパルデータベースアドレスを渡します。

Studioには、サイトの作成の続行を促すプロンプトが表示され、画面は[データベース]ページに戻ります。渡されたアドレスを入力します。データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベースのセットアップに必要な権限

データベースを作成し、初期化（または、データベースの場所を変更）するには、ローカル管理者およびドメインユーザーてなければなりません。また、特定のSQL Server権限も必要です。以下の権限は、Active Directoryのグループメンバーシップで明示的に構成または取得できます。Studioを使用する管理者にこれらの権限がない場合、SQL Serverユーザーの資格情報を入力する必要があります。

操作	目的	サーバーロール	データベースロール
データベースの作成	空のデータベースを作成します	dbcreator	
スキーマの作成	サービス固有のすべてのスキーマを作成して、サイトに最初のControllerを追加します	securityadmin *	db_owner
Controllerの追加	サイトにController（2つ目以降）を追加します	securityadmin *	db_owner
Controller（ミラーサーバー）の追加	ミラー化されたデータベースのミラーロールのデータベースサーバーにControllerログインを追加します	securityadmin *	
スキーマの更新	スキーマの更新およびHotfixを適用します		db_owner

* securityadminは、技術的にはより限定的なサーバーロールですが、実際にはsysadminサーバーロールと同等のものとして扱われます。

Studioを使ってこれらの操作を実行する場合、sysadminサーバーロールの権限が必要です。

データベースのアドレス形式

データベースのアドレスは、以下の形式のいずれかで指定できます。

- ServerName
- ServerName\InstanceName

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ServerName、PortNumber

AlwaysOn可用性グループ機能では、場所フィールドにグループのリスナーを指定します。

データベースの場所の変更

データベースの場所はサイトの作成後に変更できます。データベースの場所を変更する場合は、以下の点に注意してください。

- 変更前のデータベース内のデータは変更後のデータベースにインポートされません。
- 構成ログデータベースの場所を変更する場合、変更前のデータベースの内容は集約されなくなります。
- 変更後のデータベースの最初にデータベースの変更を示すログが記録されますが、変更前のデータベースの場所は記録されません。

データベースが切断されているときの構成変更が禁止された環境（必須ログ機能）では、構成ログの場所を変更することはできません。

データベースの場所を変更する場合は、次の手順に従います。

1. データベースを常駐させるサーバーに、サポートされているバージョンのMicrosoft SQL Serverがインストールされていることを確認します。必要に応じて、高可用性機能をセットアップします。
2. Studioのナビゲーションペインで **[構成]** を選択します。
3. 場所を変更するデータベースを選択して、［操作］ペインの **[データベースの変更]** を選択します。
4. 変更後の場所とデータベース名を指定します。
5. 必要な権限を持っているのでデータベースをStudioで作成するという場合は、**[OK]** をクリックします。確認のメッセージが表示され、 **[OK]** をクリックするとStudioによりデータベースが自動的に作成されます。現在のStudioユーザーの資格情報を使ってデータベースへのアクセスが試行されます。アクセスに失敗すると、データベースにアクセスするための資格情報を入力する画面が開きます。アクセスに成功すると、データベーススキーマがデータベースにアップロードされます（資格情報はデータベース作成時のみ保持されます）。
6. Studioにデータベースを作成させない場合、または必要な権限がない場合は、**[スクリプトを作成]** をクリックします。作成されるスクリプトには、データベースおよびミラーデータベース（構成する場合）を手動で作成するためのコマンドが記述されます。スキーマをアップロードする前に、データベースが空であること、および1人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

詳しい情報の参照先

「Advanced Concepts」セクションには、Citrixチーム全体が提供する技術的な詳細ドキュメントが含まれています。次に例を示します。

- 「Design」コレクションには、他ベースのサイズ変更ツールに関するドキュメントが含まれています。
- 「Implementation and Configuration」コレクションには、SQL Serverの高可用性のためのソリューションを使用する場合の、サイトデータベースのサイズ変更と接続文字列の構成に関するガイダンスが含まれています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配信方法

Dec 05, 2017

単一の仮想化環境ですべてのユーザーのニーズを満たすことは容易ではありません。XenAppおよびXenDesktopの管理者は、さまざまな方法（「FlexCast」と呼ばれます）を使用してユーザーエクスペリエンスをカスタマイズできます。

これらの配信方法にはそれぞれ一長一短があり、ユーザーの使用方法に応じて最適なユーザーエクスペリエンスを提供できます。

Windowsアプリケーションをモバイルデバイス用に最適化する

今日、スマートフォンやタブレットなどのタッチスクリーンデバイスが移動環境として一般的に使用されています。 これらのデバイス上で、大きな画面と従来のポインティングデバイスでの使用が前提となっているWindowsベースのアプリケーションを操作する場合、問題が生じることがあります。

XenAppとCitrix Receiverによるソリューションでは、Windowsベースのアプリケーションを修正することなく、すべての機能を安全にモバイルユーザーに提供できます。

XenAppの公開アプリケーションによる配信方法では、HDX MobileテクノロジによりWindowsアプリケーションがモバイル環境に最適化されます。 この方法では、 Windowsアプリケーションがタッチスクリーン上で操作できるようになり、 マルチタッチジェスチャ、ネイティブのメニューコントロール、カメラ、およびGPS 機能がサポートされます。XenAppおよびXenDesktopでは、アプリケーションのソースコードを変更しなくても、多くのタッチ機能がそのまま使用可能になります。

以下のタッチ操作が含まれます。

- 編集フィールド操作時にキーボードが自動的に表示されます。
- Windowsコンボボックスコントロールの代わりにタッチ操作に適したピッカーコントロールが表示されます。
- ピンチやズームなどのマルチタッチジェスチャを使用できます。
- 慣性スクロールが適用されます。
- タッチパッドまたはカーソル操作でナビゲーションできます。

PCの更新コストを削減する

多くの業種で3年から5年ごとに必要になる物理マシンの更新は面倒な作業であり、最新のオペレーティングシステムやアプリケーションが必要な部署では特に大掛かりになりがちです。 また、組織の成長による新しいマシンの導入に伴う諸経費も無視できません。

VDI Personal vDiskを使用した配信方法では、ユーザーによる完全なパーソナル設定が可能なデスクトップオペレーティングシステムをサーバーリソースからシンクライアントを含むさまざまなマシンに提供できます。 管理者は、プロセッサ、メモリ、およびストレージなどのリソースをネットワーク上のデータセンターで提供する仮想マシンを作成できます。

これにより、古いマシンの使用を延長しながら最新のソフトウェアを維持して、アップグレード時のダウンタイムを最小限に抑えることができます。

契約社員やパートナーが仮想アプリケーション/デスクトップに安全にアクセスできるようにする

ネットワークセキュリティの問題はますます重要になっており、契約社員やパートナーなどの社外作業者に社内のアプリケーションやデータへのアクセスを許可する場合は特に慎重に行う必要があります。作業者にラップトップなどのデバイスを貸与する場合も、セキュリティに対する配慮が必要です。

XenDesktopおよびXenAppでは、データ、アプリケーション、およびデスクトップがファイアウォールで保護された安全なネットワーク内に格納されます。エンドユーザーが転送する情報は、画面の更新、マウスのクリック、キーボード入力のみで

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。これらのリソースをデータセンター内に保持することで、XenDesktopおよびXenAppは一般的なSSL VPNよりも安全なリモートアクセスソリューションを提供します。

Personal vDiskを使用したVDI展開では、ネットワークサーバー上に仮想マシンを作成し、シングルユーザーデスクトップオペレーティングシステムをシンクライアントやユーザーの個人所有デバイスに配信できます。これにより、高価な装置を購入しなくても、社外作業者のセキュリティの問題に対処できます。

移行を促進する

新しいオペレーティングシステムに移行する場合、従来のアプリケーションやそのオペレーティングシステムをサポートしないアプリケーションの処置が課題になります。

アプリケーションを仮想マシンでホストすることで、ユーザーはアップグレード済みの仮想マシン上のCitrix Receiverを使用して、従来のアプリケーションを正しく実行できます。 この間にIT部署は古いアプリケーションの問題を検証および解決でき、新しいオペレーティングシステムへのユーザーの移行を容易にして、ヘルプデスクへの問い合わせを効率化できます。

さらに、移行時にXenDesktopを使用することで、以下のメリットが生じます。
- デスクトップに関する複雑さが軽減する。
- IT部署が環境をより詳細に制御できるようになる。
- エンドユーザーの使用デバイスや作業場所についての柔軟性が向上する。

デザイナーやエンジニア向けの高度な3Dグラフィックアプリケーションを仮想化する

多くの設計事務所や製造会社では、高度な3Dグラフィックアプリケーションが使用されています。 これらの組織では、グラフィックアプリケーションを実行するための強力なハードウェアに膨大なコストがかかります。また、FTPやメールなどの簡易的な手段で大きなサイズのデザインファイルを共有するなど、データ管理に関する問題も抱えています。

XenDesktopで物理デスクトップをホストする配信方法を使用すると、単一のデスクトップイメージを複数のワークステーションやブレードサーバーに提供でき、3Dグラフィックアプリケーションをネイティブのオペレーティングシステム上で実行するためのハイパーバイザーも不要です。

すべてのファイルはネットワーク内の中央データセンターに格納され、ワークステーション間で転送されることはありません。このため、ネットワーク内でデザインファイルをより高速かつ安全に共有できます。

コールセンターを効率化する

大規模なコールセンターの運営には、ピーク時と非ピーク時に適切な人員やマシンを配するという困難な課題が伴います。

VDIをプールして配信する方法を使用すると、最小限のコストで多くのユーザーに標準化されたデスクトップへのアクセスを動的に提供できます。 プールされた仮想マシンは、先にログオンしたユーザーから順に個別のセッションで割り当てられます。

セッション内のデスクトップで変更された内容はユーザーのログオフ時に破棄されるため、これらの仮想マシンに対する日々のメンテナンス作業が軽減されます。 また、セキュリティも向上します。

コールセンターを効率化するもう1つの配信方法として、XenAppでデスクトップをホストすることができます（従来の「公開デスクトップ」）。 この方法では、単一のサーバーオペレーティングシステムで複数のユーザーデスクトップをホストします。

VDIをプールする方法よりも低コストですが、ユーザーがアプリケーションをインストールしたり、システム設定を変更したり、サーバーを再起動したりすることは許可されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenAppの公開アプリケーションと公開デスクトップ

Mar 21, 2018

XenAppの公開アプリケーションと公開デスクトップは、サーバーOSマシンを使用してユーザーに配信します。

使用例

- 安価なサーバーベースのアプリケーション配信により、最小限のコストでアプリケーションを多くのユーザーに配信し、しかも高度なセキュリティと良好なユーザーエクスペリエンスを提供する。
- 明確に定義されたタスクだけを実行し、個人用設定やオフラインアクセスが不要なユーザー。たとえば、コールセンターのオペレーター、販売員、ワークステーションを共有する作業者など。
- アプリケーションの種類：任意のアプリケーション。

特長と注意事項

- データセンター内で簡単に管理できるスケーラブルなソリューション。
- 最もコスト効率に優れたアプリケーション配信ソリューション。
- ホスト上のアプリケーションを一元管理でき、ユーザーはアプリケーションを変更できません。また、安全で信頼性が高く一貫したユーザーエクスペリエンスが提供されます。
- アプリケーションにアクセスするユーザーは常にオンライン状態である必要があります。

ユーザーエクスペリエンス

- ユーザーは、StoreFront、［スタート］メニュー、または特定のURLからアプリケーションにアクセスします。
- アプリケーションはユーザーデバイス上に仮想的に配信され、シームレスかつ高品位に表示されます。
- プロファイル設定によっては、ユーザーによる変更内容がアプリケーションセッションの終了時に保存されます。それ以外の場合、変更は削除されます。

プロセス、ホスト、および配信

- アプリケーションのプロセスはユーザーデバイスではなくホストマシン上で実行されます。物理マシンまたは仮想マシンでアプリケーションをホストできます。
- アプリケーションおよびデスクトップはサーバーOSマシン上にインストールされます。
- マシンは、マシンカタログを作成することで使用可能になります。
- マシンカタログ内のマシンは、同じアプリケーションのセットをユーザーグループに配信するデリバリーグループに分けられます。
- サーバーOSマシンは、デスクトップ、またはアプリケーション、もしくはその両方をホストするデリバリーグループをサポートします。

セッション管理と割り当て

- サーバーOSマシンは、単一マシン上で複数のセッションを実行して、同時に接続する複数のユーザーに複数のアプリケーションとデスクトップを配信します。各ユーザーは、単一セッション内ですべてのアプリケーションを実行します。

  たとえば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上で1つのセッションがホストされ、ほかのユーザーはそのセッションを使用できません。2人目のユーザーが同じマシンにログオンしてアプリケーションを要求すると、2つ目のセッションがホストされ、ほかのユーザーが使用できないセッションが2つになります。これらの2人のユーザーがさらにアプリケーションを要求しても、既存のセッションを使用できるため追加のセッションはホストされません。さらに別の2人のユーザーがログオンしてデスクトップを要求すると、このマシンでは4つのセッションが4人のユーザー用にホストされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ユーザーが割り当てられるデリバリーグループ内で、最も負荷が軽いサーバー上のマシンが選択されます。ユーザーのロ
  オン時に、アプリケーション配信用のマシンがランダムに割り当てられます。

XenAppの公開アプリケーションと公開デスクトップを配信するには、次の手順に従います。

1. サポートされるWindowsサーバーOSのマスターイメージ上に、配信するアプリケーションをインストールします。
2. このマスターイメージのマシンカタログを作成するか、既存のマシンカタログをこのマスターイメージで更新します。
3. アプリケーションとデスクトップをユーザーに配信するためのデリバリーグループを作成します。アプリケーションを配
   信する場合は、配信の対象となるアプリケーションを選択してください。

詳しくは、「インストールと構成」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VM Hosted Apps

Dec 05, 2017

VM Hosted Appとは、デスクトップOSマシンを使用してユーザーに配信するアプリケーションを指します。

使用例

- セキュアなクライアントベースのアプリケーション配信により、シームレスかつ高品位に表示されるアプリケーションをユーザーに配信し、管理を一元化して単一ホストサーバー（またはハイパーバイザー）で多くのユーザーをサポートする。
- ユーザーは、内部または外部契約社員、サードパーティの協力者、臨時社員などである。ホスト上のアプリケーションへのオフラインアクセスは不要。
- アプリケーション種類：ほかのアプリケーションと共存できないアプリケーションや、オペレーティングシステムと一緒に動作するMicrosoft .NET Frameworkなどのアプリケーション。これらのアプリケーションは、仮想マシン上でのホストに適しています。

特長と注意事項

- マスターイメージ上のアプリケーションおよびデスクトップは、データセンター内のマシン上でセキュアに管理、ホスト、および実行されます。また、最もコスト効率に優れたアプリケーション配信ソリューションでもあります。
- ユーザーがログオンすると、同じアプリケーションをホストするデリバリーグループ内のマシンにランダムに割り当てられます。管理者は、ユーザーがログオンするたびに同じマシンが割り当てられるように構成することもできます。このようにマシンをユーザーに静的に割り当てると、ユーザーが仮想マシンにアプリケーションをインストールしたり独自に管理したりできるようになります。
- デスクトップOSマシンでは、複数のセッションを実行できません。このため、ユーザーがログオンするとデリバリーグループ内の1つのマシンが消費され、オフライン状態ではアプリケーションにアクセスできなくなります。
- この方法では、アプリケーションの処理のためのサーバーリソースと、ユーザーのPersonal vDisk用のストレージ容量が多くなります。

ユーザーエクスペリエンス

サーバーOSマシン上でホストされる共有アプリケーションと同様のシームレスなユーザーエクスペリエンスが提供されます。

プロセス、ホスト、および配信

仮想デスクトップOSマシンが使用されることを除き、サーバーOSマシンの場合と同様です。

セッション管理と割り当て

- 1つのデスクトップOSマシンで実行できるデスクトップセッションは1つのみです。アプリケーションにのみアクセスする場合は、各アプリケーションが個別のセッションと見なされるため、単一ユーザーが複数のアプリケーションを使用できます。
- デリバリーグループ内では、ログオンしたユーザーは、静的に割り当てられたマシン（毎回、必ず同じマシンにログオンする）、またはセッションの可用性に基づいてランダムに割り当てられたマシンにアクセスします。

VM Hosted Appを配信するには、次の手順に従います。

1. サポートされるWindowsデスクトップOSのマスターイメージ上に、配信するアプリケーションをインストールします。
2. このマスターイメージのマシンカタログを作成するか、既存のマシンカタログをこのマスターイメージで更新します。
3. マシンカタログのデスクトップエクスペリエンスを定義するときに、ユーザーがログオンするたびに新しい仮想マシンに

© 1999-2017 Citrix Systems, Inc. All rights reserved.

続するのか同じ仮想マシンに接続するのかを指定します。

4. アプリケーションをユーザーに配信するためのデリバリーグループを作成します。
5. インストール済みアプリケーションの一覧で、配信するアプリケーションを選択します。

詳しくは、インストールと構成に関する記事を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDIデスクトップ

Dec 05, 2017

デスクトップOSマシンを使用してユーザーにVDIデスクトップを配信します。

VDIデスクトップは、仮想マシン上でホストされ、各ユーザーにデスクトップオペレーティングシステムを提供します。

VDIデスクトップでは、XenAppの公開デスクトップよりも多くのリソースが必要になります。ただし、サーバーオペレーティングシステムをサポートしないアプリケーションをインストールできる点が公開デスクトップと異なります。 また、VDデスクトップの種類によっては、特定のユーザーにデスクトップを割り当てて、個々のユーザーによるデスクトップのパーソナル設定を許可できます。

VDIデスクトップのマシンカタログを作成するときは、以下のいずれかの種類のデスクトップを作成します。

- ランダムな非永続デスクトップ。「プール型のVDIデスクトップ」とも呼ばれます。この種類のデスクトップでは、ユーザーがログオンするたびに、単一のマスターイメージに基づいたデスクトッププールからデスクトップが動的に選択されます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な非永続デスクトップ。この種類のデスクトップでは、ユーザーの初回ログオン時に、単一のマスターイメージに基づいたデスクトッププールからデスクトップが割り当てられます。以降のログオンでは、同じデスクトップに接続されます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な永続デスクトップ。Personal vDiskを使用するVDIデスクトップです。ほかの種類のVDIデスクトップとは異なり、ユーザーによるデスクトップのパーソナル設定が許可されます。これらのデスクトップの1つを使用するために、ユーザーが初めてログオンしたときに、単一のマスターイメージに基づいたデスクトッププールからデスクトップが割り当てられます。そのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。デスクトップに対するユーザーの変更内容はPersonal vDisk内に保持されるため、マシンを再起動しても破棄されません。

VDIデスクトップは、以下の手順で配信します。

1. WindowsデスクトップOSを実行するマスターイメージを作成します。
2. このマスターイメージのマシンカタログを作成するか、既存のマシンカタログをこのマスターイメージで更新します。マンカタログのデスクトップエクスペリエンスを定義するときに、ユーザーがログオンするたびに新しい仮想マシンに接続するのか同じ仮想マシンに接続するのかを指定します。ユーザーが同じマシンに接続する場合は、デスクトップへの変更を保持する方法を指定できます。
3. デスクトップをユーザーに配信するためのデリバリーグループを作成します。

詳しくは、インストールと構成に関する記事を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ネットワークポート

Mar 21, 2018

次の表は、XenAppおよびXenDesktop Delivery Controllers、Windows VDA、Director、Citrixライセンスサーバーで使用されるデフォルトのネットワークポート一覧です。 Citrixコンポーネントをインストールすると、これらのデフォルトのネットワークポートと一致するように、オペレーティングシステムのファイアウォールもデフォルトで更新されます。

他のCitrixテクノロジおよびコンポーネントで使用されている通信ポートの概要については、CTX101810を参照してください。

以下のように、このポートの情報が必要な場合があります。

- 法的なコンプライアンスが必要である。
- これらのコンポーネントと他のCitrix製品またはコンポーネントとの間にネットワークファイアウォールがある場合、ファイアウォールを適切に構成できる。
- オペレーティングシステムのホストファイアウォールではなく、アンチマルウェアパッケージなどが付属したサードパーティ製のホストファイアウォールを使用する。
- これらのコンポーネントでホストファイアウォールの構成を変更する（通常Windowsファイアウォールサービス）。
- これらのコンポーネントの機能を再構成して、別のポートやポート範囲を使用し、構成で使用されていないポートを無効にする、またはブロックする必要がある。詳しくは、コンポーネントのドキュメントを参照してください。

StoreFrontおよびProvisioning Servicesのような他のコンポーネントのポート情報について詳しくは、コンポーネントの現在の「システム要件」記事を参照してください。

表は、受信ポートのみの一覧です。送信ポートは、通常オペレーティングシステムによって決定され、無関係な番号を使用します。送信ポートの情報は通常、上記に記載された目的には必要ありません。

これらのポートの一部は、Internet Assigned Numbers Authority（IANA）に登録されています。 こうした割り当てについて詳しくは、http://www.iana.org/assignments/port-numbersを参照してください。IANAの説明は、最新の使用状況に対応していない場合もあることに注意してください。

また、VDAおよびDelivery Controllerのオペレーティングシステムには、専用の受信ポートが必要です。 詳しくは、Microsof Windowsのドキュメントを参照してください。

コンポーネント	用途	プロトコル	デフォルトの受信ポート	注
VDA	ICA/HDX	TCP、UDP	1494	EDTプロトコルでは、UDP用に1494が開放されている必要があります。 「ICAのポリシー設定」を参照してください。
VDA	ICA/HDX（セッション画面の保持機能）	TCP、UDP	2598	EDTプロトコルでは、UDP用に2598が開放されている必要があります。 「ICAのポリシー設定」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA	ICA/HDX（TLS経由）	TCP	443	すべてのCitrix Receiver
VDA	ICA/HDX（WebSocket経由）	TCP	8008	Citrix Receiver for HTML5、Citrix Receiver for Chrome 1.6以前のみ
VDA	ICA/HDX（UDPでのオーディオリアルタイムトランスポート）	UDP	16500から16509	
VDA	ICA/HDX/Framehawk	UDP	3224から3324	
VDA	ICA/Universal Print Server	TCP	7229	Universal Print Server印刷データストリームCGP（Common Gateway Protocol）リスナーが使用。
VDA	ICA/Universal Print Server	TCP	8080	HTTP/SOAP要求の受信のためにUniversal Print Serverのリスナーが使用。
VDA	Wake On LAN	UDP	1041	リモートPCアクセスの電源管理
VDA	ウェイクアッププロキシ	TCP	135	リモートPCアクセスの電源管理
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA、StoreFront、Director、Studio	TCP	80	
Delivery Controller	StoreFront、Director、Studio（TLS経由）	TCP	443	
Delivery Controller	Delivery Controller、VDA	TCP	89	ローカルホストキャッシュ（ポート89の使用は将来のリリースで変更される可能性があります）
Delivery Controller	オーケストレーション	TCP	9095	オーケストレーション
Director	Delivery Controller	TCP	80、443	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrixライセンスの場合

コンポーネント	用途	プロトコル	デフォルトの受信ポート	注
ライセンスサーバー	ライセンスサーバー	TCP	27000	
ライセンスサーバー	Citrixのライセンスサーバー（ベンダーデーモン）	TCP	7279	
ライセンスサーバー	ライセンス管理コンソール	TCP	8082	
ライセンスサーバー	Web Services for Licensing	TCP	8083	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX

Dec 05, 2017

> **警告**
>
> レジストリエディターの編集を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix HDXには、高品位なユーザーエクスペリエンスを提供する、幅広い機能セットが含まれています。

デバイスでは

ユーザーデバイスのコンピューティング能力を利用して、ユーザーエクスペリエンスを拡張および最適化します。HDXテクノロジにより、スムーズでシームレスなマルチメディアコンテンツが仮想デスクトップやアプリケーションに提供されます。ワークスペースコントロール機能により、仮想デスクトップやアプリケーションのセッションを一時停止して、ほかのデバイスでそのセッションでの作業を再開できます。

ネットワークでは

HDXによる高度な最適化およびアクセラレーションにより、待機時間が長く低帯域幅のWAN接続を含むあらゆるネットワークにおいて最高のパフォーマンスが提供されます。

HDX機能は環境のさまざまな条件に応じて最適化されます。パフォーマンスと消費帯域幅を調和させる機能。社内ネットワークからデスクトップやアプリケーションにローカルにアクセスする場合やファイアウォールの外側からリモートにアクセスする場合など、各ユーザーシナリオに応じて最適な機能が適用されます。

データセンターでは

HDXでは、サーバー側の処理能力およびスケーラビリティを利用して、クライアントデバイス側の能力に制限されずに高度なグラフィックパフォーマンスを提供できます。

Citrix Directorでは、ユーザーデバイスに接続しているHDXチャネルの状態を監視できます。

HDX Insightにより、NetScaler Network InspectorおよびPerformance ManagerがDirectorに統合されます。ICAトラフィックに関するデータを収集して、リアルタイムおよび履歴の詳細をダッシュボードに表示します。このデータには、クライアント側およびサーバー側のICAセッション遅延、ICAチャネルの帯域幅使用量、および各セッションのICA往復時間値が含まれます。

仮想デスクトップ上では、以下の操作を行うことでHDXの機能を体験できます。

- 3つのHDXマルチメディアリダイレクトテクノロジの1つであるFlashリダイレクトによりAdobe Flashマルチメディアコンテンツの配信がどのように高速化されるかを体験するには、次の手順に従います。
  1. Adobe Flash Player（http://get.adobe.com/flashplayer/）をダウンロードして仮想デスクトップおよびユーザーデバイスにインストールします。
  2. Desktop Viewerのツールバーで **[基本設定]** をクリックします。［Desktop Viewer基本設定］ダイアログボックス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

の［Flash］タブで、［コンテンツを最適化する］を選択します。
3. FlashリダイレクトによるFlashマルチメディアコンテンツの配信パフォーマンスを体験するには、仮想デスクトップでYouTubeなどのWebサイトにアクセスして、Flashビデオを再生します。Flashリダイレクトはシームレスであるため、ユーザー側にはいつ動作しているかはわかりません。ただし、Flashリダイレクトが使用されているかどうかは確認できます。Flash Playerが起動する前に画面上に一瞬だけカラーブロックが現れます。また、ビデオを右クリックすると、メニューに［Flashリダイレクト］が表示されます。

- HDXにより高品位オーディオがどのように配信されるかを体験するには、次の手順に従います。
  1. Citrix Receiverで、最高の音質を選択します。詳しくは、Citrix Receiverのドキュメントを参照してください。
  2. デスクトップ上のデジタルオーディオプレーヤー（iTunesなど）で音楽ファイルを再生します。

HDXでは、特別な構成を行わなくてもデフォルトで、一般的なユーザーに適したグラフィックおよびビデオ配信が提供されます。Citrixポリシー設定は、一般的な使用環境で最適なユーザーエクスペリエンスが提供されるようにデフォルトで有効になっています。

- HDXは、クライアントプラットフォーム、アプリケーション、およびネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、状況の変化に応じて自動調整します。
- HDXは、2Dおよび3Dのグラフィックおよびビデオのパフォーマンスを最適化します。
- HDXは、インターネットやイントラネット上のマルチメディアコンテンツなどをホストサーバーを介さず直接ユーザーデバイス上にストリーム配信します。このクライアント側でのコンテンツ取得に必要な条件が満たされない場合、メディア配信はサーバー側でのコンテンツ取得とマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能に関するポリシーを変更する必要はありません。
- マルチメディアリダイレクトが利用できない場合、HDXは仮想デスクトップにサーバー側でレンダリングしたビデオコンテンツを提供します。 http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/などのサイトにアクセスして、高品位ビデオを含むWebサイト上のビデオをご覧ください。

ヒント：

- HDX機能に関するサポートおよび要件については、システム要件の記事を参照してください。 特に注記のあるものを除き、WindowsサーバーOSマシン、WindowsデスクトップOSマシン、およびリモートPCアクセスのデスクトップでHDX機能を使用できます。
- このセクションのトピックでは、ユーザーエクスペリエンスをさらに最適化したり、サーバーのスケーラビリティを改善したり、消費帯域幅を抑えたりする方法について説明します。Citrixポリシーおよびそのポリシー設定について詳しくは、このリリースの「Citrixポリシー」を参照してください。
- レジストリを編集する場合は細心の注意が必要です。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

制限事項

セッション内でリモート音声およびビデオ拡張機能（RAVE）を有効にしてWindows Media Playerを使用しているときに、ビデオコンテンツを右クリックして［プレイビューを常に手前に表示］を選択すると、画面表示が黒くなることがあります。

ホストされるアプリケーションまたはデスクトップにアクセスすると、ネットワークが中断される場合があります。再接続をスムーズに行うために、クライアントの自動再接続とセッション画面の保持が利用できます。デフォルト構成では、セッション画面の保持が起動した後、クライアントの自動再接続が起動します。

クライアントの自動再接続

クライアントの自動再接続によってクライアントのエンジンが再起動され、切断されたセッションに再接続します。クライア

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ントの自動再接続によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。クライアントの自動再接続の実行中に、システムからユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます。

- **デスクトップ。** セッションウィンドウが灰色表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。
- **アプリケーション。** セッションウィンドウがクローズし、ダイアログが開いて再接続が試行されるまでの時間を示すカウントダウンタイマーが表示されます。

クライアントの自動再接続中に、セッションはネットワーク接続を見越して再起動されます。クライアントの自動再接続の実行中は、セッションを操作できません。

再接続では、切断されたセッションは、保存された接続情報を使って再接続されます。ユーザーは、正常にアプリケーションおよびデスクトップを操作できます。

クライアントの自動再接続のデフォルト設定：

- クライアントの自動再接続のタイムアウト： 120秒
- クライアントの自動再接続： 有効
- クライアントの自動再接続時の認証： 無効
- クライアントの自動再接続のログ： 無効

詳しくは、「クライアントの自動再接続のポリシー設定」を参照してください。

セッション画面の保持

セッション画面の保持によってICAセッションは、ネットワークの中断を挟んでもシームレスに再接続されます。セッション画面の保持によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。セッション画面の保持がタイムアウトした後で、クライアントの自動再接続設定が有効になり、切断されたセッションへの再接続が行われます。セッション画面の保持の実行中に、ユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます。

- **デスクトップ。** セッションウィンドウが半透明表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。
- **アプリケーション。**ウィンドウが半透明表示になると同時に、通知領域に中断された接続のポップアップが表示されます。

セッション画面の保持がアクティブの間は、ユーザーはICAセッションを操作できません。ただし、キー入力のようなユーザー操作は、ネットワーク中断直後の数秒間バッファされ、ネットワークが再接続されたら再送信されます。

再接続されると、クライアントとサーバーは、プロトコルを交換したポイントからセッションを再開します。セッションウィンドウの半透明表示が解除され、アプリケーションに対する適切なポップアップが通知領域に表示されます。

セッション画面の保持のデフォルト設定

- セッション画面の保持のタイムアウト 180秒
- 再接続 UI の透過レベル： 80%
- セッション画面の保持の接続： 有効
- セッション画面の保持のポート番号 2598

詳しくは、「セッション画面の保持のポリシー設定」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScalerとクライアントの自動再接続およびセッション画面の保持

マルチストリームポリシーとマルチポートポリシーがサーバー上で有効化され、次の条件のいずれかまたはすべてに合致する場合、クライアントの自動再接続は機能しません。

- セッション画面の保持機能がNetScaler Gatewayで無効化されている。
- NetScalerアプライアンスでフェールオーバーが発生している。
- NetScaler GatewayでNetScaler SD-WANを使用している。

Windows 10 VDAに接続またはローミングされたタッチ対応デバイスは、デフォルトでタブレットモードで起動されます。

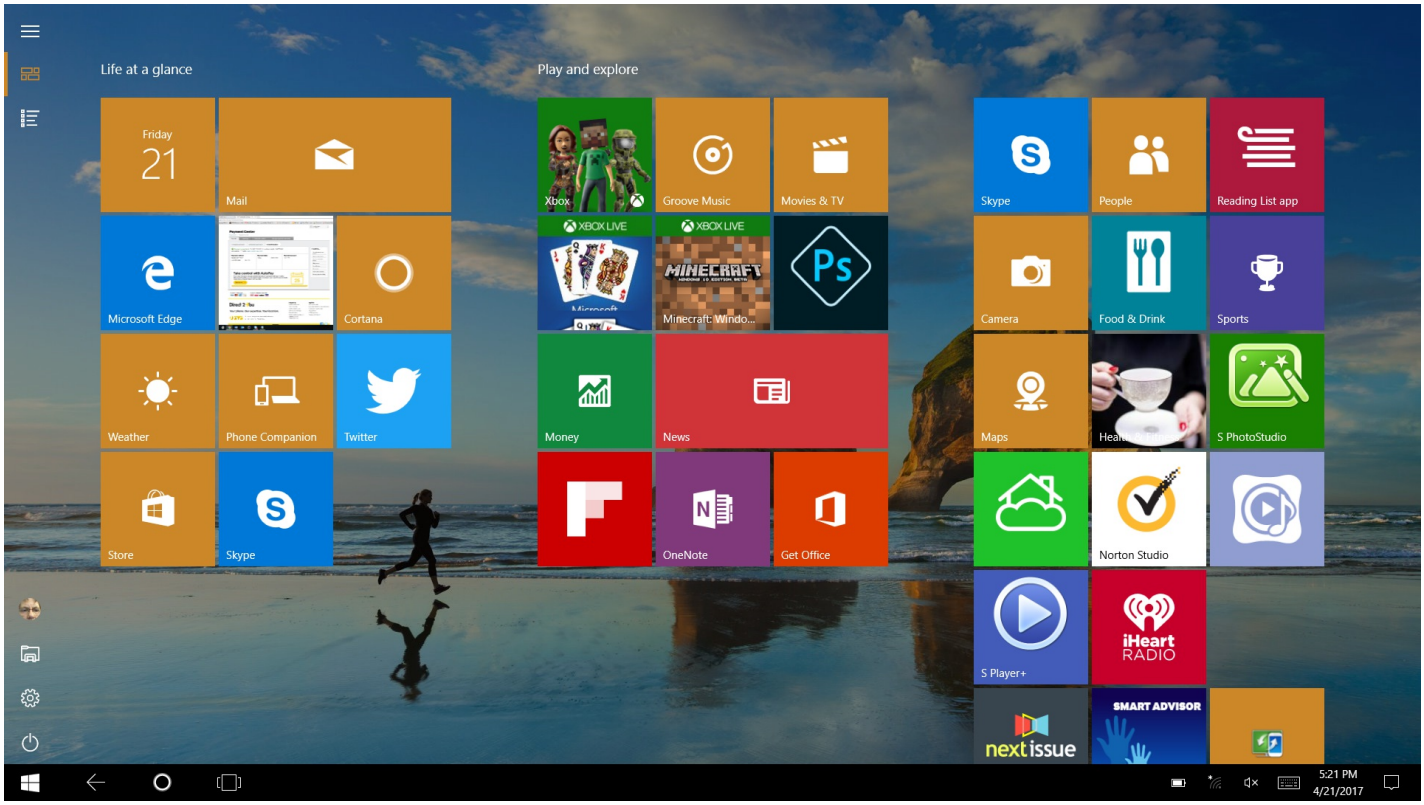
タブレットモードの使用には、XenServerバージョン7.2以上が必要です。XenServer 7.2は XenDesktop VDAと統合されており、2-in-1デバイスの仮想ファームウェア設定が有効になるようにハイパーバイザーが変更されています。Windows 10は、この更新されたBIOSを基にターゲット仮想マシンにGPIOドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるのに使用されます。詳しくは、http://docs.citrix.com/content/dam/docs/en-us/xenserver/current-release/downloads/xenserver-release-notes.pdfを参照してください

タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます。

- やや大きめのボタン
- スタート画面や開始したアプリケーションを全画面で開く
- タスクバーに［戻る］ボタンを表示
- タスクバーからアイコンを削除

File Explorerにアクセスできます。

Web Receiverではテーブルモードはサポートされません。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

ラップトップとタブレットの切り替えを許可するXenServer CLIコマンドを実行します。

xe vm-param-set uuid= platform:acpi_laptop_slate=1

タブレットモードを無効または有効にするには、XenAppおよびXenDesktopのこのレジストリ設定を構成します。

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

名前：CitrixEnhancedUserExperience
種類：REG_DWORD

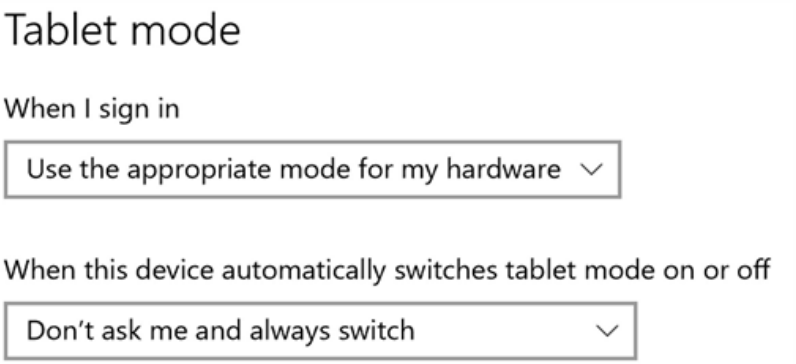
値：
0（無効）
1（有効）

セッション開始前

セッション開始前にVDAで **[設定] > [システム] > [タブレットモード]** に移動して、ドロップダウンメニューから以下のオプションを設定することをお勧めします。

- ハードウェアに適切なモードを使用する
- 確認なしで常に切り替える

セッション開始前にこれらのオプションを設定しない場合には、セッション開始後に設定し、VDAを再起動してください。



視覚表示ポリシー設定は、仮想デスクトップからユーザーデバイスに送信されるイメージの品質を制御します。

- 表示品質。ユーザーデバイス上に表示されるイメージの表示品質として、［低］、［中］、［高］、［常に無損失］、または［操作時は低品質］を指定します。デフォルトは［中］です。メディアのデフォルト設定による実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレーム数仮想デスクトップからユーザーデバイスに送信されるイメージの1秒あたりの最大フレーム数（fps）を指定します。デフォルトは30fpsです。CPUが低速なデバイスでは、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。サポートされている1秒あたりの最大フレームレートは60です。
- 表示メモリの制限。セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。デフォルトは65536KB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

です。高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は算出できます。

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介するXenAppおよびXenDesktopからの配信に最適化されています（たとえば、HDX RealTime Optimization Packを参照）。最適化されていないアプリケーションでは、HDX Webカメラビデオ圧縮を使用すると、セッションでのビデオ会議でWebカメラの帯域幅使用効率および遅延に対する耐性が向上します。この機能では、Webカメラのトラフィックが専用のマルチメディア仮想チャネルでストリーム配信されます。この機能では、HDX Plug-n-Play USBリダイレクトサポートのアイソクロナス転送に比べて帯域幅消費が少なく、WAN接続に適しています。

このデフォルト設定は、Citrix ReceiverユーザーがDesktop Viewerの［マイクとWebカメラ］設定で**[マイクおよびWebカメラを使用しない]**を選択することで無効になります。ユーザーがHDX Webカメラビデオ圧縮を無効にすることを禁止するには、ポリシーの［ICA］>［USBデバイス］の設定項目を使ってUSBデバイスのリダイレクトを無効にします。

HDX Webカメラビデオ圧縮を使用するには、以下のポリシー設定を有効にする必要があります（これらの設定項目はデフォルトで有効になっています）。

- クライアントオーディオリダイレクト
- クライアントマイクリダイレクト
- マルチメディア会議
- Windows Mediaリダイレクト

WebカメラでH.264ハードウェアエンコード機能がサポートされる場合、HDX Webカメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェアエンコードが使用されるようにするには、レジストリキーHKEY_CURRENT_USER\Software\Citrix\HdxRealTimeにDWORD値DeepCompress_ForceSWEncode=1を設定します。

QoS（Quality of Service）機能をサポートするルーターを使って単一セッションに複数の接続を使用する場合、ネットワークトラフィックの優先度を割り当てることができます。ユーザーデバイスとサーバー間のICAトラフィックでは、4つのTCPストリーム（リアルタイム、インタラクティブ、バックグラウンド、およびバルク）と2つのユーザーデータグラムプロトコル（UDP）ストリーム（ボイスおよびFramehawkディスプレイリモート）を使用できます。各仮想チャネルには特定の優先度が割り当てられており、対応する接続を使って転送が行われます。これらの仮想チャネルには、使用されるTCPポート番号に基づいて個別に優先度を設定できます。

Windows 10、Windows 8およびWindows 7マシンにインストールしたVirtual Delivery Agent（VDA）では、複数チャネルのストリーム接続がサポートされます。ネットワーク管理者に問い合わせて、［マルチポートポリシー］設定で指定したCGP（Common Gateway Protocol）ポートが、ネットワークルーター上で正しく割り当てられていることを確認してください。

QoS（Quality of Service）は、セッション画面の保持機能のポートまたはCGPポートが複数設定されている環境でのみサポートされます。

注意： この機能を使用する場合は、トランスポートセキュリティを使用してください。IPsec（Internet Protocol Security）またはTLS（Transport Layer Security）を使用することをお勧めします。TLS接続がサポートされるのは、マルチストリームICAをサポートするNetScaler Gatewayを通過するトラフィックのみです。企業内ネットワークでは、TLSを使用したマルチストリーム接続はサポートされません。

マルチストリーム接続のQoSを設定するには、ポリシーに以下のCitrixポリシー設定を追加します（詳しくは、マルチスト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リーム接続のポリシー設定」を参照してください）。

- マルチポートポリシー- 複数接続を介したICAトラフィックで使用されるポートおよびそのネットワーク優先度を指定します。
  - ［CGPデフォルトポートの優先度］ボックスの一覧で、優先度を選択します。デフォルトでは、プライマリポート（2598）に優先度［高］が設定されています。
  - ［CGPポート1］、［CGPポート2］、および［CGPポート3］ボックスに追加のCGPポートを入力して、それぞれ優先度を選択します。各ポートには異なる優先度を設定する必要があります。

  VDA側のファイアウォールで、追加したTCPトラフィックを明示的に許可する必要があります。
- マルチストリームコンピューター設定- この設定は、デフォルトでは無効になっています。Citrix NetScaler SD-WANでマルチストリーム機能をサポートする場合は、この設定項目を使用する必要はありません。このポリシー設定は、サードパーティ製のルーターや従来のBranch Repeaterを使用する環境でQoS（Quality of Service）優先度を指定するときに使用できます。
- マルチストリームユーザー設定 - この設定は、デフォルトでは無効になっています。

ポリシーの設定を反映させるには、ユーザーがネットワークに再ログオンする必要があります。

関連情報

> Graphics
> Multimedia
> General content redirection
> Adaptive transport

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アダプティブトランスポート

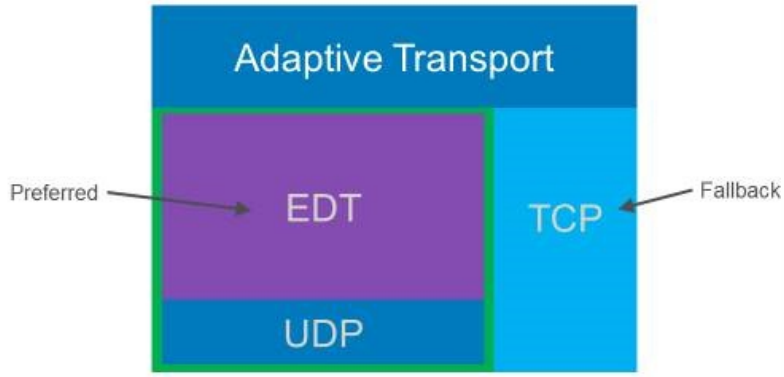
Apr 12, 2018

アダプティブトランスポートは、XenAppとXenDesktopの新しいデータ転送メカニズムです。高速で拡張性が高く、アプリケーションの対話機能が向上し、厳しい長距離のWANとインターネット接続でのインタラクティブ性を高めます。アダプティブトランスポートでは、サーバーの高スケーラビリティと帯域幅の使用効率が維持されます。アダプティブトランスポートを使用すると、ICA仮想チャネルはネットワーク状況の変化に自動的に対応します。Enlightened Data Transport（EDT）と呼ばれる新しいCitrixプロトコルとTCPとの間で、基になるプロトコルをインテリジェントに切り替えて、最適なパフォーマンスが実現されます。これにより、Thinwireディスプレイリモート、ファイル転送（クライアントドライブマッピング）、印刷、マルチメディアリダイレクトなど、すべてのICA仮想チャネルのデータスループットが向上します。同じ設定をLANとWANの両方の条件に適用できます。

[優先する]に設定すると、EDT経由のデータ転送がプライマリとして使用され、TCPにフォールバックします。

デフォルトでは、アダプティブトランスポートは無効（**オフ**）になっており、常にTCPが使用されます。

テスト目的で、**[診断モード]**に設定できます。このモードでは、EDTのみが使用され、TCPへのフォールバックは無効になります。



Citrix SD-WAN WAN最適化（WANOP）は、URLベースのビデオキャッシュを含むセッションを越えたトークン化圧縮（データ重複排除）を提供します。オフィスで2人以上のユーザーが同じクライアントが取得したビデオを見たり、同じファイルまたはドキュメントの大部分を転送または印刷したりする場合、WANOPによって大幅に帯域幅を削減できます。さらに、支社にあるアプライアンス上でICAデータ削減および印刷ジョブ圧縮プロセスを実行することにより、VDAサーバーのCPU負荷を軽減し、XenAppおよびXenDesktopサーバーでより高いスケーラビリティを実現します。

重要： TCPがデータ転送プロトコルとして使用される場合、Citrix WANOPは前の段落で説明した最適化をサポートします。ネットワーク接続でCitrix WANOPを使用する場合は、TCPを選択します。WANOPは、TCPフロー制御と輻輳制御を使用することにより、低速で中程度のパケット損失がある状況でEDTと同等の対話機能を提供できます。

- XenAppおよびXenDesktop：バージョン7.13以降
- デスクトップOS用VDA：バージョン7.13以降

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- サーバーOS用VDA：バージョン7.13以降
- StoreFront：バージョン3.9以降
- Citrix Receiver for Windows：バージョン4.7以降
- Citrix Receiver for Mac：バージョン12.5以降
- Citrix Receiver for iOS：バージョン7.2以降
- Citrix Receiver for Linux：直接VDA接続のみの場合はバージョン13.6、NetScaler Gatewayを使用するDTLSサポート（または直接VDA接続用のDTLS）の場合は13.7。
- Citrix Receiver for Android：直接VDA接続のみの場合はバージョン3.12.3、NetScaler Gatewayを使用するDTLSサポート（または直接VDA接続用のDTLS）の場合は3.13。
- IPv4 VDAのみIPv6およびIPv6とIPv4の混在構成はサポートされません。
- NetScaler：バージョン11.1-51.21以降。NetScaler構成について詳しくは、「Configuring NetScaler Gateway to support Advanced Transport」を参照してください。

1. XenAppおよびXenDesktopをインストールします。
2. StoreFrontをインストールします。
3. VDA（for Desktop OSまたはServer OS）をインストールします。
4. Citrix Receiver for Windows（Citrix Receiver for MacまたはCitrix Receiver for iOS）をインストールします。
5. Studioで、ポリシー設定「HDX Adaptive Transport」を有効化します（デフォルトでは無効）。また、この機能を、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。
   - ポリシー設定を有効にするには、値を［優先する］に設定し、［OK］をクリックします。
     - **優先する**：可能な場合、Adaptive transport over EDTが使用され、TCPにフォールバックします。
     - **診断モード。**EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングでのみお勧めします。
     - **Off。**TCPが強制的にオンになり、EDTが無効になります。
6. ［次へ］をクリックし、ウィザードの手順を完了します。
7. ユーザーがICAセッションに再接続するときに新しいポリシーが有効になります。任意で**gpupdate /force**を実行してポリシー設定をサーバーにプルできますが、ユーザーはやはりICAセッションを再接続する必要があります。
8. サポートされているCitrix Receiverからセッションを起動し、アダプティブトランスポートを使用して接続を確立します。
9. 外部アクセスをセキュリティで保護するために、NetScaler Unified Gateway上でDTLS暗号化を構成します。詳しくは、「Configuring NetScaler Gateway to support Advanced Transport」を参照してください。

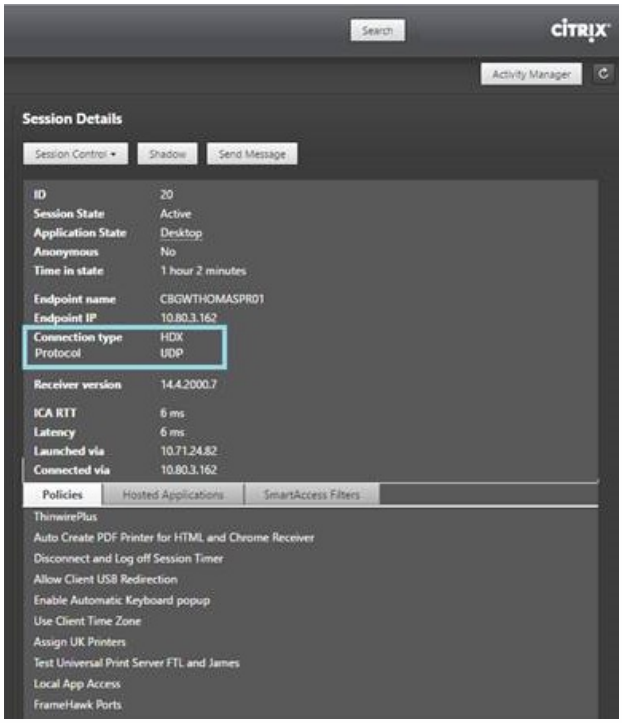
ポリシー設定の有効化を確認するには：

- **netstat -a**を使用して、ICAユーザーデータグラムプロトコル（UDP）サービスがVDA上で有効であることを確認します。
- **Director**または、VDAで利用できる**CtxSession.exe**コマンドラインユーティリティを使用して仮想チャネルがEDT経由で実行されていることを確認します。

Directorの使用例

Directorの**［セッション詳細］＞［接続の種類］**には、ポリシー設定が表示されます。［接続の種類］で**［HDX］**を探します。プロトコルが**［UDP］**の場合、EDTはこのセッションでアクティブです。プロトコルが**［TCP］**の場合、セッションはフォールバックしているか、デフォルトのモードです。［接続の種類］が**［RDP］**の場合、ICAは使用されておらず、プロトコルは、**［なし］**です。詳しくは、「セッションの監視」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



CtxSession.exeの例

この例は、UDP経由のEDTがアクティブなセッションを示しています。コマンドラインで「CtxSession.exe」と入力します。

```
C:\Program Files (x86)\Citrix\System32>CtxSession

セッション2のトランスポートプロトコル： UDP -> CGP -> ICA
```

詳細な統計情報を参照するには、-vスイッチを使用します。

```
>CtxSession -v
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

インストールと構成

Dec 05, 2017

個々の展開手順を開始する前に、参考記事を確認して、展開中に何が起こるか、何を指定する必要があるのかを前もって確認してください。

次の手順に従って、XenAppまたはXenDesktopを展開します。

準備

「インストールの準備」を確認し、必要なタスクをすべて完了します。

- コンセプト、機能、これまでのリリースとの差異、システム要件、およびデータベースに関する情報の参照先。
- コアコンポーネントのインストール先を決定する際の考慮事項。
- Active Directoryの権限と要件。
- 利用できるインストーラー、ツール、およびインターフェイスに関する情報。

コアコンポーネントのインストール

Delivery Controller、Citrix Studio、Citrix Director、Citrixライセンスサーバー、Citrix StoreFrontをインストールします。詳しくは、「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

サイトの作成

コアコンポーネントのインストール後、Studioを起動すると、操作は自動的にサイトの作成へ誘導されます。

1つまたは複数のVirtual Delivery Agent（VDA）のインストール

Windowsオペレーティングシステムが実行されているマシンにVDAをインストールします。このとき、マスターイメージにインストールすることも、各マシン上に直接インストールすることもできます。「VDAのインストール」または「コマンドラインを使ったインストール」を参照してください。Active Directory経由でVDAをインストールする場合のスクリプト例が用意されています。

Linuxオペレーティングシステムを使用しているマシンでは、「Linux Virtual Delivery Agent」のガイダンスに従ってください。

リモートPCアクセス機能を使用する場合は、オフィスにある各ユーザーのコンピューター上にVDA for Desktop OSをインストールします。コアVDAサービスのみが必要な場合は、スタンドアロンのVDAWorkstationCoreSetup.exeインストーラーと、既存の電子ソフトウェア配信（ESD）の方法を使用します。（利用できるVDAのインストーラーに関する完全な情報については、「インストールの準備」を参照してください。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

その他のオプションコンポーネントのインストール

Citrix Universal Print Serverの使用を計画している場合は、そのサーバーコンポーネントをプリントサーバーにインストールします。「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

StoreFrontでの認証オプション（SAMLアサーションなど）の使用を許可するには、Citrix Federated Authentication Serviceをインストールします。

エンドユーザーが自身のユーザーアカウントをより詳細に制御できるようにするには、セルフサービスパスワードリセットをインストールします。詳しくは、「セルフサービスパスワードリセット」ドキュメントを参照してください。

必要に応じて、XenApp/XenDesktop展開にCitrixコンポーネントをさらに統合します。

- Provisioning ServicesはXenAppおよびXenDesktopのオプションコンポーネントで、マスターイメージをターゲットデバイスにストリーム配信してマシンをプロビジョニングします。
- Citrix NetScaler Gatewayはアプリケーションアクセスのセキュリティを保護するソリューションで、詳細なアプリケーションレベルのポリシーと操作の制御機能を管理者に提供し、アプリケーションとデータへのアクセスのセキュリティを保護します。
- Citrix NetScaler SD-WANは、WAN接続のパフォーマンスを最適化するための一連のアプライアンスです。

インストールのガイダンスについては、これらのコンポーネント、機能、およびテクノロジに関するドキュメントを参照してください。

マシンカタログの作成

Studioでサイトの作成が完了すると、操作はマシンカタログの作成へ誘導されます。

カタログには、物理マシンまたは仮想マシン（VM）のどちらでも使用できます。仮想マシンはマスターイメージから作成できます。VMの提供に、ハイパーバイザーまたはクラウドサービスを使用している場合は、まず、そのホストにマスターイメージを作成します。その後、カタログ作成時に、このイメージを指定します。これはVMを作成するときに使用されます。

デリバリーグループの作成

Studioで1つ目のマシンカタログの作成が完了すると、操作はデリバリーグループの作成へ誘導されます。

デリバリーグループは、選択されたカタログにあるマシンにアクセスできるユーザーと、そのユーザーが利用可能なアプリケーションを指定します。

アプリケーショングループの作成（オプション）

デリバリーグループの作成後、オプションでアプリケーショングループを作成できます。さまざまなデリバリーグループで共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットで使用されるアプリケーションについて、アプリケーショングループを作成できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

インストールの準備

Mar 01, 2018

XenAppおよびXenDesktopの展開は、次のコンポーネントのインストールから始まります。このプロセスでは、アプリケーションとデスクトップをファイアウォール内のユーザーに配信する準備をします。

- 1つまたは複数のDelivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrixライセンスサーバー
- 1つまたは複数のCitrix Virtual Delivery Agent（VDA）
- オプションのコンポーネントやテクノロジ（たとえば、Universal Print Server、Federated Authentication Service、およびセルフサービスパスワードリセット）

ファイアウォール外のユーザーについては、NetScalerなどの追加コンポーネントをインストールして構成します。StoreFrontでNetScalerを使用する方法については、「XenAppおよびXenDesktopのNetScaler Gatewayとの統合」を参照してください。

コンポーネントをインストールできるようにするには

XenAppおよびXenDesktop ISOに含まれる全製品インストーラーを使用すると、多くのコンポーネントとテクノロジを展開できます。VDAは、スタンドアロンVDAインストーラーを使用してインストールできます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。「インストーラー」を参照してください。

> 製品ISOには、Active DirectoryのマシンのVDAをインストール、アップグレード、または削除するサンプルスクリプトも収録されています。また、これらのスクリプトを使ってMachine Creation Services（MCS）およびProvisioning Services（PVS）のマスターイメージを管理することもできます。詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

Citrix Smart Toolsではこれらのインストーラーを使用せずに、ブループリントを使用してXenAppおよびXenDesktopの展開環境を自動で作成します。詳しくは、Smart Toolsの製品マニュアルを参照してください 。

インストール前に確認する情報

- 製品の技術概要： 製品やそのコンポーネントに詳しくない場合。
- 7.xでの変更点： XenApp 6.xまたはXenDesktop 5.6展開環境から最新のバージョンに移行する場合。
- セキュリティ：展開環境について計画する場合。
- 既知の問題：このバージョンで起きる可能性がある問題。
- データベース：システムデータベースおよびこれらの設定方法について理解を深めてください。Controllerのインストール時に、サイトデータベース用にSQL Server Expressをインストールできます。コアコンポーネントをインストールした後のサイト作成時に、データベース情報のほとんどを設定します。
- リモートPCアクセス：ユーザーがオフィスの物理マシンにリモートでアクセスできる環境を展開している場合。
- 接続とリソース：ハイパーバイザーまたはクラウドサービスを使用してアプリケーションやデスクトップのVMマシンをホストまたはプロビジョニングしている場合。（コアコンポーネントをインストールした後の）サイト作成時に、最初の接続を構成することができます。仮想化環境はそれより前に、いつでも設定できます。
- Microsoft System Center Configuration Manager：ConfigMgrを使用してアプリケーションおよびデスクトップへのアク

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セスを管理しているか、リモートPCアクセスとともにWake on LAN機能を使用している場合。

コンポーネントのインストール先

サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。記載されているものを除いて、コンポーネントの必須条件は自動的にインストールされます。サポートされるプラットフォームと前提条件については、Citrix StoreFrontおよびCitrixライセンスサーバーのドキュメントを参照してください。

コアコンポーネントは、同じサーバー上にインストールしたり別のサーバー上にインストールしたりできます。

- 1つのサーバー上にすべてのコアコンポーネントをインストールすれば、評価展開、テスト展開、または小規模実稼働展開に使用できます。
- 将来の拡張に対応するには、異なるサーバーにコンポーネントをインストールすることを検討してください。たとえば、Controllerをインストールしたサーバーとは別のマシンにStudioをインストールすると、サイトをリモートで管理できます。
- 大部分の実稼働展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

Delivery ControllerとVDA for Server OSを同一サーバー上にインストールできます。インストーラーを起動して目的のDelivery Controller（およびマシンにインストールするその他のコンポーネント）を選択します。次に、もう一度インストーラーを起動してVirtual Delivery Agent for Server OSを選択します。

各オペレーティングシステムを最新の状態にアップデートしておく必要があります。たとえば、Windows更新プログラムKB2919355がインストールされていない場合、Windows Server 2012 R2へのControllerのインストールおよびWindows 8.1またはWindows Server 2012 R2へのVDAのインストールは失敗します。

すべてのマシンのシステムクロックを同期しておく必要があります。この同期は、Kerberosでマシン間の通信を保護するために必要です。

Windows 10マシンでの最適化ガイダンスは、CTX216252にあります。

コンポーネントのインストールが不適切な場所：

- Active Directoryドメインコントローラーには一切コンポーネントをインストールしないでください。
- SQL Serverクラスター化インストール、SQL Serverミラー化インストール、またはHyper-Vを実行しているサーバーにおけるノード上へのControllerのインストールはサポートされていません。
- XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2またはそれ以前のバージョンのXenAppが動作するサーバーにはStudioをインストールしないでください。

Active Directoryの権限と要件

コンポーネントをインストールするマシンのドメインユーザーおよびローカル管理者である必要があります。

スタンドアロンVDAインストーラーを使用するには、管理者権限を持っているか、**[管理者として実行]** を使用する必要があります。

インストールを開始する前に、Active Directoryドメインを設定してください。

- 「システム要件」に、サポートされるActive Directoryの機能レベルの一覧を示しています。詳細は「Active Directory」に記載されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Active Directoryドメインサービスを実行するドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーにXenAppまたはXenDesktopコンポーネントをインストールしないでください。
- Studioで組織単位名を指定するときは、スラッシュ（/）を使用しないでください。

Citrixライセンスサーバーのインストールに使用したWindowsユーザーアカウントが、そのライセンスサーバーのすべての管理タスクの実行権限を持つ委任管理者として自動的に設定されます。

さらに、以下の情報を参照してください。

- セキュリティに関する推奨事項
- 管理権限の委任
- Active Directoryの構成手順に関するMicrosoft社のドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

任意のコンポーネントのインストール時：
通常、コンポーネントの前提条件が存在していない場合は、インストーラーによってインストールされます。前提条件によっては、マシンの再起動が必要なものがあります。

インストールの前、最中、および後に作成するオブジェクトには、重複しない名前を指定してください。こうしたオブジェクトには、ネットワーク、グループ、カタログ、リソースなどがあります。

正しくインストールできないコンポーネントがあった場合は、インストールが停止してエラーメッセージが表示されます。この時点でインストール済みのコンポーネントは保持されるため、再インストールする必要はありません。

コンポーネントをインストール（またはアップグレード）すると、分析情報が自動的に収集されます。デフォルトでは、インストールの完了時に、そのデータがCitrixへ自動的にアップロードされます。また、コンポーネントをインストールすると、自動的にCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に登録され、匿名データがアップロードされます。インストール中に、メンテナンスやトラブルシューティングのために診断情報を収集するほかのCitrixプログラム（Smart Toolsなど）に参加することもできます。これらのプログラムについて詳しくは、「Citrix Insight Services」を参照してください。

VDAインストール時：

Citrix Receiver for Windowsは、VDAWorkstationCoreSetup.exeインストーラーを使用する場合を除き、VDAをインストールするときにデフォルトで含まれます。Citrix Receiverはインストールから除外できます。Citrix Receiverおよび他のCitrix Receiverは、管理者またはユーザーがCitrix Webサイトからダウンロードできます。また、StoreFrontサーバーでこれらのCitrix Receiverを公開することもできます。「Citrix Receiverインストールファイルをサーバーから入手できるようにする」、または使用しているStoreFrontバージョンの該当するコンテンツを参照してください。

サポートされるWindowsサーバーでは、印刷スプーラーサービスがデフォルトで有効になります。このサービスを無効にすると、WindowsサーバーOSに対してVDAを正常にインストールできなくなるため、このサービスが有効であることを確認してからVDAをインストールしてください。

サポートされているほとんどのWindowsのエディションには、Microsoft Media Foundationが既にインストールされています。マシンにMedia Foundationがインストールされていない場合（Nエディション等）は、複数のマルチメディア機能がインストールされず、動作しません。その制限を認識するか、VDAのインストールを中止して、Media Foundationをインストールした後に再開してください。グラフィカルユーザーインターフェイス上に、この選択がメッセージとして表示されます。制限を認識するには、コマンドラインで/no_mediafoundation_ackを使用してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAをインストールすると、Direct Access Usersと呼ばれる新しいローカルユーザーグループが自動的に作成されます。VDA for Desktop OSでは、このグループはRDP接続のみに適用されます。VDA for Server OSでは、このグループはICA接続とRDP接続に適用されます。

VDAには、通信を行うControllerの有効なアドレスが保持されている必要があります。保持されていない場合は、セッションを確立することができません。Controllerのアドレスは、VDAのインストール時に指定することも、後で指定することもできます。ただし、必ず指定しなければならないことを覚えておいてください。

VDAインストール時およびその後の再起動：

VDAのインストールプロセスの最後にマシンを再起動する必要があります。デフォルトでは、再起動は自動で行われます。

VDAインストール中の再起動の回数を最小限に抑えるには：

- VDAのインストールが開始される前に.NET Frameworkバージョンがインストールされていることを確認してください。
- WindowsサーバーOSマシンでは、RDSの役割サービスをインストールして有効にしてからVDAをインストールしてください。

VDAインストール前にこれらの前提条件をインストールしない場合：

- グラフィカルインターフェイスを使用した場合、またはコマンドラインインターフェイスを/norebootオプションなしで使用した場合、前提条件のインストール後にマシンが自動で再起動します。
- コマンドラインインターフェイスで/norebootオプションを使用した場合、手動で再起動を開始する必要があります。

再起動するたびに、もう一度インストーラーまたはコマンドを実行してVDAインストールを続行します。

インストーラー

XenAppおよびXenDesktop ISOで提供される全製品インストーラーを使用して、以下のことができます。

- XenAppおよびXenDesktopコアコンポーネント（Delivery Controller、Studio、Director、StoreFront、License Server）のインストール、アップグレード、または削除
- サーバーまたはデスクトップオペレーティングシステム用のWindows VDAのインストールまたはアップグレード
- プリントサーバーへのUniversal Print Server Ups Serverコンポーネントのインストール
- Federated Authentication Serviceのインストール
- セルフサービスパスワードリセットサービスのインストール

（Webサイト開発などで）1人のユーザー用にServer OSからデスクトップを配信するには、全製品インストーラーのコマンドラインインターフェイスを使用します。詳しくは、「サーバーVDI」を参照してください。

スタンドアロンVDAインストーラーはCitrixのダウンロードページから入手できます。スタンドアロンVDAインストーラーは全製品ISOよりはるかにサイズが小さいです。これらのインストーラーを使用すると、以下のような展開環境に簡単に対応することができます。

- ステージングするかまたはローカルにコピーした電子ソフトウェア配信（ESD）パッケージを使用する環境
- 物理マシンのある環境
- リモートオフィスのある環境

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、自己抽出型のスタンドアロンVDA内のファイルはTempフォルダーに抽出されます。Tempフォルダーのドライブには、製品ISOのVDAインストーラーを使用する場合よりも多くの空き領域が必要です。ただし、インストールの完了後、Tempフォルダーに抽出されたファイルは自動的に削除されます。もしくは、絶対パスと/extractコマンドを使用できます。

3つのスタンドアロンVDAインストーラーを、ダウンロードで入手できます。

VDAServerSetup.exe：

VDA for Server OSをインストールします。全製品インストーラーで利用できるVDA for Server OSオプションをすべてサポートしています。

VDAWorkstationSetup.exe：

VDA for Desktop OSをインストールします。全製品インストーラーで利用できるVDA for Desktop OSオプションをすべてサポートしています。

VDAWorkstationCoreSetup.exe：

リモートPCアクセス展開またはコアVDIインストールに最適化されたVDA for Desktop OSをインストールします。リモートPC アクセスマシンでは物理マシンを使用します。コアVDIインストールとは、マスターイメージには使用されないVMのことを指します。コアVDIインストールでは、こうした展開環境へのVDA接続に必要なコアサービスのみがインストールされます。このため、全製品インストーラーまたはVDAWorkstationSetupインストーラーで有効であるオプションのサブセットだけがサポートされます。

このインストーラーは、次のものに使用されるコンポーネントをインストールしないか、含みません。

- App-V。
- Profile management。インストールからCitrix Profile managementを除外すると、Citrix Directorの表示に影響があります。詳しくは、「VDAのインストール」を参照してください。
- Machine Identity Service
- Personal vDiskまたはAppDisk。

VDAWorkstationCoreSetup.exeインストーラーにCitrix Receiver for Windowsは含まれておらず、インストールされません。

VDAWorkstationCoreSetup.exeを使用することは、全製品またはVDAWorkstationSetupインストーラーを使用してDesktop OS VDAをインストールすることと同等であり、次のどちらかでインストールします。

- グラフィカルインターフェイス：**[環境]** ページで［リモートPCアクセス］オプションを選択し、**[コンポーネント]** ページで［Citrix Receiver］チェックボックスをオフにする。
- コマンドラインインターフェイス：/remotepcオプションおよび/components vdaオプションを指定する。
- コマンドラインインターフェイス：/components vdaおよび/exclude "Citrix Personalization for App-V - VDA" "Personal vDisk" "Machine Identity Service" "Citrix User Profile Manager" "Citrix User Profile Manager WMI Plugin"を指定する。

全製品インストーラーを実行すれば、省略したコンポーネントおよび機能を後からインストールできます。この操作では、不足しているコンポーネントがすべてインストールされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Azure Resource Manager仮想化環境

Dec 05, 2017

XenAppまたはXenDesktop環境でMicrosoft Azure Resource Manager を使用して仮想マシンをプロビジョニングする場合は、このガイダンスに従ってください。

XenAppまたはXenDesktopを構成して、XenAppまたはXenDesktopサイトを作成したとき（接続の作成も含みます）または（サイトを作成してから）後でホスト接続を作成したときにリソースがAzure Resource Managerでプロビジョニングされるようにすることができます。

これを行うには、以下に関する知識が必要です。

- Azure Active Directory：https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-howto-tenant/
- 同意フレームワーク：https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-integrating-applications/
- サービスプリンシパル：https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-application-objects/

Machine Creation Servicesを使用している場合、Azure Disk Encryptionはサポートされません。

Azure Resource Managerへの接続の作成

サイトまたは接続を作成するウィザードのすべてのページについて詳しくは、「サイトの作成」と「接続とリソース」を参照してください。以下の情報は、Azure Resource Managerの接続に固有の詳細のみを扱っています。

Azure Resource Managerへのホスト接続を確立するには、次の2通りの方法があります。

- Azure Resource Managerを認証して新しいサービスプリンシパルを作成する。
- 以前作成されたサービスプリンシパルからの詳細を使ってAzure Resource Managerに接続する。

始める前に、以下の項目について確認してください。

- サブスクリプションのAzure Active Directoryテナントにユーザーアカウントがあること。
- Azure ADのユーザーアカウントが、リソースのプロビジョニングに使用するAzureサブスクリプションの共同管理者でもあること。

サイトのセットアップまたは接続およびリソースの追加ウィザードで以下を行います。

1. **[接続]**ページで、接続の種類に**[Microsoft Azure]**を選択し、Azure環境を選択します。
2. **[接続の詳細]**ページで、AzureサブスクリプションIDと接続の名前を入力します。接続名は1～64文字にし、空白スペースのみにしたり記号（\/:;#.*?=<>|[]{}'"()'）を含めたりすることはできません。サブスクリプションIDおよび接続名を入力すると、**[新規作成]**ボタンが有効になります。
3. Azure Active Directoryアカウントのユーザー名とパスワードを入力します。
4. **[サインイン]**をクリックします。
5. **[承認]**をクリックして一覧表示されている権限をXenAppまたはXenDesktopに付与します。XenAppまたはXenDesktopによって、指定されたユーザーの代わりにAzure Resource Managerリソースを管理することを許可するサービスプリンシパルが作成されます。
6. **[承認]**をクリックすると、Studioの**[接続]**ページに戻ります。Azureの認証が完了すると、**[新規作成]**および**[既存を使用]**ボタンが**[接続済み]**に置き換わり、Azureサブスクリプションへの正常な接続を示す緑色のチェックマークが表

© 1999-2017 Citrix Systems, Inc. All rights reserved.

示されます。

7. 仮想マシンの作成にどのツールを使用するかを指定し、**[次へ]** をクリックします。（Azureの認証が完了し、必要な権限の付与を承認しない限り、ウィザードのこのページより先に進むことはできません）。

リソースには領域とネットワークが含まれます。

- **[リージョン]** ページで領域を選択します。
- **[ネットワーク]** ページで以下の設定を行います。
  - 1～64文字のリソース名を入力して、Studioで領域とネットワークの組み合わせを特定できるようにします。ホスト名を空白スペースのみにすることはできず、ホスト名に記号（/:;#.*?=<>|[]{}'"()'）を含めることもできません。
  - 仮想ネットワークとリソースグループのペアを選択します（複数の仮想ネットワークを同じ名前にすることが可能なため、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります）。前のページで仮想ネットワークのない領域を選択した場合は、前のページに戻って仮想ネットワークのある領域を選択する必要があります。

ウィザードを完了します。

手動でサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続して、後述のPowerShellコマンドレットを使用します。

前提条件

- $SubscriptionId：VDAをプロビジョニングするサブスクリプションのAzure Resource Manager SubscriptionID。
- $AADUser：サブスクリプションのADテナントに対するAzure ADユーザーアカウント。
- $AADUserをサブスクリプションの共同管理者にしてください。
- $ApplicationName：Azure ADで作成されるアプリケーションの名前。
- $ApplicationPassword：アプリケーションのパスワード。このパスワードは、ホスト接続を作成するときのアプリケーションシークレットとして使用します。

サービスプリンシパルを作成するには、次の手順に従ってください。

手順1：Azure Resource Managerサブスクリプションに接続します。

```
Login-AzureRmAccount.
```

手順2：サービスプリンシパルを作成するAzure Resource Managerサブスクリプションを選択します。

```
Select-AzureRmSubscription -SubscriptionID $SubscriptionId;
```

手順3：ADテナントでアプリケーションを作成します。

```
$AzureADApplication = New-AzureRmADApplication -DisplayName $ApplicationName -HomePage
"https://localhost/$ApplicationName" -IdentifierUris https://$ApplicationName -Password $ApplicationPassword
```

手順4：サービスプリンシパルを作成します。

```
New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.ApplicationId
```

手順5：サービスプリンシパルに役割を割り当てます。

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
$AzureADApplication.ApplicationId –scope /subscriptions/$SubscriptionId
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順6：PowerShellコンソールの出力ウィンドウから、ApplicationIdをメモします。このIDは、ホスト接続を作成するときに使用します。

サイトのセットアップまたは接続およびリソースの追加ウィザードで以下を行います。

1. **[接続]** ページで、接続の種類に **[Microsoft Azure]** を選択し、Azure環境を選択します。
2. **[接続の詳細]** ページで、AzureサブスクリプションIDと接続の名前を入力します。（接続名は1～64文字にし、空白スペースのみにしたり記号（\/:;#.*?=<>|[]{}'"()'）を含めたりすることはできません）。
3. **[既存を使用]** をクリックします。サブスクリプションID、サブスクリプション名、認証URL、管理URL、ストレージのサフィックス、Active Directory IDまたはテナントID、アプリケーションID、および既存のサービスプリンシパルのアプリケーションシークレット。詳細を入力すると、 **[OK]** ボタンが有効になります。 **[OK]** をクリックします。
4. 仮想マシンの作成にどのツールを使用するかを指定し、 **[次へ]** をクリックします。入力したサービスプリンシパルの詳細は、Azureサブスクリプションへの接続に使用されます（［既存を使用］オプションの有効な詳細を入力しない限り、ウィザードの次のページに進めません）。

リソースには領域とネットワークが含まれます。

- **[リージョン]** ページで領域を選択します。
- **[ネットワーク]** ページで以下の設定を行います。
  - 1～64文字のリソース名を入力して、Studioで領域とネットワークの組み合わせを特定できるようにします。ホスト名を空白スペースのみにすることはできず、ホスト名に記号（/:;#.*?=<>|[]{}'"()'）を含めることもできません。
  - 仮想ネットワークとリソースグループのペアを選択します（複数の仮想ネットワークを同じ名前にすることが可能なため、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります）。前のページで仮想ネットワークのない領域を選択した場合は、前のページに戻って仮想ネットワークのある領域を選択する必要があります。

ウィザードを完了します。

Azure Resource Managerマスターイメージを使用して、マシンカタログを作成する

これは、「マシンカタログの作成」のガイダンスを補完する情報です。

マスターイメージは、マシンカタログの仮想マシンの作成に使用されることになるテンプレートです。マシンカタログを作成する前に、Azure Resource Managerでマスターイメージを作成します。マスターイメージの一般的な情報については、「マシンカタログの作成」を参照してください。

Studioでのマシンカタログを作成する場合は、以下を確認してください。

- **[オペレーティングシステム]** ページと **[マシン管理]** ページには、Azure固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
- **[マスターイメージ]** ページで、リソースグループを選択してからコンテナー内を移動（ドリルダウン）して、マスターイメージとして使用するAzure VHDに移動します。VHDにはCitrix VDAがインストールされている必要があります。仮想マシンにVHDが接続されている場合、仮想マシンを停止する必要があります。
- **[ストレージとライセンスの種類]** ページは、Azure Resource Managerマスターイメージを使用しているときのみ表示されます。

  ストレージの種類（StandardまたはPremium）を選択します。ストレージの種類は、ウィザードの仮想マシンページで提供されるマシンのサイズに影響します。これらのストレージの種類はどちらも、単一のデータセンター内でデータの

© 1999-2017 Citrix Systems, Inc. All rights reserved.

複数の同期コピーを作成します。Azureのストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください。

https://azure.microsoft.com/ja-jp/documentation/articles/storage-introduction/

https://azure.microsoft.com/ja-jp/documentation/articles/storage-premium-storage/

https://azure.microsoft.com/ja-jp/documentation/articles/storage-redundancy/

既存のオンプレミスのWindows Serverライセンスを使用するかどうかを選択します。既存のオンプレミスのWindows Serverイメージを使用する場合にそのように選択すると、Azure Hybrid Use Benefits（HUB）が利用されます。詳しくは、https://azure.microsoft.com/pricing/hybrid-use-benefit/を参照してください。

HUBを使用すると、AzureギャラリーからWindows Serverライセンスを追加する価格が不要になるため、Azureでの仮想マシン実行のコストがベース計算レートまで低下します。HUBを使用するためのオンプレミスのWindows Serversイメージを Azureに用意する必要があります。Azureギャラリーのイメージはサポートされません。オンプレミスのWindows Clientライセンスは、現在サポートされていません。https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/%23comment-145を参照してください。

プロビジョニングされた仮想マシンがHUBを正常に利用しているかどうか確認するには、powershellコマンド

```
Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
```

を実行し、ライセンスの種類がWindows_Serverであることを確認します。追加の説明は、https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/にあります。

- **[仮想マシン]** ページで、作成する仮想マシンの数を指定します。少なくとも1つは指定してください。マシンのサイズを選択します。マシンカタログを作成した後で、マシンのサイズを変更することはできません。後で他のサイズに変更したくなった場合は、カタログを削除してから、同じマスターイメージを使用した新しいカタログを作成し、希望のマシンサイズを指定します。

  仮想マシンの名前に、ASCII以外の文字や特殊文字を含めることはできません。

- **[ネットワークカード]** ページ、**[コンピューターアカウント]** ページ、および **[概要]** ページには、Azure固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Azure仮想化環境

Dec 05, 2017

コネクション構成

Studioを使用して、Microsoft Azure接続を作成する場合、Microsoft Azure発行設定ファイルの情報が必要です。各サブスクリプションで使用されるこのXMLファイルには、以下の例にあるような情報が入っています（実際の管理証明書はこれよりも長くなります）。

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl; sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

以下の手順では、Studioから接続を作成し、サイトの作成ウィザード、または接続の作成ウィザードのどちらかを起動したことを前提にしています。

1. Webブラウザーで、https://manage.windowsazure.com/publishsettings/indexに移動します。
2. 発行設定ファイルをダウンロードします。
3. Studioで、ウィザードの **[接続]** ページからMicrosoft Azureの接続の種類を選択し、［インポート］をクリックします。
4. 複数のサブスクリプションがある場合は、目的のサブスクリプションを選択するためのプロンプトが表示されます。

IDと証明書が自動的にStudioにインポートされます。メッセージやプロンプトは表示されません。

接続を使った電源操作は、しきい値に左右されます。一般に、デフォルト値が適切で、変更すべきではありません。ただし、接続を編集して、変更することができます（接続を作成するときには、これらの値は変更できません）。詳しくは、「接続の編集」を参照してください。

仮想マシン

Studioでマシンカタログを作成する場合、各仮想マシンのサイズの選択は、Studioの示すオプション、選択したVMインスタンスの種類のコストとパフォーマンス、およびスケーラビリティに左右されます。

Studioは、Microsoft Azureによって利用可能にされたVMインスタンスオプションをすべて、選択された領域に表示します。Citrixはこの表示を変更できません。したがって、自分が使用しているアプリケーションとそのCPU、メモリ、I/O要件を熟知しておく必要があります。価格やパフォーマンスの異なる選択肢がいくつか用意されています。Microsoftのサイトで以下の記事を参照して、オプションをよく理解してください。

- MSDN – Azure の仮想マシンおよびクラウドサービスのサイズ :https://msdn.microsoft.com/ja-jp/library/azure/dn197896.aspx
- 仮想マシンの価格 : https://azure.microsoft.com/ja-jp/pricing/details/virtual-machines/

Basic層 : 接頭辞「Basic」がついたVMは基本ディスクを表します。これらは当初、MicrosoftのサポートするIOPSのレベルが300に制限されています。デスクトップOS（VDI）やサーバーOS RDSH（リモートデスクトップセッションホスト）のワークロードには推奨されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Standard層： Standard層のVMには、4シリーズがあります。 A、D、DS、Gです。

シリーズ	Studioでの表示
A	極小、小、中、大、極大、A5、A6、A7、A8、A9、A10、A11。デスクトップOS（VDI）ワークロードを使ったテストには中、サーバーOS（RDSH）ワークロードの場合は大を推奨します。
D	Standard_D1、D2、D3、D4、D11、D12、D13、D14。これらのVMは一時ストレージ用にSSDを提供します。
DS	Standard_DS1、DS2、DS3、DS4、DS11、DS12、DS13、DS14。これらのVMはすべてのディスクにローカルSSDストレージを提供します。
G	Standard_G1～G5。これらVMは高性能コンピューティング用です。

Azure Premium Storageでマシンのプロビジョニングを行う場合、Premium Storageのアカウントでサポートされているマシンサイズを選択してください。

日本での、VMインスタンス1つの1時間当たりのコストについては、
https://azure.microsoft.com/ja-jp/pricing/details/virtual-machines/を参照してください。

クラウド環境では、実際のコンピューティング要件を理解することが重要です。概念実証などのテスト作業では、高性能な種類のVMインスタンスを使いたくなるかもしれません。また、コスト節減のため、性能の低いVMを使いたくなることもあるでしょう。タスクに見合ったVMを使用するようにしましょう。最高のパフォーマンスで始めても、必要な結果を得られないことがありますし、時間の経過に伴って、場合によっては1週間以内に、コストが非常に高額になります。パフォーマンスが低く、コストも安い種類のVMインスタンスでは、パフォーマンスとユーザーの操作性がタスクに適さない可能性があります。

デスクトップOS（VDI）またはサーバーOS（RDSH）ワークロードの場合、中程度のワークロードに対してLoginVSIを使用したテスト結果から、インスタンスの種類に中（A2）と大（A3）を選択すると、価格性能比が最高になることがわかりました。

中（A2）と大（A3またはA5）は、ワークロードの評価において、最高の価格性能比を発揮します。これ以下の設定はお勧めしません。より高い性能を持つ7VMシリーズはアプリケーションやユーザーが要求するパフォーマンスや操作性をもたらすかもしれませんが、性能の高い種類のVMインスタンスに本当の価値があるかどうかを判断するには、これら3種類のインスタンスの1つを基準にするのが一番です。

ホストユニットでのカタログのスケーラビリティに影響を与える制約は数種類あります。Azureサブスクリプションにある CPUコアの個数など、Microsoft Azureのサポートに連絡して、デフォルト値（20）を増やしてもらえば緩和される制約もあります。また、仮想ネットワークにおけるサブスクリプション1件あたりのVM数（2048）など、変更できないものもあります。

現在、Citrixはカタログ1つあたり40個のVMをサポートしています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1カタログまたはホストあたりのVM数を増やすには、Microsoft Azureサポートにお問い合わせください。Microsoft Azureのデフォルト制限は、VMがある一定の数以上に増加するのを阻止しています。ただし、この制限は頻繁に変更されますので、http://azure.microsoft.com/ja-jp/documentation/articles/azure-subscription-service-limits/で最新情報を確認してください。

Microsoft Azure仮想ネットワーク1つあたり、サポートされているVMの数は最高2048個です。

Microsoftは、1クラウドサービスあたりの標準ディスクVMの数を40に制限するよう推奨しています。拡張する場合は、接続全体に含まれるVMの個数に対して必要なクラウドサービスの数を考慮してください。また、ホストされたアプリケーションの提供に必要なVMSも考えましょう。

ワークロードをサポートするために、CPUコアのデフォルトの制限値を引き上げる必要があるかどうかの判断は、Microsoft Azureのサポートにご相談ください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft System Center Virtual Machine Manager仮想化環境

Dec 05, 2017

Hyper-VとMicrosoft System Center Virtual Machine Manager（VMM）を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

このリリースは、「システム要件」に記載されたVMMバージョンをサポートします。

Provisioning ServicesおよびMachine Creation Servicesを使用して、次のものをプロビジョニングできます。

- 第1世代デスクトップまたはサーバーOSのVM
- 第2世代Windows Server 2012 R2、Windows Server 2016、Windows 10 VM（Secure Bootあり、またはなし）

- VMM 2012からVMM 2012 SP1またはVMM 2012 R2へのアップグレード
  VMMおよびHyper-Vホストの要件については、 http://technet.microsoft.com/ja-jp/library/gg610649.aspxを参照してください。 VMMコンソールの要件については、 http://technet.microsoft.com/ja-jp/library/gg610640.aspxを参照してください。

  Hyper-Vの混在クラスターはサポートされません。 混在クラスターとは、Hyper-V 2008とHyper-V 2012が混在するものなどを指します。

- VMM 2008 R2からVMM 2012 SP1へのアップグレード
  VMM 2008 R2を使用するXenDesktop 5.6をアップグレードする場合は、XenDesktopのダウンタイムを避けるため、次の順序でアップグレードしてください。
  1. VMM 2008 をVMM 2012にアップグレードします（これにより、XenDesktop 5.6とVMM 2012が動作することになります）。
  2. XenDesktopをアップグレードします（これにより、アップグレードされたXenDesktopとVMM 2012が動作することになります）。
  3. VMM を2012から2012 SP1にアップグレードします（これにより、アップグレードされたXenDesktopとVMM 2012 SPが動作することになります）。
- VMM 2012 SP1からVMM 2012 R2へのアップグレード
  VMM 2012 SP1を使用するXenDesktopまたはXenApp 7.xをアップグレードする場合は、ダウンタイムを避けるため、次の順序でアップグレードしてください。
  1. XenDesktopまたはXenAppをアップグレードします（これにより、アップグレードされたXenDesktopまたは XenAppとVMM 2012 SP1が動作することになります）。
  2. VMM 2012 SP1をVMM 2012 R2にアップグレードします（これにより、アップグレードされたXenDesktopまたはXenAppとVMM 2012 R2が動作することになります）。

1. ハイパーバイザーをインストールして構成します。
   1. サーバー上にMicrosoft Hyper-V ServerおよびVMMをインストールします。すべてのDelivery ControllerがVMMサーバーと同じフォレストに含まれている必要があります。
   2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。
   3. 次のアカウント情報を確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Studioでホストを指定するために使用するアカウントは、VMM管理者またはそのHyper-VマシンのVMM委任管理者である必要があります。このアカウントにVMMの委任管理者の役割のみがある場合は、ホストの作成時にストレージデータがStudioの一覧に表示されません。
- Studio統合に使用されるユーザーアカウントは、仮想マシンのライフサイクル管理（仮想マシンの作成、更新、および削除など）を実行できるように、各Hyper-Vサーバー上のAdministratorsローカルセキュリティグループのメンバーでもある必要があります。

注： Hyper-Vが動作するサーバー上にControllerをインストールすることはサポートされていません。

2. マスター仮想マシンを作成します。
   1. マスター仮想マシンにVirtual Delivery Agentをインストールします。このとき、デスクトップを最適化するオプションを選択してください。これにより、パフォーマンスが向上します。
   2. バックアップのため、マスター仮想マシンのスナップショットを作成します。
3. 仮想デスクトップを作成します。MCSを使用して仮想マシンを作成する場合、サイトまたは接続の作成時に次の手順に従います。
   1. ホストの種類として［Microsoft仮想化］を選択します。
   2. アドレスとして、ホストサーバーの完全修飾ドメイン名を入力します。
   3. 新しいVMを作成する権限を持つ、先にセットアップした管理者アカウントの資格情報を入力します。
   4. ［ホスト詳細］ダイアログボックスで、仮想マシンの作成時に使用するクラスターまたはスタンドアロンホストを選択します。
      重要： 単一Hyper-Vホストによる展開でも、クラスターまたはスタンドアロンホストを参照して選択します。

SMB 3ファイル共有の仮想マシンストレージ上でMCSを使用して作成されたマシンカタログの場合、ControllerのHCL（Hypervisor Communications Library）からの呼び出しをSMBストレージに適切に接続できるよう、資格情報が以下の要件を満たしていることを確認する必要があります。

- VMMのユーザー資格情報には、SMBストレージに対する完全な読み取りおよび書き込みアクセス権限が必要です。
- 仮想マシンのライフサイクルイベント中のストレージ仮想ディスク操作では、Hyper-Vサーバーを介してVMMのユーザー資格情報が使用されます。

Windows Server 2012のHyper-VとVMM 2012 SP1でSMBをストレージとして使用する場合は、Controllerから各Hyper-VマシンへのCredSSP（Authentication Credential Security Support Provider）を有効にしてください。詳しくは、CTX137465を参照してください。

標準のPowerShell V3リモートセッションを使用すると、HCLはCredSSPを使ってHyper-Vマシンへの接続を開きます。この機能では、Kerberosで暗号化されたユーザーの資格情報がHyper-Vマシンに渡され、この資格情報（この場合はVMMユーザーの資格情報）を使用してリモートのHyper-Vマシン上のセッション内でPowerShellコマンドが実行されます。これにより、ストレージに対する通信コマンドが正しく動作します。

以下のタスクでは、HCLからHyper-Vマシンに送信されてSMB 3.0ストレージ上で動作するPowerShellスクリプトを使用します。

- **マスターイメージの統合** - マスターイメージにより、新しいMCSプロビジョニングスキーム（マシンカタログ）が作成されます。作成された新しいディスクから新しい仮想マシンを作成できるようにマスター仮想マシンを複製およびフラット化（および元のマスター仮想マシンの依存関係を削除）します。
  root\virtualization\v2名前空間でConvertVirtualHardDiskを実行します。

  次に例を示します。

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **差分ディスクの作成** - マスターイメージを統合して作成されたマスターイメージから差分ディスクを作成します。この差分ディスクは、新しい仮想マシンに接続されます。
  root\virtualization\v2名前空間でCreateVirtualHardDiskを実行します。

  例：
  ```
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
  $result = $ims.CreateVirtualHardDisk($vhdastext);
  $result
  ```
- **IDディスクのアップロード** - HCLでは、IDディスクをSMBストレージに直接アップロードすることはできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-VマシンはControlleからディスクを読み取れないため、HCLはHyper-Vマシンを介してIDディスクをコピーしておく必要があります。
  1. HCLは管理者共有を介してIDディスクをHyper-Vマシンにアップロードします。
  2. PowerShellリモートセッションで実行されるPowerShellスクリプトにより、Hyper-VマシンがIDディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、（リモートPowerShell接続を介して）そのフォルダーに対する権限がVMMユーザーのみにロックされます。
  3. HCLが管理者共有からファイルを削除します。
  4. HCLがHyper-VマシンへのIDディスクのアップロードを完了すると、リモートPowerShellセッションによってIDディスクはSMBストレージにコピーされ、Hyper-Vマシンから削除されます。
     IDディスクフォルダーが削除された場合は再作成され、再使用できるようになります。

- **IDディスクのダウンロード** - アップロードと同様に、IDディスクがHyper-VマシンからHCLに渡されます。次の処理により、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが作成されます（存在しない場合）。
  1. PowerShell V3リモートセッションで実行されるPowerShellスクリプトにより、Hyper-VマシンがSMBストレージからローカルのHyper-VストレージにIDディスクをコピーします。
  2. HCLがHyper-Vマシンの管理者共有からIDディスクをメモリ内に読み取ります。
  3. HCLが管理者共有からファイルを削除します。
- **Personal vDiskの作成** - 管理者がPersonal vDiskマシンカタログで仮想マシンを作成する場合、空のディスク（Personal vDisk）を作成する必要があります。
  空のディスクを作成する呼び出しでは、ストレージへの直接アクセスが不要です。メインまたはオペレーティングシステムディスクとは異なるストレージ上にPersonal vDiskがある場合は、リモートPowerShellを使って作成元の仮想マシンと同じ名前のディレクトリにPersonal vDiskを作成します。CSVまたはLocalStorageに対しては、リモートPowerShellを使用しないでください。空のディスクを作成する前にディレクトリを作成しておくと、VMMコマンドエラーを避けることができます。

  Hyper-Vマシンから、ストレージ上でmkdirを実行します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VMware仮想化環境

Dec 05, 2017

VMwareを使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

vCenter Serverおよび必要な管理ツールをインストールします（vSphere vCenterのリンクモードはサポートされません）。

MCSを使用する計画のある場合は、vCenter Serverのデータストアの参照機能を無効化しないでください（詳しくはhttps://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567を参照してください）。この機能を無効にすると、MCSが正しく動作しなくなります。

必要な権限

以下の権限の組み合わせまたはそのすべてを使用して、VMwareユーザーアカウントおよび1つまたは複数のVMwareの役割を作成します。さまざまなXenAppまたはXenDesktop処理をいつでも要求できるようにするためのユーザーの権限に必要な特定の粒度レベルでの役割作成をベースにしています。いつでもユーザー固有の権限を付与できるようにするために、DataCenter以上のレベルで、ユーザーを各役割に関連付けます。

以下のテーブルは、XenAppおよびXenDesktop処理と、最低限必要なVMWare権限の間のマッピングを示しています。

接続およびリソースの追加

SDK	ユーザーインターフェイス
System.Anonymous、System.Read、およびSystem.View	自動的に追加されます。組み込みの読み取り専用の役割を使用できます。

マシンのプロビジョニング（Machine Creation Services）

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[データストア] > [領域の割り当て]
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
Network.Assign	[ネットワーク] > [ネットワークの割り当て]
Resource.AssignVMToPool	[リソース] > [仮想マシンのリソースプールへの割り当て]
VirtualMachine.Config.AddExistingDisk	[仮想マシン] > [構成] > [既存ディスクの追加]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VirtualMachine.Config.AddNewDisk	[仮想マシン] > [構成] > [新規ディスクの追加]
VirtualMachine.Config.AdvancedConfig	[仮想マシン] > [構成] > [詳細]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Inventory.CreateFromExisting	[仮想マシン] > [インベントリ] > [既存のものから作成]
VirtualMachine.Inventory.Create	[仮想マシン] > [インベントリ] > [新規作成]
VirtualMachine.Inventory.Delete	[仮想マシン] > [インベントリ] > [削除]
VirtualMachine.Provisioning.Clone	[仮想マシン] > [プロビジョニング] > [仮想マシンのクローン作製]
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2およびvSphere 5.1, Update 1： [仮想マシン] > [状態] > [スナップショットの作成] vSphere 5.5： [仮想マシン] > [スナップショット管理] > [スナップショットの作成]

作成する仮想マシンにタグを設定する場合は、ユーザーアカウントに次の権限も必要です。

SDK	ユーザーインターフェイス
Global.ManageCustomFields	[グローバル] > [カスタム属性の管理]
Global.SetCustomField	[グローバル] > [カスタム属性の設定]

クリーンな基本イメージで新しい仮想マシンを作成できるように、Machine Creation Servicesで作成された仮想マシンにタグを設定して、基本イメージとして使用する仮想マシンの一覧から除外してください。

マシンのプロビジョニング（Provisioning Services）

「マシンのプロビジョニング（Machine Creation Services）」からのすべての権限と、次のSDKが必要です。

SDK	ユーザーインターフェイス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VirtualMachine.Config.AddRemoveDevice	［仮想マシン］>［構成］>［デバイスの追加または削除］
VirtualMachine.Config.CPUCount	［仮想マシン］>［構成］>［CPUカウントの変更］
VirtualMachine.Config.Memory	［仮想マシン］>［構成］>［メモリ］
VirtualMachine.Config.Settings	［仮想マシン］>［構成］>［設定］
VirtualMachine.Provisioning.CloneTemplate	［仮想マシン］>［プロビジョニング］>［テンプレートのクローン作成］
VirtualMachine.Provisioning.DeployTemplate	［仮想マシン］>［プロビジョニング］>［テンプレートの展開］

電源の管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	［Virtual machine］>［Interaction］>［Power Off］
VirtualMachine.Interact.PowerOn	［Virtual machine］>［Interaction］>［Power On］
VirtualMachine.Interact.Reset	［Virtual machine］>［Interaction］>［Reset］
VirtualMachine.Interact.Suspend	［Virtual machine］>［Interaction］>［Suspend］

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	［データストア］>［領域の割り当て］
Datastore.Browse	［データストア］>［データストアの参照］
Datastore.FileManagement	［データストア］>［低レベルのファイル操作］
Network.Assign	［ネットワーク］>［ネットワークの割り当て］

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Resource.AssignVMToPool	[リソース] > [仮想マシンのリソースプールへの割り当て]
VirtualMachine.Config.AddExistingDisk	[仮想マシン] > [構成] > [既存ディスクの追加]
VirtualMachine.Config.AddNewDisk	[仮想マシン] > [構成] > [新規ディスクの追加]
VirtualMachine.Config.AdvancedConfig	[仮想マシン] > [構成] > [詳細]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Inventory.CreateFromExisting	[仮想マシン] > [インベントリ] > [既存のものから作成]
VirtualMachine.Inventory.Create	[仮想マシン] > [インベントリ] > [新規作成]
VirtualMachine.Inventory.Delete	[仮想マシン] > [インベントリ] > [削除]
VirtualMachine.Provisioning.Clone	[仮想マシン] > [プロビジョニング] > [仮想マシンのクローン作製]

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VirtualMachine.Inventory.Delete	[仮想マシン] > [インベントリ] > [削除]

AppDiskの作成（VMware vSphereバージョン5.5以降とXenAppおよびXenDesktopバージョン7.8以降で有効）

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[データストア] > [領域の割り当て]
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.AddExistingDisk	[仮想マシン] > [構成] > [既存ディスクの追加]
VirtualMachine.Config.AddNewDisk	[仮想マシン] > [構成] > [新規ディスクの追加]
VirtualMachine.Config.AdvancedConfig	[仮想マシン] > [構成] > [詳細]
VirtualMachine.Config.EditDevice	[仮想マシン] > [構成] > [デバイス設定の変更]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]

AppDiskの削除（VMware vSphereバージョン5.5以降とXenAppおよびXenDesktopバージョン7.8以降で有効）

SDK	ユーザーインターフェイス
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

証明書の取得とインポート

vSphere通信を保護するため、HTTPではなくHTTPSを使用することをお勧めします。HTTPSを使用するにはデジタル証明書が必要です。組織のセキュリティポリシーに従って、証明書機関により発行されるデジタル証明書を使用することをお勧めします。

証明機関のデジタル証明書を使用できない場合は、VMwareによりインストールされる自己署名証明書を使用することもできます（組織のセキュリティポリシーで許可される場合）。VMware vCenterの証明書を各Controllerに追加します。次の手順に従います。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのホストファイル（%SystemRoot%/WINDOWS/system32/Drivers/etc/）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメイン名システムに登録されていない場合にのみ必要です。
2. 以下のいずれかの方法で、vCenterの証明書を入手します。
   - vCenterサーバーからコピーする。
     1. vCenterサーバー上のrui.crtファイルを、Delivery Controllerからアクセス可能な場所にコピーします。
     2. Controllerで、エクスポートした証明書の保存先に移動し、rui.crtファイルを開きます。
   - Webブラウザーでダウンロードする。Internet Explorerで証明書をダウンロードするには、Internet Explorerを右クリックして［管理者として実行］を選択しなければならない場合があります。
     1. Webブラウザーを開き、vCenterサーバーへの保護された接続（https://server1.domain1.comなど）を確立します。
     2. セキュリティに関する警告を受け入れます。
     3. 証明書のエラーが表示されるアドレスバーをクリックします。
     4. 証明書を表示して、［詳細］タブをクリックします。
     5. ［ファイルへコピー］を選択して、任意のファイル名を指定してCER形式でエクスポートします。
     6. エクスポートした証明書を保存します。
     7. エクスポートした証明書のCERファイルを開きます。
   - 管理者として実行するInternet Explorerで直接インポートする。
     1. Webブラウザーを開き、vCenterサーバーへの保護された接続（https://server1.domain1.comなど）を確立します。
     2. セキュリティに関する警告を受け入れます。
     3. 証明書のエラーが表示されるアドレスバーをクリックします。
     4. 証明書を表示します。
   - 各Controller上の証明書ストアに証明書をインポートします。
     1. ［証明書のインストール］をクリックして［ローカルマシン］を選択し、［次へ］をクリックします。
     2. ［証明書をすべて次のストアに配置する］を選択して、［参照］をクリックします。
     3. Windows Server 2008 R2の場合：
        1. ［物理ストアを表示する］チェックボックスをオンにします。
        2. ［信頼されたユーザー］を開きます。
        3. ［ローカルコンピューター］を選択します。
        4. ［次へ］をクリックし、［完了］をクリックします。

        Windows Server 2012、Windows Server 2012 R2、またはWindows Server 2016を使用している場合：

        1. ［信頼されたユーザー］を選択し、［OK］をクリックします。
        2. ［次へ］をクリックし、［完了］をクリックします。

重要：インストール後にvSphereサーバーの名前を変更する場合は、サーバー上で新しい自己署名証明書を作成してから、新しい証明書をインポートする必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理者は、ユーザーのデスクトップおよびアプリケーションを提供するためのマスター仮想マシンを作成します。ハイパーバイザーで、次の作業を行います。

1. マスター仮想マシンにVDAをインストールします。このとき、デスクトップを最適化するオプションを選択すると、パフォーマンスが向上します。
2. バックアップのため、マスター仮想マシンのスナップショットを作成します。

既存のマシンカタログを選択する代わりにStudioで仮想マシンを作成する場合は、仮想デスクトップ作成用のホストインフラストラクチャをセットアップするときに以下の情報を指定します。

1. ホストの種類としてVMware vSphereを選択します。
2. vCenter SDKのアクセスポイントのアドレスを入力します。
3. 新しい仮想マシンを作成する権限を持つ、既存のVMwareユーザーアカウントの資格情報を入力します。ユーザー名を「domain/username」形式で指定します。

VMware SSLの拇印機能は、VMware vSphereハイパーバイザーへのホスト接続を確立するときに頻繁に報告されるエラーに対処するためのものです。これまでは、接続を確立する前に、管理者がサイトのDelivery Controllerとハイパーバイザーの証明書の信頼関係を手動で作成する必要がありました。VMware SSLの拇印機能により、この手作業が不要になりました。信頼性されていない証明書の拇印がサイトのデータベースに保管されるようになったため、ハイパーバイザーは、Controllerから信頼されているとみなされない場合も、XenAppやXenDesktopからは常に信頼できるとみなされます。

StudioでvSphereのホスト接続を確立する場合、接続しようとしているマシンの証明書をダイアログボックスで見ることができます。その証明書を見て、信頼するかどうかを選択できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft System Center Configuration Manager環境

Dec 05, 2017

Microsoft System Center Configuration Manager（Configuration Manager）で物理デバイス上のアプリケーションやデスクトップへのアクセスを管理しているサイトでは、Configuration Managerの管理機能をXenAppやXenDesktop環境まで拡張できます。以下の統合オプションを使用できます。

- **Citrix Connector 7.5 for Configuration Manager 2012** — Citrix Connectorより、Configuration ManagerとXenApp/XenDesktopが連係して動作するようになります。Connectorを使用すると、Configuration Managerによる物理環境とXenApp/XenDesktopによる仮想環境の両方の保守・管理操作を統一させることができます。Connectorについて詳しくは、「Citrix Connector 7.5 for System Center Configuration Manager 2012」を参照してください。
- **Configuration Managerのウェイクアッププロキシ機能** — リモートPCアクセスのWake on LAN機能を使用するにはConfiguration Managerが必要です。詳しくは、後述の説明を参照してください。
- **XenApp/XenDesktopのプロパティ** — XenAppおよびXenDesktopのプロパティ設定により、Configuration Managerで管理するCitrix仮想デスクトップを識別できるようになります。これらのプロパティはCitrix Connectorにより自動的に設定されますが、以下で説明するように手作業での構成も可能です。

Microsoft System Center Configuration Managerでは仮想デスクトップを管理するためのプロパティを利用できます。

Configuration Managerに表示されるプロパティのブール値は、trueとfalseではなく1と0で表示されることがあります。

これらのプロパティは、 Root\Citrix\DesktopInformation名前空間のCitrix_virtualDesktopInfoクラスで使用できます。これらのプロパティの名前は、Windows Management Instrumentation（WMI）プロバイダーでのものです。

プロパティ	説明
AssignmentType	IsAssignedの値を設定します。以下の値を指定します。 • クライアントIP • ClientName • なし • User — これによりIsAssignedがTrueに設定されます。
BrokerSiteName	サイト名です。HostIdentifierと同じ値を返します。
DesktopCatalogName	デスクトップに関連付けられたマシンカタログの名前です。
DesktopGroupName	デスクトップに関連付けられたデリバリーグループの名前です。
HostIdentifier	サイト名です。BrokerSiteNameと同じ値を返します。
IsAssigned	デスクトップを各ユーザーに割り当てる場合はTrue、ランダムデスクトップの場合はFalseを設定します。
IsMasterImage	マスターイメージかどうかを指定します。たとえば、すべてのマシンがクリーンな状態で

© 1999-2017 Citrix Systems, Inc. All rights reserved.

プロパティ	説明
	起動するように、プロビジョニングされたマシン上ではなくマスターイメージ上にアプリケーションをインストールできます。以下の値を指定します。 • マスターイメージとして使用される仮想マシンではTrueになります（この値は、選択オプションに基づいてインストール時に設定されます）。 • マスターイメージからプロビジョニングされる仮想マシンではClearedになります。
IsVirtualMachine	仮想マシンではtrue、物理マシンではfalseになります。
OSChangesPersist	再起動時にデスクトップのオペレーティングシステムイメージをクリーンな状態にリセットする場合はfalse、リセットしない場合はtrueになります。
PersistentDataLocation	Configuration Managerが永続データを格納する場所です。ユーザーはアクセスできません。
PersonalvDiskDriveLetter	デスクトップでPersonal vDiskを使用する場合に、そのPersonal vDiskに割り当てるドライブ文字です。
BrokerSiteName、DesktopCatalogName、DesktopGroupName、HostIdentifier	デスクトップのコントローラーへの登録時に設定されるため、未登録のデスクトップではNullになります。

これらのプロパティを収集するには、Configuration Managerでハードウェアインベントリを実行します。プロパティを表示するには、Configuration Managerのリソースエクスプローラーを使用します。これらのインスタンスでは、名前にスペースが含まれたり、プロパティ名とわずかに違ったものになったりすることがあります。たとえば **BrokerSiteName**は、Broker Site Nameと表示されることがあります。

- Configuration Managerを構成してCitrix VDAからCitrix WMIプロパティを収集する。
- Citrix WMIプロパティを使用してクエリベースのデバイスコレクションを作成する。
- Citrix WMIプロパティに基づいてグローバル条件を作成する。
- グローバル条件を使用してアプリケーションの展開の種類の要件を定義する。

また、MicrosoftクラスのCCM_DesktopMachineのMicrosoftプロパティをRoot\ccm_vdi名前空間で使用することもできます。詳しくは、Microsoft社のドキュメントを参照してください。

リモートPCアクセスのWake on LAN機能を構成するには、以下のタスクを完了してから社内PCにVDAをインストールし、StudioでリモートPCアクセス展開を作成または編集します。

- 組織内でConfigMgr 2012、2012 R2、または2016を構成します。リモートPCアクセス用のすべてのマシンにConfigMgrクライアントを展開し、スケジュールされているSCCMインベントリサイクルが実行されるのを待ちます（必要に応じて、手動で強制的に実行することもできます）。StudioでConfigMgr接続を構成するときのアクセス資格情報には、セキュリティスコープにコレクションが含まれており、リモートツールオペレーターロールが付与されている必要があります。
- Intel社のActive Management Technology（AMT）を使用する場合。
  - PCでAMT 3.2.1以降がサポートされている必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - 適切な資格情報およびプロビジョニングプロセスを使用して、PCでAMTが使用されるようにプロビジョニングします。
    - ConfigMgr 2012と2012 R2のみを使用できます。ConfigMgr 2016は使用できません。
- ConfigMgrのウェイクアッププロキシやマジックパケットを使用する場合。
    - 各PCのBIOS設定で、Wake on LAN機能を有効にします。
    - ウェイクアッププロキシの場合は、ConfigMgrでウェイクアッププロキシを有効にします。リモートPCアクセスのWake on LAN機能を使用するPCが属する各サブネットで、センチネルマシンとして動作可能なものが3台以上あることを確認します。
    - マジックパケットの場合は、サブネット宛てのブロードキャストまたはユニキャストを使用して、ネットワーク経路およびファイアウォールでパケットの転送がブロックされないようにします。

社内PC上にVDAをインストールしたら、Studioでリモート PCアクセス展開を作成するときに電源管理機能を有効または無効にします。

- 電源管理機能を有効にする場合は、接続の詳細としてConfigMgrのアドレス、アクセス資格情報、および名前を指定します。
- 電源管理機能を無効にした場合でも、電源管理（Configuration Manager）接続を後から追加して、リモートPCアクセスのマシンカタログを編集してこの接続を指定し、電源管理機能を有効にできます。

電源管理接続を編集すると、ConfigMgrのウェイクアッププロキシやマジックパケットの使用、およびパケットの転送方法を構成できます。

詳しくは、「リモートPCアクセス」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nutanix仮想化環境

Mar 01, 2018

XenAppまたはXenDesktop環境でNutanix Acropolisを使用して仮想マシンを提供する場合は、このガイダンスに従ってくださ
い。セットアップ処理には、次のタスクが含まれます。

- XenAppまたはXenDesktop環境にNutanixプラグインをインストールして登録する。
- Nutanix Acropolisハイパーバイザーとの接続を作成する。
- Nutanixハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成する。

詳しくは、Nutanixサポートポータルにある『Nutanix Acropolix MCSプラグインのインストールガイド：
https://portal.nutanix.com』を参照してください。

NutanixおよびProvisioning Servicesに関するサポート情報については、Knowledge Centerの記事CTX131239を参照してくだ
さい。

Nutanixプラグインのインストールと登録

XenAppまたはXenDesktopコンポーネントをインストールした後、次の手順に従って、Delivery ControllerにNutanixプラグイ
ンをインストールして登録します。これにより、Studioを使用してNutanixハイパーバイザーとの接続を作成し、Nutanix環境
で作成したマスターイメージのスナップショットを使用するマシンカタログを作成できるようになります。

1. NutanixプラグインをNutanixから入手して、Delivery Controllerにインストールします。
2. C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0にNutanix Acropolisフォルダーが作成さ
   れたことを確認します。
3. **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot "C:\Program
   Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"**を実行します。
4. Citrix Host Service、Citrix Broker Service、およびCitrix Machine Creation Serviceを再起動します。
5. 次のPowerShellコマンドレットを実行して、Nutanix Acropolisプラグインが登録されたことを確認します。

   Add-PSSnapin Citrix*
   Get-HypHypervisorPlugin

Nutanixとの接続の作成

接続を作成するウィザードのすべてのページについて詳しくは、「サイトの作成」と「接続とリソース」を参照してくださ
い。

サイトのセットアップまたは接続およびリソースの追加ウィザードの**[接続]**ページで、接続の種類に**[Nutanix]**を選択
し、ハイパーバイザーのアドレスと資格情報、接続の名前を指定します。**[ネットワーク]**ページで、ホスティングユニッ
トのネットワークを選択します。

Nutanixスナップショットを使用するマシンカタログの作成

© 1999-2017 Citrix Systems, Inc. All rights reserved.

これは、「マシンカタログの作成」のガイダンスを補完する情報です。Nutanixに固有のフィールドのみを説明しています。

選択するスナップショットは、マシンカタログの仮想マシンの作成に使用されることになるテンプレートです。マシンカタログを作成する前に、Nutanixでイメージとスナップショットを作成します。

- マスターイメージの一般的な情報については、「マシンカタログの作成」を参照してください。
- Nutanixでイメージとスナップショットを作成する手順については、上述のNutanixのドキュメントを参照してください。

[オペレーティングシステム] ページと **[マシン管理]** ページには、Nutanix固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。

[コンテナー] ページ（Nutanix固有のページ）で、仮想マシンのディスクを配置するコンテナーを選択します。

[マスターイメージ] ページで、イメージのスナップショットを選択します。XenAppおよびXenDesktopで使用するAcropolisのスナップショット名は、"XD_"ではじめる必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新された一覧を表示します。

[仮想マシン] ページで、仮想CPUの数と各仮想CPUのコアの数を指定します。

[ネットワークカード] ページ、 **[コンピューターアカウント]** ページ、および **[概要]** ページには、Nutanix固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コアコンポーネントのインストール

Dec 05, 2017

コアコンポーネントとは、Delivery Controller、Studio、Director、StoreFront、およびLicense Serverです。

重要： インストールを始める前に、「インストールの準備」を確認してください。また、インストールを開始する前にこの記事を確認してください。

この記事では、コアコンポーネントをインストールする場合のインストールウィザードの手順を説明します。同等の機能をもつコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順1：製品ソフトウェアをダウンロードしてウィザードを起動する

Citrixアカウント資格情報を使用して、XenAppおよびXenDesktopのダウンロードページにアクセスします。製品のISOファイルをダウンロードします。

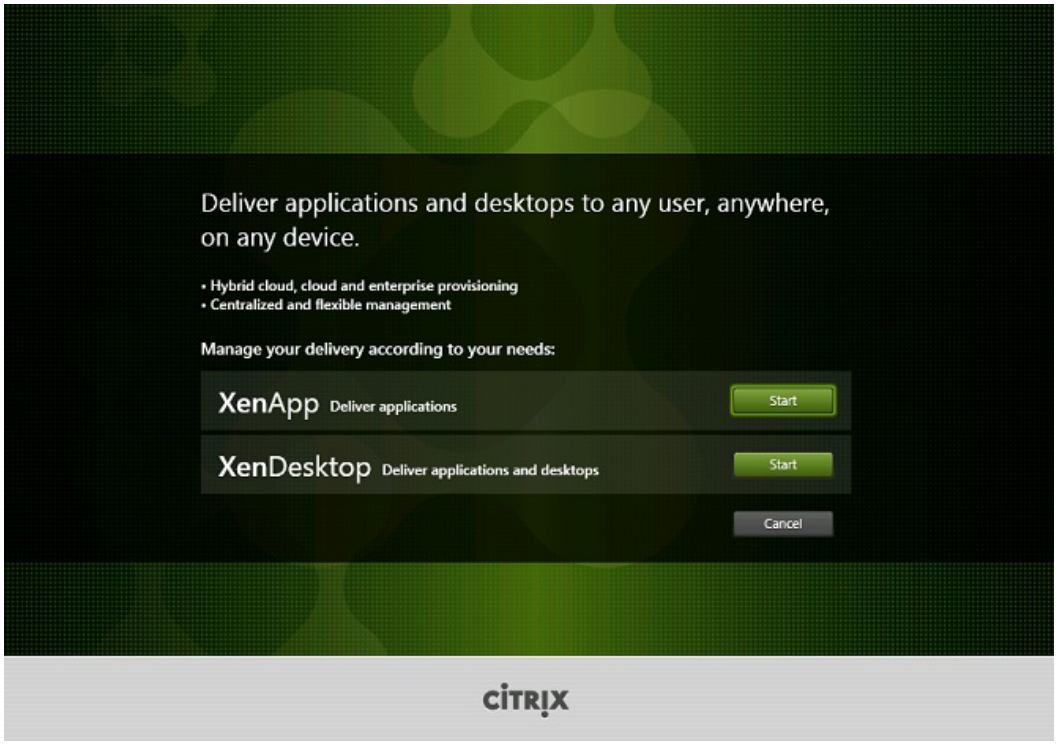
ファイルを解凍します。必要な場合は、ISOファイルからDVDを作成します。

ローカルの管理者アカウントを使って、コアコンポーネントのインストール先マシンにログオンします。

DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**ファイルまたはマウントしたドライブをダブルクリックします。

手順2：インストールする製品を選択する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



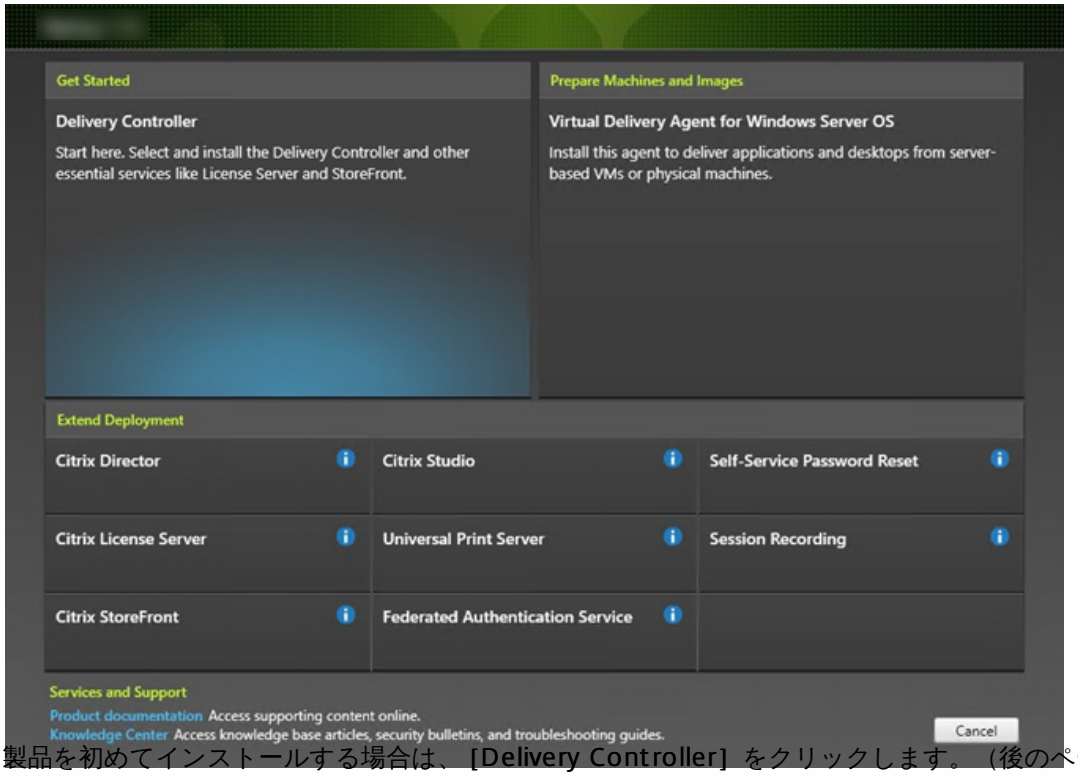
インストールする製品の隣の **[開始]** をクリックします： XenAppまたはXenDesktop。

（マシンにXenAppまたはXenDesktopコンポーネントが既にインストールされている場合、このページは表示されません）。

コマンドラインオプション： XenAppをインストールする場合は/xenapp。オプションを省略するとXenDesktopがインストールされます

手順3：インストールするものを選択する

© 1999-2017 Citrix Systems, Inc. All rights reserved.

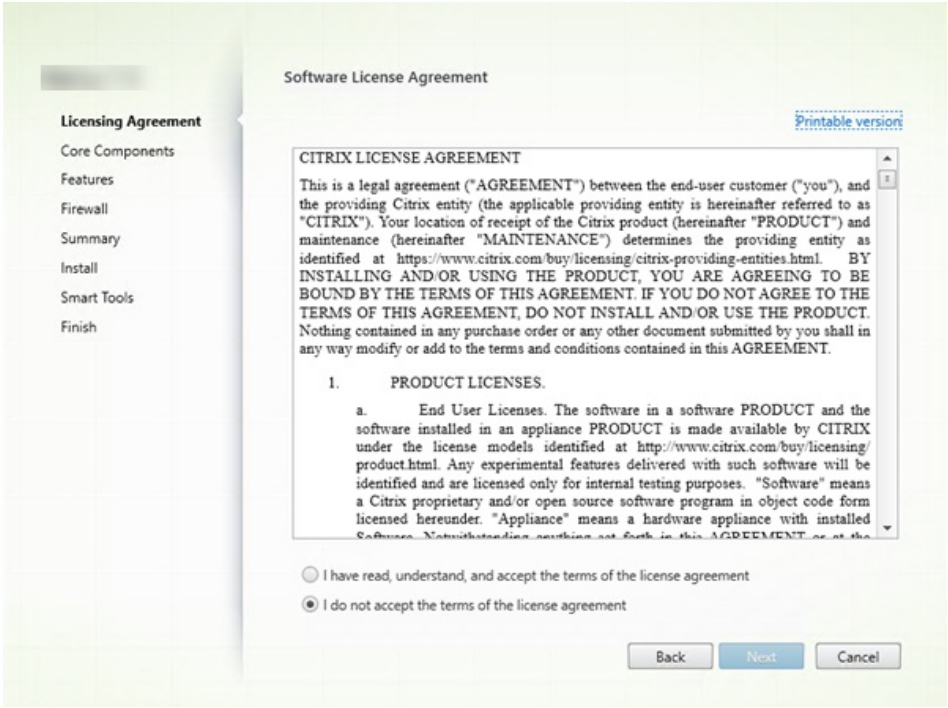


製品を初めてインストールする場合は、[Delivery Controller] をクリックします。（後のページで、このマシンにインストールする特定のコンポーネントを選択します）。

Controllerが（このマシンまたは別のマシンに）既にインストールされていて、別のコンポーネントをインストールする場合は、［拡張展開］セクションからコンポーネントを選択します。

コマンドラインオプション： /controllers

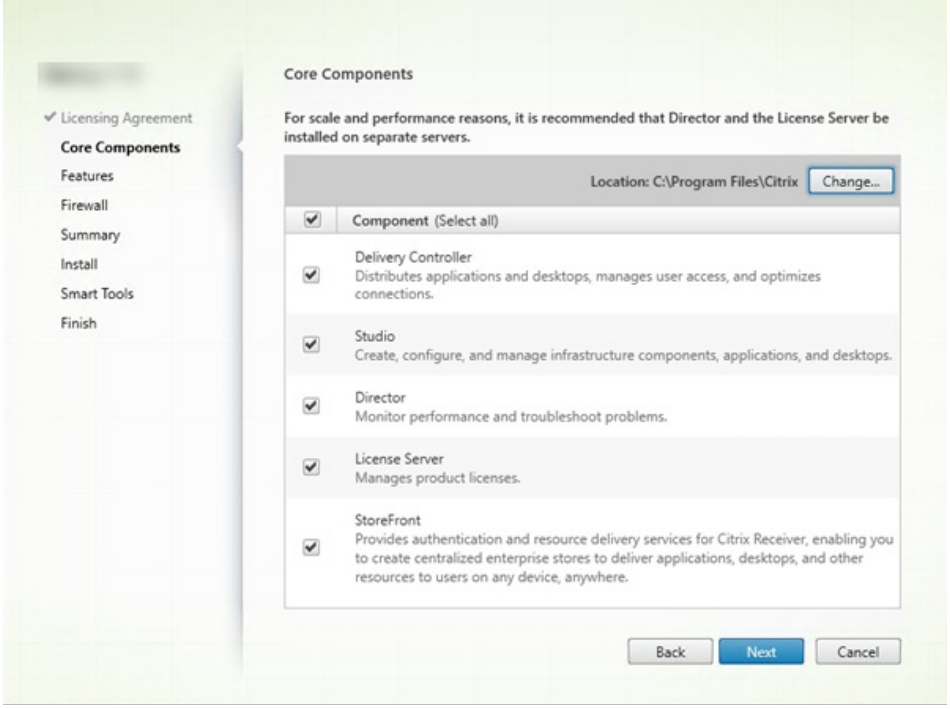
手順4：ライセンス契約書を読み、同意する



© 1999-2017 Citrix Systems, Inc. All rights reserved.

[ライセンス契約] ページで、ライセンス契約を読み、読んで同意したことを明示します。次に[次へ] をクリックします。

手順5：インストールするコンポーネントおよびインストール場所を選択する



[コア コンポーネント] ページで次の作業を行います。

- **場所：** デフォルトでは、C:\Program Files\Citrixに各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Serviceアカウントでの実行権限が必要です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **コンポーネント**：デフォルトではすべてのコアコンポーネントが選択されます。1つのサーバー上にすべてのコアコンポーネントをインストールすることは、概念実証展開、テスト展開、または小規模実稼働展開には十分です。より大きな稼働環境では、Director、StoreFront、およびLicense Serverを別々のサーバーにインストールすることをお勧めします。

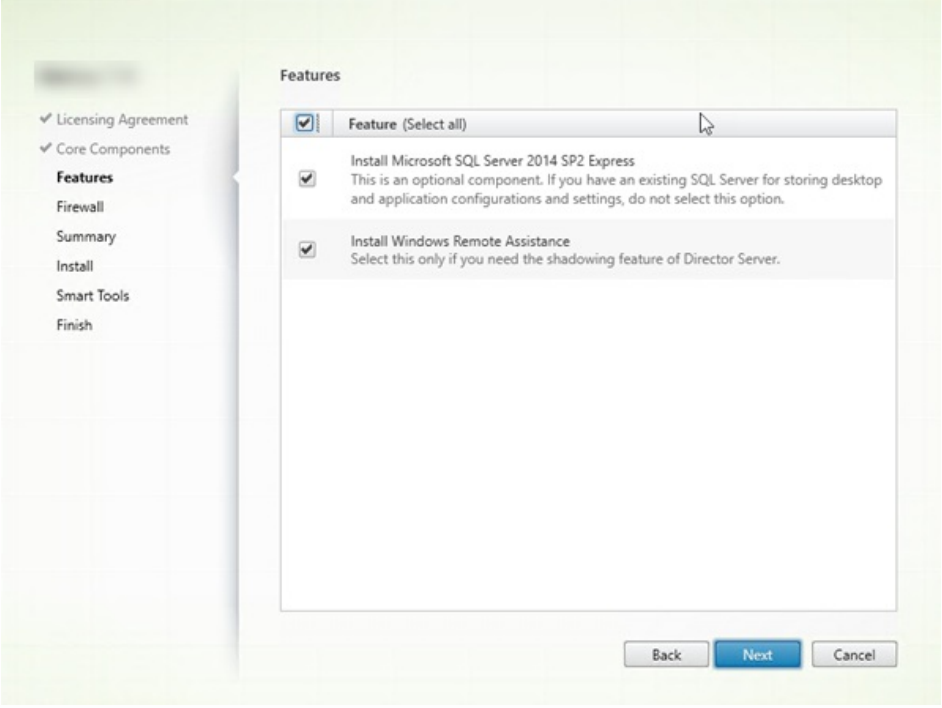
  このマシンにインストールするコンポーネントのみを選択します。このマシンにコンポーネントをインストールした後、他のマシン上で再びインストーラーを実行して他のコンポーネントをインストールできます。

  このマシン上で必要なコアコンポーネントをインストールしないように選択すると、アイコンの警告が表示されます。この警告では、このマシンでは不要であるにも関わらず、このコンポーネントをインストールするように通知されます。

[次へ] をクリックします。

コマンドラインオプション：/installdir、/components、/exclude

手順6：機能を有効または無効にする



[機能] ページで次のように実行します。

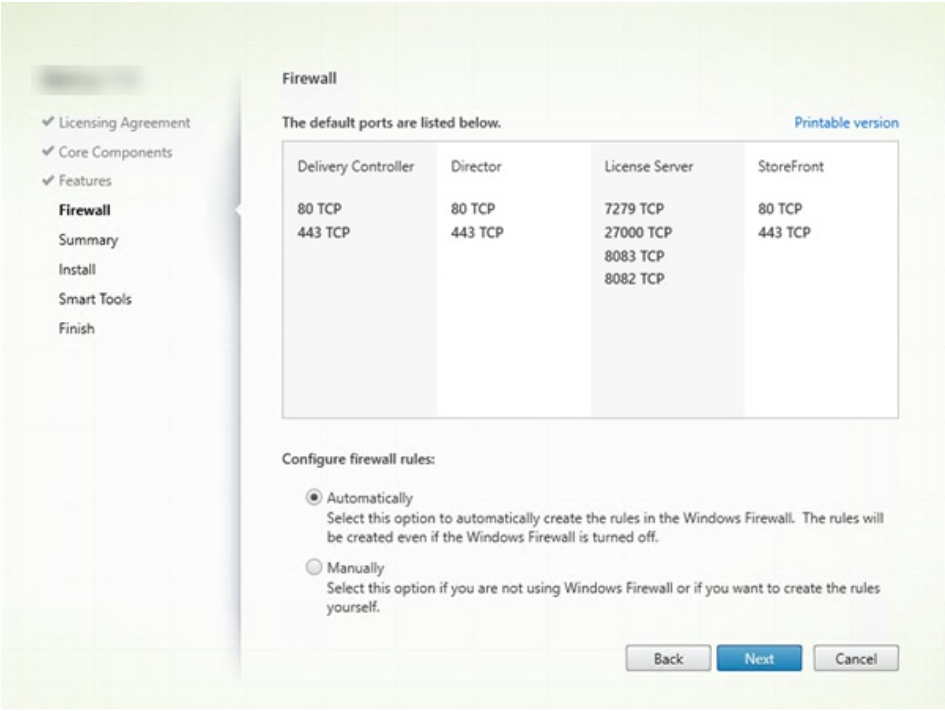
- Microsoft SQL Server Expressをサイトデータベースとして使用するためにインストールするかどうかを選択します。デフォルトでは、これはオンになっています。「データベース」を参照し、XenAppおよびXenDesktopデータベースについての理解を深めてください。
- Directorをインストールすると、Windowsリモートアシスタンスも自動的にインストールされます。Directorユーザーのシャドウで使用するためにWindowsリモートアシスタンスのシャドウ機能を有効にするかどうかを選択します。シャドウ機能を有効にすると、TCPポート3389が開きます。この機能は、デフォルトで有効になります。ほとんどの展開ではデフォルト設定で十分です。この機能はDirectorのインストール時のみ表示されます。

[次へ] をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コマンドラインオプション：/nosql（インストールを阻止するため）、 /no_remote_assistance（有効化を阻止するため）

手順7：Windowsファイアウォールポートを自動的に開放する



Windowsファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、デフォルトで**[ファイアウォール]**ページに示されているポートが自動的に開放されます。ほとんどの展開ではデフォルト設定で十分です。詳しくは、「ネットワークポート」を参照してください。

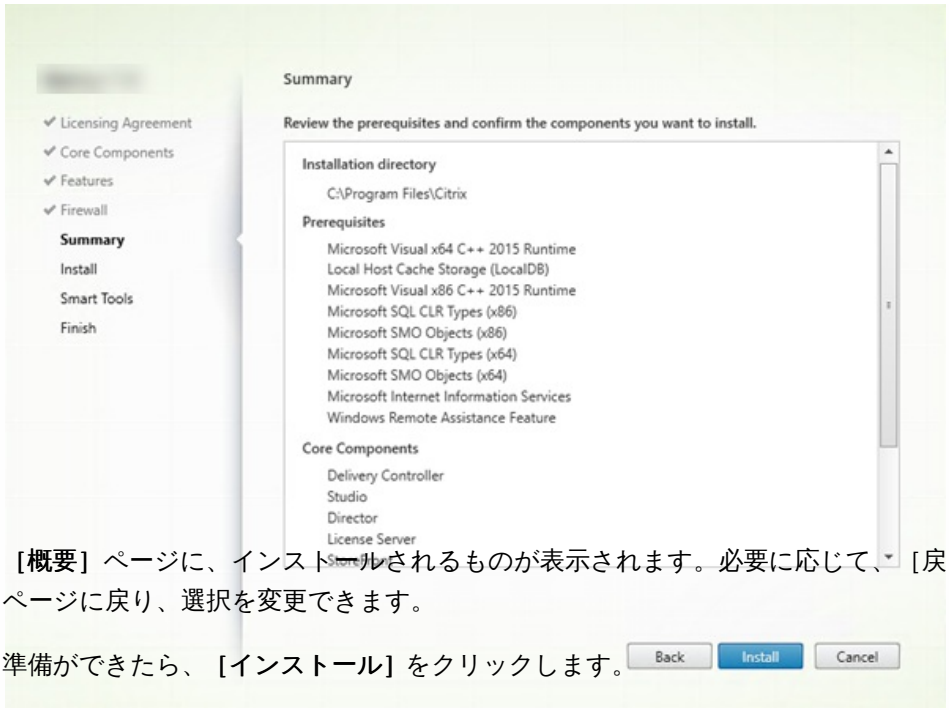
[次へ]をクリックします。

（この図は、すべてのコアコンポーネントをこのマシンにインストールした場合のポート一覧を示します。このようなタイプのインストールは通常、テスト展開でのみ行われます）。

コマンドラインオプション：/configure_firewall

手順8：インストール前に前提条件を確認する

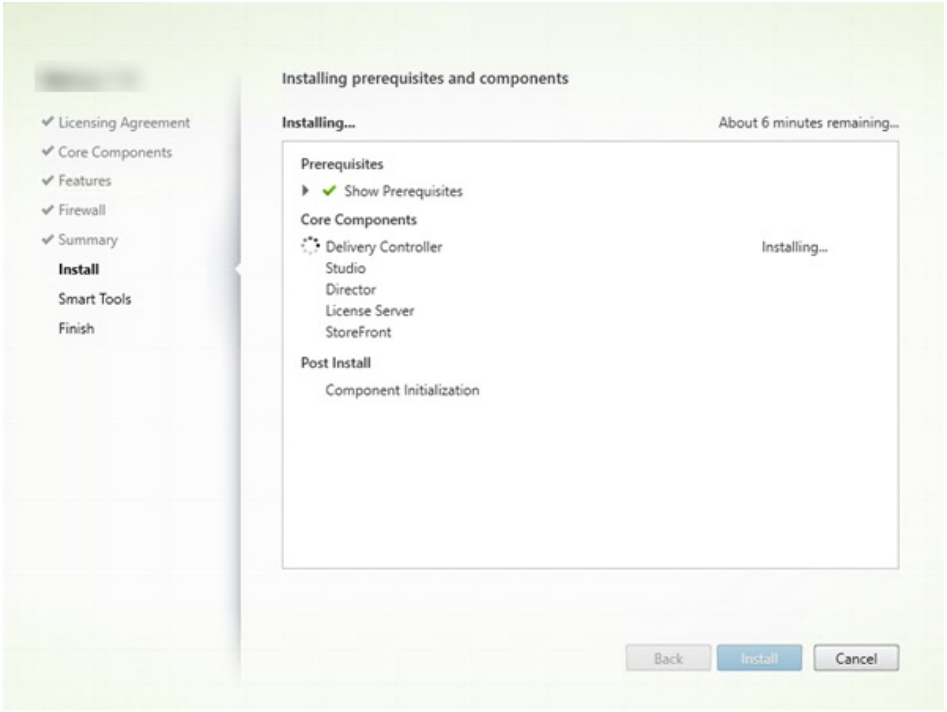
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[概要] ページに、インストールされるものが表示されます。必要に応じて、［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

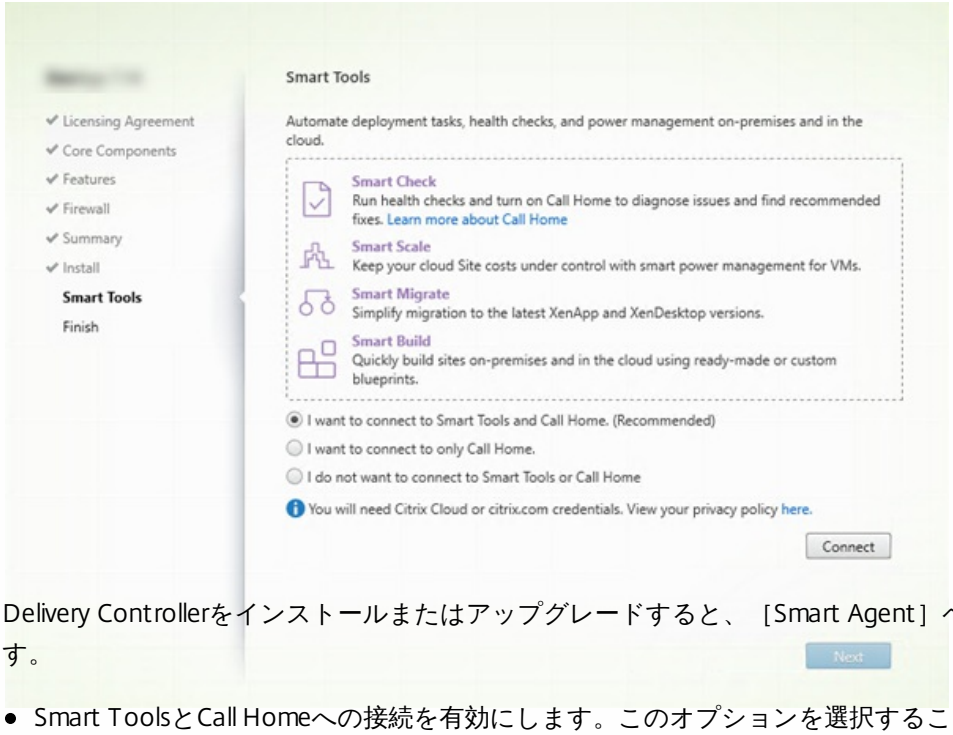
準備ができたら、**[インストール]** をクリックします。

画面にインストールの進捗が表示されます。



手順9：Smart ToolsとCall Homeに接続する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Delivery Controllerをインストールまたはアップグレードすると、［Smart Agent］ページに複数のオプションが表示されます。

- Smart ToolsとCall Homeへの接続を有効にします。このオプションを選択することをお勧めします。
- Call Homeへの接続を有効にします。Call Homeが既に有効な場合、またはインストーラーでCitrix Telemetry Serviceに関連するエラーが発生した場合には、アップグレード時にこのオプションは表示されません。
- Smart ToolsまたはCall Homeへの接続を有効にしないでください。

StoreFront（Controllerではない）をインストールすると、**Smart Tools**ページがウィザードに表示されます。その他のコアコンポーネントはインストールされている（がControllerまたはStoreFrontはインストールされていない）場合、ウィザードには［**Smart Tools**］ページも［**Call Home**］ページも表示されません。

Smart ToolsとCall Homeへの接続を有効にするオプションを選択した場合は、以下を行います。

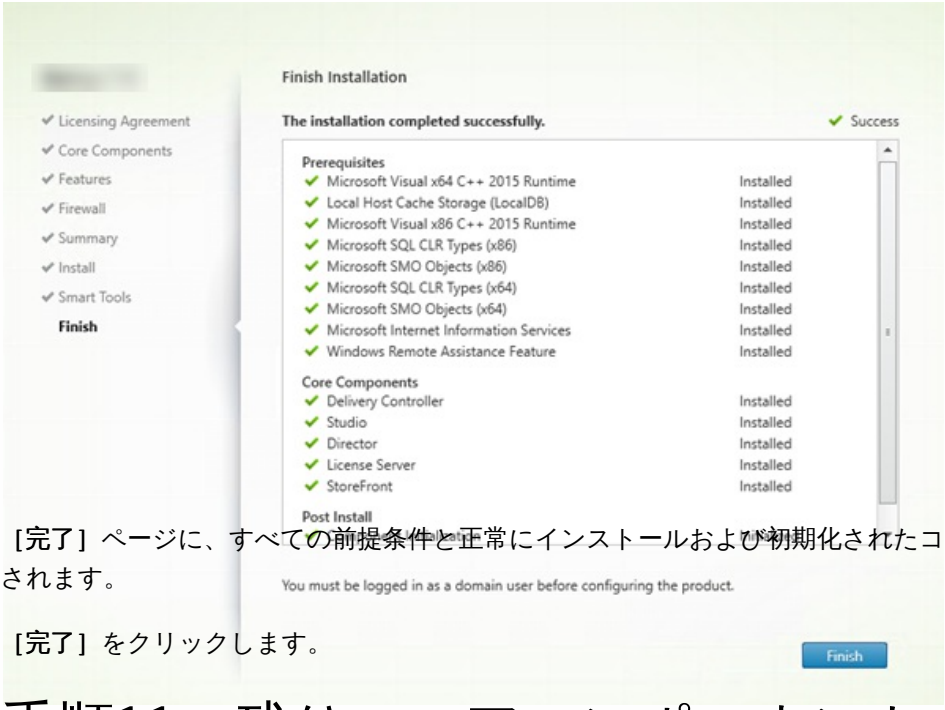
1. ［**接続**］をクリックします。
2. CitrixまたはCitrix Cloudの資格情報を入力します。
3. 資格情報が検証された後、Smart Agent証明書がダウンロードされます。これが正常に終了したら、［**接続**］ボタンの横に緑のチェックマークが表示されます。この処理中にエラーが発生した場合、参加に関する選択を変更してください（参加しないに変更）。後で登録することもできます。
4. ［**次へ**］をクリックしてインストールウィザードを続行します。

参加しないことを選択した場合、［**次へ**］をクリックします。

コマンドラインオプション：/exclude "Smart Tools Agent"（インストールしない）

手順10：インストールを完了する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[完了] ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了] をクリックします。

手順11：残りのコアコンポーネントを他のマシンにインストールする

1台のマシンにすべてのコアコンポーネントをインストールした場合、次の手順に進みます。それ以外の場合は、その他のマシンでインストーラーを実行し、残りのコアコンポーネントをインストールします。追加のControllerを他のサーバーにインストールすることもできます。

次の手順

必要なコアコンポーネントをすべてインストールしたら、Studioを使用してサイトを作成します。

サイトを作成したら、VDAをインストールします。

いつでも全製品インストーラーを使用して展開を拡張し、次のコンポーネントを含めることができます。

- Universal Print Serverコンポーネント： プリントサーバー上でインストーラーを起動します。［拡張展開］セクションで [Universal Print Server] を選択します。ライセンス契約を承諾し、ウィザードを完了します。ほかに指定または選択するものはありません。コマンドラインからのこのコンポーネントをインストールするには、「コマンドラインを使ったインストール」を参照してください。
- Federated Authentication Service：「Federated Authentication Service」を参照してください。
- セルフサービスパスワードリセットサービス：セルフサービスパスワードリセットサービスのドキュメントを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAのインストール

Dec 05, 2017

Windowsマシン用には2種類のVDAがあります。VDA for Server OSとVDA for Desktop OSです（Linuxマシン用のVDAについては、「Linux Virtual Delivery Agent」を参照してください）。

重要： インストールを始める前に、「インストールの準備」を確認してください。たとえば、マシンに最新のWindows更新プログラムが必要です。必要な更新プログラム（KB2919355など）がない場合は、インストールに失敗します。

VDAをインストールする前に、コアコンポーネントをインストールしておく必要があります。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順1：製品ソフトウェアをダウンロードしてウィザードを起動する

全製品インストーラーを使用する場合：

- XenAppおよびXenDesktopのISOをまだダウンロードしていない場合：
  - Citrixアカウント資格情報を使用して、XenAppおよびXenDesktopのダウンロードページにアクセスします。製品のISOファイルをダウンロードします。
  - ファイルを解凍します。必要な場合は、ISOファイルからDVDを作成します。
- VDAをインストールするイメージまたはマシン上で、ローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**ファイルまたはマウントしたドライブをダブルクリックします。
- インストールウィザードが起動します。

スタンドアロンパッケージを使用する場合：

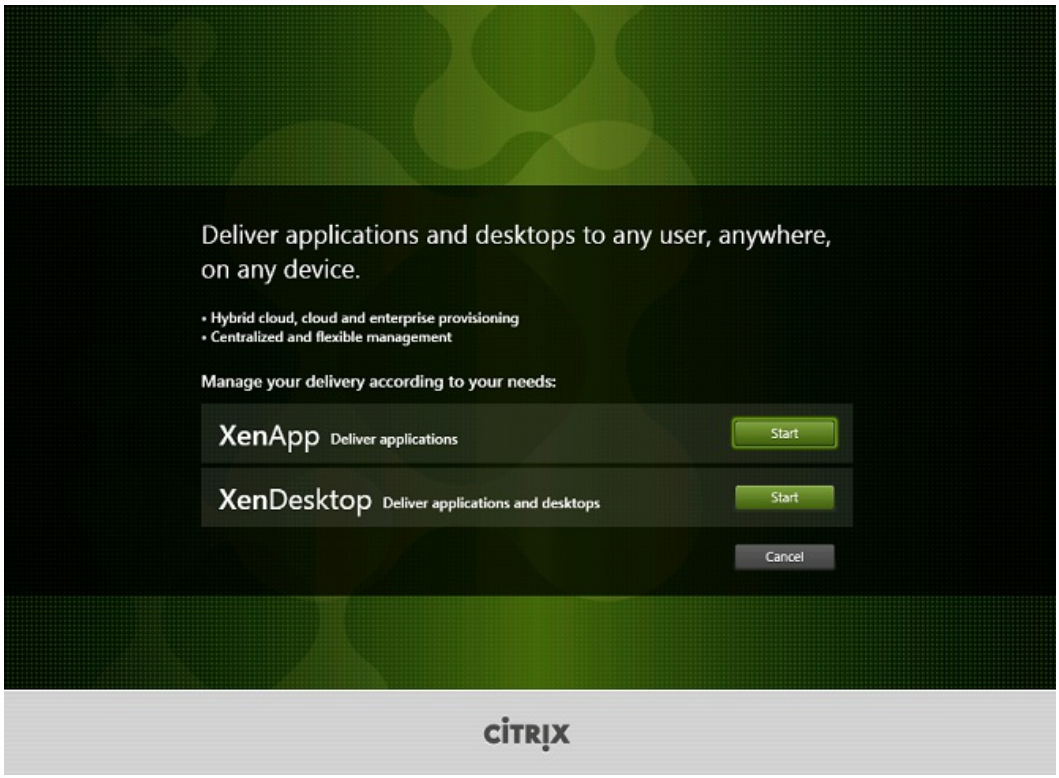
- Citrixアカウント資格情報を使用して、XenAppおよびXenDesktopのダウンロードページにアクセスします。適切なパッケージをダウンロードします。

ダウンロードページ上のコンポーネント名	インストーラーのファイル名
サーバーOS用Virtual Delivery Agent *<バージョン>*	VDAServerSetup.exe
デスクトップOS用Virtual Delivery Agent *<バージョン>*	VDAWorkstationSetup.exe
デスクトップOS用Core Services Virtual Delivery Agent *<バージョン>*	VDAWorkstationCoreSetup.exe

- このパッケージを右クリックして、**[管理者として実行]を選択します。**
- インストールウィザードが起動します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順2：インストールする製品を選択する

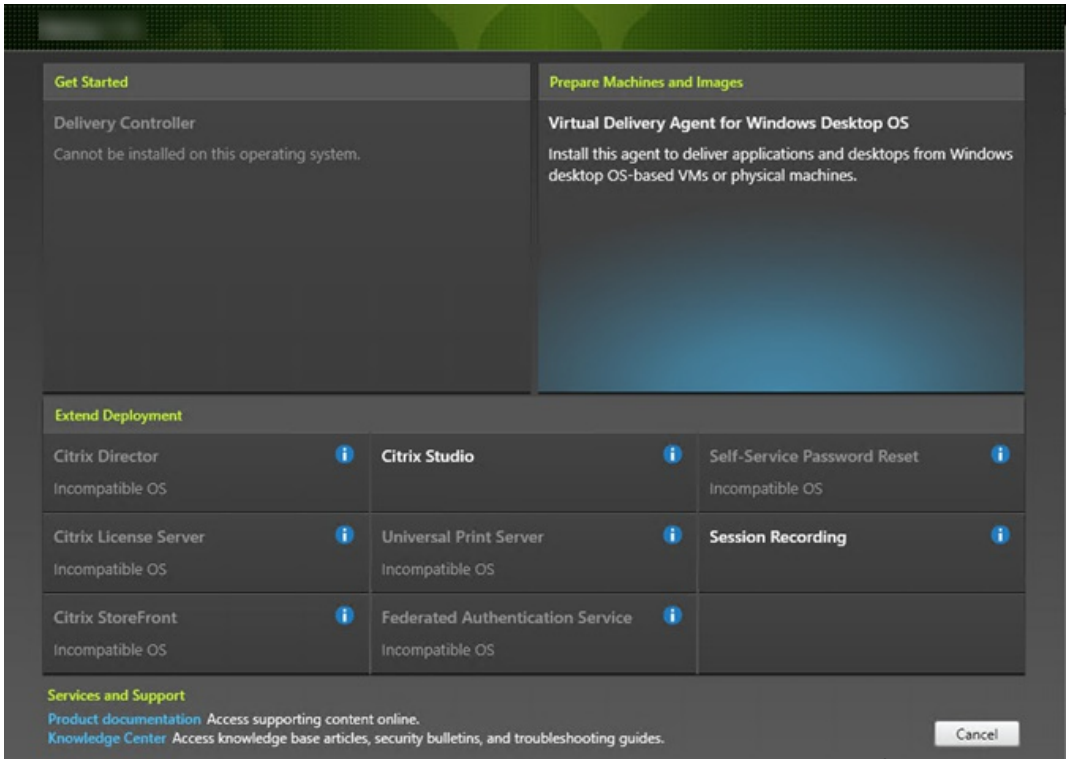


インストールする製品の隣の **[開始]** をクリックします： XenAppまたはXenDesktop。（マシンにXenAppまたはXenDesktopコンポーネントが既にインストールされている場合、このページは表示されません）。

コマンドラインオプション： XenAppをインストールする場合は/xenapp。オプションを省略するとXenDesktopがインストールされます

手順3：VDAを選択する

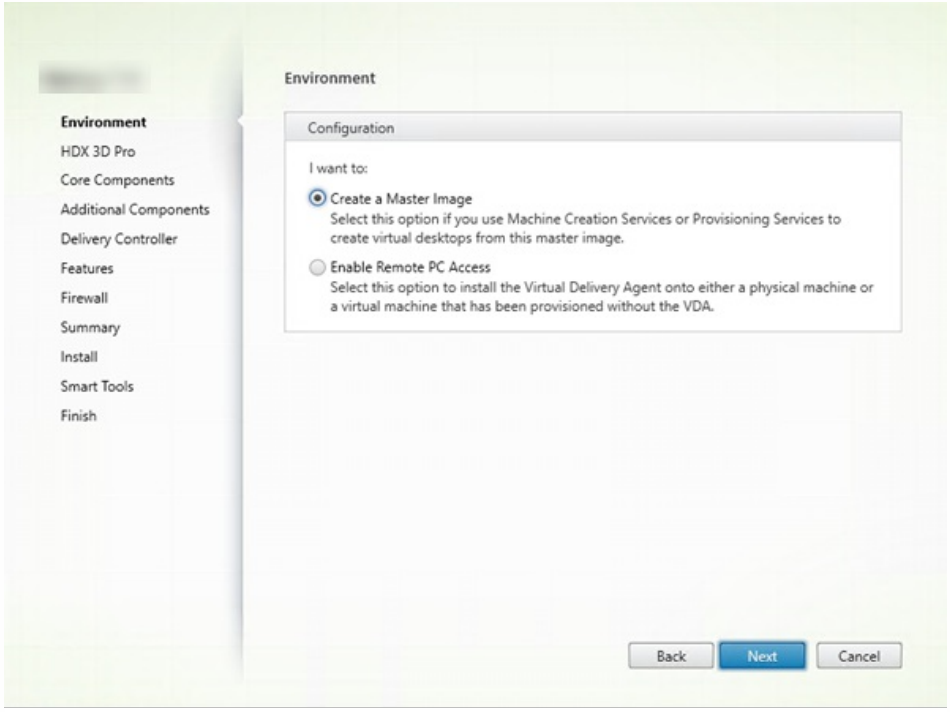
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Virtual Delivery Agentエントリを選択します。インストーラーはデスクトップOSとサーバーOSのいずれの上で実行されているかを認識しているので、適切な種類のVDAのみが提示されます。

たとえば、Windows 10マシンでインストーラーを実行すると、VDA for Desktop OSのオプションが利用可能になります。VDA for Server OSのオプションは提示されません。

手順4：VDAの使用方法を指定する



© 1999-2017 Citrix Systems, Inc. All rights reserved.

[環境] ページで、VDAの使用方法を指定します。次のいずれかのオプションを選択します。

- **マスターイメージ：**（デフォルト）マスターイメージ上にVDAをインストールしています。Citrixツール（Machine Creation ServicesやProvisioning Servicesなど）を使用して、そのマスターイメージから仮想マシンを作成することを計画しています。
- **[サーバー マシンへの接続を有効にする]**（サーバー上にインストールする場合）または **[リモート PC アクセス]**（デスクトップマシン上にインストールする場合）：物理マシン、またはVDAを使用せずにプロビジョニングされた仮想マシン上にVDAをインストールしています。リモートPCアクセスオプションを選択すると、以下のコンポーネントはインストールまたは有効化されません。
  - App-V
  - Profile management
  - Machine Identity Service
  - Personal vDisk

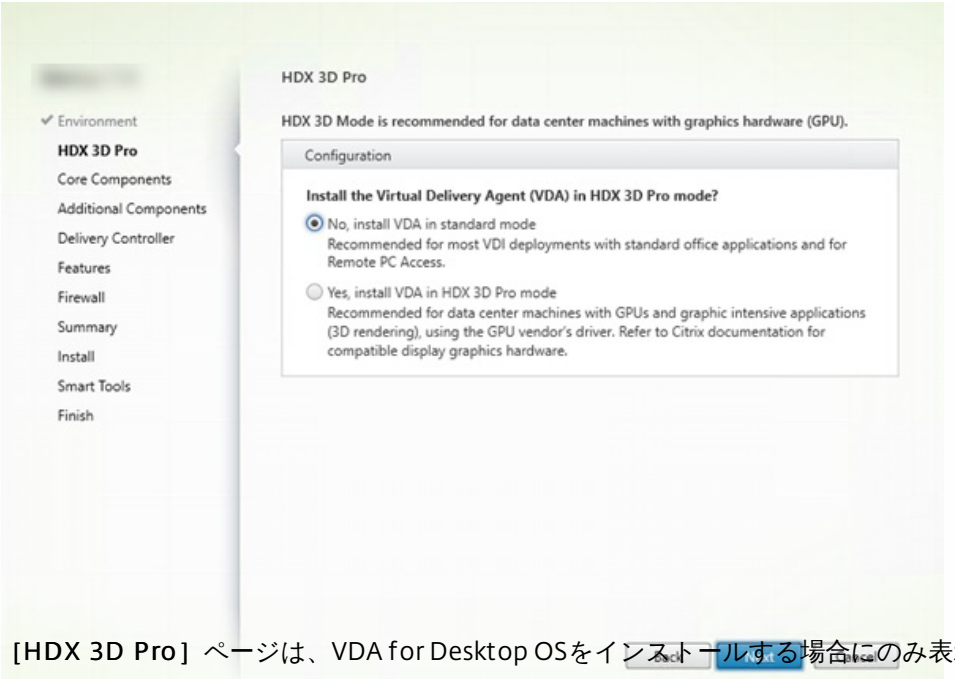
[Next] をクリックします。

コマンドラインオプション： /masterimage、/remotepc

VDAWorkstationCoreSetup.exeインストーラーを使用している場合、このページはウィザードに表示されず、コマンドラインオプションは無効です。

手順5：HDX 3D Proモードを有効にするかどうかを選択する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[HDX 3D Pro] ページは、VDA for Desktop OSをインストールする場合にのみ表示されます。

- Microsoft RemoteFXで有効にされたデスクトップを含む、ほとんどのデスクトップで、標準モードでのVDAの使用をお勧めします。デフォルトでは標準モードのVDAです。
- HDX 3D Pro VDAでは、グラフィックを多用するプログラムおよびメディアを駆使したアプリケーションのパフォーマンスが最適化されます。HDX 3D Pro VDAモードは、3Dレンダリングを行うためにマシンがグラフィックプロセッサにアクセスする場合にお勧めします。
- リモートPCアクセスの場合、VDAは通常、標準モードのVDAで構成されます。HDX 3D Proで構成されているリモートPCアクセスの場合、モニターのブランキングは次でサポートされます。
  - Intel Iris Pro graphicsとIntel HD graphics 5300以上（第5世代Intel Coreプロセッサおよび第6世代Intel Core i5プロセッサ）
  - NVIDIA QuadroとNVIDIA GRID GPU
  - AMD RapidFire

標準モード	HDX 3D Proモード
通常、グラフィックのハードウェアアクセラレーションのない仮想デスクトップおよびリモートPCアクセスに最適です。	5つ以上のモニターが必要でない限り、通常、グラフィックハードウェアアクセラレーションのあるデータセンターデスクトップに最適です。
リモートPCアクセスには、あらゆるGPUを使用できます（アプリケーション互換性の制限あり）。 • Windows 7、8、および8.1では、DirectX用GPUアクセラレーションの機能レベルは最大9.3です。一部のDirectX 10、11、12アプリケーションは、DirectX 9へのフォールバックをしない場合、実行されないことがあります。 • Windows 10の場合、GPUアクセラレーションはウィンドウ表示のDirectX 10、11、および12アプリに提供されます。DX 9アプリはWARPによってレンダリングされ	任意のGPUによるGPUアクセラレーションをサポートします。ただし、コンソールのブランキング、非標準画面解像度、およびTrue Multi MonitorサポートにはNVIDIA GRID、Intel Iris ProまたはAMD RapidFireグラフィックスが必要です。 広範なアプリケーション互換性のためにグラフィックベンダーのドライバーを活用します。 • GPUがサポートするすべての3D API（DirectXまたはOpenGL）。

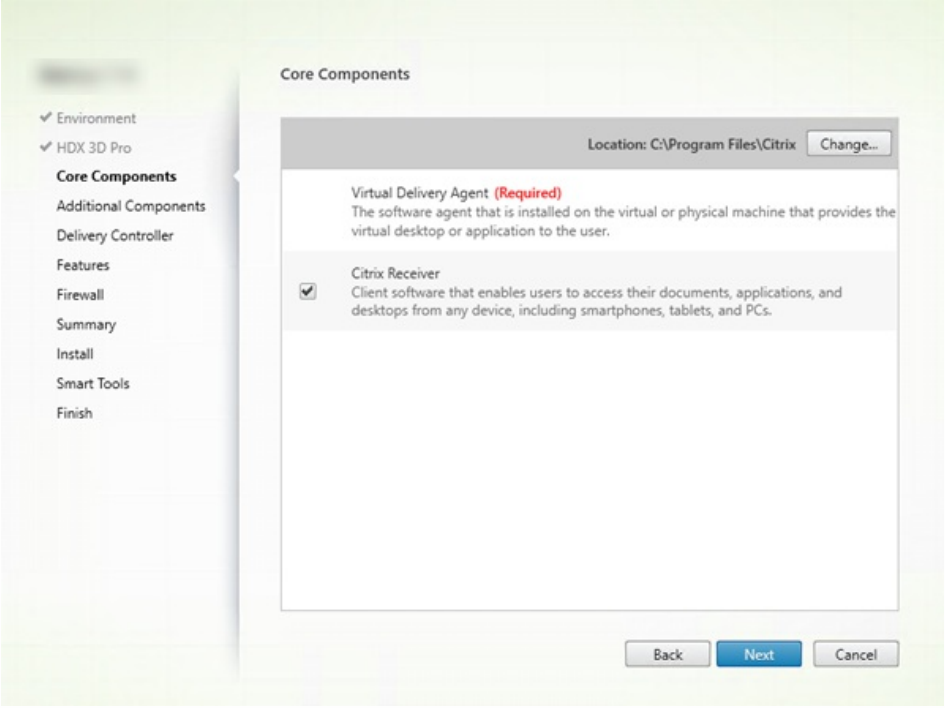
© 1999-2017 Citrix Systems, Inc. All rights reserved.

ます。DXアプリを全画面モードで使用できません。 • GPUベンダーによってサポートされている場合はリモートセッションでのOpenGLアプリケーションアクセラレーション（現時点ではNVIDIAのみ）。	• Intel Iris Pro（Win10のみ）、NVIDIA GRID、およびAMD RapidFireでの全画面3Dアプリケーションサポート。 • カスタムドライバー拡張およびAPIのサポート（CUDAやOpenCLなど）。
任意のモニター解像度（上限はWindows OSおよびパフォーマンスによって決まります）および最大8つのモニター。	最大で4つのモニターをサポートします。
Intel Iris Proグラフィックプロセッサで利用可能なH.264ハードウェアエンコーディング。	Intel Iris Proグラフィックスプロセッサおよび NVIDIAカードを搭載してH.264ハードウェアエンコーディングが使用可能です。

[次へ] をクリックします。

コマンドラインオプション： /enable_hdx_3d_pro

手順6：インストールするコンポーネントおよびインストール場所を選択する



[コア コンポーネント] ページで次の作業を行います。

- **場所：** デフォルトでは、C:\Program Files\Citrixに各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Serviceアカウントでの実行権限が必要です。

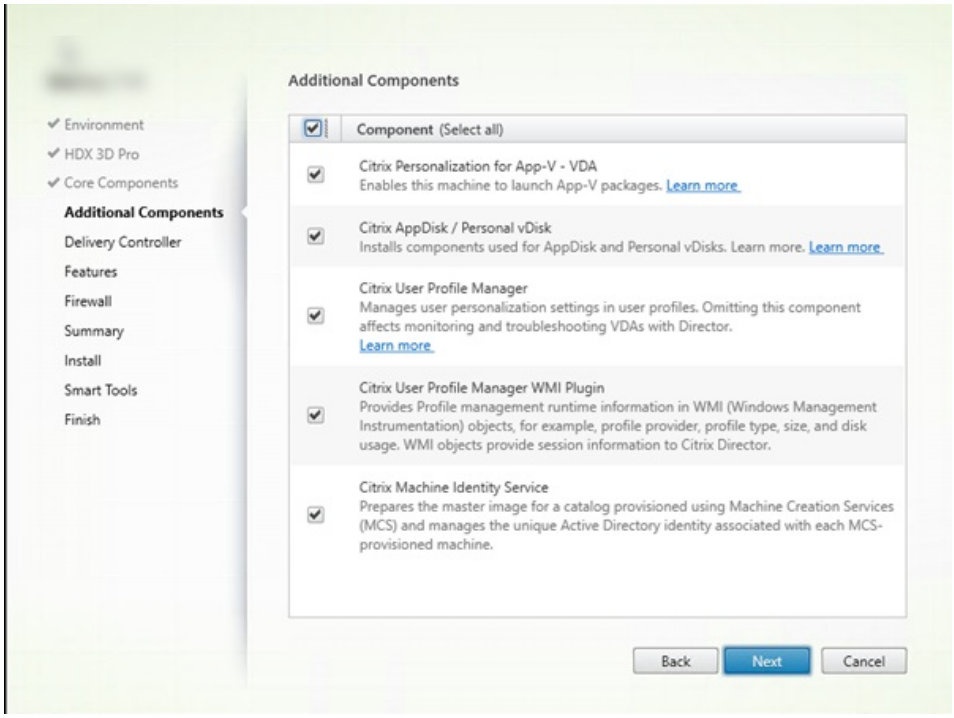
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **コンポーネント**：デフォルトで、Citrix Receiver for WindowsはVDAとともにインストールされます（VDAWorkstationCoreSetup.exeインストーラーを使用する場合を除く）。Citrix Receiverをインストールしない場合は、チェックボックスをオフにします。VDAWorkstationCoreSetup.exeインストーラーを使用している場合、Citrix Receiver for Windowsはインストールされないため、このチェックボックスは表示されません。

[Next] をクリックします。

コマンドラインオプション： （/installdir、Citrix Receiver for Windowsのインストールを阻止するには「/components vda」を使用）

手順7：追加コンポーネントのインストール



[追加コンポーネント] ページには、VDAのほかの機能やテクノロジのインストールを有効または無効にするチェックボックスがあります。次の場合、このページは表示されません。

- VDAWorkstationCoreSetup.exeインストーラーを使用している。また、追加コンポーネント用のコマンドラインオプションはこのインストーラーでは無効です。
- VDAをアップグレードしており、追加コンポーネントが既にすべてインストールされている。（追加コンポーネントのいつかが既にインストールされている場合、このページにはインストールされていないものだけが表示されます。）

Citrix Personalization for App-V：

Microsoft App-Vパッケージのアプリケーションを使用する場合、このコンポーネントをインストールします。詳しくは、「App-V」を参照してください。

コマンドラインオプション： /exclude "Citrix Personalization for App-V – VDA"を使用してコンポーネントがインストールされないようにする

Citrix AppDiskおよびPersonal vDisk：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

仮想マシン上にVDA for Desktop OSをインストールする場合にのみ有効です。AppDiskおよびPersonal vDiskに使用されるコンポーネントがインストールされます。詳しくは、「AppDisk」および「Personal vDisk」を参照してください。

コマンドラインオプション： /exclude "Personal vDisk"を使用して、AppDiskとPersonal vDiskのコンポーネントがインストールされないようにする

Citrix Profile Management

このコンポーネントは、ユーザープロファイル内のユーザーの個人設定を管理します。詳しくは、「Profile Management」を参照してください。

インストールからCitrix Profile managementを除くと、Citrix Directorを使ったVDAの監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの［個人設定］パネル、および［EndPoint］ページの［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと［傾向］ページでは、Profile managementがインストールされているマシンについてのデータしか［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Managementサービスをインストールして実行することをお勧めします。Citrix Profile Managementサービスの有効化は、必須ではありません。

コマンドラインオプション： /exclude "Citrix User Profile Manager"を使用してコンポーネントがインストールされないようにする

Citrix User Profile Manager WMI Plugin

このプラグインは、WMI（Windows Management Instrumentation）オブジェクトに格納して、プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用など、Profile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

コマンドラインオプション： /exclude "Citrix User Profile Manager WMI Plugin"を使用してコンポーネントがインストールされないようにする

Citrix Machine Identity Service：

このサービスは、MCSでプロビジョニングしたカタログのマスターイメージを準備します。またプロビジョニングした各マシン固有のActive Directory IDを管理します。

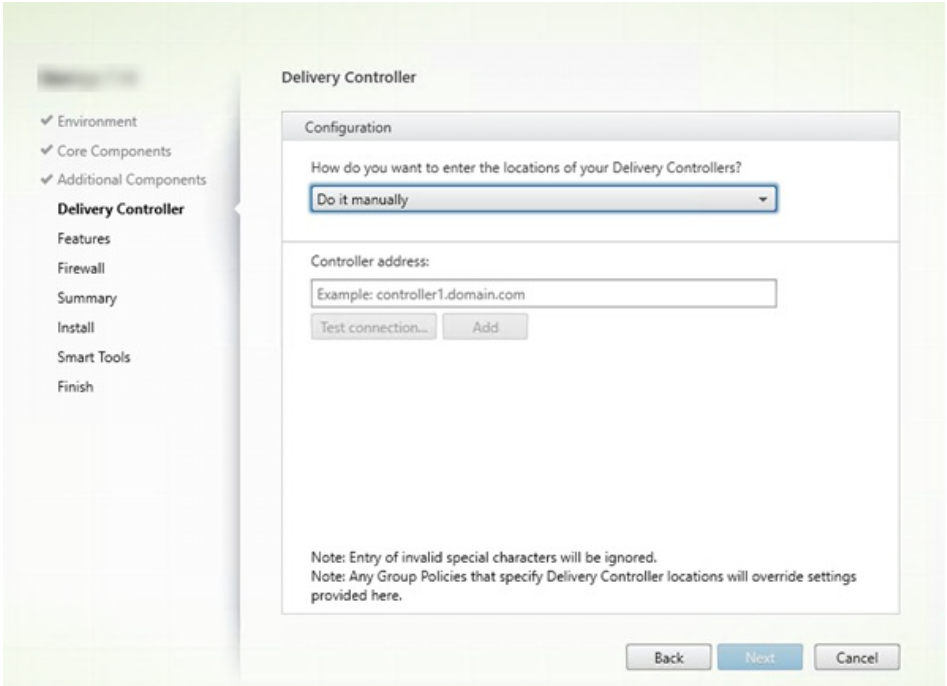
コマンドラインオプション： /exclude "Machine Identity Service"を使用してコンポーネントがインストールされないようにする

グラフィカルインターフェイスでのデフォルト値：

- **[環境]** ページで［マスター イメージを作成する］を選択すると（手順4）、**[追加コンポーネント]** ページにある項目はデフォルトで有効になります。
- **[環境]** ページで［リモート PC アクセスを有効にする］または［サーバー マシンへの接続を有効にする］を選択した場合、**[追加コンポーネント]** ページにある項目はデフォルトで無効になります。

手順8：Delivery Controllerアドレス

© 1999-2017 Citrix Systems, Inc. All rights reserved.



［**Delivery Controller**］ページで、インストール済みのControllerのアドレスを入力する方法を選択しますVDAのインストール時に、アドレスを指定することをお勧めします（［手動で指定する］）。VDAは、この情報がないとControllerに登録できません。VDAが登録されない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で指定する：**（デフォルト）：インストールされているControllerのFQDNを入力し、**［追加］**をクリックします。追加のControllerをインストールした場合は、アドレスを追加します。
- **後で実行（上級）**：このオプションを選択すると、ウィザードは、続行する前に、選択を確認するよう求めてきます。後でアドレスを指定する場合は、インストーラーを再実行するか、Citrixグループポリシーを使用することができます。ウィザードは、**［概要］**ページでも確認を求めます。
- **Active Directory から場所を選択する**：マシンがドメインに参加していて、ユーザーがドメインユーザーである場合にのみ有効です。
- **Machine Creation Servicesで自動的に指定する**：MCSを使用してマシンをプロビジョニングする場合のみ有効です。

［次へ］をクリックします。［後で実行 (上級)］を選択した場合、後でコントローラーのアドレスを指定することを確認するメッセージが表示されます。

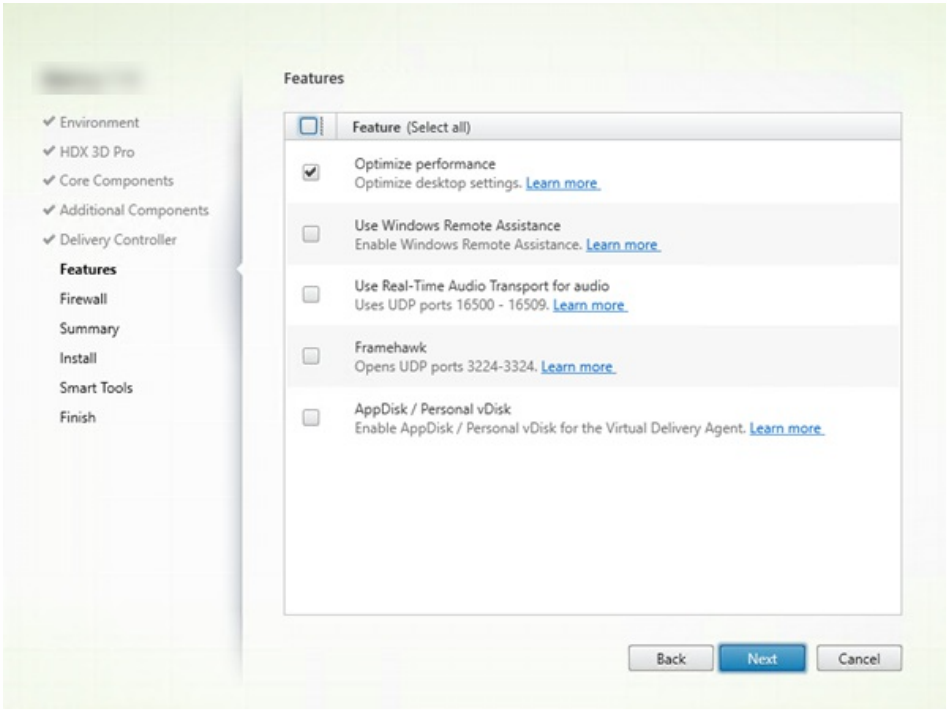
そのほかの考慮事項

- アドレスに{ | } ~ [\ ] ^ ' : ; < = > ? & @ ! " # $ % ( ) + / ,の文字を含めることはできません。
- VDAのインストールおよびグループポリシーでアドレスを指定すると、インストール中に行われた設定がポリシーの設定によって上書きされます。
- VDA登録を行うには、Controllerを使用した通信に使用されるファイアウォールポートが開いている必要があります。デフォルトではウィザードの**［ファイアウォール］**ページで有効化されます。
- （VDAのインストール時またはその後に）Controllerのロケーションを指定すると、Controllerが追加または削除された場合に、自動更新機能を使用してVDAを更新できます。VDAによるControllerの検出方法、およびVDAをControllerとともに登録する方法について詳しくは、「Delivery Controller」を参照してください。

コマンドラインオプション：/controllers

手順9：機能を有効または無効にする

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[機能] ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

パフォーマンス最適化：

VDAを物理マシンではなく、仮想マシンにインストールしている場合にのみ有効です。この機能を有効にすると（デフォルト）、ハイパーバイザー上の仮想マシンにインストールされるVDAが最適化されます。仮想マシンの最適化には、オフラインファイルの無効化、バックグラウンド最適化（デフラグ処理）の無効化、およびイベントログサイズの縮小などの操作が含まれます。詳しくは、CTX125874を参照してください。

コマンドラインオプション： /optimize

VDAWorkstationCoreSetup.exeインストーラーを使用している場合、この機能はウィザードに表示されず、コマンドラインオプションは無効です。リモートPCアクセス環境で他のインストーラーを使用している場合は、この機能を無効にします。

Windowsリモートアシスタンスの使用：

この機能を有効にすると、Directorのユーザーシャドウ機能でWindowsリモートアシスタンスが使用されます。Windowsリモートアシスタンスによってファイアウォールで動的ポートが解放されます。（デフォルト = 無効）

コマンドラインオプション： /enable_remote_assistance

オーディオにリアルタイムオーディオ転送を使用:

ネットワークでVoice over IPが広く使われている場合、この機能を有効化します。この機能を使用すると、遅延が短縮され、損失の多いネットワーク経由の音声復元性が改善されます。オーディオデータをUDPトランスポート経由のRTPを使用して伝送することが可能になります。（デフォルト = 無効）

コマンドラインオプション： /enable_real_time_transport

Framehawk：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この機能を有効にすると、双方向のUDPポート3224～3324が開放されます。（デフォルト = 無効）

ポート範囲は、Citrixポリシー設定の［Framehawkディスプレイチャネルポートの範囲］を使用して後で変更できます。その場合は、ローカルファイアウォールポートを開放する必要があります。UDPネットワークパスは、内部のファイアウォール（VDAからCitrix ReceiverまたはNetScaler Gateway）および外部のファイアウォール（NetScaler GatewayからCitrix Receiver）で開放されている必要があります。NetScaler Gatewayが展開されると、FramehawkのデータグラムはDTLS（デフォルトのUDPポート443）を使用して暗号化されます。詳しくは、「Framehawk」を参照してください。

コマンドラインオプション： /enable_framehawk_port

AppDisk / Personal vDisk：

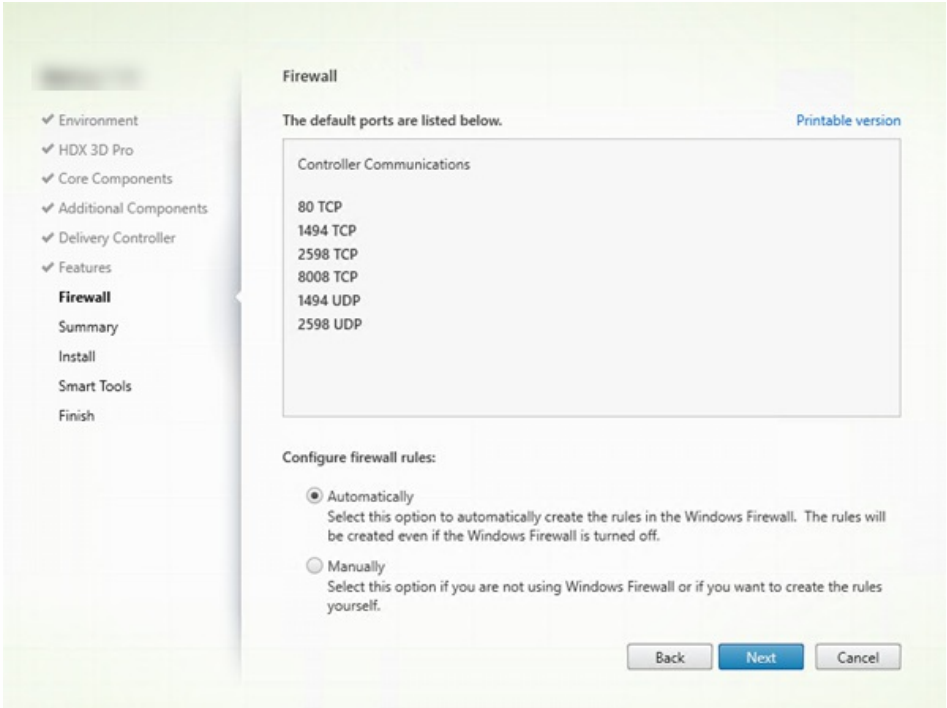
仮想マシン上にVDA for Desktop OSをインストールする場合にのみ有効です。このチェックボックスは**[追加コンポーネント]**ページで［Citrix AppDisk］または［Personal vDisk］のチェックボックスがオンの場合にのみ利用可能です。このチェックボックスをオンにすると、AppDiskおよびPersonal vDiskを使用できます。詳しくは、「AppDisks」および「Personal vDisks」を参照してください。

コマンドラインオプション： /baseimage

VDAWorkstationCoreSetup.exeインストーラーを使用している場合、この機能はウィザードに表示されず、コマンドラインオプションは無効です。

［次へ］をクリックします。

手順10：ファイアウォールポート



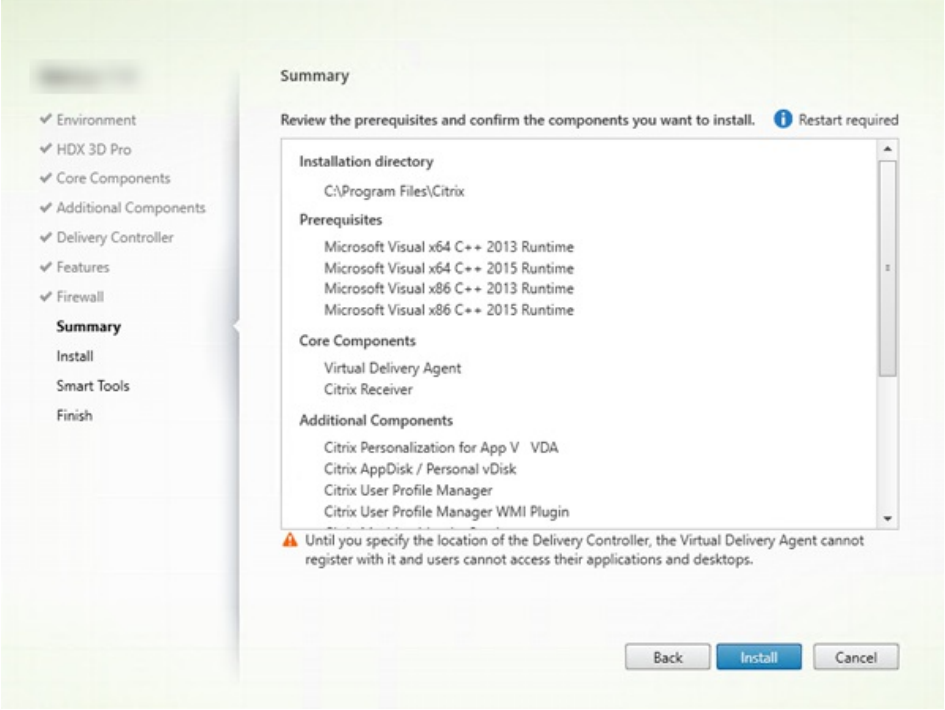
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windowsファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、**[ファイアウォール]**ページに示されているポートがデフォルトで開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートの情報については、「ネットワークポート」を参照してください。

[次へ]をクリックします。

コマンドラインオプション： /enable_hdx_ports

手順11：インストール前に前提条件を確認する



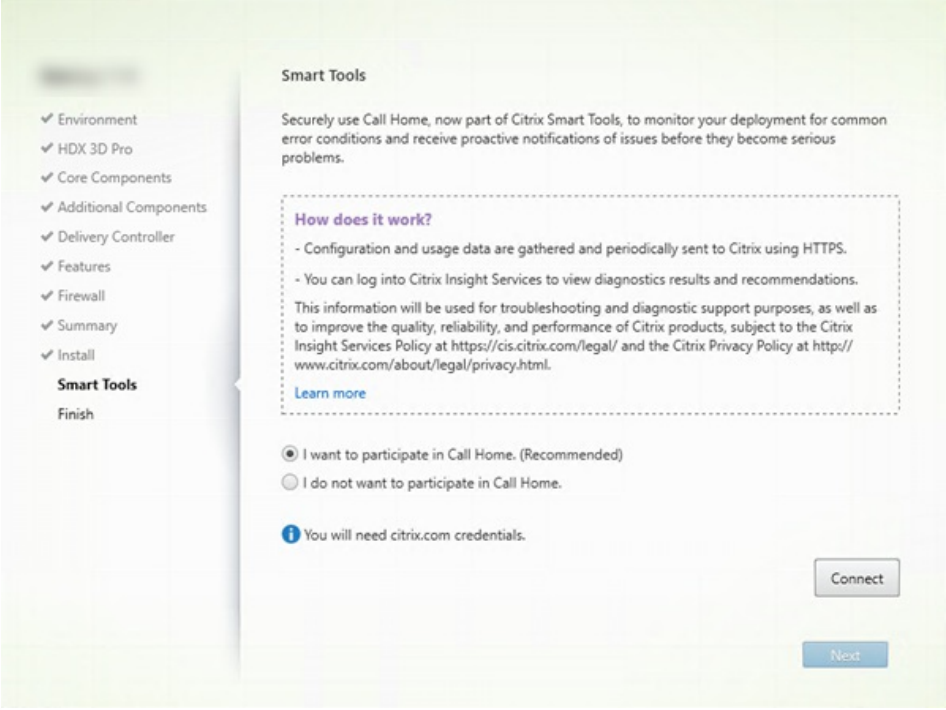
© 1999-2017 Citrix Systems, Inc. All rights reserved.

［概要］ページに、インストールされるものが表示されます。［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

準備ができたら、**［インストール］**をクリックします。

前提条件がまだインストール/有効化されていない場合、マシンが1～2回再起動する場合があります。「インストールの準備］を参照してください。

手順12：Smart Toolsに参加する

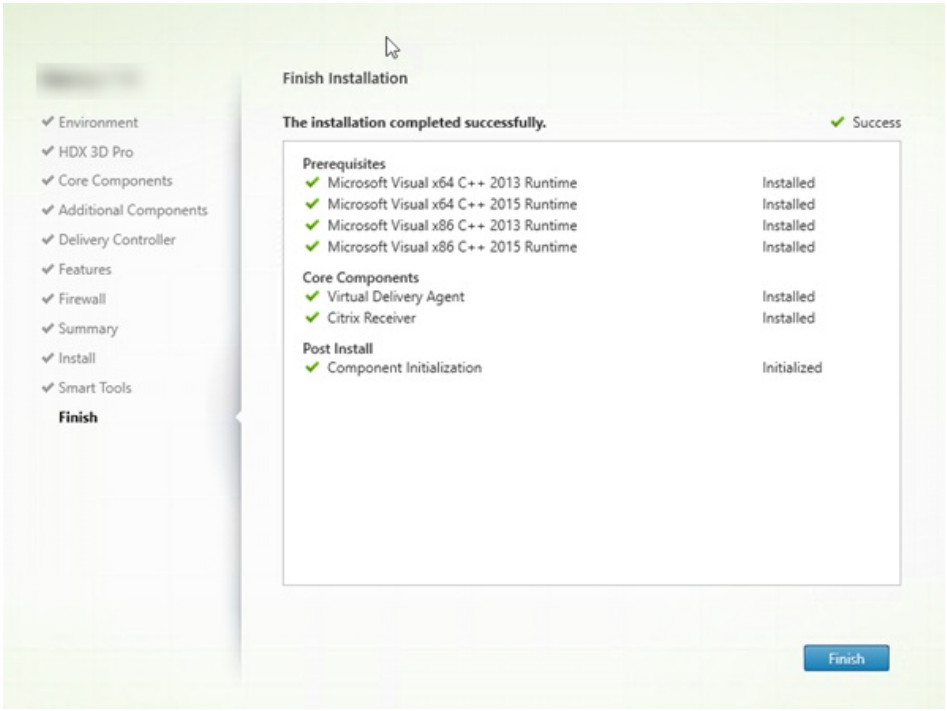


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[Smart Tools]ページで、Citrix Smart Toolsの一部であるCitrix Call Homeに参加するかどうかを選択します。参加することを選択する場合（デフォルト）、 [接続]をクリックします。求められたら、Citrixアカウント資格情報を入力します。

資格情報が確認されたら（あるいは参加しないことを選択した場合）、[次へ]をクリックします。

手順13：このインストールを完了する



[完了]ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了]をクリックします。デフォルトでは、マシンは自動的に再起動します（自動再起動を無効にすることもできますが、マシンを再起動するまでVDAは使用できません）。

次：他のVDAをインストールして構成を続ける

必要に応じて上の手順を繰り返し、他のマシンまたはイメージ上にVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。サイトをまだ作成していない場合は、そのタスクのガイドが自動的に表示されます。それが済んだら、ガイドに従ってマシンカタログ、デリバリーグループを作成します。以下の情報も参照してください。

- サイトの作成

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- マシンカタログの作成
- デリバリーグループの作成

インストールした後に、VDAをカスタマイズすることもできます。

1. プログラムを削除または変更するWindowsのコントロールパネルで**[Citrix Virtual Delivery Agent]** または **[Citrix Remote PC Access/VDI Core Services VDA]** を選択します。次に右クリックして **[変更]** を選択します。
2. **[Virtual Delivery Agent設定のカスタマイズ]** を選択します。インストーラーが起動したら、次を変更できます。

- Controllerのアドレス
- Controllerへの登録に使用されるTCP/IPポート（デフォルトは80）
- Windowsファイアウォールポートを自動的に開放するかどうか

トラブルシューティング

Microsoft System Center Configuration Managerを使用する環境では、VDAのインストールに成功しても終了コード3により失敗したというメッセージが表示されることがあります。この不正なメッセージが表示されなくなるようにするには、インストールコマンドをCMDスクリプト内に記述するか、Configuration Managerパッケージの成功コードを変更してください。詳しくは、http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/にあるフォーラムディスカッションを参照してください。

デリバリーグループのStudio表示では、［詳細］ペインの［インストール済み VDA のバージョン］エントリがマシンにインストールされているバージョンではないことがあります。マシンのWindowsの［プログラムと機能］には、VDAの実際のバージョンが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コマンドラインを使ったインストール

Jan 24, 2018

この記事は、Windowsオペレーティングシステムがインストールされたマシンへのコンポーネントのインストールに適用さ
ます。Linuxオペレーティングシステムの VDAについては、「Linux Virtual Delivery Agent」を参照してください。

ここでは次のことについて説明します。

- 全製品インストーラーの使用
- スタンドアロンVDAインストーラーの使用
- コアコンポーネントのインストールに使用されるコマンドラインオプション
- 例：コアコンポーネントのインストール
- VDAのインストールに使用されるコマンドラインオプション
- 例：VDAのインストール
- コマンドラインを使ったVDAのカスタマイズ
- コマンドラインを使ったUniversal Print Serverのインストール

重要：この記事では、製品のインストールコマンドの実行方法を説明します。インストールを始める前に、「インストールの準備」を読んでください。そのアーティクルには、利用できるインストーラーの説明があります。

コマンドの実行状態を確認して値を返すには、マシンの管理者であるか**[管理者として実行]** を使用する必要があります。詳しくは、Microsoft社のコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用するだけでなく、製品ISOにあるサンプルスクリプトを使用して、Active DirectoryでVDAマシンをインストール、アップグレード、または削除できます。詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

全製品インストーラーの使用

全製品インストーラーのコマンドラインインターフェイスへのアクセス：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要な場合は、ISOファイルからDVDを作成します。
3. ローカルの管理者アカウントを使って、インストール先のサーバーにログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. 製品メディアの\x64\XenDesktop Setupディレクトリから適切なコマンドを実行します。

コアコンポーネントのインストール：

> **XenDesktopServerSetup.exe**コマンドを実行します。これには、「コアコンポーネントのインストールに使用されるコマンドラインオプション」セクションに記載されているオプションを使用します。

VDAのインストール：

> **XenDesktopVDASetup.exe**コマンドを実行します。これには、「VDAのインストールに使用されるコマンドラインオプション」セクションに記載されているオプションを使用します。

Universal Print Serverのインストール：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「コマンドラインを使ったUniversal Print Serverのインストール」のガイダンスに従ってください。

Federated Authentication Serviceのインストール：

グラフィカルインターフェイスを使うことをお勧めします。

セルフサービスパスワードリセットサービスのインストール：

セルフサービスパスワードリセットサービスのドキュメントの手順に従います。

スタンドアロンVDAインストーラーの使用

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールの前に管理者権限を設定す
か、または**[管理者として実行]**を使用する必要があります。

- Citrixから適切なパッケージをダウンロードします。

ダウンロードページ上のコンポーネント名	インストーラーのファイル名
サーバーOS用Virtual Delivery Agent *<バージョン>*	VDAServerSetup.exe
デスクトップOS用Virtual Delivery Agent *<バージョン>*	VDAWorkstationSetup.exe
デスクトップOS用Core Services Virtual Delivery Agent *<バージョン>*	VDAWorkstationCoreSetup.exe

- まず、パッケージから既存のディレクトリにファイルを抽出して、インストールコマンドを実行するか、またはただパッケージを実行します。

  インストール前にファイルを抽出するには、「.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia」のように絶対パスと**/extract**を使います。（ディレクトリはあらかじめ存在する必要があります。そうでない場合、抽出は失敗します）。次に、新しいコマンドプロンプトを開いて、抽出先フォルダー（上の例ではCitrixVDAInstallMedia）から**XenDesktopVdaSetup.exe**を実行します。「VDAのインストールに使用されるコマンドラインオプション」セクションの有効なオプションを使用してください。

  ダウンロードしたパッケージを実行する場合は、次の名前のファイルを実行するだけです。**VDAServerSetup.exe**、**VDAWorkstationSetup.exe**、または**VDAWorkstationCoreSetup.exe**。「VDAのインストールに使用されるコマンドラインオプション」セクションの有効なオプションを使用してください。

  全製品インストーラーに慣れている場合：

  スタンドアロンのVDAServerSetup.exeまたはVDAWorkstationSetup.exeは名前以外、XenDesktopVdaSetup.exeコマンドと同じですので、同様に実行してください。

  VDAWorkstationCoreSetup.exeインストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているので異なります。

コアコンポーネントのインストールに使用されるコマ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンドラインオプション

次のオプションは、**XenDesktopServerSetup.exe**コマンドを使用してコアコンポーネントをインストールするときに有効です。オプションについて詳しくは、「コアコンポーネントのインストール」を参照してください。

/components <*component*> [,<*component*>] ...

インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します。

CONTROLLER：Controller

DESKTOPSTUDIO：Studio

DESKTOPDIRECTOR：Director

LICENSESERVER：Citrixライセンスサーバー

STOREFRONT：StoreFront

このオプションを指定しない場合、すべてのコンポーネントがインストール（または、/removeオプションも指定されている場合は削除）されます。

/configure_firewall

Windowsファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、インストールされるコンポーネントで使用されるポートが開放されます。サードパーティ製のファイアウォールを使用している場合は、適切なポートを手動で開く必要があります。

/disableexperiencemetrics

Citrix Insight Servicesへのインストール、アップグレード、または削除中に収集される分析の自動アップロードが阻止されます。

/exclude

二重引用符で囲まれた機能、サービス、またはテクノロジをインストールしません。複数の機能、サービス、またはテクノロジを指定する場合は、カンマで区切って、二重引用符で囲みます。以下の値を指定します。

"Local Host Cache Storage (LocalDB)"：ローカルホストキャッシュに使用されるデータベースのインストールが阻止されます。このオプションは、サイトデータベースとして使うためにSQL Server Expressがインストールされているかどうかには影響しません。

"Smart Tools Agent"：Citrix Smart Toolsエージェントのインストールが阻止されます。

/helpまたは/h

コマンドのヘルプを表示します。

/installdir <*directory*>

コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値：c:\Program Files\Citrix

/logpath <*path*>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。Default = 「%TEMP%\Citrix\XenDesktop Installer」

/no_remote_assistance

Directorをインストールする場合にのみ有効です。Windowsリモートアシスタンス機能を使用するシャドウ機能を無効化します。

/noreboot

インストール後の再起動を無効にします（ほとんどのコアコンポーネントでは、デフォルトで再起動が無効になっています）。

/nosql

Controllerのインストール先サーバーにMicrosoft SQL Server Expressをインストールしない場合に指定します。このオプションを指定しない場合、SQL Server Expressがサイトデータベースとして使用するためにインストールされます。（このオプションは、ローカルホストキャッシュに使用されるSQL Server Express LocalDBのインストールには影響しません）。

/quietまたは/passive

ユーザーインターフェイスを表示せずにインストールを実行します。インストールプロセスは、Windowsタスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

/remove

/componentsオプションで指定したコアコンポーネントを削除します。

/removeall

インストール済みのすべてのコアコンポーネントを削除します。

/sendexperiencemetrics

Citrix Insight Servicesへのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

/tempdir <*directory*>

インストール時に一時ファイルを作成するディレクトリを指定します。デフォルト値：c:\Windows\Temp

/xenapp

XenAppをインストールします。このオプションを指定しない場合、XenDesktopがインストールされます。

例：コアコンポーネントのインストール

次のコマンドを実行すると、XenDesktop、Controller、Studio、Citrixライセンスサーバー、およびSQL Server Expressがサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/configure_firewall

次のコマンドを実行すると、XenApp、Controller、Studio、およびSQL Server Expressがサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall

VDAのインストールに使用されるコマンドラインオプション

次のオプションは次のコマンドの1つまたは複数で有効です：**XenDesktopVDASetup.exe**、**VDAServerSetup.exe**、**VDAWorkstationSetup.exe**、または**VDAWorkstationCoreSetup.exe**。

/baseimage

仮想マシン上にVDA for Desktop OSをインストールする場合にのみ有効です。マスターイメージでのPersonal vDiskの使用を有効にします。詳しくは、「Personal vDisk」を参照してください。

このオプションはVDAWorkstationCoreSetup.exeインストーラーの使用時には無効です。

/components <*component*>[,<*component*>]

インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します。

VDA：Virtual Delivery Agent

PLUGINS：Citrix Receiver for Windows（CitrixReceiver.exe）

たとえば、Citrix Receiverではなく、VDAをインストールするには、/components vdaを指定します。

このオプションを指定しない場合、すべてのコンポーネントがインストールされます。

このオプションはVDAWorkstationCoreSetup.exeインストーラーの使用時には無効です。そのインストーラーはCitrix Receiverをインストールできません。

/controllers "<*controller*> [<*controller*>] [...]"

VDAが通信するControllerのFQDNを、引用符で囲んだスペース区切りのリストで指定します。/site_guidと/controllersを一緒に指定しないでください。

/disableexperiencemetrics

Citrix Insight Servicesへのインストール、アップグレード、または削除中に収集される分析の自動アップロードが阻止されます。

/enable_framehawk_port

Framehawkで使用されるUDPポートを開放します。デフォルト値：false

/enable_hdx_3d_pro

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAをHDX 3D Proモードでインストールします。

/enable_hdx_ports

Windowsファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、Controllerおよび有効な機能（Windowsリモートアシスタンスは除く）で必要なポートが開放されます。Windows以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートの情報については、「ネットワークポート」を参照してください。

ヒント： HDXアダプティブトランスポートがControllerとの通信に使用するUDPポートを解放するには、このオプションに加えて、/enable_hdx_udp_portsオプションを指定します。

/enable_hdx_udp_ports

Windowsファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、HDXアダプティブトランスポートに必要なポートがWindowsウォールで開放されます。Windows以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートの情報については、「ネットワークポート」を参照してください。

ヒント： VDAがControllerおよび有効化された機能との通信に使用するUDPポートを新たに解放するには、このオプションに加えて、/enable_hdx_portsオプションを指定します。

/enable_real_time_transport

オーディオパケットでUDPを使用してパフォーマンスを向上させる機能（リアルタイムオーディオ転送）を有効または無効にします。この機能を有効にすると、オーディオパフォーマンスを向上させることができます。Windowsファイアウォールサービスが検出されたときにUDPポートが開放されるようにするには、/enable_hdx_portsを指定してください。

/enable_remote_assistance

Directorで使用するWindowsリモートアシスタンスのシャドウ機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスによってファイアウォールで動的ポートが解放されます。

/exclude "<*component*>"[,"<*component*>"]

二重引用符で囲まれた、オプションコンポーネントをインストールしません。複数のコンポーネントを指定する場合は、カンマで区切って、二重引用符で囲みます。たとえば、MCSが管理していないイメージ上でVDAをインストールまたはアップグレードする場合、Personal vDiskコンポーネントやMachine Identity Serviceコンポーネントは必要ありません。以下の値を指定します。

Personal vDisk

Machine Identity Service

Citrix User Profile Manager

Citrix User Profile Manager WMI Plugin

Citrix ユニバーサルプリントクライアント

Citrixテレメトリサービス

Citrix Personalization for App-V - VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

インストールからCitrix Profile Managementを除くと（/exclude "Citrix User Profile Manager"オプションを使用）、Citrix Directorを使ったVDAの監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの［個人設定］パネル、および［EndPoint］ページの［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと［傾向］ページでは、Profile managementがインストールされているマシンについてのデータしか［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Managementサービスをインストールして実行することをお勧めします。Citrix Profile Managementサービスの有効化は、必須ではありません。

このオプションはVDAWorkstationCoreSetup.exeインストーラーの使用時には無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

/hまたは/help

コマンドのヘルプを表示します。

/hdxflashv2only

セキュリティを強化するため、従来のFlashリダイレクトのバイナリをインストールしません。

このオプションはグラフィックインターフェイスでは使用できません。

/installdir <*directory*>

コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値：c:\Program Files\Citrix

/logpath <*path*>

ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。Default = 「%TEMP%\Citrix\XenDesktop Installer」

このオプションはグラフィックインターフェイスでは使用できません。

/masterimage

仮想マシン上にVDAをインストールする場合にのみ有効です。VDAをマスターイメージとしてセットアップします。

このオプションはVDAWorkstationCoreSetup.exeインストーラーの使用時には無効です。

/no_mediafoundation_ack

MicrosoftのMedia Foundationがインストールされていなければ、複数のHDXマルチメディア機能はインストールされず、動作しないものがあることを認識します。このオプションが省略されていて、Media Foundationがインストールされていない場合、VDAインストールは失敗します。サポートされているほとんどのWindowsのエディションには、Nエディションの例外を除けば、Media Foundationが既にインストールされています。

/nocitrixwddm

WDDMドライバーを含まないWindows 7マシン上でのみ有効です。Citrix WDDMドライバーのインストールを無効にします。

このオプションはグラフィックインターフェイスでは使用できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/nodesktopexperience

VDA for Server OSをインストールする場合にのみ有効です。デスクトップエクスペリエンス拡張機能を無効にします。この機能の有効/無効は、Citrixポリシーの［デスクトップエクスペリエンス拡張］設定でも制御できます。

/noreboot

インストール後の再起動を無効にします。VDAは、再起動後にのみ使用できます。

/noresume

デフォルトでは、インストール中にマシンの再起動が必要になった場合、再起動が完了すると自動的にインストーラーが再開します。デフォルトを上書きするには、/noresumeを指定します。これは、メディアを再マウントする必要がある場合、または自動インストール中に情報をキャプチャする必要がある場合に役立ちます。

/optimize

仮想マシン上にVDAをインストールする場合にのみ有効です。ハイパーバイザー上の仮想マシンにインストールするVDAを最適化します。仮想マシンの最適化には、オフラインファイルの無効化、バックグラウンド最適化（デフラグ処理）の無効化、およびイベントログサイズの縮小などの操作が含まれます。リモートPCアクセスの展開では、このオプションを指定しないでください。詳しくは、CTX125874を参照してください。

/portnumber <*port*>

/reconfigオプションを指定する場合にのみ有効です。Virtual Delivery AgentとController間の通信で使用されるポート番号を変更します。変更前のポートは無効になります（ポート80を除く）。

/quietまたは/passive

ユーザーインターフェイスを表示せずにインストールを実行します。インストールおよび構成プロセスは、Windowsタスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

/reconfig

インストール済みのVirtual Delivery Agent設定をカスタマイズします。/portnumber、/controllers、または/enable_hdx_portsオプションと一緒に使用します。/quietオプションを指定しない場合は、VDAをカスタマイズするためのグラフィカルインターフェイスが開きます。

/remotepc

リモートPCアクセスの展開でのみ有効です。デスクトップOSで次のコンポーネントのインストールを除外します。

Citrix Personalization for App-V

Citrix User Profile Manager

Citrix User Profile Manager WMI Plugin

Machine Identity Service

Personal vDisk

このオプションはVDAWorkstationCoreSetup.exeインストーラーの使用時には無効です。このインストーラーは、上記のコンポーネントのインストールを自動的に除外します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/remove

/componentsオプションで指定したコンポーネントを削除します。

/removeall

インストール済みのすべてのコンポーネントを削除します。

/sendexperiencemetrics

Citrix Insight Servicesへのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

/servervdi

Windowsサーバー上にVDA for Desktop OSをインストールします。Windowsサーバー上にVDA for Server OSをインストールする場合は、このオプションを指定しないでください。このオプションを使用する前に、「サーバーVDI」を参照してください。

このオプションは、全製品VDAインストーラーでのみ使用してください。このオプションはグラフィックインターフェイスでは使用できません。

/site_guid <*guid*>

サイトのActive Directory組織単位（OU）のグローバル一意識別子（GUID）を指定します。Active Directory OUベースのController検出を使用する場合、GUIDにより仮想デスクトップとサイトが関連付けられます（デフォルトの検出方法である自動更新を使用することをお勧めします）。サイトGUIDは、Studioに表示されるサイトプロパティです。/site_guidと/controllersを一緒に指定しないでください。

/tempdir <*directory*>

インストール時に一時ファイルを作成するディレクトリを指定しますデフォルト値：c:\Windows\Temp

このオプションはグラフィックインターフェイスでは使用できません。

/virtualmachine

仮想マシン上にVDAをインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きして、BIOS情報を仮想マシンに渡して物理マシンとして振る舞うようにします。

このオプションはグラフィックインターフェイスでは使用できません。

例：VDAのインストール

全製品インストーラーでVDAをインストールする：

次のコマンドを実行すると、仮想マシン上のデフォルトの場所にVDA for Desktop OSおよびCitrix Receiverがインストールされます。このVDAはマスターイメージとして使用されます。VDAは、まず「mydomain」ドメインの「Contr-Main」サーバー上で動作するControllerに登録され、Personal vDisk、最適化機能、およびWindowsリモートアシスタンスが有効になります。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Main.mydomain.local" /enable_hdx_ports /optimize /masterimage /baseimage /enable_remote_assistance

VDAWorkstationCoreSetupスタンドアロンインストーラーでデスクトップOS VDAをインストールする：

次のコマンドは、リモートPCアクセスまたはVDI展開で使用するためにデスクトップOSにCore Services VDAをインストールします。Citrix Receiverとその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービスのポートが自動的に開放されます。管理者が再起動を処理します。

VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot

コマンドラインを使ったVDAのカスタマイズ

VDAをインストールした後で、いくつかの設定をカスタマイズできます。製品メディアの\x64\XenDesktop Setupディレクトリから、XenDesktopVdaSetup.exeコマンドを実行します。このとき、以下のオプションを指定します（各オプションについては「VDAのインストールに使用されるコマンドラインオプション」を参照してください）。

- /reconfigure（VDAをカスタマイズする場合は必須のオプションです）
- /hまたは/help
- /quiet
- /noreboot
- /controllers
- /portnumber
- /enable_hdx_ports

コマンドラインを使ったUniversal Print Serverのインストール

各プリントサーバー上で、次のいずれかのコマンドを実行します。

- サポートされている32ビットオペレーティングシステムで、 Citrixインストールメディアの\x86\Universal Print Server\ディレクトリから、**UpsServer_x86.msi**を実行します。
- サポートされている64ビットオペレーティングシステムで、 Citrixインストールメディアの\x64\Universal Print Server\ディレクトリから、**UpsServer_x64.msi**を実行します。

プリントサーバーにUniversal Print Serverコンポーネントをインストールした後で、「プリンターのプロビジョニング」の説明に従って、このコンポーネントを構成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スクリプトを使用したVDAのインストール

Dec 05, 2017

この記事は、WindowsオペレーティングシステムがインストールされたマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステムの VDAについては、「Linux Virtual Delivery Agent」を参照してください。

インストールメディアには、Active Directory環境のマシンでVirtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが収録されています。また、このスクリプトを使ってMachine Creation ServicesおよびProvisioning Servicesのマスターイメージを管理することもできます。

以下のアクセス権限が必要です。

- スクリプトを実行するには、VDAインストールコマンドがあるネットワーク共有に対するすべてのユーザーの読み取りアクセスが必要です。インストールコマンドはフルバージョンの製品ISOのXenDesktopVdaSetup.exe、またはスタンドアロンインストーラーのVDAWorkstationSetup.exeまたはVDAServerSetup.exeです。
- ログの詳細は各ローカルマシンに保存されます。また、レビューおよび分析のために結果ログをネットワーク上に保存する場合は、そのネットワーク共有に対するすべてのユーザーの読み取りおよび書き込みアクセスが必要です。

スクリプトの実行結果をチェックするには、ネットワーク共有のログを調べます。このログには、スクリプトログ、インストーラーログ、およびMSIインストールログが含まれます。各インストールまたは削除に関するログは、日時を示すフォルダー内に保存されます。フォルダー名には、操作の結果としてPASSまたはFAILのプレフィックスが付きます。失敗したインストールまたは削除処理を検索できるように、ネットワーク共有を使用します。これにより、ターゲットマシンのローカルライブに代わるツールが提供されます。

重要：インストールを始める前に、「インストールの準備」を読んで、必要なタスクを完了しておいてください。

スクリプトを使ってVDAをインストールまたはアップグレードする

1. インストールメディアの\Support\AdDeploy\からサンプルスクリプトのInstallVDA.batを開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します。
   - インストールするVDAのバージョンを指定します（SET DESIREDVERSION）。Version 7の場合はバージョンを「7.0」と指定できます。完全な値はインストールメディアのProductVersion.txtファイルに記述されています（7.0.0.3018など）。ただし、完全に一致させる必要はありません。
   - 実行するインストーラーのネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指定します。スクリプトにより、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に実行されます。たとえば、SET DEPLOYSHARE=\\fileserver1\share1と指定します。
   - オプションとして、ログを保存するためのネットワーク共有を指定します。たとえば、SET LOGSHARE=\\fileserver1\log1と指定します。
   - 「コマンドラインを使ったインストール」の説明に従って、VDAの構成オプションを指定します。/quietおよび/norebootオプションはデフォルトでスクリプトに含まれ、必須です（SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT）。
3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDAをインストールするマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、サポートされるオペレーティングシステムの各マシン上にVDAがインストールされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スクリプトを使ってVDAを削除する

1. インストールメディアの\Support\AdDeploy\からサンプルスクリプトのUninstallVDA.batを開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します（SET CHECK_VDA_VERSION）。Version 7の場合はバージョンを「7.0」と指定できます。完全な値はインストールメディアのProductVersion.txtファイルに記述されています（7.0.0.3018など）。ただし、完全に一致させる必要はありません。
   - オプションとして、ログを保存するためのネットワーク共有を指定します。
3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDAを削除するマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、各マシンからVDAが削除されます。

トラブルシューティング

スクリプトにより、スクリプトの進捗を示す内部ログファイルが生成されます。スクリプトは、展開の開始後すぐにKickoff_VDA_Startup_Scriptログをネットワーク共有にコピーします。これにより、処理全体が実行中であることを確認できます。このログがネットワーク共有にコピーされない場合は、ローカルマシンを調べることでトラブルシューティングを実行します。スクリプトにより、各マシンの%temp%フォルダーに以下の2つのデバッグログファイルが生成されます。

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

これらのログから、次の点を確認します。

- スクリプトが正しく実行されたかどうか。
- ターゲットのオペレーティングシステムが正しく検出されているかどうか。
- DEPLOYSHARE共有でROOT（AutoSelect.exeファイルを含んでいるフォルダー）が正しく構成されているかどうか。
- DEPLOYSHAREおよびLOGで指定した両方のネットワーク共有にアクセスできるかどうか。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サイトの作成

Dec 05, 2017

*サイト*とは、XenAppまたはXenDesktopの展開環境に名前を付けたものを指します。サイトは、Delivery Controllerなどのコアコンポーネント、VDA（Virtual Delivery Agent）、ホストへの接続、およびマシンカタログやデリバリーグループで構成されます。コアコンポーネントをインストールしたら、最初のマシンカタログやデリバリーグループを作成する前に、サイトを作成します。

サイトを作成すると、Citrixのカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPでは、統計情報や使用状況が匿名で収集され、Citrixに送信されます。最初のデータパッケージは、サイトを作成してから約7日後にCitrixに送信されます。登録内容は、サイトの作成後いつでも変更できます。Studioのナビゲーションペインで **[構成]** を選択し、［製品サポート］タブでガイダンスに従って操作します。詳しくは、http://more.citrix.com/XD-CEIPを参照してください。

サイトを作成する管理者には、そのサイトのすべての管理タスクの実行権限が設定されます。詳しくは 管理権限の委任」を参照してください。

サイトの作成ウィザードを開始する前に、この文書を確認してください。

サイトを作成するには：

Studioが起動していない場合は起動します。サイトの作成ウィザードを開始する手順が自動的に表示されます。ウィザードページには、以下の構成が含まれます。

サイトには、以下の2種類があります。いずれかを選択します。

- **アプリケーションとデスクトップを配信するサイト**：アプリケーションおよびデスクトップの配信サイトを作成する場合は、完全展開サイト（推奨）または空のサイトのいずれかを選択できます。空のサイトには一部の構成のみが含まれ、通常Citrix製品の管理に慣れた管理者がこのオプションを選択します。
- **リモートPCアクセスサイト**：リモートPCアクセスサイトは、特定のユーザーにオフィスにある自分のコンピューターへのセキュアなリモートアクセスを提供します。

ここでアプリケーションとデスクトップを配信するサイトを作成しても、リモートPCアクセス展開を後で追加できます。また、ここでリモートPCアクセス展開を選択しても、完全展開を後で追加できます。

サイトの名前を入力します。サイトの作成後、この名前がStudioのナビゲーションペイン（ **[Citrix Studio**（）］）の上部に表示されます。

[データベース] ページには、サイトのセットアップ、監視、および構成ログデータベースに関する選択が含まれます。データベースセットアップでの選択肢および要件について詳しくは、「データベース」を参照してください。

サイトのデータベースとして使用する目的でSQL Server Expressをインストールするように選択した場合（これはデフォルト設定です）、このソフトウェアのインストール後に再起動が行われます。SQL Server Expressソフトウェアをサイトのデータベースとしてインストールしない場合、再起動は行われません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、マシンにSQL Serverソフトウェアがインストールされていることを確認してください。サポートされるバージョンについては、「システム要件」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サイトにControllerを追加する必要があり、Controllerソフトウェアが別のサーバーに既にインストールされている場合、このページからこれらのControllerを追加できます。データベースをセットアップするスクリプトを生成する予定の場合には、スクリプトを生成する前にControllerを追加します。

既存のライセンスを使用するか、ライセンスファイルを後から追加できる30日間無料のお試し版を使用するかを決定します。サイトの作成ウィザード内で、ライセンスファイルをダウンロードしたりライセンスサーバーに追加したりすることもできます。詳しくは、Citrixライセンスのドキュメントを参照してください。

ライセンスサーバーのアドレスを、:[]の形式で指定します。名前はFQDN、NetBIOS、またはIPアドレスにする必要があります。推奨はFQDNです。ポート番号（）を入力しない場合は、デフォルトの27000が使用されます。**[接続]**をクリックします。ライセンスサーバーに接続されるまでは、ウィザードの次のページに進めません。

「リモートPCアクセス」を参照してください。

ハイパーバイザーまたはクラウドサービスで仮想マシンを使用してアプリケーションおよびデスクトップを提供する場合、必要に応じて、ホストへの最初の接続を作成できます。その接続のストレージリソースとネットワークリソースも指定できます。サイトの作成後、この接続やリソースを変更したり、追加の接続を作成したりできます。詳しくは、「接続とリソース」を参照してください。

[接続]ページ：「接続の種類の情報ソース」を参照してください。

ハイパーバイザーまたはクラウドサービスで仮想マシンを使用している場合（またはStudioを使用して専用ブレードPC上でデスクトップを管理する場合）には、接続の種類として**[なし]**を選択します。

リモートPCアクセスサイトを構成しており、Wake on LAN機能を使用する予定の場合、**[Microsoft System Center Configuration Manager]**を選択します。

接続の種類に加え、仮想マシンの作成でCitrixのツール（Machine Creation Servicesなど）を使用するか、その他のツールを使用するかも指定します。

[ストレージ]ページと[ネットワーク]ページ: ストレージの種類と管理方法について詳しくは、「ホストストレージ」、「ストレージの管理」、および「ストレージの選択」を参照してください。

機能を選択してサイトをカスタマイズできます。情報の入力が必要な項目のチェックボックスをオンにすると、構成ボックスが開きます。

AppDNA統合

AppDiskを使用していて、AppDNAがインストールされている場合には有効です。AppDNA統合では、AppDisk内のアプリケーションを分析できます。互換性の問題を確認し、それらの問題を解決するための修復アクションを実施できます。詳しくは、「AppDisks」を参照してください。

App-V公開

App-Vサーバー上のMicrosoft App-Vパッケージのアプリケーションを使用する場合は、この機能を選択します。App-V管理サーバーのURLと、App-V公開サーバーのURLおよびポート番号を入力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ネットワーク共有上にあるApp-Vパッケージのアプリケーションのみを使用する場合は、この機能を選択する必要はありません。

この機能は、後でStudioから有効/無効にする、または構成することもできます。詳しくは、App-Vを参照してください。

リモートPCアクセス展開について詳しくは、「リモートPCアクセス」を参照してください。

Wake on LAN機能を使用している場合、サイトを作成する前にMicrosoft System Center Configuration Managerの構成手順を実行します。詳しくは、「Microsoft System Center Configuration Manager」を参照してください。

リモートPCアクセスサイトを作成する場合：

- Wake on LAN機能を使用している場合、Microsoft System Center Configuration Managerのアドレス、資格情報、および接続情報を**[電源管理]**ページで指定します。
- **[ユーザー]**ページで、ユーザーまたはユーザーグループを指定します。すべてのユーザーを自動的に追加するためのデフォルトの機能はありません。また、**[マシンアカウント]**ページでマシンアカウント（ドメインおよびOU）情報も指定します。

  ユーザー情報を追加するには、**[ユーザーの追加]**をクリックします。ユーザーおよびユーザーグループを選択し、**[ユーザーの追加]**をクリックします。

  マシンアカウント情報を追加するには、**[マシンアカウントの追加]**をクリックします。マシンアカウントを選択し、**[マシンアカウントを追加]**をクリックします。**[組織単位の追加]**をクリックします。ドメインおよび組織単位を選択して、サブフォルダー内の項目を含めるかどうかを指定します。**[組織単位の追加]**をクリックします。

リモートPCアクセスサイトの作成時には、リモートPCユーザーマシンアカウントという名前のマシンカタログが自動的に作成されます。このカタログには、サイトの作成ウィザードで追加したすべてのマシンアカウントが含まれています。リモートPCユーザーデスクトップという名前のデリバリーグループが、自動的に作成されます。このグループには、追加したすべてのユーザーおよびユーザーグループが含まれています。

サイトの作成ウィザードの最終ページには、指定した情報がまとめられています。内容を変更する場合は、**[戻る]**をクリックします。終了したら、**[作成]**をクリックするとサイト作成が開始されます。

サイト構成のテスト

サイトの作成後にテストを実行するには、ナビゲーションペインの上部で**[Citrix Studio（サイト*<サイト名>*）]**を選択します。中央のペインで、**[サイトのテスト]**をクリックします。テスト結果は、HTML形式のレポートで確認できます。

Windows Server 2016にインストールされたControllerでは、サイトのテスト機能がエラーになる場合があります。サイトデータベースにローカルのSQL Server Expressが使用され、SQL Server Browserサービスが開始されていない場合にエラーが発生します。このエラーを回避するには、以下のタスクを行います。

1. （必要に応じて）SQL Server Browserサービスを有効にして開始する。
2. SQL Server（SQLEXPRESS）サービスを再開始する。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

トラブルシューティング

サイトを成したら、Studioをインストールし、MMCを介してスナップインとしてリモートマシンに追加します。そのスナップインを後に削除しようとすると、MMCの応答が停止する場合があります。この問題が発生した場合は、MMCを再起動してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マシンカタログの作成

Apr 16, 2018

物理マシンまたは仮想マシンのグループは、「マシンカタログ」と呼ばれる単一のエンティティとして管理されます。カタログ内のマシンは、オペレーティングシステムの種類（サーバーまたはデスクトップ）がすべて同じです。サーバーOSマシンを含むカタログには、WindowsマシンまたはLinuxマシンのいずれかのみを含めることができ、両方を含めることはできません

サイトを作成した後、Studioでは最初のマシンカタログを作成する手順が表示されます。最初のカタログを作成した後、Studioでは最初のデリバリーグループを作成する手順が表示されます。作成したカタログを後で変更したり、追加のカタログを作成したりすることができます。

概要

仮想マシンのカタログの作成時には、それらの仮想マシンのプロビジョニング方法を指定します。Machine Creation Services（MCS）やProvisioning Services（PVS）などのCitrixツールを使用できます。または、独自のツールを使用してマシンをプロビジョニングすることもできます。

- PVSを使用してマシンを作成する場合、手順についてはProvisioning Servicesのドキュメントを参照してください。
- MCSを使用して仮想マシンをプロビジョニングする場合、カタログ内に同じ仮想マシンを作成するためのマスターイメージ（またはスナップショット）を提供します。カタログを作成する前に、まずハイパーバイザーまたはクラウドサービスのツールを使用し、マスターイメージを作成して構成します。この処理には、イメージへのVirtual Delivery Agent（VDA）のインストールが含まれます。その後、Studioでマシンカタログを作成します。そのイメージ（またはイメージのスナップショット）を選択し、カタログで作成する仮想マシンの数を指定して、追加情報を構成します。
- マシンが既に提供されており、マスターイメージが必要ない場合でも、マシンに対して1つまたは複数のマシンカタログを作成する必要があります。

MCSまたはPVSを使用して最初のカタログを作成する場合、サイトの作成時に構成したホスト接続を使用します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、その接続に関する情報を変更したり、追加接続を作成したりすることができます。

カタログの作成ウィザードを完了すると、テストが自動的に実行され、正しく構成されているかどうかが検証されます。テストが完了したら、テストレポートを表示できます。Studioからテストをいつでも実行できます。

オンプレミス展開の場合のみ：MCSまたはPVSを使用して最初のカタログを作成する場合、サイトの作成時に構成したホスト接続を使用します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、その接続に関する情報を変更したり、追加接続を作成したりすることができます。

ヒント： PowerShell SDKを使用してカタログを直接作成する場合、イメージまたはそのスナップショットの代わりに、ハイパーバイザーテンプレート（VMTemplates）を指定できます。

仲介セッションを起動する場合、検討対象のDelivery Controller（オンプレミス展開用）またはCloudコネクタ（Citrix Cloud展開用）にVDAが登録されている必要があります。VDAが登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDAが登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Studioでは、カタログ作成ウィザードで、マシンをカタログからDelivery Groupに登録した後に、トラブルシューティング情報が提供されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

カタログ作成ウィザードで、既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージによって問題のあるマシンが特定された場合は、該当のマシンを（**[削除]** ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（登録されたことがないなどの理由により）マシンに関する情報を取得できないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

機能レベルに関するメッセージについては、「VDAバージョンと機能レベル」を参照してください。

VDA登録に関するトラブルシューティングについて詳しくは、CTX136668を参照してください。

以下は、カタログの作成ウィザードに情報を入力した後のデフォルトのMCS操作の簡単な概要です。

- （スナップショットではなく）マスターイメージを選択した場合、MCSでスナップショットが作成されます。
- MCSでスナップショットの完全コピーが作成され、ホスト接続で定義されたストレージの各場所に格納されます。
- MCSによってマシンがActive Directoryに追加され、そこで一意の識別子が作成されます。
- ウィザードで指定した数の仮想マシンがMCSによって作成され、各仮想マシンに対して2つのディスクが定義されます。1つの仮想マシンにつき2つのディスクに加えて、同じストレージの場所にマスターも保存されます。ストレージの場所が複数定義されている場合、それぞれの場所に以下の種類のディスクが割り当てられます。
  - スナップショットの完全コピー（前述の説明を参照）。読み取り専用であり、作成した仮想マシン間で共有されます。
  - 各仮想マシンに一意の識別子を与える、一意のIDディスク（16MB）。各仮想マシンに対し、1つのIDディスクが割り当てられます。
  - 仮想マシンへの書き込みを保存する、一意の差分ディスク。このディスクは（ホストストレージでサポートされている場合）シンプロビジョニングされ、必要に応じてマスターイメージの最大サイズまで拡大します。各仮想マシンに対し、1つの差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保存されます。専用デスクトップの場合、この変更は無期限に保存されます。プールされたデスクトップの場合、再起動のたびにこの変更は削除され、新しい変更が作成されます。

または、仮想マシンを作成して静的デスクトップを配信する場合、（カタログの作成ウィザードの**[マシン]** ページで）シックな（完全コピーの）仮想マシンのクローンを指定できます。完全なクローンでは、すべてのデータストアにマスターイメージを保持する必要はありません。各仮想マシンに独自のファイルが存在します。

ハイパーバイザーまたはクラウドサービスでのマスターイメージの準備

ヒント： ハイパーバイザーおよびクラウドプロバイダーへの接続の作成については、 接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化しないアプリケーション、VDA、およびそのほかのソフトウェアをインストールしておきます。

ヒント：

- マスターイメージは、「クローンイメージ」、「ゴールデンイメージ」、「ベース仮想マシン」、または「基本イメージ」と呼ばれることがあります。ホストベンダーとクラウドサービスプロバイダーで、異なる用語を使用する場合もあります。
- PVSを使用する場合は、マスターイメージまたは物理コンピューターをマスターターゲットデバイスとして使用できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PVSでは、イメージを指すのにMCSとは異なる用語を使用します。詳しくは、Provisioning Servicesのドキュメントを参照してください。

- ハイパーバイザーまたはクラウドサービスに、作成されたマシン数に対応する十分なプロセッサ、メモリー、ストレージがあることを確認してください。
- デスクトップとアプリケーションで必要な適切な量のハードディスクスペースを構成します。この値は、後で、またはマシンカタログ内で変更することはできません。
- リモートPCアクセスのマシンカタログでは、マスターイメージを使用しません。
- MCS使用時のMicrosoft KMSライセンス認証に関する注意事項：VDA 7.xをXenServer 6.1、XenServer 6.2、vSphere、またはMicrosoft System Center Virtual Machine Managerホストで使用している場合、Microsoft WindowsやMicrosoft Officeのライセンスを手動でリセットする必要はありません。VDA 5.xをXenServer 6.0.2ホストで使用している場合は、CTX128580を参照してください。
- マスターイメージに以下のソフトウェアをインストールして構成します。
  - ハイパーバイザー用の統合ツール（XenServer Tools、Hyper-V統合サービス、VMware Toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく動作しなくなる場合があります。
  - VDA。最新の機能を利用できるように、最新バージョンをインストールすることをお勧めします。マスターイメージにVDAをインストールできないと、カタログ作成が失敗します。
  - アンチウイルスプログラムや電子ソフトウェア配信エージェントなどのサードパーティツール（必要に応じて）。ユーザーやマシンの種類に適した設定で、サービス（更新機能など）を構成します。
  - 仮想化せずにユーザーに提供するサードパーティのアプリケーション。ただし、可能な場合はアプリケーションを仮想化することをお勧めします。仮想化することで、アプリケーションを追加したり再構成したりするたびにマスターイメージを更新する必要がなくなり、コストが削減されます。また、各デスクトップにインストールするアプリケーションが少なくなるため、マスターイメージのハードディスクのサイズを減らしてストレージコストを節約できます。
  - App-Vアプリケーションを公開する場合は、推奨設定のApp-Vクライアント。App-V Clientは、Microsoft社から提供されます。
  - MCSで作成したマシンカタログで、ローカライズされたMicrosoft Windowsを配信する場合は、マスターイメージに言語パックをインストールして言語オプション（システムロケールや表示言語など）を設定しておく必要があります。これにより、プロビジョニング時にスナップショットが作成されると、その言語パックおよび言語オプションが仮想マシンで使用されます。

重要： PVSまたはMCSを使用する場合は、マスターイメージ上でMicrosoft System Preparation Utility（Sysprep）を実行しないでください。

マスターイメージを準備するには

1. ハイパーバイザーの管理ツールを使用して、マスターイメージを作成してから、オペレーティングシステムと、すべてのサービスパックおよび更新プログラムをインストールします。仮想CPUの数を指定します。また、PowerShellを使用してマシンカタログを作成する場合、仮想CPUの値を指定することもできます。Studioを使用してカタログを作成する場合には、仮想CPUの数は指定できません。デスクトップとアプリケーションで必要な量のハードディスクスペースを構成します。この値は、後で、またはカタログ内で変更することはできません。
2. ハードディスクはデバイスの場所「0」で接続されている必要があります。多くの標準マスターイメージテンプレートでは、デフォルトでこの場所にハードディスクが構成されますが、カスタムテンプレートを使用する場合は注意してください。
3. マスターイメージに前述のソフトウェアをインストールして構成します。
4. PVSを使用する場合は、マスターターゲットデバイスをドメインに追加する前に、マスターターゲットデバイスから作成したvDiskのVHDファイルを作成します。詳しくは、Provisioning Servicesのドキュメントを参照してください。
5. MCSを使用していない場合、マスターイメージはアプリケーションとデスクトップがメンバーとなっているドメインに統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。MCSを使用している場合、ドメインへのマスターイメージの統合は必要ありません。プロビジョニングされたマシンは、カタログの作成ウ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ザードで指定されたドメインに統合されます。
6. マスターイメージのスナップショットを作成して、わかりやすい名前を付けておくことをお勧めします。カタログの作成時にスナップショットの代わりにマスターイメージを指定すると、Studioによりスナップショットが作成されますが、そのスナップショットにわかりやすい名前を付けることはできません。

ホストインフラストラクチャとしてXenServerを使用する場合は、GPU対応マシンに専用のマスターイメージが必要です。これらの仮想マシンには、GPUをサポートするビデオカードドライバーが必要です。仮想マシンがGPUを使用して稼働するソフトウェアによって動作できるように、GPU対応のマシンを構成します。

1. XenCenterを使用して、標準的なVGA、ネットワーク、およびvCPUを指定して仮想マシンを作成します。
2. 作成した仮想マシンの構成を変更して、GPU機能（パススルーまたは仮想GPU）を有効にします。
3. 仮想マシンに適切なオペレーティングシステムをインストールして、RDPを有効にします。
4. XenServer ToolsとNVIDIAドライバーをインストールします。
5. パフォーマンスを最適化するため、Virtual Network Computing（VNC）Admin Consoleをオフにして、仮想マシンを再起動します。
6. RDPの使用を確認するメッセージが表示されます。RDPを使用してVDAをインストールし、仮想マシンを再起動します。
7. 必要に応じて、仮想マシンのスナップショットを作成します。このスナップショットは、ほかのGPUマスターイメージのテンプレートとして使用できます。
8. RDPを使用して、GPUを使用するアプリケーションを仮想マシンにインストールします。

Studioでのカタログの作成

カタログの作成ウィザードを開始する前に、このセクションを確認して、選択する項目および指定する情報について理解しておいてください。

重要：マスターイメージを使用している場合、カタログを作成する前に、イメージにVDAがインストールされていることを確認してください。

Studioで以下の操作を行います。

- サイトは作成したがマシンカタログは作成していない場合は、カタログを作成するための説明が表示されます。
- 既存のマシンカタログがあり、別のマシンカタログを作成する場合は、Studioのナビゲーションペインで**[マシンカタログ]** を選択します。その後、［操作］ペインの **[マシンカタログの作成]** を選択します。

ウィザードの指示に従って、以下の操作を行います。選択内容によっては、異なるウィザードページが表示されることがあります。

各カタログでは、以下のいずれかの種類のマシンを追加します。

- **サーバーOS：**サーバーOSのカタログでは、ホストされた共有デスクトップおよびアプリケーションが提供されます。マシンでは、サポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、両方をカタログに含めることはできません。（このOSについて詳しくは、Linux VDAのドキュメントを参照してください）。
- **デスクトップOS：**デスクトップOSのカタログでは、さまざまなユーザーに割り当てることができるVDIデスクトップやアプリケーションが提供されます。
- **リモートPCアクセス：**リモートPCアクセスのカタログでは、オフィスにあるユーザーの物理デスクトップマシンへのリモートアクセスが提供されます。リモートPCアクセスでは、セキュリティを保護するためのVPNが不要です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

このページは、リモートPCアクセスカタログを作成するときには表示されません。

[マシン管理] ページでは、マシンの管理方法と、マシンの展開に使用するツールが示されます。

Studioを使用してカタログ内のマシンの電源を管理するかどうかを選択します。

- Studioで電源管理したりクラウド環境でプロビジョニングしたりするマシン（仮想マシンやブレードPCなど）。このオプションは、ハイパーバイザーやクラウドサービスへの接続が構成済みの場合にのみ使用可能です。
- Studioで電源管理しないマシン（物理マシンなど）。

マシンがStudioで電源管理されるか、クラウド環境でプロビジョニングされるよう指定した場合、仮想マシンの作成に使用するツールを選択します。

- **Citrix MCS（Machine Creation Services）** - マスターイメージを使用して仮想マシンを作成および管理します。クラウド環境内のマシンカタログではMCSが使用されます。MCSは物理マシンでは使用できません。
- **Citrix PVS（Provisioning Services）** - 複数のターゲットデバイスを単一のデバイスコレクションとして管理します。マスターターゲットデバイスからイメージ作成されたPVS vDiskを使用して、デスクトップとアプリケーションを配信します。このオプションはクラウド展開では使用できません。
- **ほかのサービスまたはテクノロジ—** 上記以外のツールでデータセンター内の既存のマシンを管理します。この場合、Microsoft System Center Configuration Managerまたはほかのサードパーティアプリケーションを使用してカタログ内のマシン構成の一貫性を保つことをお勧めします。

このページは、デスクトップOSマシンを含むカタログを作成しているときにのみ表示されます。

[デスクトップエクスペリエンス] ページで、ユーザーがログオンするたびに何が起きるかを特定できます。次のいずれかを選択します。

- ユーザーは、ログオンするたびに新しい（ランダムの）デスクトップに接続されます。
- ユーザーは、ログオンするたびに同じ（静的な）デスクトップに接続されます。

2つめのオプションを選択し、PVSを使用してマシンをプロビジョニングしている場合、デスクトップへのユーザー変更の処理方法を構成できます。

- ユーザー変更を個別のPersonal vDisk上のデスクトップに保存する。
- ユーザー変更をローカルディスク上のデスクトップに保存する。
- ユーザーがログオフしたらユーザー変更を破棄し、仮想デスクトップをクリアする。

このページは、MCSを使用して仮想マシンを作成するときにのみ表示されます。

ホストハイパーバイザーまたはクラウドサービスへの接続を選択してから、過去に作成したスナップショットまたは仮想マシンを選択します。最初のカタログを作成する場合、サイトの作成時に構成した接続のみを使用できます。

そのほかの注意事項：

- MCS（またはPVS）を使用する場合は、マスターイメージ上でMicrosoft System Preparation Utility（Sysprep）を実行しないでください。
- スナップショットの代わりにマスターイメージを指定すると、Studioでスナップショットが作成されますが、そのスナッ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ショットにわかりやすい名前を付けることはできません。

最新の製品機能を使用できるようにするため、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトで選択されている最小VDAは変更しないでください。ただし、以前のバージョンのVDAを使用する必要がある場合には、「VDAバージョンと機能レベル」を参照してください。

ウィザードで過去に選択したマシン管理テクノロジとの互換性がないスナップショットまたは仮想マシンを選択すると、エラーメッセージが表示されます。

仮想マシンをホストするのにクラウドサービスやプラットフォームを使用している場合（Azure Resource Manager、Nutanix、Amazon Web Servicesなど）、カタログの作成ウィザードにホストに特有の追加ページが含まれることがあります。

詳しくは、「接続の種類に関する情報の参照先」を参照してください。

このページは、PVSを使用して仮想マシンを作成するときにのみ表示されます。このページには、まだカタログに追加されていないデバイスコレクションおよびデバイスが表示されます。

使用するデバイスコレクションを選択してください。詳しくは、Provisioning Servicesのドキュメントを参照してください。

このページは、リモートPCアクセスカタログを作成するときには表示されません。

このページのタイトルは、**[マシン管理]** ページの **[マシン]**、**[仮想マシン]**、**[仮想マシンとユーザー]** で選択した項目によって変わります。

MCSを使ってマシンを作成する場合：

- 作成する仮想マシンの数を指定します。
- 各仮想マシンのメモリ量（MB単位）を選択します。
- **重要：** 作成された各仮想マシンにハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- **[デスクトップエクスペリエンス]** ページでユーザーによる静的デスクトップへの変更を専用のPersonal vDiskに保存することを指定した場合は、vDiskサイズ（GB単位）とドライブ文字を指定します。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的なデスクトップ仮想マシンを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- Personal vDiskを使用しないランダムなデスクトップ仮想マシンを作成する場合は、各マシンの一時データに対して使用するキャッシュを構成できます。「一時データ用キャッシュの構成」を参照してください。

PVSを使ってマシンを作成する場合：

[デバイス] ページには、前のウィザードページで選択したデバイスコレクションにあるマシンが一覧表示されます。このページでは、マシンを追加または削除することができません。

他のツールを使ってマシンを配信する場合：

Active Directoryマシンアカウント名の追加（またはアカウント名一覧のインポート） 仮想マシンのActive Directoryアカウント名は、追加またはインポートした後に変更できます。 **[デスクトップエクスペリエンス]** ウィザードページで静的なマシンを指定すると、追加する各仮想マシンにオプションでActive Directoryユーザー名を指定できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前を追加またはインポートした後で、**[削除]**ボタンを使用して、ユーザーはウィザードページ上のままで一覧から名前を削除できます。

PVSまたは他のツール（MCS以外）を使う場合：

追加（またはPVSデバイスコレクションからインポート）される各マシンのアイコンとツールチップは、カタログに追加できない可能性のあるマシン、またはDelivery Controllerで登録できない可能性のあるマシンの特定に役立ちます。詳しくは、「VDAバージョンと機能レベル」を参照してください。

仮想マシンコピーモード

[マシン]ページで指定するコピーモードによって、MCSがマスターイメージからシン（簡易コピー）クローンまたはシック（完全コピー）クローンのどちらを作成するかが決定されます。（デフォルトはシンクローン）

- 簡易コピークローンは、効率的にストレージを使用し、すばやくマシンを作成したい場合に使います。
- 完全コピークローンは、マシン作成後にIOPSが潜在的に低下した場合に、質の高いデータの復元と移行サポートが必要な場合に使います。

VDAバージョンと機能レベル

カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要な場合があります。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能がカタログで利用できるようになります。ただし、以前のVDAバージョンのカタログにあるマシンは登録できません。

[マシン]（または**[デバイス]**）ページの下部近くにあるドロップダウンを使って、登録できる最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトで、オンプレミスの展開には最新の機能レベルが選択されます。Citrixの推奨事項に従ってVDAとコアコンポーネントを常に最新のバージョンでインストールおよびアップグレードする場合は、この選択を変更する必要がありません。以前のVDAバージョンを使用し続ける必要がある場合は、正しい値を選択してください

XenAppおよびXenDesktopリリースには、新しいVDAバージョンが含まれないことがあります。または、新しいVDAは、機能レベルに影響を与えません。このような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントより以前のVDAバージョンであることを示します。たとえば、XenAppおよびXenDesktop 7.15 LTSRには、7.15 VDAが含まれますが、デフォルトの機能レベル（7.9以降）が最新のまま保持されます。このため、コンポーネントのインストール、または7.9～7.14から7.15 LTSRへのアップグレード後にデフォルトの機能レベルを変更する必要はありません。

（Citrix Cloudの展開では、Studioは最新の機能レベルより古い可能性のあるデフォルトの機能レベルを使用します）。

選択した機能レベルは、このレベルのマシンの一覧に影響します。一覧で、各エントリの横にあるツールチップは、マシンのVDAがその機能レベルでカタログと互換性があるかどうかを示します。

各マシンのVDAが選択した最小機能レベルを満たさない、または超過している場合、ページにメッセージが表示されます。ウィザードは続行できますが、これらのマシンは後でControllerによって登録できない可能性があります。代わりに、以下を行うことができます。

- 古いVDAが含まれるマシンを一覧から削除し、VDAをアップグレードしてからマシンをカタログに追加し直します。
- 低い機能レベルを選択します。ただし、これによって最新の製品機能にアクセスできなくなります。

マシンの種類が正しくないためにマシンがカタログに追加されなかった場合には、メッセージも表示されます。たとえば、テ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スクトップOSカタログにサーバーを追加しようとした場合、ランダム割り当て用に作成されたデスクトップOSマシンを静的マシンのカタログに追加した場合などです。

一時データ用キャッシュの構成

仮想マシンでローカルに行う一時データのキャッシュはオプションです。MCSを使用してカタログ内のプールされた（専用ではない）マシンを管理するときに、マシンの一時データキャッシュの使用を有効にできます。カタログで一時データのストレージを指定する接続を使用する場合は、カタログ作成時に一時データキャッシュ情報を有効にして構成できます。

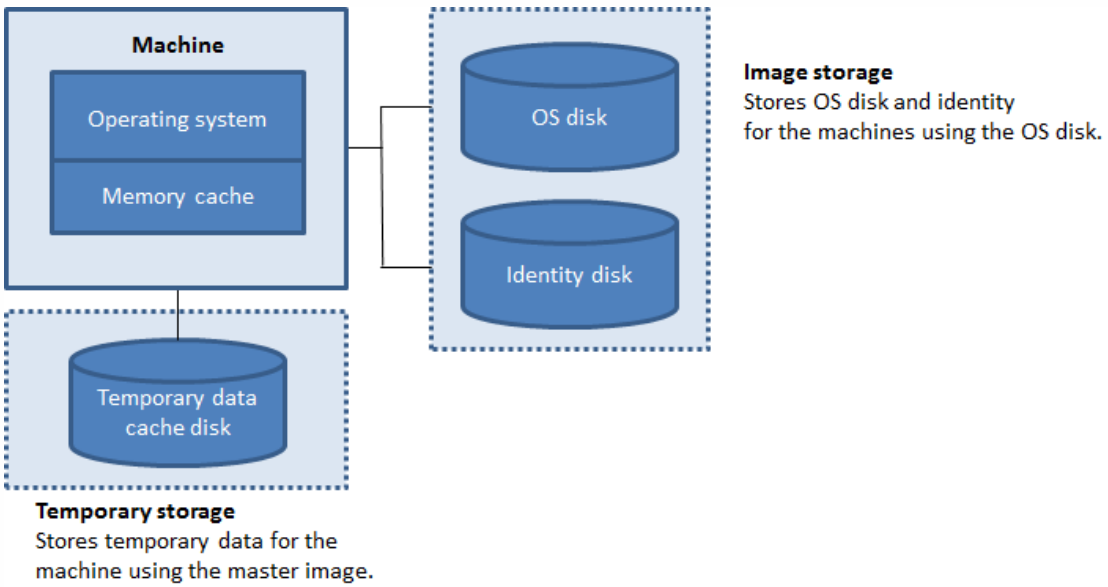
一時データのキャッシュを有効にするには、カタログの各マシンのVDAをバージョン7.9以上にする必要があります。

カタログで使用する接続を作成するときに、一時データで共有ストレージとローカルストレージのどちらを使用するかを指定します。詳しくは「接続とリソース」を参照してください。カタログでの一時キャッシュの有効化と構成には、**[キャッシュに割り当てられたメモリ（MB）]**と**[ディスクキャッシュサイズ（GB）]**という2つのチェックボックスと値があります。デフォルト値は、接続の種類により異なります。通常は、デフォルト値で十分なことが多いですが、次のデータに必要な容量を検討します。

- Windowsページファイルなどの、Windows自体が作成する一時データファイル
- ユーザープロファイルデータ
- ユーザーのセッションに同期されるShareFileデータ
- セッションユーザーによって作成またはコピーされるデータや、ユーザーがセッション内にインストールするアプリケーション

Windowsでは、マシンカタログのマシンがプロビジョニングされる元のマスターイメージの空き容量より極端に大きいキャッシュディスクをセッションで使用することはできません。たとえば、マスターイメージの空き容量が10GBしかないのに、20GBのキャッシュディスクを指定してもメリットはありません。

[ディスクキャッシュサイズ]チェックボックスをオンにした場合は、一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが、構成されている制限（**[キャッシュに割り当てられたメモリ]**の値）に到達すると、最も古いデータが一時データキャッシュディスクに移動されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

メモリキャッシュは、各マシンの合計メモリ容量の一部であるため、**[キャッシュに割り当てられたメモリ]** チェックボックスをオンにする場合は、各マシンの合計メモリ容量の増加を考慮します。

[キャッシュに割り当てられたメモリ] チェックボックスをオフにし、**[ディスクキャッシュサイズ]** チェックボックスをオンのままにすると、一時データはメモリキャッシュの最小量に達するまでキャッシュディスクに直接書き込まれます。

[ディスクキャッシュサイズ] をデフォルト値から変更すると、パフォーマンスに影響が及ぶ可能性があります。サイズはユーザー要件とマシンの負荷に合わせる必要があります。

重要： ディスクキャッシュの容量が不足すると、ユーザーセッションは利用できなくなります。

[ディスクキャッシュサイズ] チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合は、**[キャッシュに割り当てられたメモリ]** にすべての一時データを格納できる十分に大きい値を指定します。この設定ができるのは、大容量のRAMを各仮想マシンに割り当てられる場合だけです。

両方のチェックボックスをオフにすると、一時データはキャッシュされず、各仮想マシンの差分ディスク（OSストレージにあります）に書き込まれます。（これは、7.9より前のリリースでは、プロビジョニングアクションです。）

このカタログを使用してAppDiskを作成しようとしている場合は、キャッシュを有効にしないでください。

Nutanixホスト接続を使用している場合、この機能は使用できません。

マシンカタログの作成後は、キャッシュ値を変更できません。

このページは、リモートPCアクセスカタログを作成するときには表示されません。

複数のNICを使用する場合は、各NICに仮想ネットワークを関連付けます。たとえば、特定のセキュアネットワークへのアクセスに1枚のNICを割り当てて、より一般的なネットワークへのアクセスに別のNICを割り当てることができます。また、このページでNICを追加または削除することもできます。

このページは、リモートPCアクセスカタログを作成するときにのみ表示されます。

ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を指定して追加します。組織単位名にはスラッシュ（/）を使用しないでください。

構成済みの電源管理接続を選択するか、電源管理を使用しないことを選択します。電源管理に必要な接続が構成済みでない場合は、マシンカタログの作成後に新しい接続を作成してから、そのマシンカタログを編集して電源管理設定を更新できます。

このページは、MCSを使用して仮想マシンを作成するときにのみ表示されます。

カタログ内の各マシンには、対応するActive Directoryコンピューターアカウントを割り当てる必要があります。新しいアカウントを作成するか既存のものを選択して、アカウントの場所を指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 新しいアカウントを作成する場合は、マシンが存在するドメインのドメイン管理者権限が必要です。

  作成するマシンのアカウント名前付けスキームを指定します。番号記号（#）により、名前に追加される連番または文字とその位置が定義されます。組織単位名にはスラッシュ（/）を使用しないでください。名前の先頭に番号記号を配置することはできません。たとえば、名前付けスキームとして「PC-Sales-##」を指定して［0～9］を選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウント名が作成されます。

- 既存のアカウントを使用する場合、アカウントを参照するか、［インポート］をクリックしてアカウント名の一覧のCSVファイルを指定します。インポートするファイルでは、次の形式を使用する必要があります。

  [ADComputerAccount]
  ADcomputeraccountname.domain

  ...

  追加するマシンに十分な数のアカウントをインポートする必要があります。これらのアカウントはStudioで管理されるため、すべてのアカウントのパスワードのリセットをStudioに許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

物理マシンまたは既存のマシン用のカタログでは、既存のアカウントを選択またはインポートして、各マシンをActive Directoryコンピューターアカウントおよびユーザーアカウントに割り当てます。

PVSで作成されたマシンでは、ターゲットデバイスのコンピューターアカウントは異なる方法で管理されます。詳しくは、Provisioning Servicesのドキュメントを参照してください。

ウィザードの**［概要］**ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報は、Studioに表示されます。

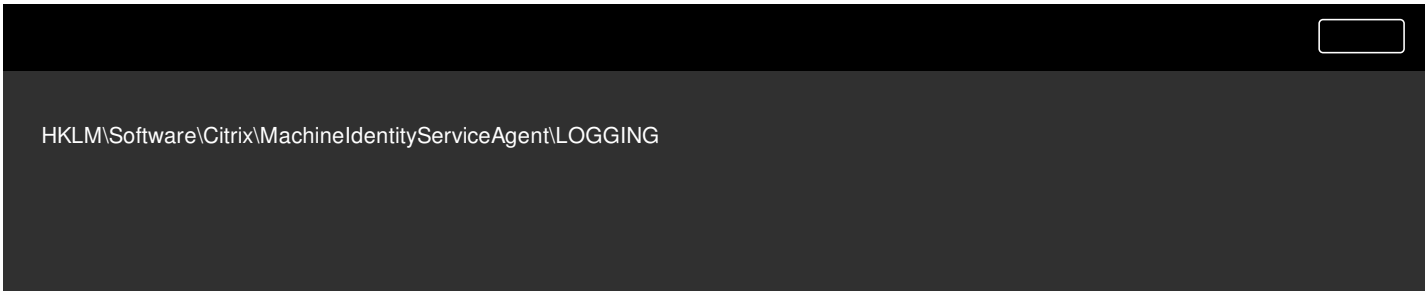
指定した情報を確認してから、**［完了］**をクリックしてカタログ作成を開始します。

トラブルシューティング

このセクションの情報を使用して、マシンカタログで作業する時に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行います。

サポートチームが解決策を提供するのに役立つログを収集することをお勧めします。このセクションで、ログファイルを生成する手順を説明します。

1. マスターイメージで次のレジストリキーを作成し、値（DWORD（32ビット）の値）を1に設定します。



2. マスターイメージを閉じて、新しいスナップショットを作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. DDCで、Citrix PowerShellスナップインを読み込んでPowerShellを起動し、次のコマンドを実行します。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True
```

4. このスナップショットに基づいて新しいカタログを作成します。

5. ハイパーバイザーで準備用仮想マシンが作成されたら、C:\:のルートからログインして次のファイルを抽出します。

- Image-prep.log
- PvsVmAgentLog.txt

6. マシンをシャットダウンすると、その時点でエラーが報告されます。

7. 次のPowerShellコマンドを実行して、イメージ準備マシンの自動シャットダウンを再度有効にします。

```
Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

マシンカタログの管理

Dec 05, 2017

ここでは次のことについて説明します。

- はじめに
- マシンカタログへのマシンの追加
- マシンカタログからのマシンの削除
- マシンカタログの説明やリモートPCアクセスの設定を変更する
- マシンカタログ名の変更
- 別のゾーンへのマシンカタログの移動
- マシンカタログの削除
- マシンカタログにおけるActive Directoryコンピューターアカウントの管理
- マシンカタログの更新
- マシンカタログのアップグレード

はじめに

マシンカタログにマシンを追加したり、カタログからマシンを削除したり、マシンカタログの名前や説明を変更したりすることができます。また、カタログのActive Directoryコンピューターアカウントを管理できます。

カタログの管理には、最新のOSアップデート、アンチウイルスプログラムのアップデート、オペレーティングシステムのアップグレード、または構成の変更が各マシンに適用されていることの確認も含めることができます。

- Machine Creation Services（MCS）を使用して作成されたプール（ランダム）マシンが含まれるカタログの場合は、カタログで使用されるマスターイメージを更新してからマシンを更新することにより、マシンを管理できます。これにより、多数のユーザーマシンを効率的に更新することができます。Provisioning Servicesで作成されたマシンの場合は、vDiskを介してマシンを更新します。詳しくは、Provisioning Servicesのドキュメントを参照してください。
- 静的で恒久的に割り当てられたマシンが含まれるカタログと、リモートPCアクセスマシンカタログの場合は、ユーザーのマシンに対する更新をStudioの外で管理します。サードパーティ製のソフトウェア配信ツールを使用して、個々のデスクトップまたはデスクトップのグループを管理します。

ホストハイパーバイザーおよびクラウドサービスへの接続の作成と管理については、 接続とリソース」を参照してください。

ヒント： マシンの状態が「Power State Unknown」の場合、CTX131267を参照してください。

マシンカタログへのマシンの追加

以下の点に注意してください。

- 追加するマシンの数に応じて十分なプロセッサ、メモリ、ストレージが仮想化ホスト（ハイパーバイザーまたはクラウドサービスプロバイダー）上にあることを確認してください。
- 十分な数のActive Directoryコンピューターアカウントが使用可能であることを確認してください。既存のアカウントを使用している場合、使用可能なアカウントの数により、追加できるマシンの数が制限されることに注意してください。
- 追加するマシン用にStudioでActive Directoryコンピューターアカウントを作成する場合は、適切なドメイン管理者権限も

© 1999-2017 Citrix Systems, Inc. All rights reserved.

必要です。

マシンカタログにマシンを追加するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシンの追加]** を選択します。
3. 追加する仮想マシンの数を選択します。
4. 追加する仮想マシンの数に対し、既存のActive Directoryアカウントの数が不足している場合は、作成するアカウントのドメインと場所を選択します。アカウント名前付けスキームを指定します。番号記号（#）により、名前に追加される連番または文字とその位置が定義されます。組織単位名にはスラッシュ（/）を使用しないでください。名前の先頭に番号記号を配置することはできません。たとえば、名前付けスキームとして「PC-Sales-##」を指定して［0～9］を選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウント名が作成されます。
5. 既存のActive Directoryアカウントを使用する場合、アカウントを参照するか、**[インポート]** をクリックしてアカウント名の一覧のCSVファイルを指定します。追加するマシンに十分な数のアカウントをインポートする必要があります。これらのアカウントはStudioで管理されるため、すべてのアカウントのパスワードのリセットをStudioに許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

マシンの作成はバックグラウンドプロセスとして実行され、多くのマシンを追加する場合には時間がかかることがあります。Studioを終了してもマシンの作成処理は続行されます。

マシンカタログからのマシンの削除

マシンをマシンカタログから削除すると、ユーザーはそのマシンにアクセスできなくなります。そのため、マシンを削除する前に以下の点について確認してください。

- マシン上に重要なユーザーデータがなく、データがある場合はバックアップ済みであること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンに新たに接続できなくなります
- マシンの電源がオフになっていること。

カタログからマシンを削除するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシン カタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. 1台または複数のマシンを選択し、［操作］ペインの **[削除]** を選択します。

マシンを削除するかどうかを選択します。マシンを削除する場合は、マシンのActive Directoryアカウントを残すか、無効にするか、削除するかを指定します。

マシンカタログの説明やリモートPCアクセスの設定を変更する

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシンカタログの編集]** を選択します。
3. （リモートPCアクセスカタログのみ）**[電源管理]** ページでは、電源管理設定を変更したり、電源管理接続を選択したりすることができます。 **[組織単位]** ページでは、Active Directory組織単位を追加または削除します。
4. **[説明]** ページでは、カタログの説明を変更します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注：Citrix Cloud XenAppおよびXenDesktopサービスのリモートPCアクセスカタログの場合は、CTX220737のガイダンスに従ってください。

マシンカタログ名の変更

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシンカタログの名前を変更]** を選択します。
3. 新しい名前を入力します。

別のゾーンへのマシンカタログの移動

展開に複数のゾーンがある場合、カタログをゾーン間で移動させることができます。

注意： カタログをそのカタログの仮想マシンが含まれるハイパーバイザーまたはクラウドサービスプロバイダー以外のゾーンに移動すると、パフォーマンスが低下する可能性があります。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. カタログを選択し、［操作］ペインの **[移動]** を選択します。
3. カタログの移動先ゾーンを選択します。

マシンカタログの削除

カタログを削除する前に、以下の点について確認してください。

- すべてのユーザーがログオフしており、実行中の切断セッションがないこと。
- カタログ内のすべてのマシンのメンテナンスモードがオンで、新たに接続できないこと。
- カタログ内のすべてのマシンの電源がオフになっていること。
- そのカタログがデリバリーグループに関連付けられていないこと。すなわち、そのカタログのマシンがデリバリーグループに含まれていないこと。

カタログを削除するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシンカタログの削除]** を選択します。
3. カタログ内のマシンを削除するかどうかを指定します。マシンを削除する場合は、マシンのActive Directoryコンピューターアカウントを残すか、無効にするか、削除するかを指定します。

マシンカタログにおけるActive Directoryコンピューターアカウントの管理

マシンカタログのActive Directoryアカウントについて、次の操作を行えます。

- デスクトップOSカタログおよびサーバーOSカタログからActive Directoryコンピューターアカウントを削除して未使用のマシンアカウントを解放する。解放したアカウントは、ほかのマシンで使用可能になります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- カタログに追加するマシン用のコンピューターアカウントを追加しておく。 組織単位名にはスラッシュ（/）を使用しないでください。

Active Directoryアカウントを管理するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. カタログを選択し、［操作］ペインの **[Active Directoryアカウント管理]** を選択します。
3. 必要に応じてコンピューターアカウントを追加または削除します。アカウントを追加する場合は、すべてのアカウントのパスワードをリセットするか、すべてのアカウントに適用されるパスワードを入力するかを選択します。アカウントの現在のパスワードがわからない場合は、すべてのアカウントのパスワードをリセットするオプションを選択します。パスワードをリセットするための権限が必要です。パスワードを指定する場合は、アカウントのインポート時にパスワードが変更されます。アカウントを削除する場合は、そのアカウントをActive Directory内で保持するか、無効にするか、または削除するかを選択します。

注： マシンをカタログから削除するか、カタログを削除する場合にも、Active Directoryアカウントを保持するか、無効にするか、または削除するかを指定することができます。

マシンカタログの更新

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存しておくことをお勧めします。データベースには、各マシンカタログで使用されたマスターイメージの履歴記録が保持されます。デスクトップの更新によりユーザーの操作に問題が発生した場合は、カタログ内のマシンをロールバックして以前のバージョンのマスターイメージに戻し、ユーザーのダウンタイムを最小限に抑えることができます。マスターイメージの削除、移動、または名前変更は行わないでください。これらの操作を行うと、カタログを元に戻してマスターイメージを使用することができなくなります。

Provisioning Servicesが使用されているカタログで変更内容を反映させるには、新しいvDiskを公開する必要があります。詳しくは、Provisioning Servicesのドキュメントを参照してください。

マシンは、更新後に自動的に再起動されます。

ヒント：接続の管理について詳しくは、「接続とリソース」を参照してください。

マシンカタログを更新する前に、既存のマスターイメージを更新するか、またはホストハイパーバイザー上で新規作成します。

1. ハイパーバイザー上またはクラウドサービスプロバイダー上で、現在の仮想マシンのスナップショットを作成してわかりやすい名前を付けます。このスナップショットを使用して、カタログ内のマシンを元に戻す（ロールバックする）ことができます。
2. 必要に応じて、マスターイメージをオンにしてログオンします。
3. 更新をインストールするか、マスターイメージに対して必要な変更を加えます。
4. マスターイメージでPersonal vDiskが使用される場合は、インベントリを更新します。
5. Windows 10マシンでは、「*インストールの準備*」にリンクされている最適化リソースを参照してください。
6. 仮想マシンの電源を切ります。
7. 仮想マシンのスナップショットを作成してわかりやすい名前を付けます。この名前は、Studioでのカタログの更新時に使用されます。Studioでスナップショットを作成することもできますが、ハイパーバイザー側の管理コンソールでスナップショットを作成し、それをStudioで選択することをお勧めします。これにより、スナップショットに自動生成される名前を付けるのではなく、わかりやすい名前と説明を指定できます。GPUの仮想化機能を使用したマスターイメージを更新する場合は、XenServerのXenCenterを使用する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更新を準備し、カタログ内のすべてのマシンにロールアウトするには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. カタログを選択して、［操作］ペインの **[マシンの更新]** を選択します。
3. **［マスターイメージ］** ページで、ホストおよびロールアウトするイメージを選択します。
4. **［ロールアウト方法］** ページで、マシンカタログ内のマシンを新しいマスターイメージによって更新するタイミング（次回シャットダウン時または即時）を選択します。詳しくは、以下を参照してください。
5. **［概要］** ページで情報を確認し、**[完了]** をクリックします。各マシンは、更新後に自動的に再起動されます。

ヒント： Studioではなく、PowerShell SDKを使用してカタログを直接更新する場合、イメージまたはそのスナップショットの代わりに、ハイパーバイザーテンプレート（VMTemplates）を指定できます。

ロールアウト方法

Citrix Connector for System Center Configuration Managerを使用している場合、次回シャットダウン時にイメージを更新することができます。

イメージを即時に更新する場合、配信時間および通知を構成します。

- **配信時間：** すべてのマシンを同時に更新するか、またはカタログ内のすべてのマシンの更新を開始するまでの合計時間を指定することができます。内部アルゴリズムにより、その時間内において各マシンの更新および再起動のタイミングが決定されます。
- **通知：** 左の通知ボックスで、更新を開始する前に、マシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。更新開始の15分前にメッセージが表示されるように（右のボックスで）選択した場合、最初のメッセージの後、5分ごとにメッセージが繰り返し送信されるように選択することができます。デフォルトでは、メッセージは繰り返して送信はされません。すべてのマシンの同時更新を選択した場合を除き、通知メッセージは、内部アルゴリズムによって計算された、更新開始前の適切なタイミングで各マシンに表示されます。

更新後または新規のマスターイメージは、ロールアウトした後にロールバックすることができます。ロールバックは、新たに更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックした場合、カタログ内のマシンは前回の動作イメージまでロールバックされます。より新しいイメージを必要とする新機能は、利用できなくなります。ロールアウトと同様に、ロールバックでもマシンは再起動されます。

1. Studioのナビゲーションペインで **[マシン カタログ]** を選択します。
2. マシンカタログを選択し、［操作］ペインの **[マシン更新のロールバック]** を選択します。
3. ロールアウト処理について前に説明したとおり、古いマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、復元が必要なマシンにのみ適用されます。たとえば、マスターイメージの更新時にログアウトしなかったユーザーなど、更新したマスターイメージが適用されていないマシンのユーザーは、通知メッセージを受信したり強制的にログオフされたりすることはありません。

マシンカタログのアップグレードまたはアップグレードを元に戻す

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マシン上のVDAを新しいバージョンにアップグレードした場合は、マシンカタログをアップグレードする必要があります。すべてのVDAを最新バージョンにアップグレードして、最新の機能をすべて使用できるようにすることをお勧めします。

マシンカタログをアップグレードする前に、次の操作を行います。

- Provisioning Servicesを使用している場合は、Provisioning ServicesコンソールでVDAをアップグレードします。
- アップグレードしたマシンを起動します。これにより、マシンがControllerに登録されます。このときに、そのマシンカタログ内のマシンについてアップグレードが必要かどうかがStudioによりチェックされます。

マシンカタログをアップグレードするには、以下の手順に従います。

1. Studioのナビゲーションペインで **[マシンカタログ]** を選択します。
2. カタログを選択します。下ペインの［詳細］タブにバージョン情報が表示されます。
3. **［カタログのアップグレード］** を選択します。Studioによりアップグレードが必要なことが検出されると、メッセージが表示されます。画面の指示に従って操作します。アップグレードできないマシンがある場合は、その理由を説明するメッセージが示されます。すべてのマシンを適切に動作させるため、マシンカタログをアップグレードする前にマシンの問題を解決しておくことをお勧めします。

カタログをアップグレードした後でマシンを以前のVDAバージョンに戻すには、カタログを選択し、［操作］ペインの**[元に戻す]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デリバリーグループの作成

Dec 05, 2017

デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。デリバリーグループでは、それらのマシンを使用できるユーザーと、そのユーザーに提供するアプリケーションまたはデスクトップ（もしくはその両方）を指定します。

サイトおよびマシンカタログを作成した後、展開の構成における次の手順となるのが、デリバリーグループの作成です。その後、最初のデリバリーグループにおける初期設定を変更し、別のデリバリーグループを作成することができます。また、デリバリーグループの作成時ではなく、その編集時にのみ構成できる機能と設定もあります。

リモートPCアクセスでサイトを作成すると、**リモートPCアクセスデスクトップ**という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには、次の手順に従います。

1. サイトおよびマシンカタログを作成した後でデリバリーグループを作成していない場合は、デリバリーグループを作成するための説明が表示されます。既存のデリバリーグループがあり、別のデリバリーグループを作成する場合は、Studioのナビゲーションペインで **[デリバリーグループ]** を選択し、［操作］ペインの **[デリバリーグループの作成]** を選択します。
2. デリバリーグループの作成ウィザードが起動され、**[はじめに]** ページが開きます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、以下のページの操作を行います。各ページの操作を終えたら、最後のページに到達するまで **[次へ]** をクリックします。

マシンカタログを選択して、そのマシンカタログから使用するマシンの数を選択します。

ヒント：

- マシンカタログに未使用のマシンが残っていない場合、そのカタログを選択することはできません。
- 同じマシンカタログを複数のデリバリーグループで選択することができます。ただし、同じマシンを複数のデリバリーグループで使用することはできません。
- 1つのデリバリーグループで、複数のマシンカタログのマシンを使用できますが、これらのマシンカタログに同じ種類のマシン（サーバーOS、デスクトップOS、リモートPCアクセス）が含まれている必要があります。つまり、異なる種類のマシンをデリバリーグループに混在させることはできません。同様に、展開にWindowsマシンのカタログとLinuxマシンのカタログが含まれている場合、デリバリーグループには、両方ではなくいずれかの種類のオペレーティングシステムのマシンのみを含めることができます。
- すべてのマシンに最新のVDAバージョンをインストールするか、またはすべてのマシンにおいてVDAを最新バージョンにアップグレードしてから、必要に応じてマシンカタログおよびデリバリーグループをアップグレードすることをお勧めします。デリバリーグループの作成時に、異なるVDAバージョンがインストールされたマシンを選択した場合、デリバリーグループは最も古いバージョンと互換性を持ちます（これは、グループの*機能レベル*と呼ばれます）。 たとえば、選択したマシンの1つにVDA Version 7.1がインストールされており、ほかのマシンには最新バージョンがインストールされている場合、グループ内のすべてのマシンで使用できるのは、VDA 7.1でサポートされていた機能のみです。すなわち、より新しいVDAバージョンを必要とする機能を、このデリバリーグループで利用できない可能性があります。たとえば、AppDiskの機能を使用するには、VDA（およびグループの機能レベル）のバージョンは7.8以上である必要があります。
- リモートPCアクセスマシンカタログの各マシンは、デリバリーグループに自動的に関連付けられます。リモートPCアクセスサイトを作成すると、「**リモートPCアクセスマシン**」という名前のマシンカタログと、「**リモートPCアクセスデスクトップ**」という名前のデリバリーグループが自動的に作成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

このページは、静的（割り当て済み）デスクトップOSマシンを含むマシンカタログを選択した場合にのみ開きます。［配信の種類］ページで、**［アプリケーション］**または**［デスクトップ］**のいずれかをクリックします。両方とも有効にすることはできません。

サーバーOSまたはデスクトップOSランダム（プール）カタログのマシンを選択した場合、配信の種類はアプリケーションとデスクトップと見なされ、アプリケーションかデスクトップ、またはその両方を配信できます。

AppDiskを追加するには、**［追加］**をクリックします。［AppDiskの選択］ダイアログボックスでは、左側の列に選択可能なAppDiskが一覧表示されます。右側の列にAppDiskのアプリケーションが一覧表示されます（右側の列の上部の**［アプリケーション］**タブを選択すると、［スタート］メニューに似た形式でアプリケーションが表示され、**［インストール済みのパッケージ］**タブを選択すると、［プログラムと機能］に似た形式でアプリケーションが表示されます）。

1つまたは複数のチェックボックスをオンにします。

詳しくは、「AppDisks」を参照してください。

このデリバリーグループで配信されるアプリケーションやデスクトップを使用できるユーザーおよびユーザーグループを指定します。

ユーザー一覧の指定場所

以下の作成時または編集時に、Active Directoryユーザー一覧を指定します。

- サイトのユーザーアクセス一覧（Studioでは構成しません）。デフォルトでは、アプリケーション資格ポリシー規則には全ユーザーが含まれます。詳しくは、PowerShell SDKのBrokerAppEntitlementPolicyRuleコマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーションAの使用を構成するには次のように設定します。

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- （アプリケーショングループが構成されている場合）アプリケーションA～Lに管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーションAのプロパティを構成します。

認証が必要なユーザーおよび認証が不要なユーザー

ユーザーには、認証が必要なユーザーと認証が不要なユーザーの2種類があります（認証が不要なユーザーは「匿名ユーザー」とも呼ばれます）。いずれか一方または両方の種類のユーザーをデリバリーグループ内に構成できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

認証が必要なユーザー

特定のアカウント名で指定するユーザーおよびグループメンバーは、アプリケーションおよびデスクトップにアクセスするときにStoreFrontまたはCitrix Receiverで資格情報（スマートカード、またはユーザー名とパスワードなど）による認証が必要です（デスクトップOSマシン用のデリバリーグループでは、デリバリーグループを編集することにより、後でユーザーデータ（ユーザーの一覧）をインポートすることができます）。

認証が不要なユーザー（匿名ユーザー）

サーバーOSマシン用のデリバリーグループでは、StoreFrontまたはCitrix Receiverでの認証が不要な匿名アクセスを許可できます。たとえば、キオスクでは、アプリケーション自体での認証が必要な場合がありますが、Citrixのアクセスポータルやツールでは資格情報が要求されません。最初のDelivery Controllerをインストールすると、匿名のユーザーグループが作成されます。

認証が不要なユーザーのアクセスを許可するには、デリバリーグループの各マシンにVDA for Windows Server OS（Version 7.6以降）がインストールされている必要があります。認証が不要なユーザーのアクセスを有効にする場合は、認証が不要なStoreFrontストアを作成しておく必要があります。

認証が不要なユーザーアカウントはセッション開始時にオンデマンドで作成され、AnonXYZ（XYZは一意の3桁の値）という名前が付きます。

認証が不要なユーザーのセッションにはデフォルトで10分のアイドルタイムアウトが設定され、セッションを切断すると自動的にログオフされます。切断セッションへの再接続、デバイス間のローミング、およびワークスペースコントロールはサポートされません。

次の表は、［ユーザー］ページの選択肢を示しています。

アクセスを許可するユーザー	ユーザーおよびユーザーグループを追加/割り当てるかどうか	［認証が不要な（匿名）ユーザーのアクセスを許可する］チェックボックスをオンにするかどうか
認証が必要なユーザーのみ	はい	なし
認証が不要なユーザーのみ	なし	はい
認証が必要なユーザーおよび認証が不要なユーザー	はい	はい

ヒント：

- リモートPCアクセスのデリバリーグループにアプリケーションを追加することはできません。
- 新規アプリケーションをデリバリーグループに追加すると、デフォルトでは「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。詳しくは、「アプリケーションの管理」を参照してください。
- アプリケーションのプロパティは、デリバリーグループへの追加時、または後で変更できます。詳しくは、「アプリケーションの管理」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- アプリケーションの追加時に、そのフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。名前の変更を拒否すると、アプリケーションはサフィックス付きで追加され、そのアプリケーションフォルダー内で名前が一意になります。
- アプリケーションを複数のデリバリーグループに追加する場合、そのすべてのデリバリーグループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したデリバリーグループをすべて含めるようにします。
- 2つのアプリケーションを同じ名前で同じユーザーに公開する場合は、Studioで［アプリケーション名（ユーザー用）］ボックスに別の名前を入力します。これを行わないと、ユーザーのReceiverに同じ名前が2つ表示されます。

［追加］ボックスをクリックして、アプリケーションのソースを表示します。

- **［スタート］メニューから：**選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して**［OK］**をクリックします。
- **手動で定義：**サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。これらの情報を入力したら、**［OK］**をクリックします。
- **既存：**過去にサイトに追加された、おそらく別のデリバリーグループのアプリケーションこのソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して**［OK］**をクリックします。
- **App-V：**App-Vパッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページでApp-Vサーバーまたはアプリケーションライブラリを選択します。表示結果からグループに追加するアプリケーションを選択し、**［OK］**をクリックします。詳しくは、「App-V」を参照してください。

あるアプリケーションのソースまたはアプリケーションが選択できない、または無効な場合、そのアプリケーションは見ることができないか、選択できないかのどちらかです。たとえば、サイトに追加されたアプリケーションがない場合、**［既存］**のソースを選択することはできません。アプリケーションが、選択したマシンカタログのマシン上でサポートされるセッションタイプとの互換性を備えていない場合も同様です。

このページのタイトルは、ウィザードの前半で選択したマシンカタログによって異なります。

- プールされたマシンを含むマシンカタログを選択した場合、このページのタイトルは「デスクトップ」です。
- 割り当てられたマシンを含むマシンカタログを選択し、［配信の種類］ページで「デスクトップ」を指定した場合、このページのタイトルは「デスクトップユーザー割り当て」です。
- 割り当てられたマシンを含むマシンカタログを選択し、［配信の種類］ページで「アプリケーション」を指定した場合、このページのタイトルは「アプリケーションマシンユーザー割り当て」です。

［Add］をクリックします。ダイアログボックスで次の操作を実行します。

- ［表示名］と［説明］フィールドで、Citrix Receiverに表示される情報を入力します。
- デスクトップにタグ制約を追加するには、**［次のタグを持つマシンに起動を制約する］**を選択し、タグをドロップダウンから選択します（詳しくは、「タグ」を参照してください）。
- ラジオボタンを使用して、（プールされたマシンのグループの）デスクトップを起動できるユーザー、または（割り当てられたマシンのグループの）デスクトップを起動した場合にマシンに割り当てられるユーザーを指定します。このデリバリーグループにアクセスできるあらゆるユーザー、または特定のユーザーやユーザーグループを指定できます。
- 割り当て済みのマシンがグループに含まれる場合、ユーザーあたりの最大デスクトップ数を指定します。1以上の値を入力する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- （プールされたマシンの）デスクトップ、または（割り当て済みのマシンに対する）デスクトップ割り当て規則を有効または無効にします。デスクトップを無効にすると、デスクトップ配信が停止されます。デスクトップ割り当て規則を無効にすると、ユーザーへのデスクトップの自動割り当てが停止されます。
- ダイアログボックスの操作を終了したら、**[OK]** をクリックします。

デリバリーグループの名前を入力します。オプションで説明を入力することもできます。説明は、Citrix ReceiverとStudioで表示されます。

概要の情報を確認し、**[完了]** をクリックします。アプリケーションを1つも選択しなかった場合、または配信するデスクトップを1つも指定しなかった場合、続行するかどうかを確認するメッセージが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デリバリーグループの管理

Dec 05, 2017
ここでは次のことについて説明します。

- はじめに
- デリバリーグループでのユーザー設定の変更
- デリバリーグループのユーザーの追加または削除
- デリバリーグループの配信の種類の変更
- StoreFrontアドレスの変更
- デスクトップのタグ制約の追加、変更、または削除
- デリバリーグループのアップグレード、またはアップグレードの取り消し
- リモートPCアクセスのデリバリーグループの管理
- デリバリーグループのマシンのシャットダウンと再起動
- デリバリーグループのマシンの電源管理
- デリバリーグループのマシンに対する再起動スケジュールの作成
- デリバリーグループのマシンに対する複数の再起動スケジュールの作成
- デリバリーグループのマシンへのユーザーの接続を禁止する（メンテナンスモード）
- デリバリーグループのユーザーへのマシン割り当ての変更
- デリバリーグループのユーザーあたりの最大マシン数の変更
- デリバリーグループのマシンの負荷管理
- デリバリーグループからのマシンの削除
- デリバリーグループのマシンへのアクセス制限
- デリバリーグループのマシンの更新
- セッションのログオフ/切断、またはデリバリーグループユーザーへのメッセージ送信
- セッションの事前起動およびセッション残留の構成

はじめに

この記事では、デリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更できるほかに、デリバリーグループ作成時には使用できなかった設定を構成することも可能です。

デリバリーグループのアプリケーションを追加または削除する方法や、アプリケーションプロパティを変更する方法など、デリバリーグループのアプリケーションの管理について詳しくは、「アプリケーション」を参照してください。

デリバリーグループを管理するには、デリバリーグループ管理者組み込みの役割の配信管理者権限が必要です。詳しくは、「委任管理」を参照してください。

ヒント

- デリバリーグループのStudioの表示では、［詳細］パネルの［インストール済み VDA のバージョン］が、マシンにインストールされている実際のバージョンと異なる可能性があります。マシンのWindowsの［プログラムと機能］には、VDAの実際のバージョンが表示されます。
- マシンの状態が「Power State Unknown」の場合、CTX131267を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controllerで登録されていないVDAは、仲介されたセッションの起動時に考慮されず、利用可能なリソースが十分に活用されなくなります。VDAが登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Studioではカタログ作成ウィザードで、またはカタログをデリバリーグループに登録した後に、トラブルシューティング情報を提供します。

デリバリーグループを作成すると、そのグループと関連付けられているマシンの詳細がStudioに表示されます。デリバリーグループの［詳細］ペインに、登録の必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードでないはないのに、Controllerに現在登録されていないマシンが1台または複数台存在することが考えられます。「未登録だが登録する必要がある」マシンが表示された場合は、［詳細］ペインの［トラブルシューティング］タブに、考えられる原因と推奨される修正アクションが示されます。

機能レベルに関するメッセージについては、「VDAバージョンと機能レベル」を参照してください。

VDA登録に関するトラブルシューティングの詳細は、CTX136668を参照してください。

デリバリーグループでのユーザー設定の変更

このページの名前には「**ユーザー設定**」または「**基本設定**」のどちらかが表示されます。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[ユーザー設定]**（または **[基本設定]**）ページで、次の表のいずれかの設定を変更します。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

設定	説明
説明	StoreFrontでユーザーに表示される説明です。
デリバリーグループの有効化	このデリバリーグループを有効にするかどうかを設定します。
タイムゾーン	
Secure ICAを有効にする	デリバリーグループのマシンとの通信をSecureICAで保護します。これにより、ICAプロトコルが暗号化されます（デフォルトレベルは128ビットです。このレベルはSDKを使用して変更できます）。公共のネットワークが使用される環境では、TLSなどの暗号化方法を追加することをお勧めします。また、SecureICAでは、メッセージの整合性チェックが行われません。

デリバリーグループのユーザーの追加または削除

ユーザーについて詳しくは、「デリバリーグループの作成」の記事で「ユーザー」のセクションを参照してください。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[ユーザー]** ページで、ユーザーを追加する場合は、**[追加]** をクリックし、追加するユーザーを指定します。ユーザーを削除する場合は、1人または複数のユーザーを選択し、**[削除]** をクリックします。また、チェックボックスをオンまたはオフにして、匿名ユーザーによるアクセスを有効化または無効化することもできます。.
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

物理デスクトップOSマシン用のデリバリーグループでは、デリバリーグループを作成した後でCSVファイルからユーザー情報をインポートできます。ユーザー情報をCSVファイルにエクスポートすることもできます。以前の製品バージョンでのユーザー情報をCSVファイルに含めることもできます。

このCSVファイルの最初の行は、コンマで区切られた列見出し（順不同）でADComputerAccount、AssignedUser、VirtualMachine、およびHostIdが含まれます。以降の行には、コンマで区切られたデータが含まれます。ADComputerAccountエントリは、共通名、IPアドレス、識別名、またはドメインとコンピューター名のペアです。

ユーザー情報をインポートまたはエクスポートするには、次の手順に従います。

1. Studioのナビゲーションペインで **[デリバリー グループ]** を選択します。
2. デリバリーグループを選択して、［操作］ペインの **[デリバリーグループの編集]** を選択します。
3. **[マシン割り当て]** ページで、一覧の **[インポート]** または **[エクスポート]** を選択し、ファイルの場所を参照します。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

デリバリーグループの配信の種類の変更

配信の種類は、アプリケーション、デスクトップ、またはその両方のうち、そのグループが配信できるものを示します。

この種類を **[アプリケーションのみ]**、または **[デスクトップおよびアプリケーション]** から **[デスクトップのみ]** に変更する前に、グループからすべてのアプリケーションを削除します。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[配信の種類]** ページで、目的の配信の種類を選択します。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

StoreFrontアドレスの変更

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[StoreFront]** ページで、StoreFrontのURLを選択または追加します。このURLはデリバリーグループの各マシンにインストールされたCitrix Receiverで使用されます（ユーザーがこのマシンにアクセスするときに使用するURLではありません）。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

StoreFrontサーバーのアドレスは、後で指定することもできます。これを行うには、Studioのナビゲーションペインで**[構**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

成] > [StoreFront] の順に選択します。

デスクトップのタグ制約の追加、変更、または削除

重要：タグ制約を追加、変更、および削除すると、どのデスクトップが起動の対象となるかについて、予期しない効果を招くことがあります。「タグ」に記載されている考慮事項と注意を必ず確認してください。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[デスクトップ]** ページでデスクトップを選択し、**[編集]** をクリックします。
4. タグ制約を追加するには、**[次のタグを持つマシンに起動を制約する：]** を選択し、タグを選択します。
5. タグ制約を変更または削除するには、異なるタグを選択するか、**[次のタグを持つマシンに起動を制約する：]** をオフにして、タグ制約を完全に削除します。
6. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

デリバリーグループのアップグレード、またはアップグレードの取り消し

デリバリーグループのアップグレードは、マシン上のVDA、およびデリバリーグループで使用されているマシンを含むマシンカタログをアップグレードしてから行ってください。

デリバリーグループのアップグレードを開始する前に、以下の操作を行います。

- Provisioning Servicesを使用する環境では、Provisioning ServicesコンソールでVDAのバージョンをアップグレードします。
- アップグレードしたVDAがインストールされているマシンを起動して、Delivery Controllerに登録します。この処理によって、デリバリーグループで必要なアップグレードがStudioで特定されます。
- VDAをアップグレードせずに使用を継続すると、新しい製品機能を使用できなくなる場合があります。詳しくは、アップグレードに関連する記事を参照してください。

デリバリーグループをアップグレードするには、次の手順に従います。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択して、［操作］ペインの **[デリバリーグループのアップグレード]** を選択します。アップグレードされたVDAをStudioが検知した場合のみ、**[デリバリーグループのアップグレード]** アクションが表示されます。

アップグレードできないマシンがある場合は、そのマシンとアップグレードできない理由が表示されます。この場合はアップグレードをキャンセルし、マシンの問題を解決してから、アップグレードを再度開始できます。

アップグレードが完了した後でマシンを元の状態に戻すには、デリバリーグループを選択し、［操作］ペインの**[元に戻す]** を選択します。

リモートPCアクセスのデリバリーグループの管理

リモートPCアクセス用のマシンカタログでユーザーに割り当てられていないマシンは、そのカタログに関連付けられたデリバリーグループに一時的に割り当てられます。この一時的な割り当てにより、そのマシンを後でユーザーに割り当てられるよう

© 1999-2017 Citrix Systems, Inc. All rights reserved.

になります。

デリバリーグループとマシンカタログとの関連付けには優先度値があります。この優先度により、マシンをシステムに登録したりユーザーにマシンを割り当てたりするときのデリバリーグループが決定されます。値が低ければ低いほど、優先度は高くなります。リモートPCアクセスマシンカタログに複数のデリバリーグループ割り当てがある場合、優先度が最も高い割り当てが選択されます。この優先度値はPowerShell SDKを使用して設定できます。

リモートPCアクセス用のマシンカタログの初回作成時に、デリバリーグループが関連付けられます。つまり、このカタログに後から追加したコンピューターアカウントまたは組織単位を、このデリバリーグループに追加することができます。この関連付けは、必要に応じて有効にしたり無効にしたりできます。

リモートPCアクセスマシンカタログの関連付けを追加または削除するには、次の手順に従って操作します。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. リモートPCアクセスのグループを選択します。
3. ［詳細］セクションで **[マシンカタログ]** タブを選択し、リモートPCアクセス用のカタログを選択します。
4. 関連付けを追加または復元するには、**[デスクトップの追加]** を選択します。関連付けを削除するには、**[関連付けの削除]** を選択します。

デリバリーグループのマシンのシャットダウンと再起動

ここで説明する内容は、リモートPCアクセスマシンではサポートされません。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. マシンを選択し、［操作］ペインで以下のいずれかを選択します（マシンの状態によっては選択できないオプションもあります）。

- **強制シャットダウン。**マシンの電源を強制的に切って、マシン一覧を更新します。
- **再起動。**オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、マシンの状態は変更されません。
- **強制再起動。**オペレーティングシステムを強制的にシャットダウンしてから、マシンを再起動します。
- **一時停止。**マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
- **シャットダウン。**オペレーティングシステムにシャットダウンを要求します。

非強制操作の場合、マシンが10分以内にシャットダウンしないと、電源が切れ、強制的にシャットダウンされます。シャットダウン中にWindowsが更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

セッション中はデスクトップOSマシンのユーザーに **[シャットダウン]** の選択を禁止することをお勧めします。詳しくは、Microsoftのポリシーのドキュメントを参照してください。

接続でマシンをシャットダウンし再起動することもできます。「接続とリソース」を参照してください。

デリバリーグループのマシンの電源管理

電源を管理できるのは、仮想デスクトップOSマシンのみです。物理マシンの電源を管理することはできません（リモートPC

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アクセスマシンを含む）。GPU機能が有効なデスクトップOSマシンは一時停止できないため、電源を切ることはできません。サーバーOSマシンでは、再起動のスケジュールを作成できます。これについては、このアーティクルでも説明されています。

プールされたマシンが含まれるデリバリーグループでは、仮想デスクトップOSマシンは次のうちいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 未割り当て、未接続

静的なマシンが含まれるデリバリーグループでは、仮想デスクトップOSマシンは次のうちいずれかの状態になります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（準備は完了）
- 未割り当て、未接続

通常、静的なデリバリーグループには、永続的に割り当てられたマシンと未割り当てマシンの両方が含まれています。最初、すべてのマシンは未割り当て状態です（デリバリーグループ作成時に手動で割り当てられたマシンを除く）。ユーザーが接続すると、マシンが永続的に割り当てられます。静的なデリバリーグループでは未割り当てマシンの電源を完全に管理できますが、永続的に割り当てられたマシンでは一部の電源管理のみを実行できます。

プールおよびバッファー：未割り当てマシンが含まれる静的なデリバリーグループ、およびプールされたデリバリーグループの場合、（ここでの）「プール」は、電源が入っていてユーザーが接続可能な、未割り当てまたは一時的に割り当てられたマシンのセットを指し、ユーザーがログオンすると直ちにマシンが割り当てられます。プールサイズ（電源が入った状態のマシンの数）は時刻によって構成できます。静的なデリバリーグループでは、SDKを使用してプールを構成します。

「バッファー」は追加の未割り当てマシンの「待機」セットを指し、プール内のマシンの数がデリバリーグループのサイズに対する割合により設定されたしきい値を下回ると、バッファーのマシンの電源がオンになります。大規模なデリバリーグループの場合、このしきい値により多数のマシンの電源がオンになることがあります。このため、デリバリーグループのサイズを小さくするか、SDKを使ってデフォルトのバッファーサイズを調節してください。

電源状態タイマー：電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にすることができます。たとえば、業務時間終了後にユーザーが切断してから10分が経過したマシンを自動的に一時停止状態にできます。ランダムなマシンまたはPersonal vDisksを使用しているマシンは、ユーザーがログオフすると自動的にシャットダウンします（SDKでデリバリーグループのShutdownDesktopsAfterUseプロパティを構成している場合を除く）。

平日と週末、ピーク期間とオフピーク期間のタイマーを構成できます。

永続的に割り当てられたマシンの部分的な電源管理: 永続的に割り当てられたマシンでは、電源の状態タイマーを設定することはできますが、プールまたはバッファーを設定することはできません。各ピーク時間の開始時にマシンの電源がオンになり、各オフピーク時間の開始時に電源がオフになります。このため、未割り当てマシンの場合とは異なり、使用中のマシンを補うためのマシンの数を詳細に調整できません。

仮想デスクトップOSマシンの電源を管理するには、次の手順に従います。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[電源管理]** ページの［マシンの電源管理］ボックスで **[1 - 平日]** を選択します。平日は、デフォルトで月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、**[電源をオンするマシン]** で **[編集]** をクリックして、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **[ピーク時]** で、平日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間およびオフピーク時間の電源状態タイマーを設定します。 **[ピーク時の電源管理]** > **[切断時]** で、ユー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ザーが切断してからマシンを一時停止状態にするまでの時間（分）を指定して［一時停止］を選択します。 **[オフピーク時の電源管理] > [切断時]** で、ユーザーがログオフしてからマシンの電源をオフにするまでの時間を指定して**[シャットダウン]** を選択します。このタイマーはランダムマシンのデリバリーグループでは使用できません。

7. ［マシンの電源管理］ボックスで **[2 - 週末]** を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

SDKを使用すると、以下の設定が可能です。

- 電源状態タイマーの設定に基づいてマシンを（一時停止ではなく）シャットダウンする場合や、ユーザーの（切断時ではなく）ログオフ時にタイマーが起算されるように設定する。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にする。CTX217289を参照してください。

デリバリーグループのマシンに対する再起動スケジュールの作成

注： このセクションでは、Studioで単一の再起動スケジュールを構成する方法について説明します。または、PowerShellを使用して、デリバリーグループ内のマシンの異なるサブセットに対して複数の再起動スケジュールを構成できます。詳しくは、次のセクションを参照してください。

再起動のスケジュールにより、デリバリーグループ内のすべてのマシンを定期的に再起動するタイミングが指定されます。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[再起動のスケジュール]** ページでは、デリバリーグループのマシンを自動再起動しない場合、**[いいえ]** をクリックし、この処理の最後の手順に進みます。再起動のスケジュールまたはロールアウト方法は構成されません。スケジュールが過去に構成されている場合、この選択によってそのスケジュールは取り消されます。
4. デリバリーグループのマシンを自動的に再起動する場合、**[はい]** をクリックします。
5. **[再起動]** 頻度に対し、 **[毎日]** か、または再起動する曜日を選択します。
6. 対応するフィールドに、再起動の開始時刻を24時間制で指定します。
7. **[再起動時間]** で、すべてのマシンを同時に再起動するか、またはデリバリーグループ内のすべてのマシンの再起動を開始するまでの合計時間を選択します。内部アルゴリズムにより、この時間内において各マシンの再起動タイミングが決定されます。
8. 左の **[通知]** ボックスで、再起動を開始する前に、影響を受けるマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。再起動開始の15分前にメッセージが表示されるように（ **[繰り返し通知]** ボックスで）選択した場合、最初のメッセージの後、5分ごとにメッセージが繰り返し送信されるように選択することができます。デフォルトでは、メッセージは繰り返して送信はされません。
9. **[通知メッセージ]** ボックスに通知テキストを入力します。デフォルトテキストはありません。再起動までの分数をメッセージに含める場合、変数**%m%** を使用します（例：警告：お使いのコンピューターは、%m%分後に自動的に再起動されます）。繰り返し通知の間隔を選択し、メッセージに%m%プレースホルダーが含まれている場合、メッセージが繰り返されるごとに値が5分ずつ減少します。すべてのマシンの同時再起動を選択した場合を除き、通知メッセージは、内部アルゴリズムによって計算された、再起動前の適切なタイミングで、デリバリーグループの各マシンに表示されます。
10. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

Studioでは、マシンの電源を自動的に投入したりシャットダウンしたりすることはできません。再起動のみを実行できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デリバリーグループのマシンに対する複数の再起動スケジュールの作成

PowerShellコマンドレットを使用して、デリバリーグループ内のマシンに対して複数の再起動スケジュールを作成できます。各スケジュールは、指定されたタグを持つグループ内のマシンだけを対象とするように構成できます。このタグ制約機能を使用すると、デリバリーグループ内のマシンの異なるサブセットに対して複数の再起動スケジュールを簡単に作成できます。

たとえば、社内のすべてのマシンに対して1つのデリバリーグループを使用しているとします。すべてのマシンを毎週少なくも1回（日曜日の夜）再起動するようにしたいのですが、経理チームが使用するマシンは毎日再起動する必要があります。すべてのマシンに対して週次スケジュール、および経理チームが使用するマシンだけに日次スケジュールを設定できます。

スケジュールの重複

複数のスケジュールが重複することがあります。上の例で、経理が使用するマシンは、両方のスケジュールの対象となり、日曜日に二回再起動される可能性があります。

スケジュールコードは、同じマシンを必要以上に再起動しないよう設計されていますが、保証はされません。両方のスケジュールで開始時刻と処理時間が正確に一致する場合、マシンが一度のみ再起動される可能性の方が高そうです。ただし、スケジュールの開始時刻や処理時間が異なるほど、再起動が2回起きる可能性が高くなります。また、スケジュールの対象となるマシン数も、重複の可能性に影響します。例では、すべてのマシンを再起動する週次スケジュールは、日次スケジュールより大幅に高速の再起動を開始できました（それぞれについて構成された処理期間により異なる）。

要件

複数の再起動スケジュールの作成と、再起動スケジュールでのタグ制約の使用のサポートは、現在、XenAppおよびXenDesktop 7.12に新しく搭載されたRebootScheduleV2 PowerShellコマンドレットを使用するPowerShellコマンドラインでのみ利用できます（これらはこの記事では「V2」コマンドレットと呼ばれます）。

V2コマンドレットの使用に必要な条件：

- Delivery Controller Version 7.12（最小要件）。
  - 最新のSDKプラグインを7.12より前のControllerとともに使用する場合、作成する新しいスケジュールはいずれも意図どおりに機能しません。
  - 混在サイト（一部の、ただしすべてではないControllerがアップグレード済み）では、V2コマンドレットはデータベースがアップグレードされるまで機能せず、少なくとも1つのControllerがアップグレードされ、使用されています（V2 コマンドレットで–adminaddress パラメーターを指定）。
  - ベストプラクティス：すべてのサイトのControllerがアップグレードされるまで、新しいスケジュールをいっさい作成しません。
- XenAppおよびXenDesktop 7.12（最小）とともに提供されるPowerShell SDKスナップイン。コンポーネントおよびサイトをインストールまたはアップグレードした後、asnp Citrix.*を実行して、最新のコマンドレットをロードします。

Studioは現在、以前のV1 RebootSchedule PowerShellコマンドレットを使用しており、V2コマンドレットで作成されたスケジュールは表示しません。

タグ制約を使用する再起動スケジュールを作成し、後からStudioを使用して再起動間隔（サイクル）中に対象のマシンからタグを削除するか、再起動サイクル中に追加のマシンにタグを追加した後、それらの変更は次の再起動サイクルまで有効ではありません（変更は現在の再起動サイクルには影響しません）。

PowerShellコマンドレット

© 1999-2017 Citrix Systems, Inc. All rights reserved.

次のRebootScheduleV2コマンドレットをコマンドラインから使用して複数のスケジュールを作成し、スケジュールでタグ制約を使用します。

新しい（V2）コマンドレット	置き換えられる以前の（V1）コマンドレット
New-BrokerRebootScheduleV2	New-BrokerRebootSchedule
Get-BrokerRebootScheduleV2	Get BrokerRebootSchedule
Set- BrokerRebootScheduleV2	Set-BrokerRebootSchedule
Remove-BrokerRebootScheduleV2	Remove-BrokerRebootSchedule
Rename-BrokerRebootScheduleV2	-

完全なコマンドレットの構文およびパラメーターの説明を見るには、**Get-Help –full** <*cmdlet-name*>と入力します。

用語に関する注意：PowerShell SDKでは、DesktopGroupパラメーターは、デリバリーグループを識別します。

再起動スケジュールを作成するためのStudioインターフェイスをよく知っている場合、V2コマンドレットを使用してスケジュールを作成または更新する場合、それらのパラメーターのすべてを利用できます。さらに、以下のことが可能です。

- スケジュールを、指定されたタグを持つマシンに制限する。
- その間は新しいセッションが対象のマシンに仲介されない、最初の警告メッセージを送信するまでの間隔を指定する。

構成

タグ制約を使用する再起動スケジュールを構成する場合、スケジュールの対象とするマシンにそのタグを追加（適用）する必要もあります（詳しくは、「タグ」を参照してください）。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. スケジュールの対象となるマシンを含むデリバリーグループを選択します。
3. ［マシンの表示］を選択し、タグを追加するマシンを選択します。
4. ［操作］ペインで **[タグの管理]** を選択します。
5. タグが既に存在する場合、タグ名の隣にあるチェックボックスをオンにします。タグが存在しない場合、**[作成]** をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成したタグ名の隣にあるチェックボックスをオンにします。
6. ［タグの管理］ダイアログボックスの **[保存]** をクリックします。

タグを作成、追加（適用）したら、V2コマンドレットでスケジュールを作成または編集するときに、-RestrictToTagパラメーターを使用してタグ名を指定します。

以前のXenAppまたはXenDesktopバージョンで再起動スケジュールを作成する場合

Studioは、現在V1 RebootScheduleコマンドレットを使用しています。7.12（最小）にアップグレードする前に作成された再起動スケジュールがある場合、引き続きV1コマンドレットを使用してStudioで管理することができますが、Studioを使用してそのスケジュールにタグ制約を追加したり、追加のスケジュールを作成したりすることはできません（StudioがV2コマンド

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レットをサポートしないため）。既存のスケジュールにV1コマンドレットを使用する限り、再起動スケジュールに関して正しい情報が表示されます。

または、新しいV2 RebootScheduleコマンドレットを使用して、コマンドラインから既存のスケジュールを編集できます。新しいV2コマンドレットを使用すると、そのスケジュールでタグ制約パラメーターを使用したり、追加の再起動スケジュールを作成したりできます。ただし、V2コマンドレットを使用して既存のスケジュールを変更すると、Studioには完全なスケジュール情報が表示されません（V1情報しか認識できないため）。タグ制約が使用されているかどうか、またはスケジュールの名前と説明は表示されません。

デリバリーグループのマシンへのユーザーの接続を禁止する（メンテナンスモード）

一時的に新しい接続を停止する必要がある場合は、デリバリーグループの1台またはすべてのマシンに対してメンテナンスモードを有効にすることができます。パッチを適用したりメンテナンスツールを使用したりする場合は、メンテナンスモードを有効にしてから実行することをお勧めします。

- メンテナンスモードのサーバーOSマシンでは、既存のセッションに接続することはできますが、新しいセッションを開始することはできません。
- メンテナンスモードのデスクトップOSマシン（またはリモートPCアクセスを使用しているPC）では、新しいセッションを開始することも既存のセッションに再接続することもできません。実行中の接続は、ユーザーが切断またはログオフするまでは保持されます。

メンテナンスモードをオンまたはオフにするには、次の手順に従います。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択します。
3. デリバリーグループのすべてのマシンをメンテナンスモードにするには、［操作］ペインの**[メンテナンスモードをオンにする]** を選択します。1つのマシンをメンテナンスモードにするには、［操作］ペインの**[マシンの表示]** を選択します。マシンを選択し、［操作］ペインの **[メンテナンスモードをオンにする]** を選択します。
4. 特定のマシンまたはデリバリーグループのすべてのマシンのメンテナンスモードを解除するには、上記の手順に従って、［操作］ペインでは **[メンテナンスモードをオフにする]** を選択します。

Windowsリモートデスクトップ接続（RDC）の設定も、サーバーOSマシンをメンテナンスモードにするかどうかに影響します。次の状態のいずれかが発生すると、サーバーがメンテナンスモードになります。

- 上記の手順で［メンテナンスモードをオンにする］が選択された。
- RDCが **[このコンピューターへの接続を許可しない]** に設定された。
- RDCが **[このコンピューターへの接続を許可しない]** に設定されておらず、リモートホスト構成のユーザーログオンモード設定が **[再接続を許可するが、新しいログオンを許可しない]** または **[再接続を許可するが、サーバーが再起動するまで新しいログオンを許可しない]** に設定されている。

また、接続（該当する接続を使用するマシンに影響）またはマシンカタログ（該当するカタログ内のマシンに影響）に対してメンテナンスモードをオンまたはオフにすることもできます。

デリバリーグループのユーザーへのマシン割り当ての変更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デスクトップOSマシンの割り当てのみを変更することができます。サーバーOSマシンやProvisioning Servicesで作成されたマシンの割り当ては、変更できません。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択します。
3. ［操作］ペインの **[デリバリー グループの編集]** を選択します。 **[デスクトップ]** または **[デスクトップ割り当て規則]** ページで（デリバリーグループで使用するマシンカタログの種類によってどちらか一方しか使用できません）新しいユーザーを指定します。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

ユーザーあたりの最大マシン数の変更

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[デスクトップ割り当て規則]** ページで、ユーザーごとのデスクトップ最大数を設定します。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

デリバリーグループのマシンの負荷管理

負荷管理できるのはサーバーOSマシンのみです。

負荷管理機能では、測定されたサーバー負荷に基づいて最適なサーバーが選択されます。この選択は、以下の基準により行われます。

サーバーのメンテナンスモードの状態：メンテナンスモードがオフのサーバーOSマシンだけが負荷分散の対象として選択されます。

サーバー負荷指数：サーバーOSマシンの配信サーバーの負荷に基づいて、そのサーバーがどれだけの接続を受け入れられるかが決定されます。サーバー負荷指数は、セッション数とパフォーマンス測定値（CPU、ディスク、メモリ使用量など）で計算される負荷評価基準の組み合わせを指します。負荷評価基準は、ポリシーの負荷管理に関する設定項目で指定します。

Director、Studioの［検索］ノード、およびSDKを使用して負荷指数を監視できます。

Studioのデフォルトでは、［負荷指数］列が表示されません。［負荷指数］列を表示するには、マシンを選択し、列見出しを右クリックして［列の選択］を選択します。［マシン］の［負荷指数］チェックボックスをオンにします。

SDKではGet-BrokerMachineコマンドレットを使用します。詳しくは、CTX202150を参照してください。

［負荷指数］列に値10000が表示される場合、そのサーバーが負荷限界状態であることを示しています。ほかに使用可能なサーバーがない場合は、ユーザーがセッションを起動したときに、デスクトップまたはアプリケーションを使用できないという内容のメッセージが表示されます。

同時ログオントレランスのポリシー設定: サーバーが同時に処理できるログオン要求の最大数です。この設定項目は、Version 7.5より前のXenAppの「負荷調整」に相当します。

すべてのサーバーが同時ログオントレランスの設定値に達した場合、それ以降のログオン要求は保留中のログオン数が最も少ないサーバーに割り当てられます。同時ログオントレランスの設定値に達しないサーバーがいくつか存在する場合は、負荷指

© 1999-2017 Citrix Systems, Inc. All rights reserved.

数が最小のサーバーにログオン要求が割り当てられます。

デリバリーグループからのマシンの削除

デリバリーグループからマシンを削除しても、そのデリバリーグループで使用するマシンカタログからは削除されません。このため、そのマシンをほかのデリバリーグループに割り当てることができます。

マシンを削除する前に、マシンをシャットダウンする必要があります。デリバリーグループから削除せずにマシンを一時的に使用できなくする場合は、そのマシンをメンテナンスモードにしてからシャットダウンしてください。

マシンには個人データが保存されている可能性があります。このため、そのマシンを別のユーザーに割り当てる場合は注意が必要です。マシンをイメージから再作成することをお勧めします。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. マシンがシャットダウン状態であることを確認します。
4. ［操作］ペインの **[デリバリーグループから削除]** を選択します。

マシンが使用する接続からも、デリバリーグループからマシンを削除できます。詳しくは、 接続とリソース」を参照してください。

デリバリーグループのマシンへのアクセス制限

デリバリーグループでマシンへのアクセス制限を変更した場合、使用する方法にかかわらず既存の設定より優先されます。マシンの追加方法

管理者のアクセスを制限する場合は、委任管理スコープを使用します。すべてのアプリケーションへのアクセスを許可するスコープや、特定のアプリケーションへのアクセスのみを許可するスコープを作成して管理者に割り当てることができます。詳しくは、「委任管理」を参照してください。

ユーザーのアクセスを制限する場合は、NetScaler Gateway経由のユーザー接続を制御するSmartAccessポリシー式を使用します。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[デリバリー グループの編集]** を選択します。
3. **[アクセスポリシー]** ページで、 **[NetScaler Gatewayを経由する接続]** チェックボックスをオンにします。
4. NetScaler Gatewayを経由する特定の接続のみを許可するには、 **[次のフィルターのいずれかに一致する接続]** チェックボックスをオンにします。次にNetScaler Gatewayサイトを定義して、接続を許可するユーザーを特定するSmartAccessポリシー式を追加、編集、または削除します。詳しくは、NetScaler Gatewayのドキュメントを参照してください。
5. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

SDKで設定するアクセスポリシーの**除外フィルターを使用してユーザーのアクセスを制限することもできます。**アクセスポリシーはデリバリーグループに適用され、接続をより詳細に制御できます。たとえば、マシンへのアクセスを一部のユーザーに限定したり、特定のユーザーデバイスに限定したりできます。除外フィルターを使用するとアクセスポリシーをより詳細に定義できます。たとえば、セキュリティ上の理由により、一部のユーザーまたはデバイスからのアクセスを拒否できます。デフォルトでは、除外フィルターは無効になっています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

たとえば、社内ネットワークのサブネットにある教育ラボで、マシンを使用するユーザーにかかわらず教育ラボから特定のデリバリーグループへのアクセスを禁止する場合は、「Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -」コマンドを使用します。

ワイルドカード文字としてアスタリスク（*）を使用し、同じポリシー式で始まるタグをすべて一致させることもできます。たとえば、タグ「VPDesktops_Direct」が追加されたマシンと、タグ「VPDesktops_Test」が追加されたマシンの両方をフィルターの対象にする場合は、Set-BrokerAccessPolicyスクリプトでタグとして「VPDesktops_*」を指定します。

Webブラウザーを使用している、またはストアで統合Citrix Receiverユーザーエクスペリエンス機能を有効にして接続している場合、クライアント名除外フィルターは使用できません。

デリバリーグループのマシンの更新

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. マシンを選択して、［操作］ペインの **[マシンの更新]** を選択します。

別のマスターイメージを選択するには、**[マスターイメージ]** を選択し、スナップショットを選択します。

変更内容を適用し、マシンのユーザーに通知するには、**[エンドユーザーへのロールアウト通知]** を選択します。次に、マスターイメージの更新タイミング（即時または次回再起動時）、再起動を分散させる時間（グループのすべてのマシンの更新を開始するまでの合計時間）、ユーザーに再起動を通知するかどうか、およびユーザーに送信されるメッセージを指定します。

セッションのログオフ/切断、またはデリバリーグループユーザーへのメッセージ送信

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. グループを選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. ユーザーをセッションからログオフするには、セッションまたはデスクトップを選択し、［操作］ペインの**[ログオフ]** を選択します。セッションが閉じて、ほかのユーザーがそのマシンを使用できるようになります（そのマシンが特定のユーザーに割り当てられてない場合）。
4. セッションを切断するには、セッションまたはデスクトップを選択し、［操作］ペインの **[切断]** を選択します。ユーザーのアプリケーションはそのまま実行され、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。
5. ユーザーにメッセージを送信するには、セッション、マシン、またはユーザーを選択し、［操作］ペインの**[メッセージの送信]** を選択します。メッセージを入力します。

デスクトップOSマシンでは、電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にしたりシャットダウンしたりすることができます。詳しくは、「マシンの電源管理」セクションを参照してください。

デリバリーグループのセッションの事前起動およびセッション残留の構成

これらの機能はサーバーOSマシンでのみサポートされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの事前起動機能とセッション残留機能を使用すると、セッションが要求される前にセッションを開始したり（セッションの事前起動）、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブな状態で保持したり（セッション残留）できます。これにより、ユーザーがアプリケーションにすばやくアクセスできるようになります。

デフォルトでは、セッションの事前起動とセッション残留は無効になっています。セッションはユーザーがアプリケーションを開始すると開始（起動）され、セッションで開いていた最後のアプリケーションを閉じるまでアクティブな状態で保持されます。

以下の点に注意してください。

- これらの機能を使用するには、デリバリーグループでアプリケーションが配信されている必要があります。また、マシンでVDA for Server OS 7.6以降が動作している必要があります。
- これらの機能はCitrix Receiver for Windowsを使用している場合にのみサポートされ、Citrix Receiver側での構成も必要です。詳しくは、適切なバージョンのReceiver for WindowsのeDocsドキュメントで「セッションの事前起動」を検索してください。
- Citrix Receiver for HTML5はサポートされないことに注意してください。
- セッションの事前起動を使用するときに、ユーザーのマシンが「一時停止」または「休止」状態の場合は、（セッションの事前起動設定にかかわらず）事前起動が機能しません。ユーザーはマシンやセッションをロックできますが、ユーザーがCitrix Receiverからログオフすると、セッションが終了し、事前起動は適用されません。
- セッションの事前起動を使用するときは、物理クライアントマシンでは一時停止または休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックすることはできますが、ログオフすることはできません。
- 事前起動セッションと残留セッションは、接続されている間のみライセンスを消費します。使用されない事前起動セッションと残留セッションは、デフォルトで15分後に切断されます。この値はPowerShell（New/Set-BrokerSessionPreLaunchコマンドレット）で構成できます。
- これらの機能が相互に補完し合うよう調整するには、ユーザーの使用状況を監視して慎重に計画することが重要です。最適に構成することで、ライセンス消費やリソース割り当ての効率化とユーザーの利便性を両立させることができます。
- Citrix Receiver側では、セッションの事前起動を有効にする時間帯を構成できます。

ユーザーがアプリケーションを起動しない場合に、使用されないセッションをどのくらい保持するかを指定するには、タイムアウトおよびサーバー負荷のしきい値を構成します。タイムアウトおよびサーバー負荷のしきい値をすべて設定することができます。この場合、最初に発生したイベントによって事前起動セッションや残留セッションが終了します。

- **タイムアウト**：使用されない事前起動セッションや残留セッションを保持する日数、時間数、または分数を指定できます。この値が短すぎるとセッションがすぐに終了してしまい、ユーザーがアプリケーションにすばやくアクセスできるというメリットが活かされません。また、タイムアウト値が長すぎると、サーバーのリソースが足りなくなり、ユーザーの接続要求が拒否される場合があります。

  このタイムアウトをStudioで無効にすることはできませんが、SDK（New/Set-BrokerSessionPreLaunchコマンドレット）で無効にできます。タイムアウトを無効にすると、Studioにタイムアウトが表示されなくなります。

- **しきい値**：サーバーの負荷が高くなったときに事前起動セッションや残留セッションを自動的に終了することができます。これにより、サーバーの負荷が低い間は可能な限りセッションが保持されます。新しいユーザーセッション用のリソースが必要になったときに事前起動セッションや残留セッションが自動的に終了するため、これらのセッションが原因で接続が拒否されることはありません。

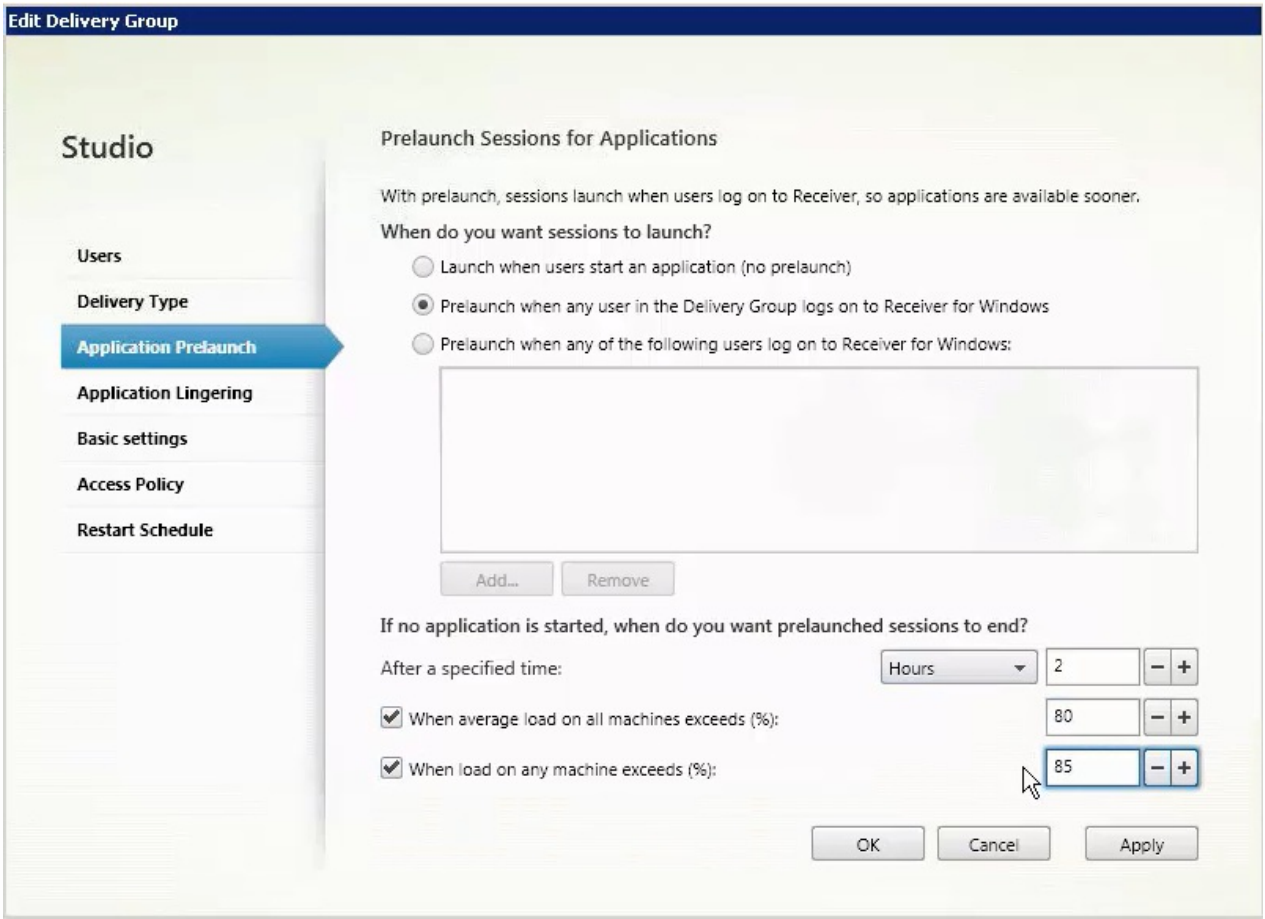
  デリバリーグループ内の全サーバーの平均負荷パーセンテージと、デリバリーグループ内のいずれかのサーバーの最大負荷パーセンテージの2つのしきい値を構成できます。サーバーの負荷がいずれかのしきい値を超えると、最も長い時間保

© 1999-2017 Citrix Systems, Inc. All rights reserved.

持された事前起動セッションまたは残留セッションが終了します。その後、負荷がしきい値を下回るまで、分間隔で1つずつセッションが終了します。しきい値を超えている間は、新たな事前起動セッションは開始されません。

Controllerに登録されていないVDAが動作するサーバーやメンテナンスモードのサーバーは、負荷限界状態として認識されます。サーバーで計画外の停止状態が発生した場合、事前起動セッションや残留セッションは自動的に終了してリソースが解放されます。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. デリバリーグループを選択して、［操作］ペインの **[デリバリーグループの編集]** を選択します。
3. **[アプリケーションの事前起動]** ページで、セッションを起動するタイミングを選択します。
   - アプリケーションの起動時にセッションを起動する。これがデフォルトの設定で、セッションの事前起動は無効になります。
   - デリバリーグループ内のすべてのユーザーでCitrix Receiver for Windowsログオン時に事前起動する。
   - 以下のユーザーでのみCitrix Receiver for Windowsログオン時に事前起動する。このオプションを選択する場合は、ユーザーまたはユーザーグループを一覧に追加してください。



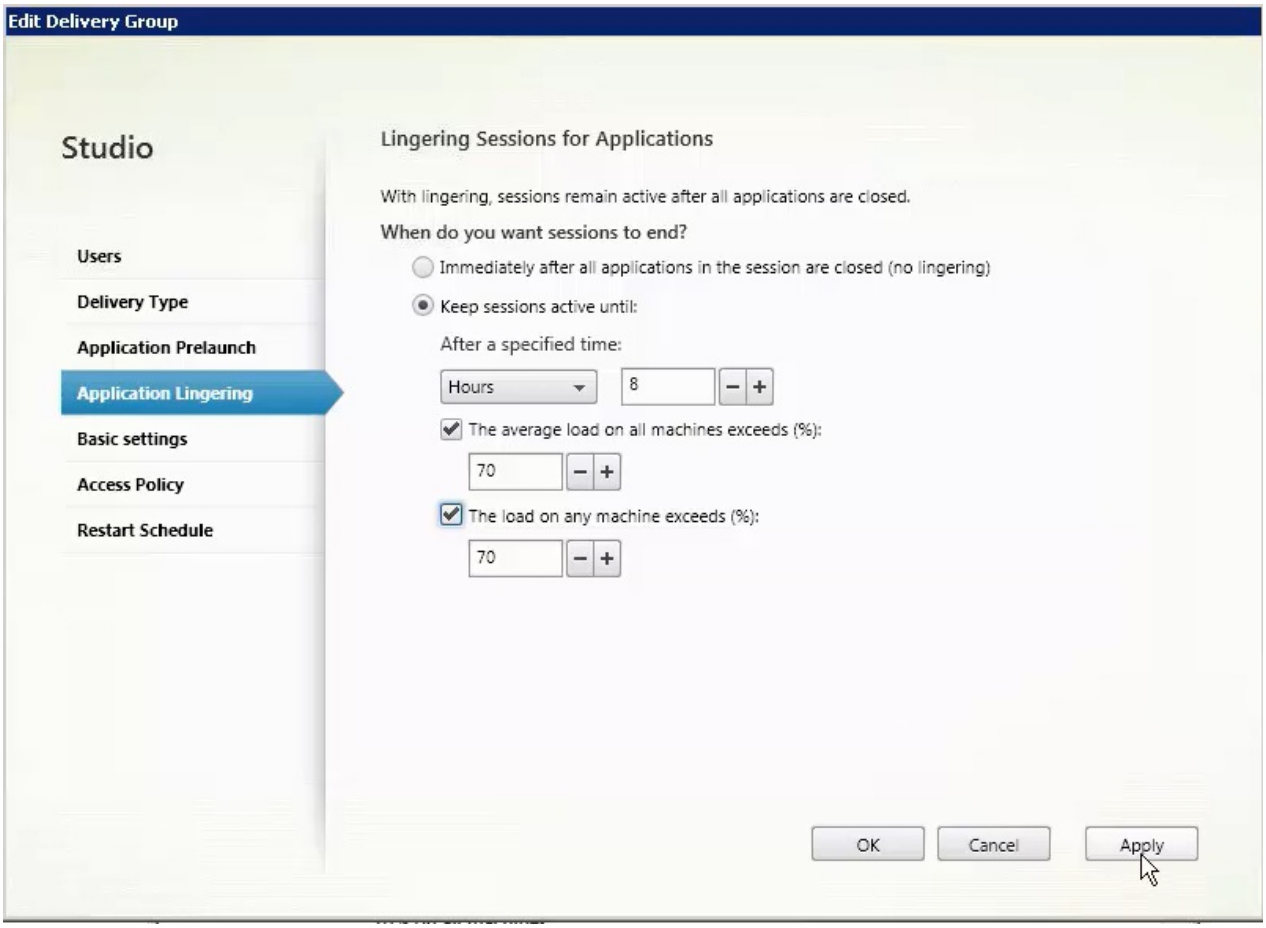
4. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。
   - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を1～99日間、1～2,376時間、または1～142,560分で指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- デリバリーグループ内のすべてのマシンの平均負荷が上限値（1～99%）を超えたときに終了する。
- デリバリーグループ内のいずれかのマシンの負荷が上限値（1～99%）を超えたときに終了する。

事前起動セッションは、ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたときのいずれかの状態が発生するまで保持されます。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. デリバリーグループを選択して、［操作］ペインの **[デリバリーグループの編集]** を選択します。
3. **[アプリケーションの残留]** ページで、**[セッションをアクティブのまま保持する期間を指定する]** をクリックします。



4. ユーザーが別のアプリケーションを起動しない場合、残留セッションを保持する時間は複数の設定によって決定されます。
   - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を1～99日間、1～2,376時間、または1～142,560分で指定します。
   - デリバリーグループ内のすべてのマシンの平均負荷が上限値（1～99%）を超えたときに終了する。
   - デリバリーグループ内のいずれかのマシンの負荷が上限値（1～99%）を超えたときに終了する。

   残留セッションは、ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたときのいずれかの状態が発生するまで保持されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーショングループの作成

Dec 05, 2017

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代わりの手段となります。デリバリーグループは複数のアプリケーショングループに関連付けることができ、アプリケーショングループは複数のデリバリーグループに関連付けることができます。

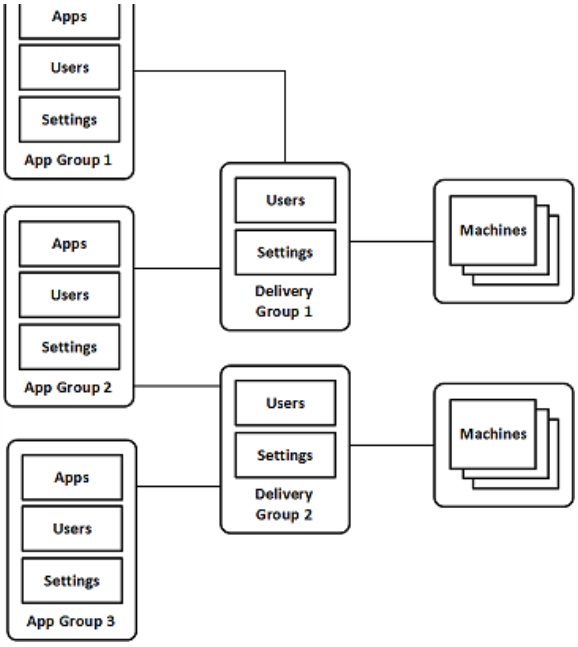
アプリケーショングループの使用は、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします。

- アプリケーションおよびその設定を論理的にグループ化することで、アプリケーションを1つの単位として管理することができます。たとえば、同じアプリケーションをそれぞれのデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間でのセッション共有により、リソースの消費を削減できます。また、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- *タグ制約*機能を使用することで、選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループからアプリケーションを公開できます。 タグ制約で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制約は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。タグ制約のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

例1

次の図は、アプリケーショングループを含むXenAppまたはXenDesktop環境を示しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループでは、使用されるマシンを指定します。（示されていませんが、マシンはマシンカタログに含まれています。）

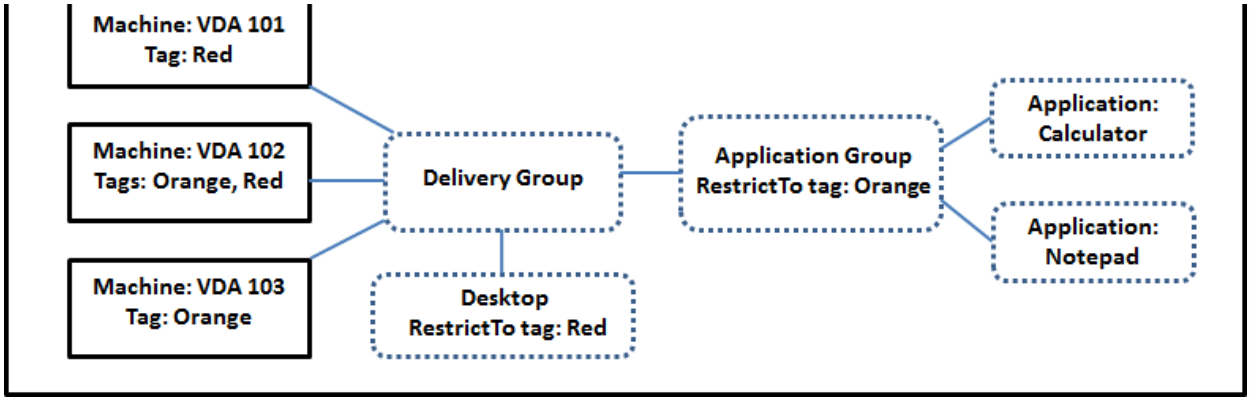
アプリケーショングループ1はデリバリーグループ1に関連付られています。アプリケーショングループ1のアプリケーションには、アプリケーショングループ1で指定されているユーザーが、デリバリーグループ1のユーザー一覧にも含まれている限り、アクセスできます。これは、アプリケーショングループのユーザー一覧は関連付けられているデリバリーグループのユーザー一覧のサブセット（制限）でなければならないというガイダンスに従っています。アプリケーショングループ1の設定（アプリケーショングループ間で共有されるアプリケーションセッション、関連付られているデリバリーグループなど）は、このグループのアプリケーションとユーザーに適用されます。デリバリーグループ1の設定（匿名ユーザーサポートなど）は、アプリケーショングループ1および2のユーザーに適用されます。この2つのアプリケーショングループがこのデリバリーグループに関連付けれらているためです。

アプリケーショングループ2は、デリバリーグループ1と2に関連付られています。この2つのデリバリーグループそれぞれにアプリケーショングループ2の優先度を割り当てることで、アプリケーション起動時にデリバリーグループをチェックする順序を指定できます。同等の優先度が割り当てられたデリバリーグループ間では、負荷が分散されます。アプリケーショングループ2のアプリケーションには、アプリケーショングループ2で指定されているユーザーが、デリバリーグループ1とデリバリーグループ2のユーザー一覧にも含まれている限り、アクセスできます。

例2：

この単純なレイアウトでは、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグ制約を使用して制御します。サイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された2つのアプリケーショングループがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3台のマシン（VDA 101～103）それぞれにタグが追加されています。

アプリケーショングループは「Orange」のタグ制約で作成されているので、各アプリケーション（計算機とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン（VDA 102および103）上でのみ起動できます。

アプリケーショングループ（およびデスクトップ）でのタグ制約の使用に関する包括的な例やガイダンスは、「タグ」を参照してください。

ガイダンスおよび考慮事項

Citrixは、アプリケーショングループとデリバリーグループの両方にではなく、どちらか一方にアプリケーションを追加することをお勧めします。両方に追加すると、アプリケーションを2種類のグループに追加することにより複雑度が増加し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループが有効になっています。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間でのアプリケーションセッションの共有が有効になっています。以下の「アプリケーショングループ間のセッション共有」を参照してください。

Citrixは、デリバリーグループを最新のバージョンにアップグレードすることをお勧めします。デリバリーグループのアップグレードは、(1)デリバリーグループで使用するマシン上のVDAのアップグレード、(2)これらのマシンを含むマシンカタログのアップグレード、(3)デリバリーグループのアップグレードの順に行う必要があります。詳しくは、「デリバリーグループの管理」を参照してください。アプリケーショングループを使用するには、コアコンポーネントがバージョン7.9以上である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みの役割の配信管理者権限が必要です。詳しくは、「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」と表現することで、このアクションと、利用可能なソースからアプリケーションの新しいインスタンスを追加することを区別しています。同様に、デリバリーグループはアプリケーショングループに関連付けられ、アプリケーショングループはデリバリーグループに関連付けられます。追加されるのでも、お互いのコンポーネントになるのでもありません。

アプリケーショングループを使用したセッション共有

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーションセッション共有を有効にすると、すべてのアプリケーションが同一のアプリケーションセッションで起動されるようになります。これにより、追加のアプリケーションセッションの起動にかかるコストが抑えられるとともに、クリップボードを使用するアプリケーション機能（コピーアンドペーストなど）を使用できます。ただし、セッション共有の無効化が必要になる場合もあります。

アプリケーショングループを使用する場合、以下の3通りの方法でアプリケーションセッション共有を構成して、デリバリーグループのみを使用ときに利用できる標準的なセッション共有の動作を拡張できます。

- アプリケーショングループ間でセッション共有を有効にする。
- 同一のアプリケーショングループに含まれるアプリケーション間でのみセッション共有を有効にする。
- セッション共有を無効にする。

アプリケーショングループ間のアプリケーションセッション共有を有効にすることも、この共有を無効化して、アプリケーションセッション共有を同一のアプリケーショングループに含まれるアプリケーションのみに限定することもできます。

アプリケーショングループ間のセッション共有を有効にすることが役立つ例：

> アプリケーショングループ1には、WordやExcelなどのMicrosoftアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などその他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーションへのアクセス権を持つユーザーが、Wordを起動してアプリケーションセッションを開始してから、メモ帳を起動するとします。Controllerにより、このユーザーのWordが実行されている既存のセッションがメモ帳の実行にも適していると判断されると、メモ帳は既存のセッション内で起動されます。メモ帳を既存のセッションで実行できない場合（タグ制約によりセッションの実行元のマシンが除外されている場合など）、セッション共有を使用せず適切なマシン上に新しいセッションが作成されます。

アプリケーショングループ間のセッション共有を無効にすることが役立つ例：

> 同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザーの2つの異なるバージョンなど、同時に使用することがあまりない一連のアプリケーションが同じマシンにインストールされています。管理者は、同じセッションで両方のバージョンを起動することをユーザーに許可しないほうがいいと考えました。
>
> ソフトウェアスイートの各バージョン用にアプリケーショングループを1つ作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追加しました。これらの各アプリケーショングループでグループ間のセッション共有を無効にすると、各グループで指定されたユーザーは同じセッションで同じバージョンのアプリケーションを実行でき、同時に他のアプリケーションを別のセッションで実行できます。ユーザーが異なるバージョンのアプリケーション（異なるアプリケーショングループに含まれるアプリケーション）を起動するか、アプリケーショングループには含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

重要： このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。完全に信頼することはできず、ユーザーが別の手段（Windowsエクスプローラーなど）を使用してセッションにアプリケーションを起動することは防げません。

マシンがフル稼働の場合、そのマシンで新しいセッションは開始されません。新しいアプリケーションは、必要に応じてセッション共有を使用し、既存のセッション内で起動されます（この動作が、ここで説明するセッション共有の制限に従っている場合）。

事前起動セッションは、アプリケーションセッション共有が許可されているアプリケーショングループでのみ利用できます（残留セッション機能を使用するセッションは、すべてのアプリケーショングループで利用できます）。 これらの機能は、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーショングループに関連付けるデリバリーグループごとに有効にして構成する必要があります。これらの機能をアプリケーショングループで構成することはできません。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は、アプリケーショングループ作成時に有効にされます。グループを作成しているときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

同一のアプリケーショングループに含まれるアプリケーション間で、アプリケーションセッション共有を無効にすることができます。

アプリケーショングループ内のセッション共有を無効にすることが役立つ例：

ユーザーが別々のモニターで、アプリケーションの複数の全画面セッションへ同時にアクセスできるようにする場合。

アプリケーショングループを作成して、そのグループにアプリケーションを追加する場合。アプリケーショングループ内のアプリケーション間でのセッション共有が禁止されている場合、グループ内で指定されたユーザーは別々のセッションでアプリケーションを1つずつ起動することになり、各アプリケーションを個別のモニターに移動することができます。

デフォルトでは、アプリケーションセッション共有はアプリケーショングループの作成時に有効にされます。グループを作成しているときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループの作成

アプリケーショングループを作成するには：

1. Studioのナビゲーションペインで **[アプリケーション]** を選択し、次に［操作］ペインで **[アプリケーショングループの作成]** を選択します。
2. アプリケーショングループの作成ウィザードが起動され、**[はじめに]** ページが開きます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、以下のページの操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで **[次へ]** をクリックします。

すべてのデリバリーグループの一覧には、各デリバリーグループに含まれるマシンの数が表示されます。

- **[互換性のあるデリバリーグループ]** の一覧には、選択できるデリバリーグループが表示されます。互換性のあるデリバリーグループには、ランダムな（永続的ではない、つまり静的に割り当てられていない）サーバーやデスクトップOSマシンが含まれます。
- **[互換性のないデリバリーグループ]** の一覧には、選択できないデリバリーグループが含まれます。各エントリで、静的に割り当てられたマシンを含む、などの互換性がない理由が説明されます。

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

また、（1）デリバリーグループに共有マシンが含まれていてこのグループがXenDesktop 7.x バージョンで作成されており、かつ（2）［デリバリーグループの編集］権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

るデリバリーグループを選択することもできます。アプリケーショングループの作成ウィザードをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

おそらくはアプリケーションを整理したり現在は使用されていないアプリケーションのストレージとして使用したりするために、デリバリーグループに関連付けないアプリケーショングループを作成することができますが、アプリケーショングループで少なくとも1つのデリバリーグループを指定するまでは、そのアプリケーショングループを使用してアプリケーションを配信することはできませんまた、デリバリーグループが指定されていない場合は、［［スタート]メニューから］ソースからアプリケーショングループにアプリケーションを追加することもできません。

選択するデリバリーグループで、アプリケーションの配信に使用するマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制約を追加するには、**[タグでマシンの起動を制限します：]**を選択し、ドロップダウンからタグを選択します。詳しくは、「タグ」を参照してください。

アプリケーショングループのアプリケーションを使用できるユーザーを指定します。1つ前のページで選択したデリバリーグループのすべてのユーザーとユーザーグループに許可するか、このデリバリーグループの特定のユーザーとユーザーグループを選択することができます。指定したユーザーの使用を制限した場合は、デリバリーグループとアプリケーショングループで指定したユーザーだけが、このアプリケーショングループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザー一覧は、デリバリーグループのユーザー一覧のフィルターとして機能します。

認証されていないユーザーによるアプリケーション使用の有効化または無効化は、デリバリーグループでのみ行えます。アプリケーショングループではできません。

ユーザー一覧の指定場所

以下の作成時または編集時に、Active Directoryユーザー一覧を指定します。

- デリバリーグループの使用権を持つユーザーの一覧。この一覧はStudioでは構成されません。デフォルトでは、アプリケーション資格ポリシー規則には全ユーザーが含まれます。詳しくは、PowerShell SDKのBrokerAppEntitlementPolicyRuleコマンドレットを参照してください。
- アプリケーショングループのユーザー一覧。
- デリバリーグループのユーザー一覧。
- アプリケーション可視性プロパティ。

StoreFront経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーションAの使用を構成するには次のように設定します。

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- アプリケーションA～Lに管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーションAのプロパティを構成します。

ヒント：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 新規アプリケーションをデリバリーグループに追加すると、デフォルトでは「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。アプリケーションの追加時に、そのフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された一意の名前を受け入れると、アプリケーションにその新しい名前が追加されます。受け入れない場合は、提案された名前を自分で変更して、追加できるようにする必要があります。詳しくは、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。「アプリケーションプロパティの変更」を参照してください。2つのアプリケーションを同じ名前で同じユーザーに公開する場合は、Studioで［アプリケーション名（ユーザー用）］プロパティの名前を変更します。これを行わないと、ユーザーのCitrix Receiverに同じ名前が2つ表示されます。
- アプリケーションを複数のアプリケーショングループに追加する場合、そのすべてのアプリケーショングループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したグループをすべて含めるようにします。

［追加］ボックスをクリックして、アプリケーションのソースを表示します。

接続元	説明
［スタート］メニューから	選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、 **［OK］**をクリックします。 このソースは、（1）デリバリーグループが関連付けられていないアプリケーショングループを選択した、（2）マシンを含まないデリバリーグループが関連付られているアプリケーショングループを選択した、（3）マシンを含まないデリバリーグループを選択した、のいずれかの場合には選択できません。
手動で定義	サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。これらの情報を入力したら、 **［OK］**をクリックします。
既存	以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、 **［OK］**をクリックします。 このソースは、サイトにアプリケーションが含まれていない場合は選択できません。
App-V	App-Vパッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページでApp-Vサーバーまたはアプリケーションライブラリを選択します。結果表示で、追加するアプリケーションのチェックボックスをオンにし、 **［OK］**をクリックします。詳しくは、「App-V」を参照してください。 このソースは、サイトでApp-Vを構成していない場合は選択できません（表示されないこともあります）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

上述のとおり、**[追加]** ボックスの特定のエントリは、そのタイプの有効なソースがない場合は選択できません。互換性のな
ソースは、一切表示されません。たとえば、アプリケーショングループにアプリケーショングループは追加できないため、こ
のソースはアプリケーショングループ作成時には表示されません。

このページは、スコープを作成済みの場合にのみ表示されます。デフォルトでは、**[すべて]** スコープが選択されています。詳しくは、「委任管理」を参照してください。

アプリケーショングループの名前を入力します。必要に応じて説明も入力できます。

概要の情報を確認し、**[完了]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーショングループの管理

Dec 05, 2017

ここでは次のことについて説明します。

- はじめに
- アプリケーショングループの有効化または無効化
- アプリケーショングループ間でのアプリケーションセッション共有の有効化または無効化
- アプリケーショングループ内のアプリケーションのセッション共有を無効にします。
- アプリケーショングループ名の変更
- アプリケーショングループとデリバリーグループの関連付けの追加、削除、または優先度変更
- アプリケーショングループのタグ制約の追加、変更、または削除
- アプリケーショングループのユーザーの追加または削除
- アプリケーショングループのスコープの変更
- アプリケーショングループの削除

はじめに

この記事では、作成済みのアプリケーショングループの管理手順について説明します。

以下の操作方法を含む、アプリケーショングループまたはデリバリーグループでのアプリケーションの管理について詳しくは、「アプリケーション」を参照してください。

- アプリケーショングループのアプリケーションの追加または削除
- アプリケーショングループの関連付けの変更

アプリケーショングループの管理には、組み込みの役割であるデリバリーグループ管理者の委任管理権限が必要です。詳しくは、「委任管理」を参照してください。

アプリケーショングループの有効化または無効化

アプリケーショングループを有効にすると、このグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、グループ内のアプリケーションもすべて無効になります。ただし、これらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合は、これらの他のアプリケーショングループから配信できます。同様に、アプリケーションが（アプリケーショングループへの追加に加えて）アプリケーショングループに関連付けられているデリバリーグループに明示的に追加されている場合は、アプリケーショングループを無効にしても、これらのデリバリーグループに追加されたアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。これをグループの作成時に変更することはできません。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択します。
3. **[設定]** ページで、**[アプリケーショングループを有効にします]** チェックボックスをオンまたはオフにします。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーショングループ間でのアプリケーションセッション共有の有効化または無効化

アプリケーショングループ間でのセッション共有は、アプリケーショングループの作成時に有効になります。これをグループの作成時に変更することはできません。アプリケーションセッション共有について詳しくは、「アプリケーション間のセッション共有」を参照してください。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択します。
3. **［設定］**ページで、**[アプリケーショングループ間のアプリケーションのセッション共有を有効にします]**チェックボックスをオンまたはオフにします。
4. **［適用］**をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループ内のアプリケーションのセッション共有を無効にします。

同じアプリケーショングループのアプリケーション間のセッション共有は、アプリケーショングループを作成した場合、デフォルトで有効です。アプリケーショングループ間でのアプリケーションセッション共有を無効化しても、同じアプリケーショングループのアプリケーション間のセッション共有は引き続き有効です。Broker PowerShell SDKを使用して、所属するアプリケーション間のセッション共有を無効化したアプリケーショングループを構成できます。状況によっては、この機能が望ましい場合もあります。たとえば、ユーザーが複数の非シームレスアプリケーションを個別のモニターのフルサイズのアプリケーションウィンドウで起動できるようにする場合などです。アプリケーションセッション共有について詳しくは、「アプリケーション間のセッション共有」を参照してください。

アプリケーショングループ内でのアプリケーションセッション共有を無効にした場合、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。適切な切断されたセッションで同じアプリケーションが動作中の利用可能なセッションがあれば、そのセッションが再接続されます。たとえば、Notepadを起動する場合、Notepadが動作中の切断されたセッションがあれば、新しいセッションを作成しないでそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、そのうちの1つのセッションが再接続先として、ランダムだが決定的な方法で選択されます。同じ状況で同じ状態が再現した場合は、同じセッションが選択されます。しかし、そうでない場合は再接続されるセッションは、予測できるとは限りません。
Broker PowerShell SDKを使用して、既存のアプリケーショングループのすべてのアプリケーションでアプリケーションセッション共有を無効化するか、アプリケーションセッション共有を無効化したアプリケーショングループを作成できます。

セッション共有を無効化するには、Broker PowerShellコマンドレットの**New-BrokerApplicationGroup**、または**Set-BrokerApplicationGroup**を**-SessionSharingEnabled**パラメーターをFalseに、**-SingleAppPerSession**パラメーターをTrueに設定して実行します。

たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効のアプリケーショングループを作成するには、以下を実行します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効化するには、以下を実行します。

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

- SingleAppPerSessionプロパティを有効化するには、SessionSharingEnabledプロパティをFalseに設定する必要があります。この2つのプロパティは、同時に有効化してはなりません。SessionSharingEnabledパラメーターは、アプリケーショングループ間のセッション共有に関するものです。
- アプリケーションセッション共有は、アプリケーショングループに割り当てられているが、デリバリーグループには割り当てられていないアプリケーションに対してのみ有効です。（デリバリーグループに直接割り当てられているアプリケーションはすべてデフォルトでセッションを共有します）。
- 1つのアプリケーションが複数のアプリケーショングループに割り当てられている場合、グループどうしで設定が矛盾（たとえば、同じオプションを一方はTrueに、他方はFalseに設定しているような場合）しないようにしてください。予想のつかない動作を引き起こします。

アプリケーショングループ名の変更

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループ名を変更します]** を選択します。
3. 新しい一意の名前を指定して **[OK]** をクリックします。

アプリケーショングループとデリバリーグループの関連付けの追加、削除、または優先度変更

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

また、（1）デリバリーグループに共有マシンが含まれていてこのグループがXenDesktop 7.x バージョンで作成されており、かつ（2）［デリバリーグループの編集］権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれるデリバリーグループを選択することもできます。デリバリーグループの種類は、［アプリケーショングループを編集します］ダイアログボックスが表示されると、自動的に「デスクトップとアプリケーション」に変換されます。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択します。
3. **[デリバリーグループ]** ページを選択します。
4. デリバリーグループを追加するには、**[追加]** をクリックします。使用可能なデリバリーグループのチェックボックスをオンにします（互換性のないデリバリーグループは選択できません）。 選択が完了したら、 **[OK]** をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして**[削除]** をクリックします。確認のメッセージが表示されたら、削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして**[優先度の編集]** を

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クリックします。優先度（0=最優先）を入力し、 **[OK]** をクリックします。
7. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのタグ制約の追加、変更、または削除

重要： タグ制約を追加、変更、および削除すると、どのマシンがアプリケーション起動の対象となるかについて、予期しない効果を招くことがあります。「タグ」に記載されている考慮事項と注意を必ず確認してください。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択します。
3. **[デリバリーグループ]** ページを選択します。
4. タグ制約を追加するには、 **[次のタグを持つマシンに起動を制約する：]** を選択し、ドロップダウンからタグを選択します。
5. タグ制約を変更または削除するには、異なるタグをドロップダウンから選択するか、**[次のタグを持つマシンに起動を制約する：]** をオフにして、タグ制約を完全に削除します。
6. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのユーザーの追加または削除

ユーザーについて詳しくは、「アプリケーショングループの作成」の記事で「ユーザー」のセクションを参照してください。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択します。
3. **[ユーザー]** ページを選択します。アプリケーショングループ内のアプリケーションの使用を、関連付けられたデリバリーグループ内のすべてのユーザーに許可するか、特定のユーザーおよびグループにのみ許可するかを指定します。ユーザーを追加するには、 **[追加]** をクリックして追加するユーザーを指定します。ユーザーを削除する場合は、1人または複数のユーザーを選択し、 **[削除]** をクリックします。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのスコープの変更

スコープの変更は、スコープを作成済みの場合のみ行うことができます（［すべて］のスコープを編集することはできません）。詳しくは、「委任管理」を参照してください。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで**[アプリケーショングループを編集します]** を選択

© 1999-2017 Citrix Systems, Inc. All rights reserved.

します。
3. **[スコープ]** ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループの削除

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付ける必要があります。アプリケーショングループの削除により1つまたは複数のアプリケーションがグループに属していない状態になる場合は、グループを削除するとこれらのアプリケーションも削除されることを通知する警告メッセージが表示されます。削除を確定またはキャンセルすることができます。

アプリケーションを削除しても、そのアプリケーションは元のソースからは削除されません。ただし、このアプリケーションを再び使用可能にするには、追加し直す必要があります。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで **[グループの削除]** をクリックします。
3. 確認のメッセージが表示されたら、削除を確定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リモートPCアクセス

Dec 05, 2017

リモートPCアクセス機能により、社内にある自分の物理的なWindows PCにどこからでもリモートアクセスできるようになります。

社内PC上にインストールするVirtual Delivery Agent（VDA）により、そのPCがCloudコネクタまたはDelivery Controllerに登録され、PCとクライアントデバイス間のHDX接続が管理されます。リモートPCアクセス機能ではセルフサービス型の構成がサポートされており、管理者がホワイトリスト（ユーザーによるアクセスを許可するマシンの一覧）を作成しておくと、各ユーザーが管理者による介在なく自分の社内PCを追加できます。クライアントデバイス上で動作するCitrix Receiverにより、リモートPCアクセスセッションから社内のPC上のアプリケーションやデータへのアクセスが可能になります。

ユーザーには、任意の数の物理PC、または物理PCと仮想デスクトップの組み合わせを含む、複数のデスクトップを割り当てることができます。

注： リモートPCアクセスではスリープモードおよび休止状態モードはサポートされません。（オンプレミスのXenAppおよびXenDesktopの展開の場合：リモートPCアクセスセッションではXenDesktopライセンスが使用され、ほかのXenDesktopセッションと同じ方法でライセンスが消費されます。）

Active Directoryに関する注意事項

リモートPCアクセスの展開サイトを構成する前に、Active Directory組織単位（OU）とセキュリティグループをセットアップして、Active Directoryユーザーアカウントを作成してください。

マシンカタログにマシンを追加した後でActive Directoryを変更しても、リモートPCアクセス機能には反映されません。必要な場合は、マシンを手動で別のマシンカタログに再割り当てできます。

Active DirectoryのOUエントリを移動または削除すると、リモートPCアクセスに使用されるOUエントリで整合性の問題が発生して、VDAとマシンカタログまたはデリバリーグループとの関連付けが解除されることがあります。

マシンカタログおよびデリバリーグループに関する考慮事項

リモートPCアクセスでは、1つのマシンを複数のマシンカタログやデリバリーグループに関連付けることはできません。

リモートPCアクセスのマシンカタログに複数のマシンを追加できます。

カタログ用のマシンアカウントを選択するときは、ほかのカタログ内のマシンとの競合を避けるため、最も低いレベルのOUを選択します。たとえば、bank/officers/tellersのOUではtellersを選択します。

リモートPCアクセスのマシンカタログに含まれるすべてのマシンを、1つまたは複数のデリバリーグループで割り当てることができます。たとえば、2つのユーザーグループに異なるポリシー設定を適用するには、それらのユーザーを異なるデリバリーグループに追加して、各デリバリーグループ用のHDXポリシーフィルターを構成します。

IT管理の責任分担がユーザーの地理的な場所、部署、またはそのほかのカテゴリによって細分化されている場合は、マシンやユーザーをカテゴリごとにグループ化して、委任管理を構成します。各管理者には、そのカテゴリ内のカタログと対応するテ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リバリーグループの両方に対する管理権限が正しく割り当てられていることを確認してください。

展開に関する考慮事項

リモートPCアクセス展開を作成した後で、従来のVirtual Desktop Infrastructure（VDI）デスクトップまたはアプリケーションを追加することができます。また、リモートPCアクセス展開を既存のVDI展開に追加することもできます。

社内のPC上にVDAをインストールするときに、［Windows Remote Assistance］チェックボックスをオンにすることを検討してください。これにより、ヘルプデスク担当者がDirectorからWindowsリモートアシスタンスを使用して、ユーザーのセッションを表示したり操作したりできるようになります。

各社内PCへのVDAのインストール方法を検討します。Active Directoryスクリプトや Microsoft System Center Configuration Managerなど、電子的なソフトウェアディストリビューションツールを使用することをお勧めします。インストールメディアには、Active Directoryスクリプトのサンプルが収録されています。

リモートPCアクセス展開のセキュリティに関する考慮事項を確認してください。

現時点では、リモートPCアクセスのセキュアブートはWindows 10でサポートされています。

各社内PCは、有線ネットワーク接続によりドメインに参加している必要があります。

社内PCでのWindows 7 Aeroがサポートされていますが、この機能を使用しなければならないということではありません。

キーボードやマウスは、社内のPCやラップトップに直接接続してください。電源がオフになることのあるモニターなどのデバイス経由で接続しないでください。キーボードやマウスをモニターなどのデバイス経由で接続する必要がある場合は、そのデバイスの電源がオフにならないようにする必要があります。

スマートカードを使用する場合は、「スマートカード」を参照してください。

リモートPCアクセスはほとんどのラップトップコンピューターでも使用できます。いつでもアクセスできるように、ラップトップコンピューターの省電力設定を、デスクトップPCと同様に構成する必要があります。次に例を示します。

- 休止機能を無効にする。
- スリープ機能を無効にする。
- カバーを閉じた場合の動作を［何もしない］に設定する。
- 電源ボタンを押したときの操作を［シャットダウン］に設定する。
- ビデオカードの省電力設定を無効にする。
- インターフェイスカードの省電力設定を無効にする。
- バッテリーの節電機能を無効にする。

以下のデバイスは、リモートPCアクセスでサポートされません。

- ラップトップのドッキングおよびドッキング解除。
- KVMスイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。
- ハイブリッドPC（オールインワンおよびNVIDIA Optimusラップトップおよび PCを含む）。

Windows 10のSurface Proデバイス上でのリモートPCアクセスがサポートされます。いつでもアクセスできるように、Surfaceデバイスを、デスクトップまたはラップトップコンピューターと同様に構成する必要があります。次に例を示します。

- 休止機能またはスリープ機能を無効にする。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 有線ネットワーク接続を使用する。
- セッションの初期化時または再接続時には常にキーボードが接続されているようにする。
- バッテリーの節電機能を無効にする。

社内PCにリモートアクセスする各クライアントデバイスにCitrix Receiverをインストールします。

同じ社内PCにリモートアクセスする複数のユーザーには、Citrix Receiverに同じアイコンが表示されます。いずれかのユーザーがそのPCにリモートからログオンすると、ほかのユーザーにはそれを使用できないことを示すアイコンが表示されます。

デフォルトでは、ローカルユーザーがそのマシンでCtrl+Alt+Delキーを押してセッションを開始すると、リモートユーザーのセッションは自動的に切断されます。自動的に切断されないようにするには、社内PCに次のレジストリエントリを追加してから、マシンを再起動します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePCで、この機能の内容をよりカスタマイズするには

RpcaMode（dword）：

1 =指定のタイムアウト期間にMessaging UIへ応答しない場合、リモートユーザーが常に獲得します。

2 =ローカルユーザーが常に獲得します。この設定を指定しない場合、リモートユーザーがデフォルトで獲得します。

RpcaTimeout（dword）：

適用されるモードの種類が決定される前に、ユーザーに対して与えられる秒数。この設定が指定されない場合、デフォルト値は30秒です。この最小値は、30秒とする必要があります。これらの変更を有効にするには、ユーザーがマシンを再起動する必要があります。

ユーザーがコンソールへ強制的にアクセスできるようにするには、ローカルユーザーがCtrl+Alt+Delキーを2回、10秒の間に押して、リモートセッション上でローカルの制御を実行できるようにして、切断イベントを強制的に実行します。

このレジストリ設定により、リモートユーザーが社内PCのセッションを使用しているときにローカルユーザーがCtrl+Alt+Deキーを押してそのPCにログオンすると、ローカルユーザーの接続を許可するかどうかを確認するメッセージがリモートユーザーに表示されます。接続を許可すると、リモートユーザーのセッションは切断されます。

リモートPCアクセスおよびHDX 3D Proモード

リモートPCアクセスの場合、VDAは通常、標準のVDAオプションを使用して構成されます。HDX 3D Proで構成されているリモートPCアクセスの場合、モニターのブランキングはIntel Iris Pro graphicsとIntel HD graphics 5300以上（第5世代Intel Coreプロセッサおよび第6世代Intel Core i5プロセッサ）、およびNVIDIA QuadroとNVIDIA GRID GPUでサポートされます。

詳しくは、「WindowsデスクトップOSのためのGPUアクセラレーション」を参照してください。

Wake-on-LAN

注：Citrix CloudでのリモートPCアクセスでは、Wake on LANはサポートされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リモートPCアクセスではWake on LANがサポートされ、物理PCをリモートから起動できます。この機能により、ユーザーが退社時にPCの電源をオフにできるようになるため、消費電力を節約できます。また、停電や気象条件などにより電源がオフになったPCにもリモートアクセスできるようになります。

リモートPCアクセスのWake on LAN機能は、以下のデバイスでサポートされます。

- BIOSでWake on LANオプションが有効になっているPC。こうしたPCではウェイクアッププロキシとマジックパケットもサポートされ、Microsoft System Cemter Configuration Manager（ConfigMgr）2012、ConfigMgr 2012 R2、またはConfigMgr 2016を使用している場合にWake on LAN機能を利用できます。
- Intel社のActive Management Technology（AMT）をサポートするPC。AMT対応マシンでは、StudioやDirectorからそのマシンを強制的にシャットダウンまたは再起動することもできます。また、StoreFrontおよびReceiverで再起動を行うこともできます。**重要**：AMTに対するサポートはConfigMgr 2012または2012 R2を使用している場合に限られており、ConfigMgr 2016を使用している場合は利用できません。

Wake on LAN機能を使用するようにConfigMgrを構成します。さらに、Studioでリモートpcアクセス展開を作成するとき（またはリモートPCアクセス用に別の電源管理接続を追加するとき）に、電源管理機能を有効にして、ConfigMgrのアクセス情報を指定します。

この構成について詳しくは、「Configuration Managerとリモートpcアクセスのwake on lan」を参照してください。

リモートPCアクセスのWake on LAN機能を構成するには、以下のタスクを完了してから社内PCにVDAをインストールします。

- 組織内でConfigMgr 2012、2012 R2、または2016を構成します。リモートPCアクセス用のすべてのマシンにConfigMgrクライアントを展開し、スケジュールされているSCCMインベントリサイクルが実行されるのを待ちます（必要に応じて、手動で強制的に実行することもできます）。StudioでConfigMgr接続を構成するときのアクセス資格情報には、セキュリティスコープにコレクションが含まれており、リモートツールオペレーターロールが付与されている必要があります。
- Intel社のActive Management Technology（AMT）を使用する場合。
  - PCでAMT 3.2.1以降がサポートされている必要があります。
  - 適切な資格情報およびプロビジョニングプロセスを使用して、PCでAMTが使用されるようにプロビジョニングします。
  - ConfigMgr 2012と2012 R2のみを使用できます。ConfigMgr 2016は使用できません。
- ConfigMgrのウェイクアッププロキシやマジックパケットを使用する場合。
  - 各PCのBIOS設定で、Wake on LAN機能を有効にします。
  - ウェイクアッププロキシの場合は、ConfigMgrでウェイクアッププロキシを有効にします。リモートPCアクセスのWake on LAN機能を使用するPCが属する各サブネットで、センチネルマシンとして動作可能なものが3台以上あることを確認します。
  - マジックパケットの場合は、サブネット宛てのブロードキャストまたはユニキャストを使用して、ネットワーク経路およびファイアウォールでパケットの転送がブロックされないようにします。

社内PC上にVDAをインストールしたら、接続とマシンカタログを作成するときに電源管理機能を有効または無効にします。

- カタログで電源管理機能を有効にする場合は、接続の詳細としてConfigMgrのアドレス、アクセス資格情報、および名前を指定します。
- 電源管理機能を無効にした場合でも、電源管理（Configuration Manager）接続を後から追加して、リモートPCアクセスのマシンカタログを編集してこの接続を指定し、電源管理機能を有効にできます。

電源管理接続を編集して、詳細設定を変更できます。以下の機能を有効にできます。

- ConfigMgrのウェイクアッププロキシ。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Wake on LAN（マジック）パケット。Wake on LANパケットを有効にする場合は、パケットの転送方法としてサブネット向けのブロードキャストまたはユニキャストを選択できます。

社内PCではAMTパワーコマンド（サポートされる場合）と、有効にした詳細設定が使用されます。AMTパワーコマンドが使用されない場合は、詳細設定が使用されます。

Citrix Cloud展開：構成順序と考慮事項

「CTX220737: How to Enable XenDesktop Remote PC Access in Citrix Cloud」を参照してください。

オンプレミス展開：構成順序と考慮事項

リモートPCアクセスサイトを作成する前に、以下を実行します。

リモートPCアクセスの電源管理機能（リモートPCアクセスのWake on LAN機能）を使用する場合、Studioでリモート PCアクセス展開を作成する前に、接続先のPCとMicrosoft System Center Configuration Manager（ConfigMgr）での構成を完了しておく必要があります。詳しくは、「Configuration Managerとリモート PCアクセスのWake on LAN」を参照してください。

サイトの作成ウィザードで、以下を実行します。

- リモートPCアクセスサイトの種類を選択します。
- 管理者は、**[電源管理]** ページで、デフォルトのリモートPCアクセスマシンカタログのマシンの電源管理機能を有効または無効にできます。電源管理を有効にする場合は、ConfigMgr接続の情報を指定します。
- **[ユーザーおよびマシンアカウント]** ページで、ユーザーおよびマシンアカウントを指定します。

リモートPCアクセスサイトを作成すると、「リモートPCアクセスマシン」という名前のデフォルトマシンカタログと、「リモートPCアクセスデスクトップ」という名前のデフォルトデリバリーグループが作成されます。

リモートPCアクセス用のマシンカタログを追加する場合は、以下の操作を行います。

- ［オペレーティングシステム］ページで［リモートPCアクセス］を選択し、電源管理接続を選択します。電源管理機能を無効にすることもできます。構成済みの電源管理接続がない場合は、マシンカタログの作成ウィザードを完了した後で接続を作成し（接続の種類は［Microsoft Configuration Manager Wake on LAN］）、カタログを編集してその接続を指定します。
- **[マシンアカウント]** ページで、一覧からマシンアカウントまたは組織単位（OU）を選択するか、マシンアカウントおよびOUを追加します。

ローカルおよびリモートアクセスで使用する社内PCにVDAをインストールします。一般的にはパッケージ管理ソフトウェアを使用してVDAを自動的に展開します。ただし、検証用または小規模な展開の場合は、各社内PC上にVDAを手動でインストールできます。リモートPCアクセス展開用にデスクトップVDAをインストールするために使用できる方法は複数あります。

全製品またはVDAWorkstationSetup.exeのインストーラーの使用

- グラフィカルユーザーインターフェイス： ウィザードの **[環境]** ページで **[リモート PC アクセス]** を選択します。 **[追加コンポーネント]** ページ上のコンポーネントはデフォルトでは選択されていません。リモートPCアクセス操作では必要ありません。
- コマンド行インターフェイス：/remotepcオプションを指定します。このオプションでは、次のコンポーネントのインストールができなくなります（これは、ウィザードの **[追加コンポーネント]** ページ上のアイテムに相当します）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V
User Profile Manager
User Profile Manager WMI Plugin
Machine Identity Service
およびPersonal vDisk

代わりに、これらの各コンポーネントを除外するのには、/excludeオプションを使用できます。

VDAWorkstationCoreSetup.exeインストーラーを使用する。このインストーラーでは、Citrix Receiverも追加コンポーネントもインストールできません。

VDAをインストールした後で、その社内PCのコンソールセッションに（ローカルまたはRDP経由で）最初にログオンしたドメインユーザーにそのリモートPCアクセスデスクトップが自動的に割り当てられます。そのコンソールセッションにさらにほかのドメインユーザーがログオンすると、それらのユーザーもデスクトップユーザーの一覧に追加されます。ただし、これらのユーザーには管理者が構成した制限事項が適用されます。

XenApp/XenDesktop環境外でRDP接続を使用するには、ユーザーまたはグループをDirect Access Usersグループに追加する必要があります。

社内PCへのリモート接続で使用するすべてのユーザーデバイスにCitrix Receiverをダウンロードおよびインストールするようユーザーに指示します。 Citrix Receiverはhttp://www.citrix.comから、または使用するモバイルデバイスのアプリケーション配布システム（アプリケーションストア）から入手できます。

トラブルシューティング

リモートPCアクセスの診断情報は、Windowsのアプリケーションイベントログに書き込まれます。情報メッセージは調整されません。エラーメッセージは重複メッセージの破棄により調整されます。

- 3300（情報） — マシンカタログへのマシンの追加
- 3301（情報） — デリバリーグループへのマシンの追加
- 3302（情報） — ユーザーへのマシンの割り当て
- 3303（エラー） — 例外の発生

オンプレミス展開の場合のみ：リモートPCアクセス用の電源管理を有効にすると、サブネット向けのブロードキャストでのマシンの起動に失敗することがあります。この問題は、Controllerとマシンが異なるサブネット上に存在する場合に発生します。AMTがサポートされない場合に異なるサブネット間でサブネット向けのブロードキャストを使用するには、ウェイクアッププロキシまたはユニキャストを使用してください。これらの詳細設定は、電源管理接続のプロパティで有効にできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V

Dec 18, 2017

XenAppおよびXenDesktopでのApp-Vの使用

Microsoft Application Virtualization（App-V）を使用すると、アプリケーションをサービスとして展開、更新、およびサポートできます。ユーザーは、自分のデバイスにインストールすることなくこれらのアプリケーションにアクセスできます。App-VおよびMicrosoft User State Virtualization（USV）では、場所やインターネット接続を問わずに、ユーザーにアプリケーションやデータへのアクセスを提供できます。

次の表は、サポートされるバージョンの一覧です。

App-V	XenDesktopおよびXenAppのバージョン	
	Delivery Controller	VDA
5.0および5.0 SP1	XenDesktop 7以降 XenApp 7.5以降	7.0～現在の
5.0 SP2	XenDesktop 7以降 XenApp 7.5以降	7.1以降
5.0 SP3および5.1	XenDesktop 7.6以降 XenApp 7.6以降	7.6.300～現在の
Windows Server 2016でのApp-V	XenDesktop 7.12以降 XenApp 7.12以降	7.12以降

App-V Clientは、アプリケーションへのオフラインアクセスをサポートしません。App-Vの統合機能により、アプリケーションでのSMB共有の使用がサポートされます。HTTPプロトコルはサポートされません。

App-Vについて詳しくは、Microsoft社のドキュメントを参照してください。以下に、本書で説明するApp-Vコンポーネントの概要を示します。

- **管理サーバー**：App-Vインフラストラクチャを管理したり、App-Vデスクトップクライアントやリモートデスクトップサービスクライアントに仮想アプリケーションを配信したりするための中央管理コンソールです。App-V管理サーバーは、セキュリティ、測定、監視、および管理者によって要求されるデータ収集を認証、要求、および提供します。このサーバーは、Active Directoryといくつかのツールを使用してユーザーとアプリケーションを管理します。
- **公開サーバー**：App-V Clientに特定ユーザー用のアプリケーションを提供し、ストリーム配信用の仮想アプリケーションパッケージをホストします。これらのパッケージは、管理サーバーから取得されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **クライアント**：公開サーバーから仮想アプリケーションを取得したり、クライアント上のアプリケーションを公開したり、Windowsデバイス上で仮想環境のランタイムを自動的にセットアップおよび管理したりします。App-V ClientはVDAにインストールされ、VDAには、各ユーザープロファイルのレジストリやファイルの変更など、ユーザー固有の仮想アプリケーション設定が格納されます。

アプリケーションは、事前構成やオペレーティングシステム設定の変更を行わなくても、シームレスに使用可能になります。以下の方法で、サーバーOSおよびデスクトップOSのデリバリーグループからApp-Vアプリケーションを起動できます。

- Citrix Receiverを使用して起動する。
- ［スタート］メニューから起動する。
- App-VクライアントおよびCitrix Receiverを使用して起動する。
- 複数のデバイス上のアプリケーションを複数ユーザーが同時に起動する。
- Citrix StoreFrontから起動する。

App-Vアプリケーションのプロパティに対する変更は、そのアプリケーションの起動時に適用されます。たとえば、アプリケーションの表示名やアイコンを変更した場合、ユーザーがそのアプリケーションを起動すると変更内容が表示されます。

App-V Sequencerで作成され、その後App-Vサーバーまたはネットワーク共有のいずれかに配置されたApp-Vパッケージを使用できます。

- **App-V サーバー：** App-Vサーバーにあるパッケージのアプリケーションを使用するには、検出、構成、VDAへのダウンロードを実施できるように、StudioとApp-Vサーバー間で継続的な通信が確立されている必要があります。この通信により、ハードウェア、インフラストラクチャ、および管理にオーバーヘッドが生じます。StudioとApp-Vサーバーは、特にユーザーの権限においては、同期されたままである必要があります。

  これは、*デュアル管理*方式と呼ばれます。App-Vパッケージとアプリケーションにアクセスするには、StudioとApp-Vサーバーコンソールの両方が必要なためです。この方式は、App-VとCitrix環境が緊密に統合されている場合に最適に機能します。

- **ネットワーク共有：** ネットワーク共有に置かれたパッケージを使用すると、App-Vサーバーとデータベースインフラストラクチャ間のStudioの依存関係が排除されるため、オーバーヘッドが軽減されます（この場合も、Microsoft App-V Clientを各VDAにインストールする必要があります）。

  これは、*シングル管理*方式と呼ばれます。App-Vパッケージとアプリケーションを使用するには、Studioのコンソールのみが必要なためです。ネットワーク共有を検索し、1つまたは複数のApp-Vパッケージを、ネットワーク共有からサイトレベルのアプリケーションライブラリに追加します。

  アプリケーションライブラリは、App-Vパッケージに関する情報を保存するキャッシングリポジトリを表すCitrixの用語です。またアプリケーションライブラリでは、ほかのCitrixアプリケーションの配信テクノロジに関する情報も保存されます。

いずれかの管理方式を使用することも、両方の管理方式を同時に使用することもできます。つまり、アプリケーションをデリバリーグループに追加する場合、App-Vサーバーとネットワーク共有に置かれたApp-Vパッケージのどちらからもアプリケーションを追加できます。

Studioのナビゲーションペインで、**［構成］＞［App-V公開］**の順に選択すると、App-Vパッケージの名前とソースが表示されます。ソースの列には、パッケージがApp-Vサーバーにあるか、またはアプリケーションライブラリにキャッシュされているかが表示されます。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションが一覧表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-Vシングル管理方式を使用するときは、分離グループを作成して、サンドボックスで実行する必要がある相互依存のアプリケーションのグループを指定できるようにします。この機能は、App-V接続グループと大きな違いはありませんが、同一ではありません。App-V管理サーバーで使用する必須またはオプションのパッケージ用語の代わりに、自動の明示的なパッケージ展開オプションが使用されます。

- ユーザーがApp-Vアプリケーション（プライマリアプリケーション）を起動すると、自動包含対象としてマークされている他のアプリケーションパッケージ用に分離グループが検索されます。それらのパッケージは自動的にダウンロードされ、分離グループに含められます。それらのパッケージを、プライマリアプリケーションを含むデリバリーグループに追加する必要はありません。
- 明示的包含対象としてマークされている分離グループのアプリケーションパッケージは、プライマリアプリケーションが含まれる同じデリバリーグループにそのアプリケーションを明示的に追加した場合に限りダウンロードされます。

これにより、すべてのユーザーがグローバルに使用できる自動包含アプリケーションが混在する分離グループの作成が可能となります。さらにこのグループには、一連のプラグインと（特定のライセンス制約のある）その他のアプリケーションを含めることができます。それにより、追加の分離グループを作成することなく特定のユーザー（デリバリーグループを通して特定）に制限できます。

たとえば、アプリケーション「app-a」を実行するにはJRE 1.7が必要です。（明示的展開の種類の）app-aと（自動展開の種類の）JRE 1.7を含む分離グループを作成できます。その後、それらのApp-Vパッケージを1つまたは複数のデリバリーグループに追加します。ユーザーがapp-aを実行すると、JRE 1.7が自動的にapp-aで展開されます。

アプリケーションは複数のApp-V分離グループに追加することができます。ただし、ユーザーがそのアプリケーションを起動したときは、アプリケーションが追加された最初の分離グループが常に使用されます。そのアプリケーションを含む他の分離グループに順位を付けすること、またはこれらを優先することはできません。

セットアップ

次の表は、XenAppおよびXenDesktopでApp-Vを使用する場合のセットアップ作業の順序をまとめたものです。

管理方式		目的
シングル管理方式	デュアル管理方式	
○	○	App-Vの展開
○	○	パッケージングと配置
	○	StudioでのApp-Vサーバーアドレスの構成
○	○	VDAマシンへのソフトウェアのインストール
○		アプリケーションライブラリへのApp-Vパッケージの追加
○		App-V分離グループの追加（オプション）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

○	○	デリバリーグループへのApp-Vアプリケーションの追加

App-Vの展開手順については、https://technet.microsoft.com/en-us/windows/hh826068を参照してください。

必要に応じて、App-V公開サーバーの設定を変更します。ControllerでSDKのコマンドレットを使用することをお勧めします。詳しくは、SDKのドキュメントを参照してください。

- 公開サーバーの設定を表示するには、「**Get-CtxAppvServerSetting -AppVPublishingServer <*pubServer*>**」と入力します。
- App-Vアプリケーションが正しく起動するようにするには、「**Set-CtxAppvServerSetting –UserRefreshonLogon 0**」と入力します。

これまでGPOポリシーを使用して公開サーバーの設定を管理していた場合、GPOでの設定は、コマンドレットでの設定を含むすべてのApp-V統合設定よりも優先されます。そのため、App-Vアプリケーションの起動に失敗する可能性があります。この問題を避けるために、すべてのGPOポリシー設定を削除し、その後SDKを使用してこれらの設定を行うことを推奨します。

どちらの管理方式でも、App-V Sequencerを使用してアプリケーションパッケージを作成します。詳しくは、Microsoft社のドキュメントを参照してください。

- シングル管理方式では、汎用名前付け規則またはサーバーメッセージブロックで共有されるネットワークの場所でパッケージを利用できるようにします。アプリケーションをデリバリーグループに追加するStudio管理者が、少なくともその場所の読み取りアクセス権限を保有していることを確認します。
- デュアル管理方式では、UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません）。

パッケージがApp-Vサーバーにあるか、ネットワーク共有上にあるかにかかわらず、Studio管理者がアクセスできるよう、そのパッケージに適切なセキュリティ権限が付与されていることを確認します。ネットワーク共有は「認証ユーザー」と共有し、デフォルトで、VDAとStudioの両方に読み取りアクセス権限が付与される必要があります。

> ## Important
>
> それらのサーバーで非デフォルトのプロパティ値を使用する場合、ControllerのPowerShellコマンドレットを使用してApp-Vサーバーのアドレスを指定することをお勧めします。詳しくは、SDKのドキュメントを参照してください。StudioでApp-Vサーバーのアドレスを変更すると、指定したサーバー接続プロパティの一部がデフォルト値にリセットされることがあります。VDAでは、これらのプロパティがApp-V公開サーバーへの接続に使用されます。この事象が発生した場合、サーバーで、リセットされたプロパティの非デフォルト値を再構成してください。

この手順は、デュアル管理方式にのみ適用されます。

デュアル管理方式では、サイトの作成中または作成後に、App-V Management serverおよび公開サーバーのアドレスを指定します。この作業は、サイトの作成中または作成後に実行できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サイトの作成中に実行する場合：

ウィザードの **[App-V]** ページで、Microsoft App-V Management serverのURLと、App-V公開サーバーのURLおよびポート番号を入力します。ウィザードを続行する前に接続をテストします。テストに失敗した場合は、下記のトラブルシューティングのセクションを参照してください。

サイトの作成後に実行する場合：

1. Studioのナビゲーションペインで、**[構成]** > **[App-V公開]** の順に選択します。
2. App-Vサーバーのアドレスをまだ指定していない場合、［操作］ペインで**[Microsoftサーバーの追加]** を選択します。
3. App-Vサーバーのアドレスを変更するには、［操作］ペインで**[Microsoftサーバーの編集]** を選択します。
4. Microsoft App-V Management serverのURLと、App-V公開サーバーのURLおよびポート番号を入力します。
5. ダイアログボックスを閉じる前に、これらのサーバーへの接続をテストします。テストに失敗した場合は、下記のトラブルシューティングのセクションを参照してください。

その後、App-V Management serverと公開サーバーへのリンクをすべて削除し、Studioでのそれらのサーバーの App-Vパッケージの検出をStudioで停止する場合は、［操作］ペインで **[Microsoftサーバーの削除]** を選択します。この操作は、それらのサーバーに置かれたパッケージのアプリケーションが、現在どのデリバリーグループでも公開されていない場合に限り実行できます。公開されている場合は、App-Vサーバーを削除する前に、そのアプリケーションをデリバリーグループから削除する必要があります。

VDAがインストールされたマシンには、App-Vをサポートするために、2セットのソフトウェアをインストールする必要があります。1セットはMicrosoft社、もう1セットはCitrixのソフトウェアです。

Microsoft App-V Client

公開サーバーから仮想アプリケーションを取得し、クライアント上のアプリケーションを公開し、Windowsデバイスにランタイムの仮想環境を自動的にセットアップおよび管理するソフトウェアです。App-V Clientには、各ユーザープロファイルのレジストリやファイルの変更など、ユーザー固有の仮想アプリケーション設定が格納されます。

App-V Clientは、Microsoft社から提供されます。App-V Clientを、VDAがインストールされた各マシン、または仮想マシンを作成するためにマシンカタログで使用されるマスターイメージにインストールします。**注**：Windows 10（1607以降）およびWindows Server 2016にはApp-V Clientが含まれます。これらのOSでのみ、PowerShellコマンドレットの**Enable-AppV**（パラメーターなし）を実行してApp-V Clientを有効にします。**Get-AppVStatus**コマンドレットは現在の有効状態を取得します。

ヒント： App-V Clientをインストールしたら、管理者権限でPowerShellの**Get-AppvClientConfiguration**コマンドレットを実行し、EnablePackageScriptsが1に設定されていることを確認します。1に設定されてない場合は、「**Set-AppvClientConfiguration -EnablePackageScripts $true**」を実行します。

Citrix App-Vコンポーネント

Citrix App-Vコンポーネントソフトウェアは、VDAのインストール時にデフォルトでインストールされ、有効化されます。

VDAのインストール時にこのデフォルトの操作を制御することもできます。グラフィカルインターフェイスの場合は、**[追加コンポーネント]** ページの **[Citrix Personalization for App-V - VDA]** チェックボックスをオフにします。コマンドラインインターフェイスの場合は、「**/exclude "Citrix Personalization for App-V - VDA"**」オプションを追加します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAのインストール中にCitrix App-Vコンポーネントのインストールを意図的に無効化し、後でApp-Vアプリケーションを使用する必要が生じた場合は、 Windowsの［プログラムと機能］の一覧で **[Citrix Virtual Delivery Agent]** を右クリックし、 **[変更]** を選択します。ウィザードが起動されます。そのウィザードで、App-V公開コンポーネントをインストールおよび有効化するオプションを有効にします。

これらの手順は、シングル管理方式にのみ適用されます。

少なくとも、App-Vパッケージが置かれたネットワーク共有への読み取りアクセスを保有している必要があります。

アプリケーションライブラリへのApp-Vパッケージの追加

1. Studioのナビゲーションペインで、 **[構成]** > **[App-V公開]** の順に選択します。
2. ［操作］ペインで **[パッケージの追加]** を選択します。
3. App-Vパッケージの置かれたネットワーク共有を検索し、1つまたは複数のパッケージを選択します。
4. **[Add]** をクリックします。

アプリケーションライブラリからのApp-Vパッケージの削除

アプリケーションライブラリからApp-Vパッケージを削除すると、Studio App-V公開ノードの表示からApp-Vパッケージが削除されます。ただし、App-Vパッケージのアプリケーションはデリバリーグループから削除されません。それらのアプリケーションは起動されたままになります。パッケージは、物理ネットワーク上に残ります（これは、App-Vアプリケーションをデリバリーグループから削除した場合とは異なります）。

1. Studioのナビゲーションペインで、 **[構成]** > **[App-V公開]** の順に選択します。
2. 削除するパッケージを1つまたは複数選択します。
3. ［操作］ペインで **[パッケージの削除]** を選択します。

App-V分離グループの追加

1. Studioのナビゲーションペインで **[App-V公開]** を選択します。
2. ［操作］ペインで **[分離グループの追加]** を選択します。
3. **[分離グループの設定の追加]** ダイアログボックスで、分離グループの名前と説明を入力します。
4. ［利用可能なパッケージ］の一覧で、分離グループに追加するアプリケーションを選択して右向き矢印をクリックします。選択したアプリケーションが［分離グループ］一覧の［パッケージ］に表示されます。各アプリケーションの横にある **[展開]** ドロップダウンで **[明示]** または **[自動]** を選択します。この一覧では、上向き矢印と下向き矢印を使用して、アプリケーションの順番を変更できます。
5. 完了したら、 **[OK]** をクリックします。

App-V分離グループの編集

1. Studioのナビゲーションペインで、 **[App-V公開]** を選択します。
2. 中央ペインで **[分離グループ]** タブを選択し、編集する分離グループを選択します。
3. ［操作］ペインで **[分離グループの編集]** を選択します。
4. **[分離グループの設定の編集]** ダイアログボックスで、分離グループの名前や説明の変更、アプリケーションの追加または削除、展開の種類の変更、アプリケーションの順番の変更を行います。
5. 完了したら、 **[OK]** をクリックします。

App-V分離グループの削除

© 1999-2017 Citrix Systems, Inc. All rights reserved.

分離グループを削除しても、アプリケーションパッケージは削除されません。グループ化のみが解除されます。

1. Studioのナビゲーションペインで、**[App-V公開]** を選択します。
2. 中央ペインで **[分離グループ]** タブを選択し、削除する分離グループを選択します。
3. ［操作］ペインで **[分離グループの削除]** を選択します。
4. 削除を確認します。

以下の手順は、App-Vアプリケーションをデリバリーグループに追加する方法を紹介するものです。デリバリーグループの作成について詳しくは、「デリバリーグループの作成」を参照してください。

手順1： 新しいデリバリーグループを作成するか、または既存のデリバリーグループにApp-Vアプリケーションを追加するかを選択します。

App-Vアプリケーションを含むデリバリーグループを作成するには、次の手順に従います。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. ［操作］ペインの **[デリバリーグループの作成]** を選択します。
3. ウィザードの後続のページで、マシンカタログとユーザーを指定します。

既存のデリバリーグループにアプリケーションを追加するには、次の手順に従います。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. ［操作］ペインの **[アプリケーションの追加]** を選択します。
3. App-Vアプリケーションを追加する1つまたは複数のデリバリーグループを選択します。

手順2： ウィザードの **[アプリケーション]** ページで、**[追加]** ドロップダウンをクリックしてアプリケーションのソースを表示します。**[App-V]** を選択します。

手順3： **[App-Vアプリケーションの追加]** ページで、App-Vのソース（App-Vサーバーまたはアプリケーションライブラリ）を選択します。アプリケーションの名前と、そのパッケージの名前とバージョンが表示されます。追加するアプリケーションの横にあるチェックボックスをオンにします。**[OK]** をクリックします。

手順4： ウィザードを完了します。

ヒント：

- App-Vアプリケーションをデリバリーグループに追加するときにApp-Vアプリケーションのプロパティを変更すると、変更はそのアプリケーションの起動時に適用されます。たとえば、アプリケーションをデリバリーグループに追加するときにアプリケーションの表示名やアイコンを変更した場合、ユーザーがそのアプリケーションを起動すると変更が反映されます。
- App-Vアプリケーションを含むデリバリーグループを後で編集した場合、デリバリーグループの配信のタイプを「デスクトップとアプリケーション」から「アプリケーションのみ」に変更しても、App-Vアプリケーションのパフォーマンスは変わりません。

トラブルシューティング

デュアル管理方式を使用した場合にのみ発生する問題は、「（デュアル）」と表示されています。

（デュアル）Studioのナビゲーションペインで **[構成]** > **[App-V公開]** を選択すると、PowerShell接続エラーが発生しま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。

- Studioの管理者はApp-Vサーバーの管理者でもありますか。Studioの管理者は、Studioと通信できるように、App-V管理サーバーの「管理者」グループに属している必要があります。

（デュアル）StudioでApp-Vサーバーのアドレスを指定するときに行う「接続テスト」に失敗します。

- App-Vサーバーの電源は入っていますか。pingコマンドを送信するかIISマネージャーを使用して、各App-Vサーバーの状態が開始済みかつ実行中であることを確認します。
- App-VサーバーのPowerShellリモート処理は有効ですか。有効でない場合は、http://technet.microsoft.com/en-us/magazine/ff700227.aspxを参照してください。
- Studioの管理者はApp-Vサーバーの管理者でもありますか。Studioの管理者は、Studioと通信できるように、App-V管理サーバーの「管理者」グループに属している必要があります。
- App-Vサーバーのファイル共有は有効ですか。Windowsエクスプローラーまたは［ファイル名を指定して実行］ダイアログボックスに、「**\\<*App-V server FQDN*>**」と入力します。
- App-Vサーバーには、App-V管理者と同じファイル共有権限が付与されていますか。App-Vサーバーで、［ユーザー名およびパスワードの保存］ダイアログボックスに「\\<*App-V Server FQDN*>」のエントリを追加して、そのApp-Vサーバーの管理者権限を持つユーザーの資格情報を指定します。詳しくは、http://support.microsoft.com/kb/306541を参照してください。
- App-VサーバーはActive Directoryに属していますか。

  StudioのマシンとApp-Vサーバーが信頼関係のない異なるActive Directoryドメインに属している場合は、StudioマシンのPowerShellコンソールで「**winrm s winrm/Config/client '@(TrustedHosts="<*App-V server FQDN*>")'**」を実行します。

  TrustedHostsがGPOで管理されている場合は、「構成設定TrustedHostsはポリシーで制御されているため変更できません。構成設定を変更するには、ポリシーを“未構成”に設定する必要があります」というエラーメッセージが表示されます。この場合は、GPOのTrustedHostsポリシー（［管理用テンプレート］>［Windowsコンポーネント］>［Windowsリモート管理（WinRM）］>［WinRMクライアント］）にApp-Vサーバーの名前を追加します。

（デュアル）App-Vアプリケーションをデリバリーグループに追加するとき、検出が失敗します。

- Studioの管理者はApp-V Management serverの管理者でもありますか。Studioの管理者は、Studioと通信できるように、App-V管理サーバーの「管理者」グループに属している必要があります。
- App-V Management serverは実行中ですか。pingコマンドを送信するかIISマネージャーを使用して、各App-Vサーバーの状態が開始済みかつ実行中であることを確認します。
- 両方のApp-VサーバーのPowerShellリモート処理は有効ですか。有効でない場合は、http://technet.microsoft.com/en-us/magazine/ff700227.aspxを参照してください。
- Studio管理者がアクセスできるように、パッケージに適切なセキュリティ権限が設定されていますか。

App-Vアプリケーションが起動しません。

- （デュアル）公開サーバーは実行中ですか。
- （デュアル）App-Vパッケージに適切なセキュリティ権限が設定されており、ユーザーがアクセスできるようになっていますか。
- （デュアル）VDAで、Tempディレクトリの参照が正しく、Tempディレクトリに十分な空き領域があることを確認してください。
- （デュアル）App-V公開サーバーで、「**Get-AppvPublishingServer ***」を実行して公開サーバーの一覧を表示します。
- （デュアル）App-V公開サーバーで、UserRefreshonLogonがFalseに設定されていることを確認します。
- （デュアル）App-V公開サーバーで、管理者として「**Set-AppvPublishingServer**」を実行し、UserRefreshonLogonを

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Falseに設定します。

- VDAに、サポート対象バージョンのApp-V Clientがインストールされていますか。VDAで、「パッケージスクリプトの有効化」設定が有効ですか。
- App-V ClientとVDAがインストールされているマシンで、レジストリエディター（regedit）からHKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppVを開きます。AppVServersキーが「+;」のフォーマット（「http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082」など）であることを確認します。
- App-V ClientとVDAがインストールされたマシンまたはマスターイメージで、PowerShell ExecutionPolicyがRemoteSignedに設定されていることを確認します。Microsoft社から提供されるApp-V Clientは署名されてないため、このExecutionPolicyで、PowerShellで無署名のローカルのスクリプトとコマンドレットを実行できるようにします。次の2つの方法のいずれかを使用して、ExecutionPolicyを設定します。（1）管理者として **Set-ExecutionPolicy RemoteSigned**コマンドレットを入力します。または、（2）グループポリシー設定で、［コンピューターの構成］>［ポリシー］>［管理用テンプレート］>［Windows コンポーネント］>［Windows PowerShell］>［スクリプトの実行を有効にする］の順に選択します。

これらの手順により問題を解決できない場合、ログを有効にして調査する必要があります。

App-Vの構成に関するログは、C:\CtxAppvLogsに生成されます。アプリケーションの起動ログは、%LOCALAPPDATA%\Citrix\CtxAppvLogsに生成されます。LOCALAPPDATAは、ログオンしたユーザーのローカルフォルダーです。アプリケーションの起動に失敗したユーザーのローカルフォルダーでログを確認する必要があります。

App-Vで使用されるStudioおよびVDAのログを有効にするには、管理者権限が必要です。メモ帳のようなテキストエディターも必要です。

Studioのログを有効にするには、次の手順に従います。

1. C:\CtxAppvLogsフォルダーを作成します。
2. C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1に移動します。テキストエディターでCtxAppvCommon.dll.configを開き、の行のコメントを解除します。
3. Broker Serviceを再起動してログの記録を開始します。

VDAのログを有効にするには、次の手順に従います。

1. C:\CtxAppvLogsフォルダーを作成します。
2. C:\Program Files\Citrix\Virtual Desktop Agentに移動します。テキストエディターでCtxAppvCommon.dll.configを開き、の行のコメントを解除します。
3. の行のコメントを解除して、値フィールドに1を設定します。
4. マシンを再起動してログの記録を開始します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDisk

Dec 05, 2017

概要

アプリケーションに加えて、アプリケーションのインストール元となるイメージも管理することは非常に困難です。CitrixのAppDisk機能により、こうした問題を解決できます。AppDiskでは、アプリケーションとアプリケーションのグループはオペレーティングシステムから分離されるため、アプリケーションを個別に管理できます。

個々のユーザーグループ向けに設計されたアプリケーションを含むさまざまなAppDiskを作成し、任意のマスターイメージ上で組み立てることができます。このようにアプリケーションをグループ化して管理することで、アプリケーションをより詳細に管理できるようになり、保守するマスターイメージの数が削減されます。これにより、IT管理が簡素化されるとともに、ユーザーのニーズにより迅速に対応できるようになります。AppDiskに含まれるアプリケーションは、デリバリーグループ経由で提供します。

自身の環境でCitrix AppDNAも使用している場合、AppDiskの機能をAppDNAと統合すると、XenAppとXenDesktopではAppDiskごとにアプリケーションの自動分析を実行できるようになります。AppDNAを使用することで、AppDiskの機能を最大限に活用できます。AppDNAを使用しない場合は、アプリケーション互換性のテストと報告は行われません。

AppDiskは、隔離と変更管理という2つの面において、ほかのアプリケーションプロビジョニングテクノロジとは異なります。

- Microsoft App-Vでは、互換性のないアプリケーションどうしを隔離することで、共存できるようにします。AppDiskの機能では、アプリケーションどうしは隔離されません。アプリケーション（および関連ファイルとレジストリキー）は、OSから分離されます。OSとユーザーには、AppDiskはマスターイメージに直接インストールされているかのように見え、そのように動作します。
- 変更管理（マスターイメージを更新し、その更新がインストール済みのアプリケーションと互換性があるかどうかをテストすること）には、非常にコストがかかる可能性があります。AppDNAレポートは、問題の特定と修復手順の提案に役立ちます。たとえば、AppDNAでは、.NETなど共通の依存関係を持つアプリケーションを特定できるため、そのようなアプリケーションを1つの共通基本イメージにインストールできます。また、OS起動シーケンスで早期にロードされるアプリケーションも特定できるため、アプリケーションが予想通りに動作することを保証できます。

ヒント：

- イメージの更新後、一部のアプリケーションが、以前にインストールされたライセンスを検証する機能が原因で、正しく機能しない場合があります。たとえば、イメージアップグレード後にMicrosoft Officeを起動すると、以下のようなエラーメッセージが表示される場合があります。

「Microsoft Office Professional Plus 2010ではこのアプリケーションのライセンスを確認できませんでした。修復できなかったか、ユーザーによって中止されました。アプリケーションがシャットダウンしません。」

この問題を解決するには、基本イメージ上でMicrosoft Officeをアンインストールし、新しいバージョンをインストールします。

- Windowsストアから公開カタログの仮想マシンにMetroアプリをダウンロードすると、時間がたってから失敗することがあります。
- すべてのMicrosoft Officeコンポーネントを常に同じAppDiskに配置することをお勧めします。たとえば、あるAppDiskにMicrosoft OfficeとProjectを、別のAppDiskにはMicrosoft Office、Project、およびVisioを配置するなどです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 一部のシステムで、イメージを更新するときにSCCMがクラッシュします。このシナリオは、基本イメージが更新、適用されるときに発生し、SCCMクライアントの障害を招きます。この問題を解決するには、先に基本イメージにSCCMクライアントインスタンスをインストールします。
- AppDisk上でインストールされたアプリケーションが、デリバリーグループに割り当てられて、ユーザーの仮想マシンを割り当てられた後、Windowsの［スタート］メニューに表示されない場合があります。詳しくは、「スタートメニューにアプリケーションを表示する方法」を参照してください。
- ユーザーは、アプリケーションとOSの分離や、AppDiskによって提供されるほかの機能を意識することはありません。アプリケーションは、イメージにインストールされているかのように動作します。 AppDiskに複雑なアプリケーションが含まれる場合、デスクトップの起動がわずかに遅れる場合があります。
- AppDiskは、ホストされる共有およびプールデスクトップとともにのみ使用できます。
- AppDiskは、ホストされる共有デスクトップとともに使用できます。
- 複数のマスターイメージやOSプラットフォームで（アプリケーションごとに）AppDiskを共有することもできますが、この方法はすべてのアプリケーションで機能するわけではありません。デスクトップOSのインストールスクリプトが搭載されたアプリケーションが複数あり、そのデスクトップOSにより、それらのアプリケーションが1つのサーバーOSで機能できない場合、この2つのOS向けにアプリケーションを別々にパッケージ化することが推奨されます。
- 多くの場合、AppDiskは複数のOSで機能します。たとえば、Windows 7の仮想マシンで作成されたAppDiskを、Windows 2008 R2マシンを含むデリバリーグループに追加する操作は、どちらのOSも同じビット数（32ビットまたは64ビット）であり、アプリケーションがどちらのOSでもサポートされる限りは可能です。ただし、新しいOSのバージョン（Windows 10など）で作成されたAppDiskを、古いOSバージョン（Windows 7など）を実行するマシンを含むデリバリーグループに追加することは、正常に機能しない場合もあるため、推奨されません。
- デリバリーグループのユーザーのサブセットのみがAppDiskのアプリケーションにアクセスできるようにする必要がある場合、グループポリシーを使用して、AppDiskのアプリケーションをほかのユーザーから見えないようにすることが推奨されます。非表示にしたアプリケーションの実行可能ファイルは使用できる状態のままですが、ほかのユーザーは実行できません。
- Windows 7 OSが稼働するロシア語および中国語の環境では、再起動ダイアログが自動的に消えません。そのような場合、提供されたデスクトップにログオンすると、再起動ダイアログが表示されてから、すぐに消えます。
- **Upload-PvDDiags**スクリプトツールを使用している場合、ユーザーのドライブ指定が「P」に設定されていないと、PVDユーザーレイヤーに関連するログ情報が欠落します。
- バスク語を表示する環境では、Windows 7 OSで、再起動プロンプト画面に言語が適切に表示されない場合があります。言語をバスク語に設定している場合には、フランス語かスペイン語が親言語としてインストールされていることを確認した後、バスク語をインストールし、それを現在の言語に設定してください。
- コンピューターをシャットダウンすると、PVDディスクが読み取り専用モードに設定されていても、PVDは通知ポップアップを更新します。
- インプレースアップグレード中でもレジストリファイル（DaFsFilter）を削除できますが、それによりアップグレードは失敗します。

> **ヒント**
>
> AppDiskを作成するには、OSのみがインストールされた（つまり、他のアプリをインストールしていない）仮想マシンを使用します。AppDiskの作成前に、OSのすべての更新を実行する必要があります。

展開の概要

次の一覧は、AppDiskの展開手順をまとめたものです。詳しくは、この文書の後半部分を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. ハイパーバイザー管理コンソールから、仮想マシンにVirtual Delivery Agent（VDA）をインストールします。
2. AppDiskを作成します。この作業には、ハイパーバイザー管理コンソールとStudioから実行する手順が含まれます。
3. ハイパーバイザー管理コンソールから、アプリケーションをAppDiskにインストールします
4. （ハイパーバイザー管理コンソールまたはStudioで）AppDiskを封印します。封印により、XenAppおよびXenDesktopで、AppDiskのアプリケーションと関連ファイルをアプリケーションライブラリ（AppLibrary）に記録できるようになります。
5. Studioにおいて、デリバリーグループを作成または編集し、そのデリバリーグループに含めるAppDiskを選択します。この手順はAppDiskの*割り当てと呼ばれます*（ただし、Studioでは**[AppDiskの管理]**を使用します）。デリバリーグループの仮想マシンの起動時に、XenAppおよびXenDesktopは、AppLibraryと連携し、Creation Services（MCS）またはProvisioning Services（PVS）、およびDelivery Controllerで動作して、AppDiskが構成された後でブートデバイスをストリーム配信します。

要件

AppDiskの使用には、「システム要件」に記載された要件のほかにもいくつかの要件があります。

AppDiskの機能がサポートされるのは、（最低でも）XenAppおよびXenDesktop 7.8のダウンロードファイルで提供されるバージョンのDelivery ControllerとStudioが動作する環境のみです。これには、インストーラーが自動的に展開する前提条件（.NET 4.5.2など）も含まれます。

AppDiskは、VDAでサポートされる同じバージョンのWindows OS上で作成できます。AppDiskを使用するデリバリーグループ用に選択されたマシンには、最低でもVDA 7.8がインストールされている必要があります。

> すべてのマシンに最新のVDAバージョンをインストールするか、またはすべてのマシンにおいてVDAを最新バージョンにアップグレードしてから、必要に応じてマシンカタログおよびデリバリーグループをアップグレードすることをお勧めします。デリバリーグループの作成時に、異なるVDAバージョンがインストールされたマシンを選択した場合、デリバリーグループは最も古いバージョンと互換性を持ちます（これは、グループの*機能レベル*と呼ばれます）。機能レベルについて詳しくは、「デリバリーグループの作成」を参照してください。

AppDiskの作成に使用される仮想マシンをプロビジョニングするには、以下を使用できます。

- 7.8 Controller以上で提供されるMCS。
- 使用中のXenAppおよびXenDesktopのバージョンのダウンロードページで提供されるPVSのバージョン。
- サポートされるハイパーバイザー：
  - XenServer
  - VMware（バージョン5.1以上）
  - Microsoft System Center Virtual Machine Manager

AppDiskは、XenAppおよびXenDesktop用にサポートされるほかのホストハイパーバイザーやクラウドサービスとともに使用することはできません。

一時データのキャッシュを使用するMCSカタログのマシンでは、AppDiskの作成はサポートされません。

> **注意**
>
> 書き込みキャッシュを使用して、AppDiskをMCSプロビジョニングマシンに接続できますが、AppDiskの作成には使用できません。

リモートPCアクセスカタログでは、AppDiskはサポートされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDiskを作成する仮想マシンで、Windowsボリュームシャドウサービスが有効である必要があります。このサービスは、テフォルトで有効になっています。

AppDiskで使用されるデリバリーグループには、サーバーOSまたはデスクトップOSマシンがインストールされたプール（ランダム）マシンカタログのマシンを含めることができます。AppDiskを、プール（静的）または専用（割り当て済み）など、ほかのカタログタイプのマシンとともに使用することはできません。

Studioがインストールされているマシンには、（インストール済みのほかの.NETのバージョンに加えて）.NET Framework 3.がインストールされている必要があります。

AppDiskはストレージに影響を及ぼす可能性があります。詳しくは、「ストレージおよびパフォーマンスの考慮事項」を参照してください。

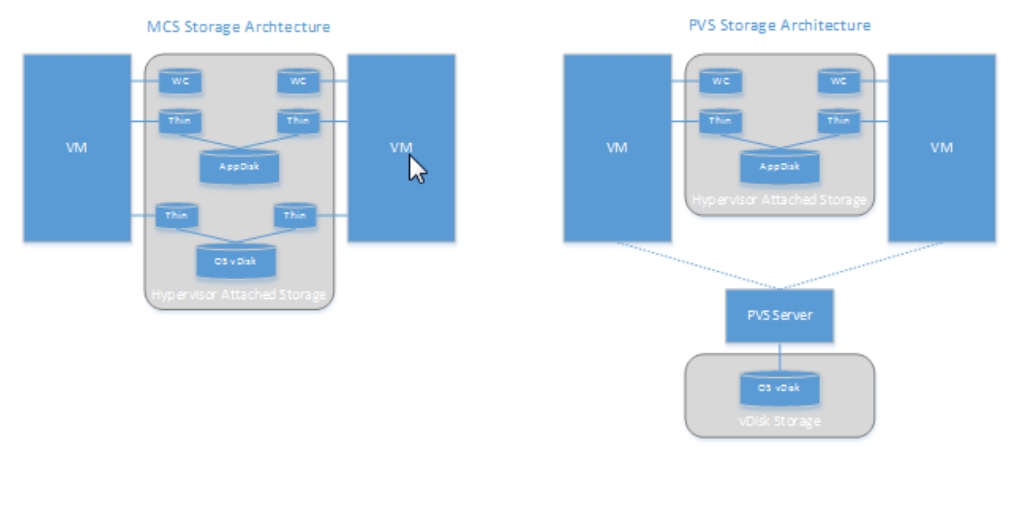
AppDNAを使用するには、以下の手順に従います。

- AppDNAのドキュメントとAppDiskのFAQを確認します。
- AppDNAソフトウェアは、Controllerとは別のサーバーにインストールする必要があります。このXenAppおよびXenDesktopのリリースで提供されるAppDNAのバージョンを使用します。AppDNAのほかの要件について詳しくは、AppDNAのドキュメントを参照してください。
- AppDNAサーバーで、デフォルトポート8199にファイアウォールの例外規則があることを確認します。
- AppDiskの作成中、AppDNA接続を無効にしないでください。
- XenAppまたはXenDesktopサイトを作成する場合、サイト作成ウィザードの **[追加機能]** ページで、AppDNAとの互換性分析を有効にできます。この機能は、Studioのナビゲーションペインの **[構成]** > **[AppDNA]** を選択することで、後で有効または無効にできます。
- Studioの［問題レポートの表示］リンクをクリックするとAppDNAレポートが表示されます。ただし、AppDNAがデフォルトで使用するOSの組み合わせは、デスクトップデリバリーグループ向けWindow 7（64ビット）とサーバーデリバリーグループ向けWindows Server 2012 R2です。デリバリーグループが異なるバーションのWindowsで構成されている場合、Studioが表示するレポートのデフォルトのイメージの組み合わせが正しくありません。この問題を回避するには、Studioがソリューションを作成した後で、AppDNAでそのソリューションを手動で編集します。
- StudioとAppDNAサーバーのバージョンには依存関係があります。
  - バージョン7.12からは、StudioのバージョンはAppDNAサーバーと同じかそれ以降である必要があります。
  - バージョン7.9と7.11では、StudioとAppDNAサーバーのバージョンは一致する必要があります。
  - 次の表は、どのバージョンが連携して動作するかの概要を示しています（はい＝連係して動作する、 - ＝連係して動作しない）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Product Version	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	はい	-	-	-	-	-
AppDNA 7.11	-	はい	-	-	-	-
AppDNA 7.12	-	-	はい	はい	はい	はい
AppDNA 7.13	-	-	はい	はい	はい	はい
AppDNA 7.14	-	-	-	-	はい	はい
AppDNA 7.15	-	-	-	-	-	はい

2つのディスクを使用してアプリケーションとOSを分離し、それらのディスクを別の場所に保存すると、ストレージ戦略に影響が出る可能性があります。次の図は、MCSおよびPVSのストレージアーキテクチャを表しています。「WC」は書き込みキャッシュを、「Thin」は仮想マシンのAppDiskとOSの仮想ディスクとの差分を保存するために使用されるシンディスクを表します。



MCS環境：

引き続き社内の既存のサイジングガイドラインを使用して、AppDiskとOSの仮想ディスク（vDisk）のサイズを調整できます。AppDiskを複数のデリバリーグループで共有すると、全体的なストレージ容量が減少する可能性があります。

OS vDiskとAppDiskは同じストレージ領域に置かれるため、AppDiskを展開するときに容量にマイナスの影響を与えないように、ストレージ容量の要件を慎重に計画してください。AppDiskはオーバーヘッドを引き起こすため、ストレージはそのオーバーヘッドとアプリケーションに対処できるようにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

OS vDiskとAppDiskは同じストレージ領域に存在するため、IOPSに対する最終的な影響はありません。MCSを使用する場合、書き込みキャッシュに関する考慮事項はありません。

PVS環境：

アプリケーションをAppDiskストレージからハイパーバイザーが接続されたストレージに移行するので、容量の増加とIOPSについて考慮する必要があります。

PVSでは、OS vDiskとAppDiskは異なるストレージ領域を使用します。OS vDiskストレージの容量は減少しますが、ハイパーバイザーが接続されたストレージの容量は増加します。 そのため、これらの変更に対処するようにPVS環境をサイジングする必要があります。

ハイパーバイザーが接続されたストレージのAppDiskでは、より高いIOPSが必要ですが、OS vDiskのAppDiskでは、より低いIOPSが必要です。

書き込みキャッシュ：PVSはNTFS形式のドライブにある動的VHDXファイルを使用します。書き込みキャッシュにブロックが書き込まれると、VHDXファイルは動的に拡張されます。 AppDiskは、関連する仮想マシンに接続されるとOS vDiskとマージされるので、ファイルシステムを統合的に確認できるようになります。通常、このマージにより、さらなるデータが書き込みキャッシュに書き込まれるため、書き込みキャッシュファイルのサイズが増加します。容量の計画において、これを考慮する必要があります。

MCS環境とPVS環境のいずれにおいても、作成したAppDiskを活用するためにOS vDiskのサイズを減らすようにしてください。減少させない場合は、より多くのストレージを使用することを計画します。

サイトの多くのユーザーが同時にコンピューターの電源をオンにすると（業務開始時間などに）、複数の起動リクエストによってハイパーバイザーに負荷がかかるため、パフォーマンスに影響が及ぶ場合があります。PVSでは、アプリケーションはOS vDiskにはないため、PVSサーバーに送信されるリクエストは少なくなります。その結果、各ターゲットデバイスの負荷は軽くなり、PVSサーバーはより多くのターゲットデバイスにストリーミングできます。ただし、ターゲットサーバーの密度が増加したことで、ブートストームのパフォーマンスにマイナスの影響が及ぶ可能性があることに注意してください。

AppDiskの作成

AppDiskを作成し、アプリケーションをインストールし、封印するには、次の2通りの方法があります。どちらの方法にも、ハイパーバイザー管理コンソールとStudioから実行する手順が含まれます。これらの方法は、大半の手順をどこで完了するかが異なります。

使用する方法にかかわらず、以下の点に注意してください。

- AppDiskの作成には30分かかります。
- AppDNAを使用する場合、上記の「要件」セクションのガイドラインに従います。AppDiskの作成中、AppDNA接続を無効にしないでください。
- AppDiskにアプリケーションを追加する場合、必ずすべてのユーザーにアプリケーションをインストールします。キーマネージメントサーバー（KMS）ライセンス認証を使用するアプリケーションをリセットします。詳しくは、アプリケーションのドキュメントを参照してください。
- AppDiskの作成中にユーザー固有の場所に作成されたファイル、フォルダー、およびレジストリエントリは、保持されません。また、一部のアプリケーションでは、アプリケーションを初めて使用するときに表示されるウィザードがインストール中に開き、ユーザーデータが作成されます。Profile managementソリューションを使用してこのデータを保存し、AppDiskが起動されるごとにこのウィザードが開くことがないようにします。
- AppDNAを使用している場合は、作成プロセスの終了後、自動的に分析が開始されます。この間、StudioでのAppDiskのス

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

テータスは「分析中」となります。

Provisioning Servicesによって作成されたマシンカタログのマシン上のAppDiskでは、AppDiskの作成中にさらなる構成が必要となります。Provisioning Servicesコンソールで次の操作を行います。

1. 仮想マシンを含むデバイスコレクションに関連する新しいバージョンのvDiskを作成します。
2. 仮想マシンをメンテナンスモードにします。
3. AppDiskの作成中、仮想マシンが再起動されるたびに、ブート画面でメンテナンスバージョンを選択します。
4. AppDiskの封印後は、仮想マシンを実稼働モードに戻し、作成したvDiskバージョンを削除します。

この手順には、AppDiskを作成し、AppDiskにアプリケーションを作成し、AppDiskを封印するという3つのタスクが含まれます。

AppDiskの作成：

1. Studioのナビゲーションペインで **[AppDisk]** を選択し、次に［操作］ペインで **[AppDiskの作成]** を選択します。
2. ウィザードの **[はじめに]** ページに表示される情報を確認し、 **[次へ]** をクリックします。
3. **[AppDiskの作成]** ページで、 **[新しいAppDiskの作成]** をクリックします。定義済みのディスクサイズ（小、中、大）を選択するか、ディスクサイズをギガバイトで指定します。指定できる最小サイズは3GBです。追加するアプリケーションを保存するのに十分なディスクサイズを指定する必要があります。 **[Next]** をクリックします。
4. **[準備用マシン]** ページで、AppDiskが構築されるマスターイメージとして使用するランダムプールカタログを選択します。注：サイトのすべてのマシンカタログが種類ごとに一覧表示されますが、選択できるのは使用可能なマシンを少なくとも1つ含むカタログのみです。 ランダムプール仮想マシンを含まないカタログを選択した場合、AppDiskの作成は失敗します。ランダムプールカタログから仮想マシンを選択したら、 **[次へ]** をクリックします。
5. **[概要]** ページで、AppDiskの名前と説明を入力します。 ウィザードの前のページで指定した情報を確認します。 Click **Finish**.

注意：PVSを使用している場合は、上述の「PVSに関する注意事項」セクションのガイドラインに従います。

ウィザードが閉じると、新しいAppDiskに対するStudioの表示は「作成中」となります。AppDiskが作成されると、表示は「アプリケーションのインストールの準備完了」に変わります。

AppDiskへのアプリケーションのインストール：

ハイパーバイザー管理コンソールから、アプリケーションをAppDiskにインストールします **ヒント：** 仮想マシン名を忘れた場合、Studioのナビゲーションペインで **[AppDisk]** を選択し、次に［操作］ペインで **[アプリケーションのインストール]** を選択すると仮想マシン名が表示されます）。 アプリケーションのインストールについて詳しくは、ハイパーバイザーのドキュメントを参照してください（**そのほかの注意事項：** ハイパーバイザー管理コンソールからアプリケーションをAppDiskにインストールする必要があります。Studioの［操作］ペインの［アプリケーションのインストール］タスクは使用しないでください）。

アプリケーションの封印：

1. Studioのナビゲーションペインで **[AppDisk]** を選択します。
2. 作成したAppDiskを選択し、次に［操作］ペインの **[AppDiskの封印]** を選択します。

AppDiskを作成したら、AppDiskにアプリケーションをインストールし、次にAppDiskを封印して、AppDiskをデリバリーグループに割り当てます。

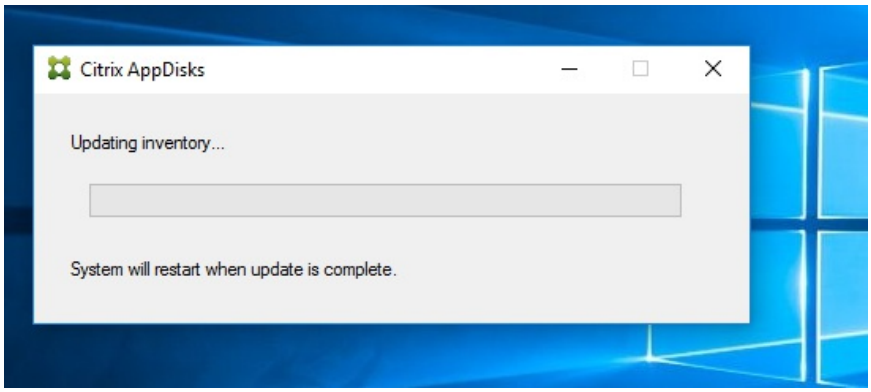
© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDiskの準備と封印の取り消し

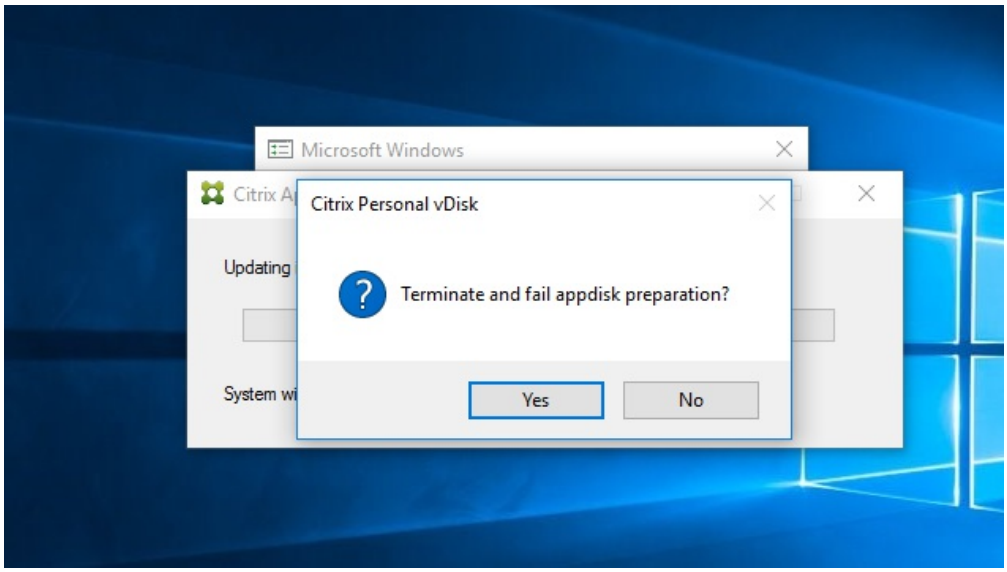
管理者によるAppDiskの作成や封印の取り消しが必要な場合があります。

1. VMにアクセスします。

2. ダイアログを閉じます。



3. ダイアログを閉じると、ポップアップメッセージが表示され、選択した操作の取り消しの確認を求められますので、**[はい]** をクリックします。



注意

AppDiskの準備を取り消した場合、マシンを再起動すると初期状態に戻ります。再起動しない場合は、新しいVMを作成する必要があります。

この手順では、ハイパーバイザー管理コンソールからAppDiskの作成と準備タスクを完了してから、AppDiskをStudioにインポートします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ハイパーバイザーでの準備、アプリケーションのインストール、およびAppDiskの封印：

1. ハイパーバイザー管理コンソールから、仮想マシンを作成し、VDAをインストールします。
2. マシンの電源を切り、マシンのスナップショットを作成します。
3. スナップショットから新しいマシンを作成し、そのマシンに新しいディスクを追加します。このディスク（このディスクがAppDiskになります）には、これからインストールするアプリケーションを保存できる十分な容量が必要です。
4. マシンを起動し、**[スタート]** > **[AppDiskの準備]** の順に選択します。この［スタート］メニューのショートカットがハイパーバイザーで使用できない場合、コマンドプロンプトを開いてC:\Program Files\Citrix\personal vDisk\binに移動し、**CtxPvD.Exe –s LayerCreationBegin**と入力します。 マシンが再起動され、ディスクが準備されます。数分後に、ディスクの準備が完了し、2度目の再起動が行われます。
5. ユーザーに使用できるようにするアプリケーションをインストールします。
6. マシンのデスクトップで、 **[AppDiskのパッケージング]** ショートカットをダブルクリックします。マシンが再び再起動され、封印プロセスが開始されます。「進行中」のダイアログボックスが閉じたら、仮想マシンの電源をオフにします。

ハイパーバイザーで作成したAppDiskのStudioへのインポート：

1. Studioのナビゲーションペインで **[AppDisk]** を選択し、次に［操作］ペインで **[AppDiskの作成]** を選択します。
2. **[はじめに]** ページに表示される情報を確認し、 **[次へ]** をクリックします。
3. **[AppDiskの作成]** ページで、 **[既存のAppDiskのインポート]** をクリックします。作成したAppDiskがあるハイパーバイザーのリソース（ネットワークとストレージ）を選択します。 **[Next]** をクリックします。
4. **[準備用マシン]** ページでマシンを参照し、ディスクを選択して **[次へ]** をクリックします。
5. **[概要]** ページで、AppDiskの名前と説明を入力します。 ウィザードの前のページで指定した情報を確認します。 Click **Finish**. StudioにAppDiskがインポートされます。

StudioにAppDiskがインポートされたら、AppDiskをデリバリーグループに割り当てます。

デリバリーグループへのAppDiskの割り当て

デリバリーグループの作成時または作成後に、1つまたは複数のAppDiskをデリバリーグループに割り当てることができます。指定するAppDiskの情報は、基本的に同じです。

作成中のデリバリーグループにAppDiskを追加する場合、デリバリーグループの作成ウィザードの**[AppDisk]** ページに示される以下のガイドラインに従います（デリバリーグループの作成ウィザードのほかのページについて詳しくは、「デリバリーグループの作成」を参照してください）。

既存のデリバリーグループにAppDiskを追加する、または既存のデリバリーグループからAppDiskを削除するには、以下を実行します。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. デリバリーグループを選択して、［操作］ペインの **[AppDiskの管理]** を選択します。 **[AppDisk]** ページの以下のガイドラインを確認します。
3. デリバリーグループのAppDiskの構成を変更する場合は、グループのマシンを再起動する必要があります。**[ロールアウト方法]** ページで、「再起動スケジュールの作成」のガイドラインに従います。

[AppDisk] ページ：

（デリバリーグループの作成ウィザード、またはAppDiskの管理フローの）**[AppDisk]** ページには、デリバリーグループに既に展開されているAppDiskとその優先順位が一覧表示されます（デリバリーグループを作成中の場合は、一覧には何も表示されません）。詳しくは、「AppDiskの優先順位」セクションを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. **[Add]** をクリックします。［AppDiskの選択］ダイアログボックスでは、左側の列にすべてのAppDiskが一覧表示されます。既にこのデリバリーグループに割り当てられているAppDiskのチェックボックスはオンになっており、選択することはできません。
2. 左側の列で、選択可能なAppDiskのチェックボックスを1つまたは複数オンにします。右側の列にAppDiskのアプリケーションが一覧表示されます（右側の列の上部の **[アプリケーション]** タブを選択すると、［スタート］メニューに似た形式でアプリケーションが表示され、 **[インストール済みのパッケージ]** タブを選択すると、［プログラムと機能］に似た形式でアプリケーションが表示されます）。
3. 選択可能なAppDiskを1つまたは複数選択し、 **[OK]** をクリックします。
4. ［AppDisk］ページで **[次へ]** をクリックします。

デリバリーグループに複数のAppDiskが割り当てられている場合、**[AppDisk]** ページ（［デリバリーグループの作成］、［デリバリーグループの編集］、および［AppDiskの管理］から開きます）では、優先順位が高い順にAppDiskが表示されます。一番上に表示されているAppDiskが、最も優先順位の高いAppDiskです。優先順位は、AppDiskが処理される順序を表します。

一覧の隣にある上下の矢印を使用して、AppDiskの優先順位を変更できます。AppDNAがAppDiskの環境と統合されている場合、AppDiskがデリバリーグループに割り当てられたときに、アプリケーションは自動的に分析されて優先順位が設定されます。後でAppDiskをデリバリーグループに追加する、またはデリバリーグループから削除する場合、 **[自動順序付け]** をクリックすると、AppDNAでは現在のAppDiskの一覧が再分析され、優先順位が決定されます。分析（および必要な場合は優先順位の再順序付け）には、数秒かかる場合があります。

AppDisksの管理

AppDiskを作成し、デリバリーグループに割り当てたら、Studioのナビゲーションペインの［AppDisk］ノードから、AppDiskの優先順位を変更できます。AppDiskのアプリケーションの変更は、ハイパーバイザー管理コンソールから行う必要があります。

> ## Important
>
> Windows Updateサービスを使用して、AppDiskのアプリケーション（Officeスイートなど）を更新できます。ただし、Windows Updateサービスを使用して、オペレーティングシステムの更新プログラムをAppDiskに適用しないでください。オペレーティングシステムの更新プログラムは、AppDiskではなく、マスターイメージに適用します。AppDiskに適用した場合、AppDiskは正しく初期化されません。
>
> - パッチやほかの更新プログラムをAppDiskのアプリケーションに適用する場合、アプリケーションに必要なものだけを適用します。ほかのアプリケーションの更新プログラムは適用しないでください。
> - Windowsの更新プログラムをインストールするには、まずすべてのエントリの選択を解除し、次に更新対象のAppDiskのアプリケーションに必要なサブセットを選択します。

AppDisk作成のウイルス対策に関する考慮事項

場合によっては、ベース仮想マシンにウイルス対策（A/V）エージェントがインストールされているシナリオで、AppDiskの作成時に問題が発生する場合があります。そのような場合、A/Vエージェントがいくつかのプロセスにフラグを立てると

© 1999-2017 Citrix Systems, Inc. All rights reserved.

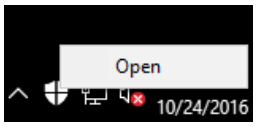
AppDisk作成が失敗する場合があります。これらのプロセス、**CtxPvD.exe**および**CtxPvDSrv.exe**は、ベース仮想マシンによって使用されるA/Vエージェントの例外一覧に追加する必要があります。

このセクションでは、次のウイルス対策アプリケーションでの例外の追加について説明します。

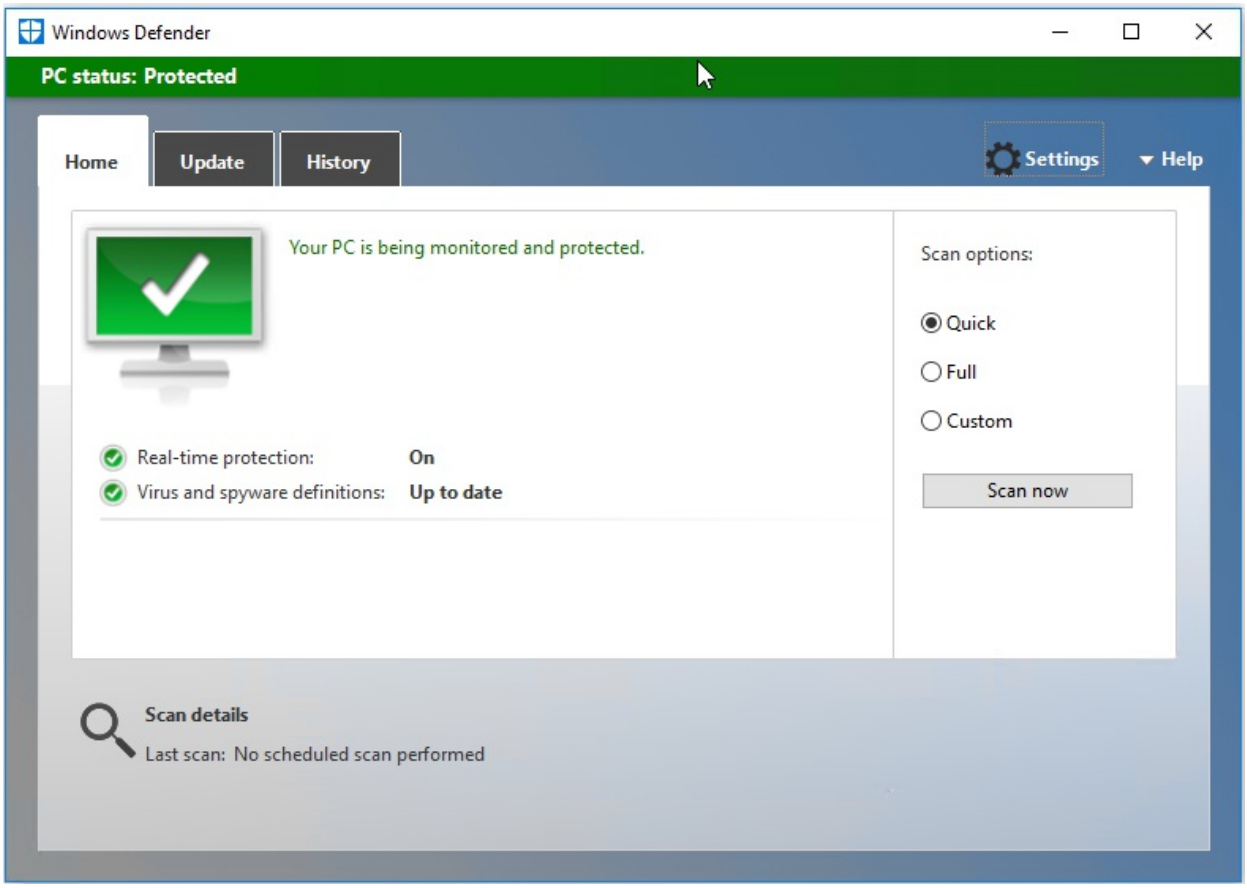
- Windows Defender（Windows 10用）
- OfficeScan（バージョン11.0）
- Symantec（バージョン12.1.16）
- McAfee（バージョン4.8）

ベース仮想マシンがWindows Defender（バージョン10）を使用している場合：

1. ローカル管理者権限でコンピューターにログオンします。
2. Windows Defenderのアイコンを選択して右クリックし、**[開く]**ボタンを表示します。

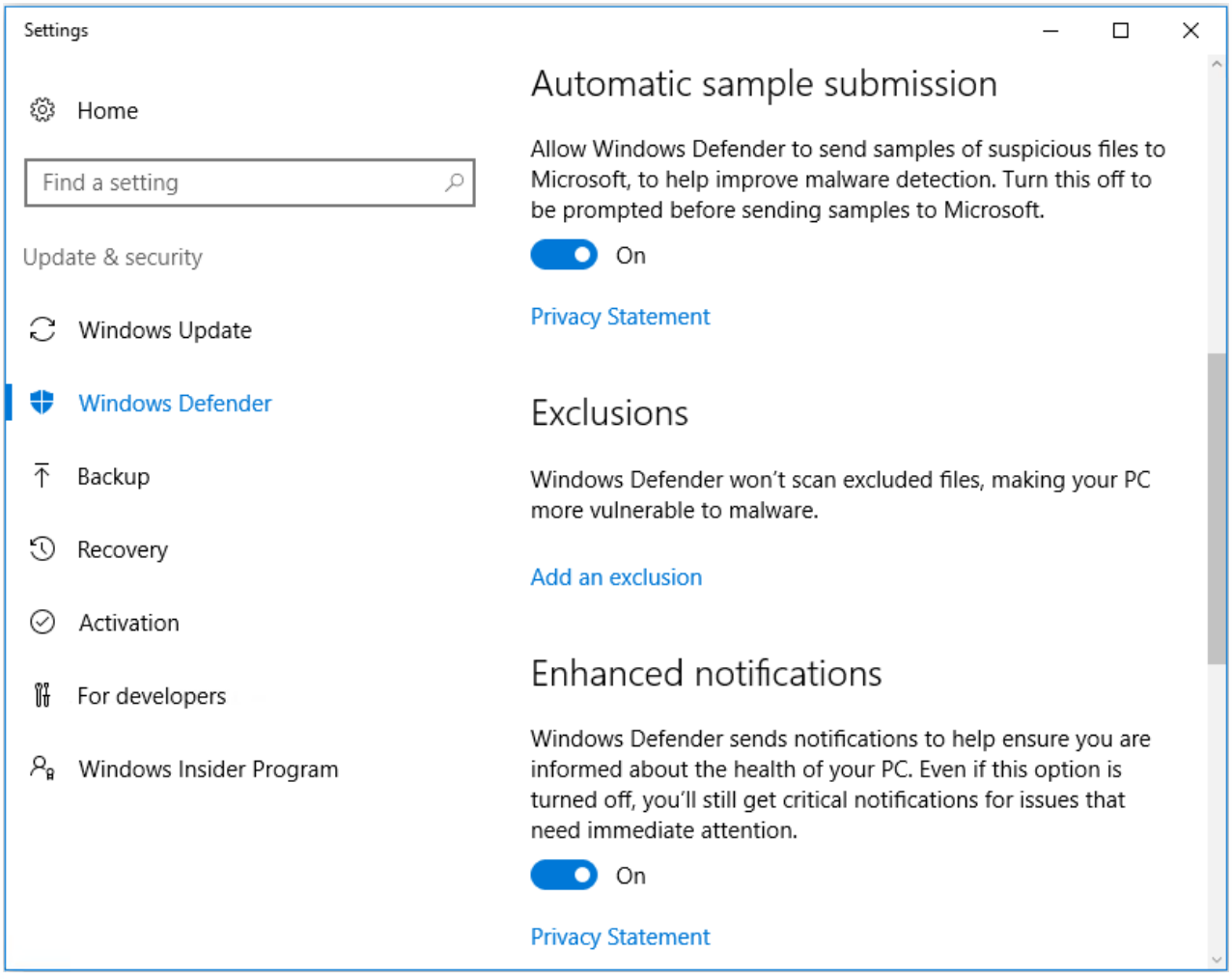


3. Windows Defenderコンソールで、インターフェイスの右上部分の**[設定]**を選択します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

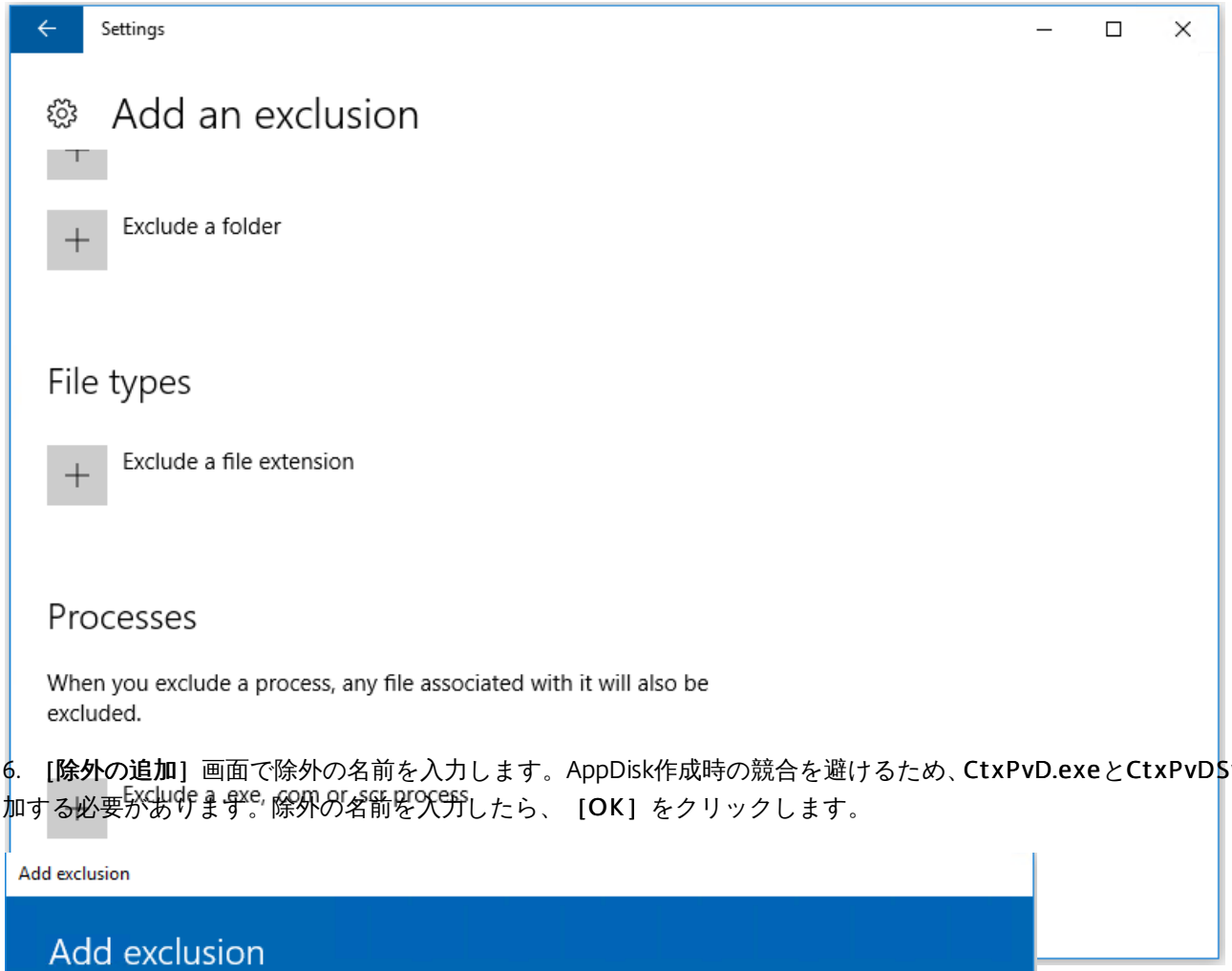
4. ［設定］画面の **[除外]** 部分で、 **[除外の追加]** をクリックします。



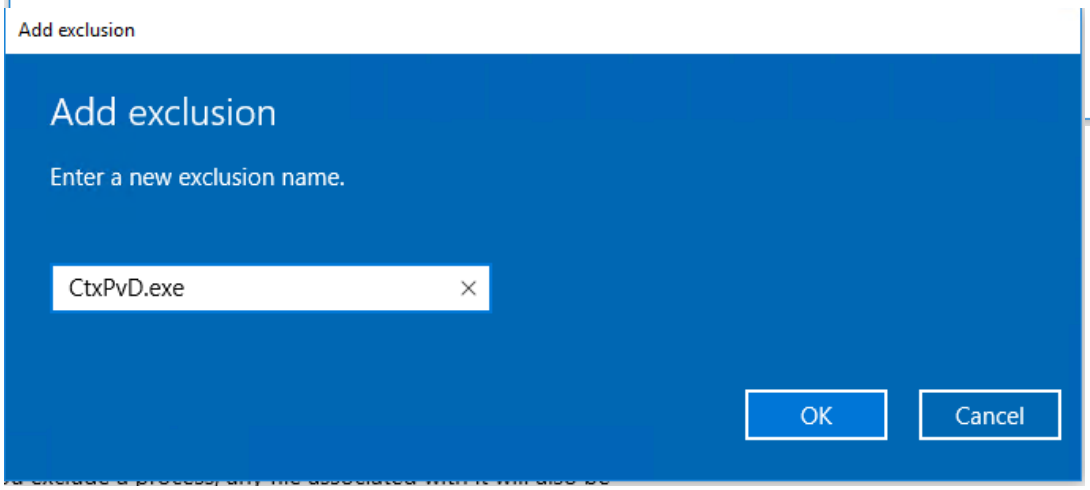
© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. **[除外の追加]** 画面で、 **[.exe、.com、または .scr プロセスを除外します]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

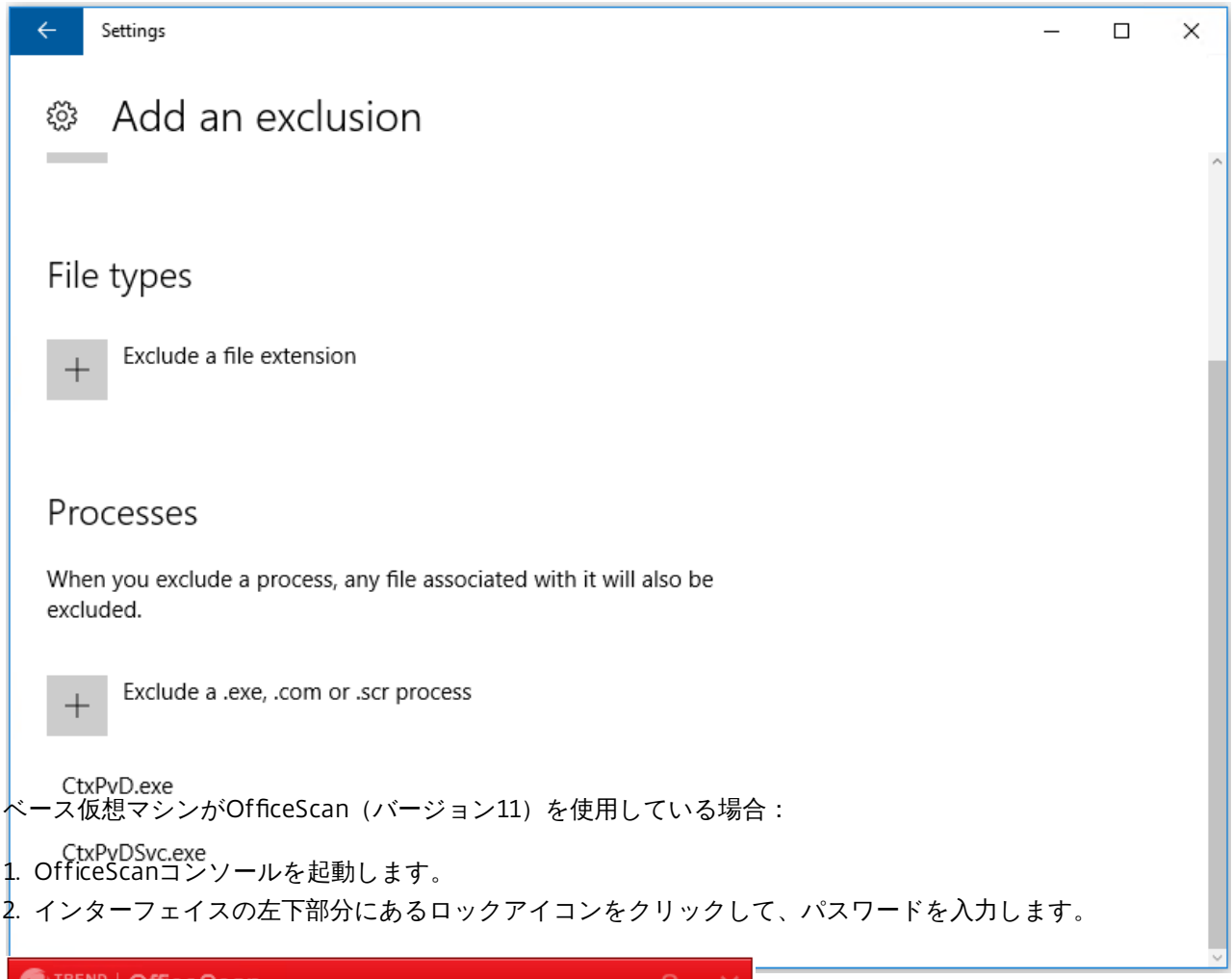


6. **[除外の追加]** 画面で除外の名前を入力します。AppDisk作成時の競合を避けるため、**CtxPvD.exe**と**CtxPvDSvc.exe**を追加する必要があります。除外の名前を入力したら、 **[OK]** をクリックします。



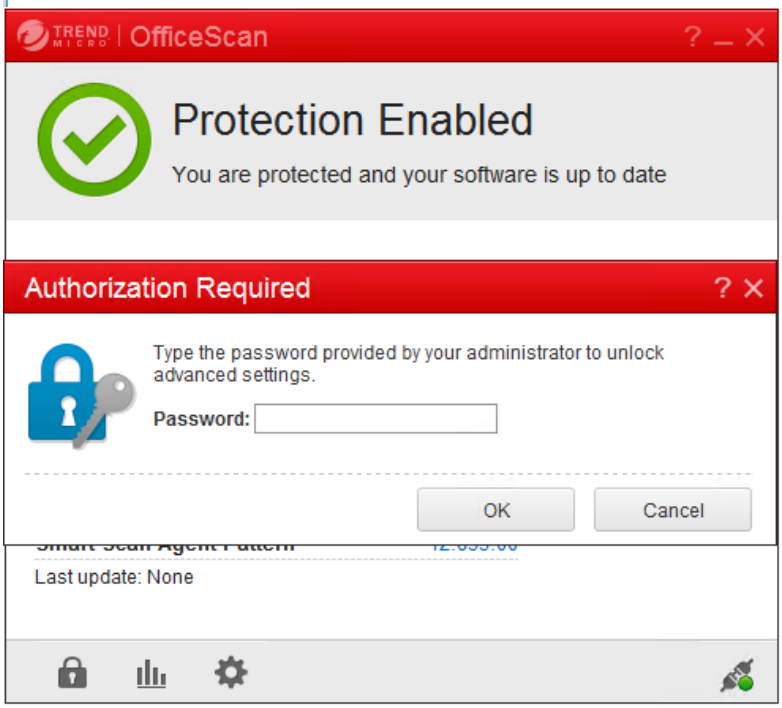
除外を追加すると、それらは **[設定]** 画面の除外されたプロセスの一覧に表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



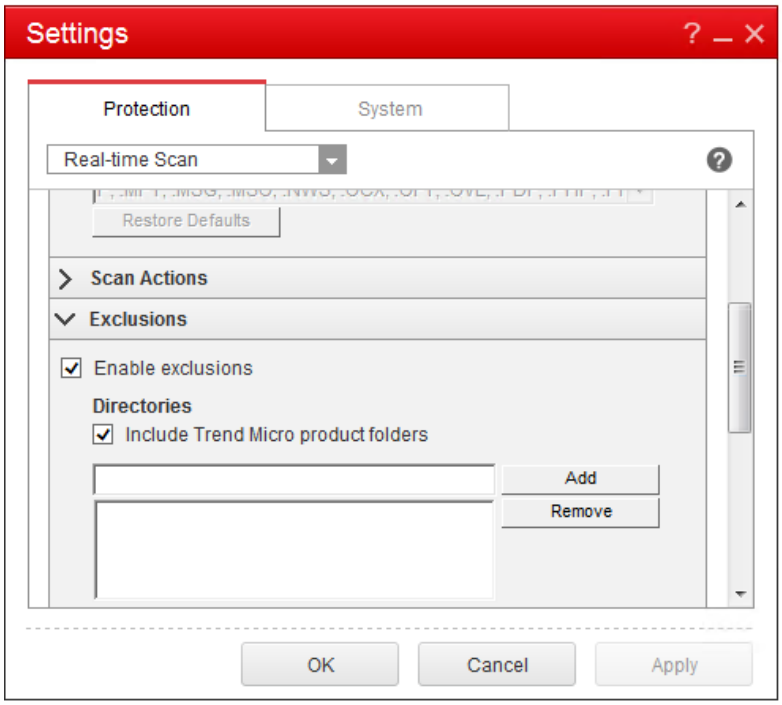
ベース仮想マシンがOfficeScan（バージョン11）を使用している場合：

1. OfficeScanコンソールを起動します。
2. インターフェイスの左下部分にあるロックアイコンをクリックして、パスワードを入力します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. **[設定]** アイコンをクリックして、構成オプションを表示します。
4. ［設定］画面で、 **[保護]** タブを選択します。
5. ［保護］タブで、 **[除外]** セクションが見つかるまでスクロールダウンします。

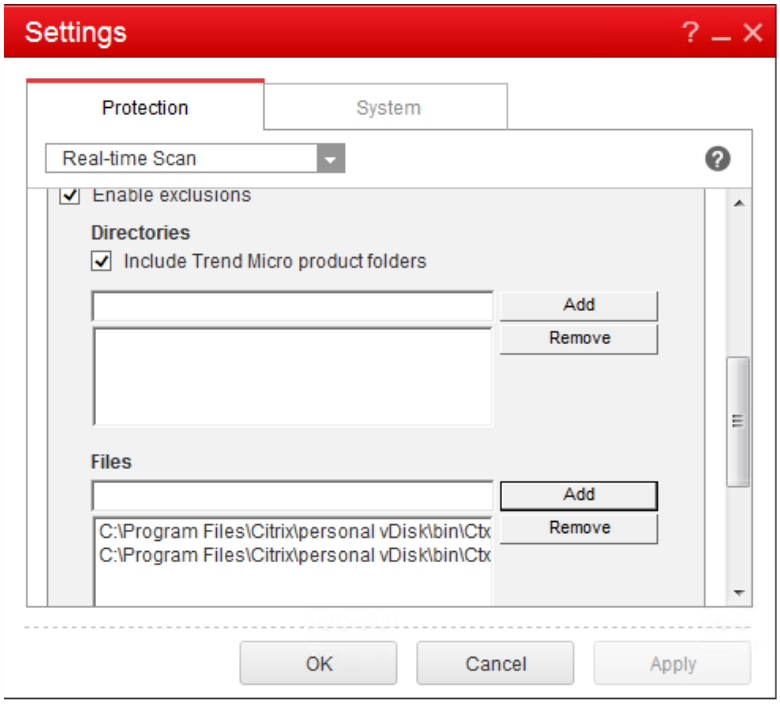


6. **[ファイル]** セクションで、 **[追加]** をクリックし、次のAppDiskプロセスを例外一覧に入力します。

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

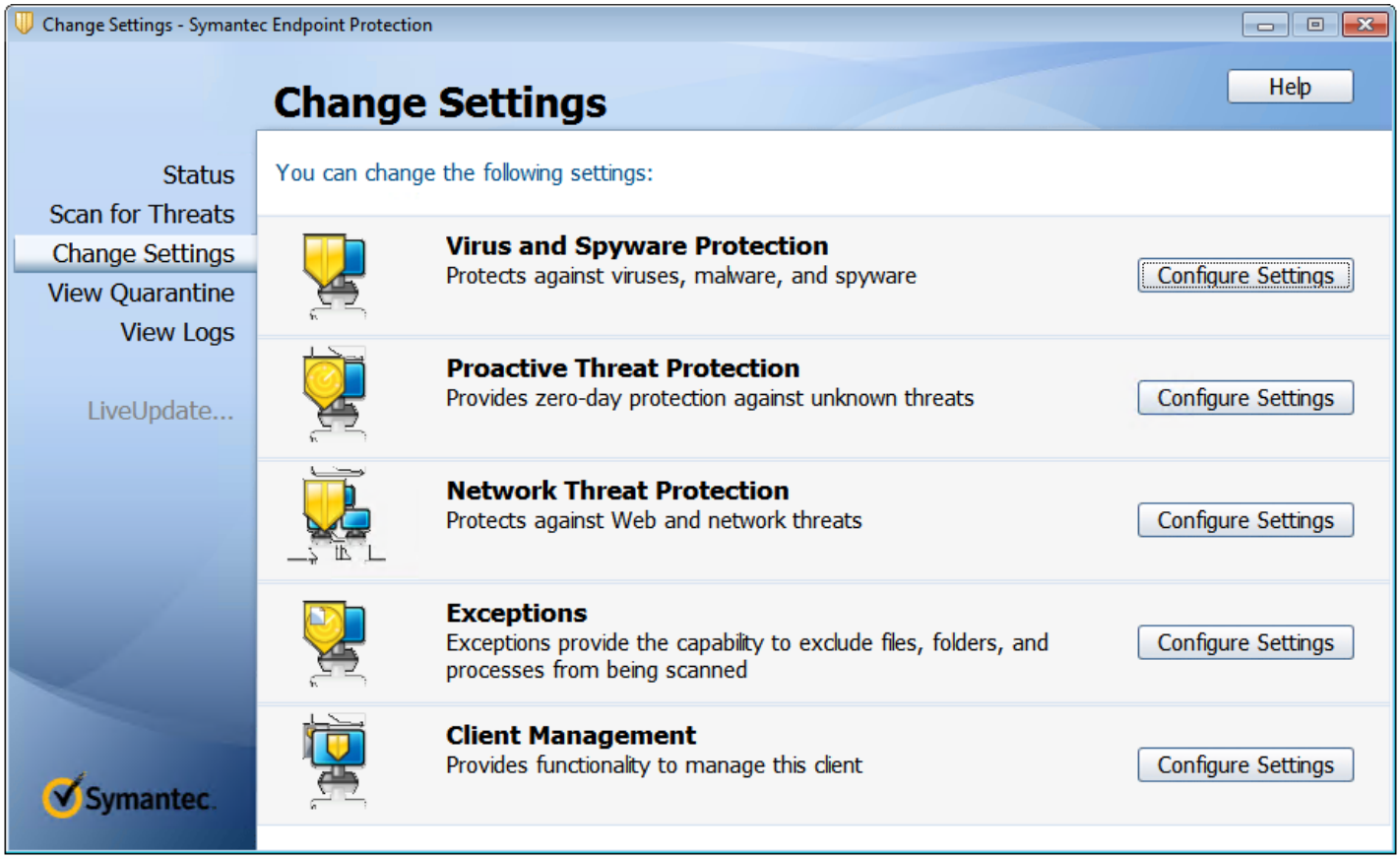


7. **[適用]** をクリックし、 **[OK]** をクリックして除外を追加します。

ベース仮想マシンがSymantec （バージョン12.1.16）を使用している場合：

1. Symantecコンソールを起動します。
2. **[設定の変更]** をクリックします。
3. **[例外]** セクションで、 **[オプションの設定]** をクリックします。

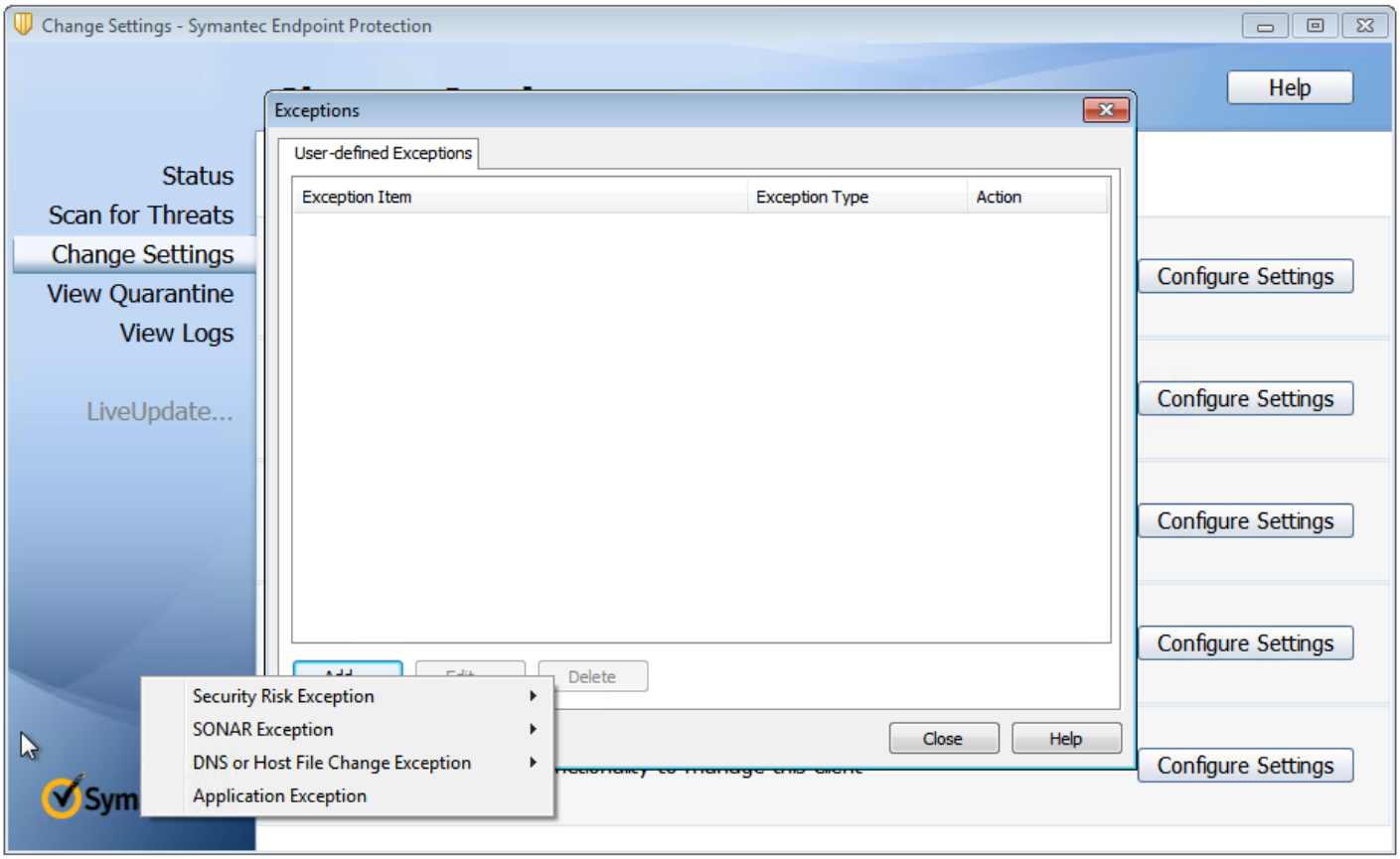
© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. ［オプションの設定］画面で **[追加]** をクリックします。

5. ［追加］をクリックすると、表示されたコンテキストメニューで、アプリケーションのタイプを指定できます。**[アプリケーション例外]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

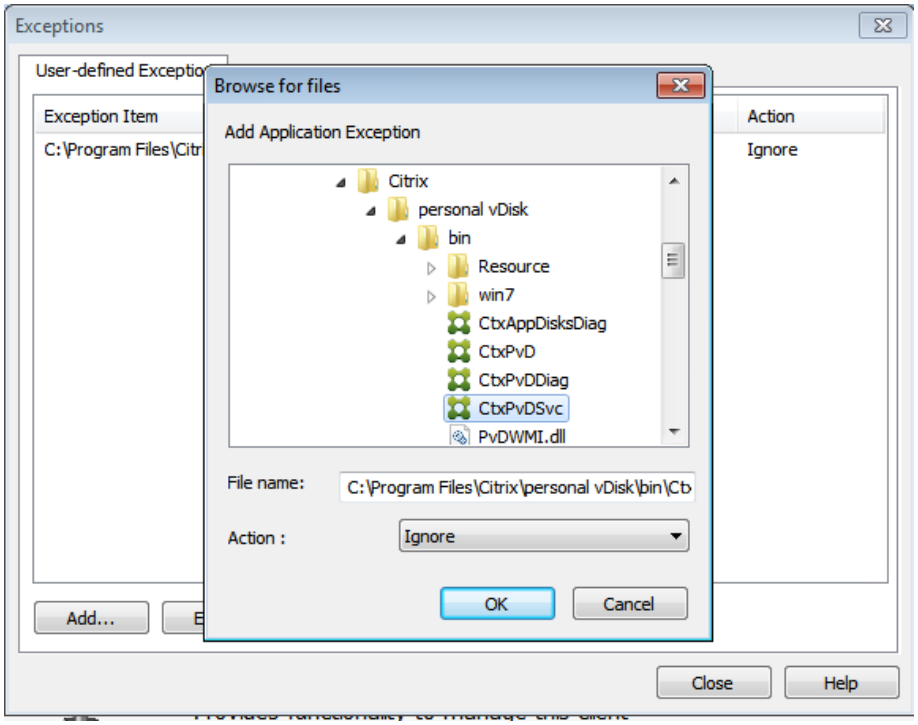


6. ［例外］画面で、次のAppDiskファイルパスを入力し、操作を**［無視］**に設定します。

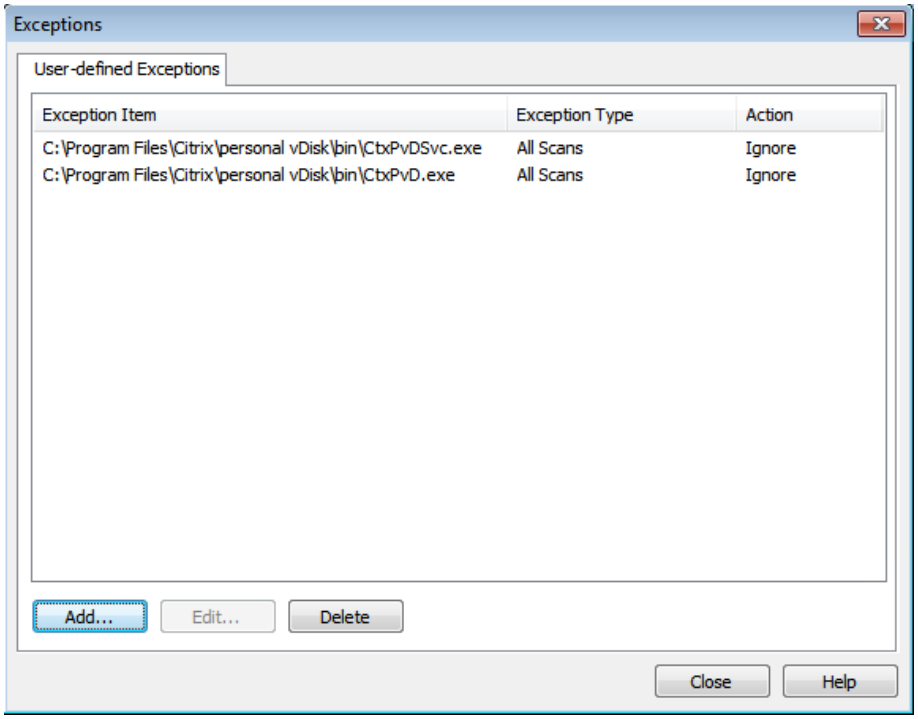
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.



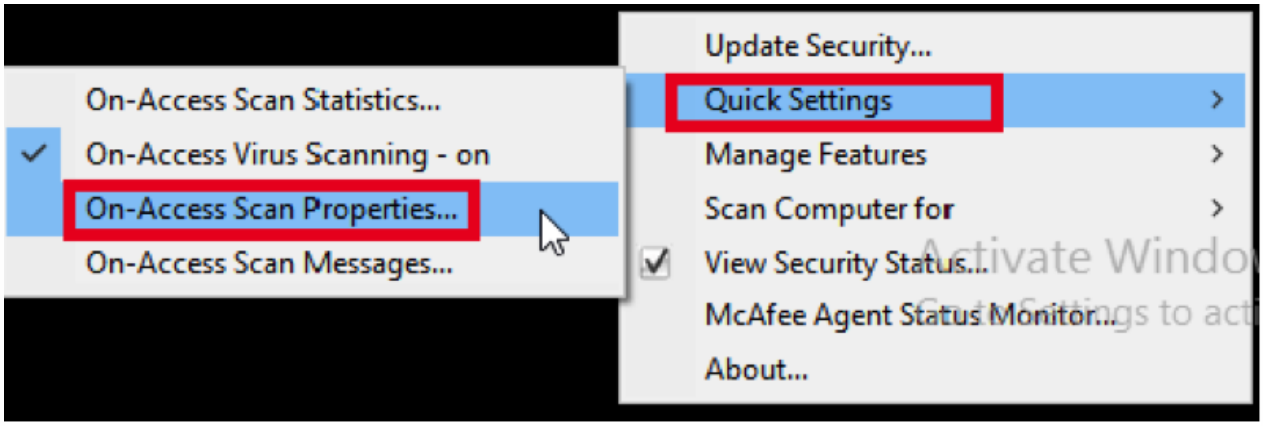
書きとめられた例外が一覧に追加されます。ウィンドウを閉じて変更を適用します。



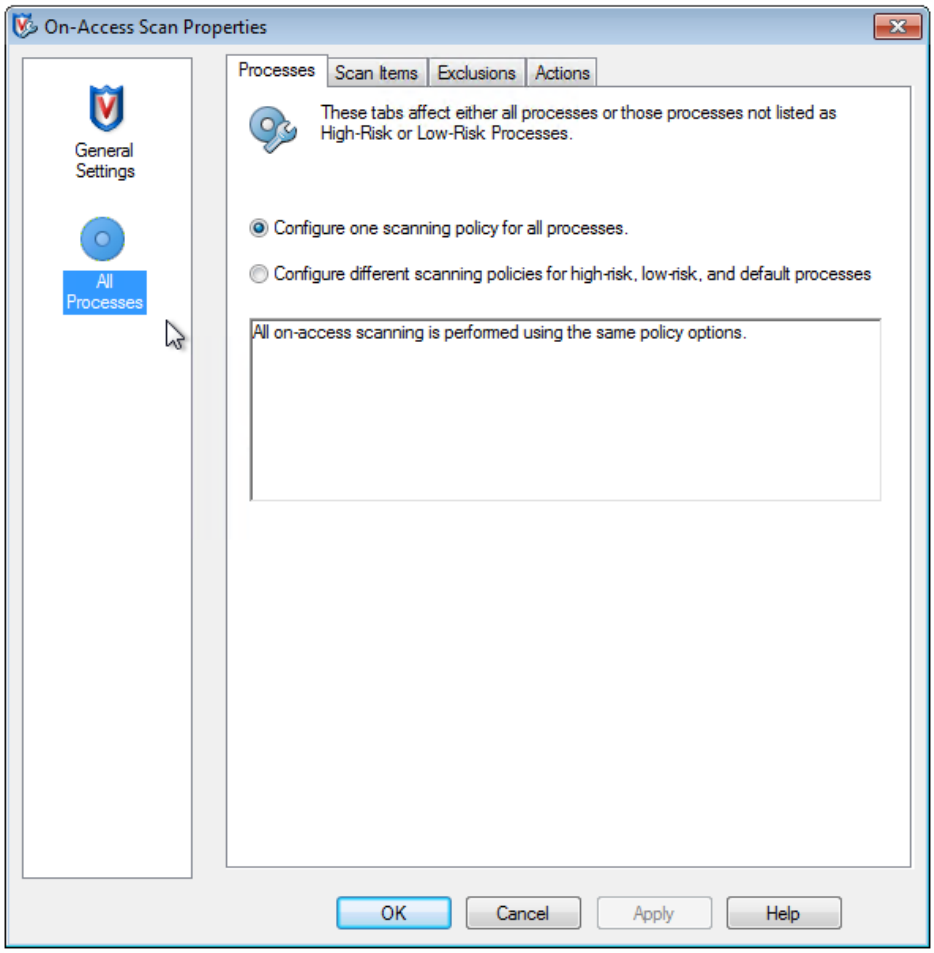
ベース仮想マシンがMcAfee（バージョン4.8）を使用している場合：

1. McAfeeアイコンを右クリックして、**[クイック設定]** オプションを展開します。
2. 展開したメニューの **[オンアクセススキャンのプロパティ]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

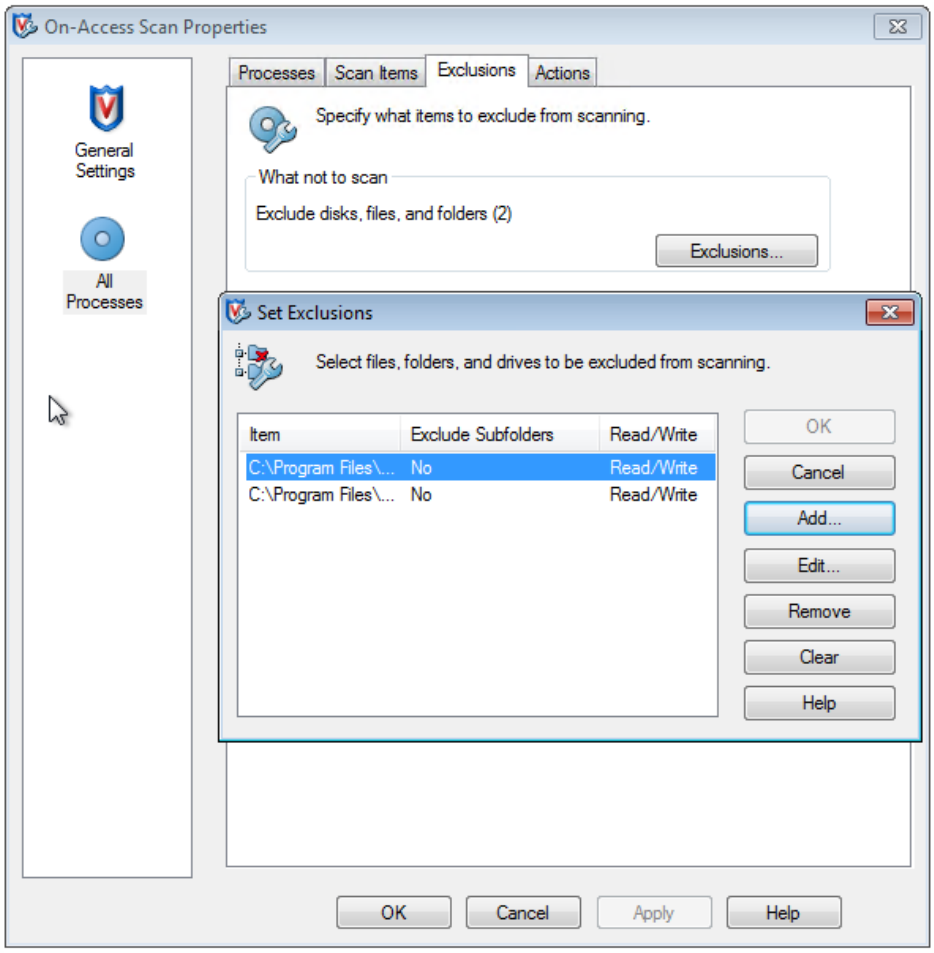


3. **[オンアクセススキャンのプロパティ]** 画面で、 **[すべてのプロセス]** をクリックします。



4. **[除外]** タブを選択します。
5. **[除外]** ボタンをクリックします。
6. **[除外の設定]** 画面で **[追加]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. **[除外項目の追加]** 画面で、 **[名前/場所（ワイルドカード*または?を使用可能）]** を選択します。 **[参照]** をクリックして、除外実行ファイルを見つけます。

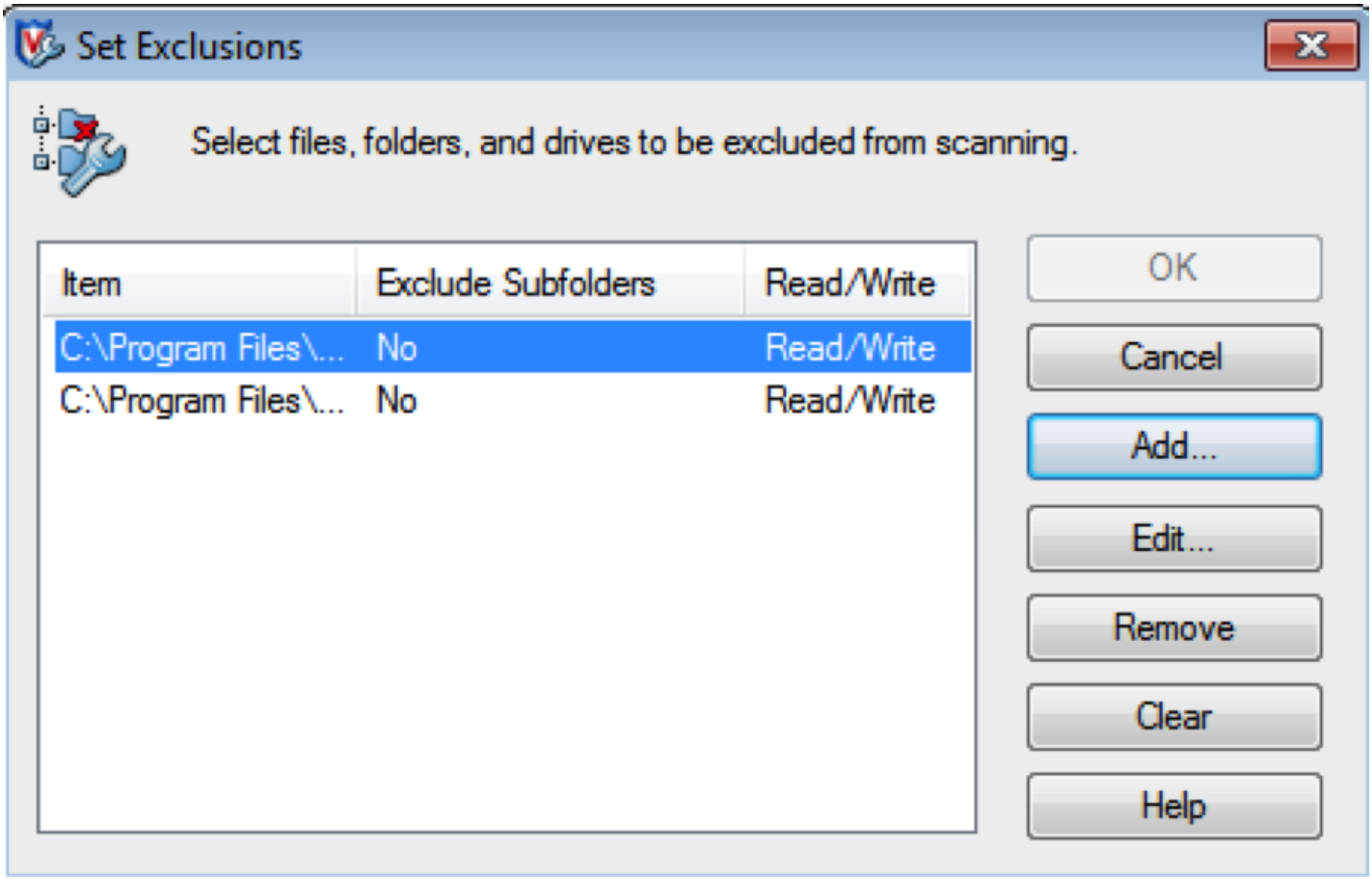
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

8. **[OK]** をクリックします。

9. **[除外の設定]** 画面に、追加された除外が表示されます。 **[OK]** をクリックして変更を適用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



> **注意**
>
> これらの除外を構成したら、AppDiskを作成します。

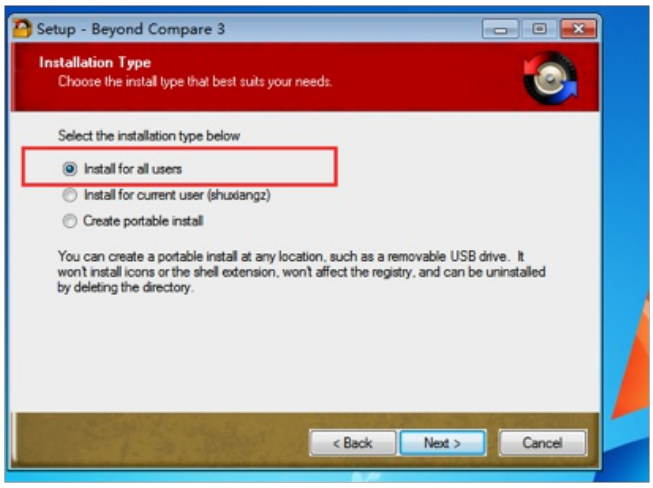
［スタート］メニューにアプリケーションを表示する方法

新しいAppDiskが作成され、アプリがすべてのユーザーから利用可能になると、ディスクはデスクトップにアタッチされ、アプリのショートカットが［スタート］メニューに表示されます。 AppDiskが現在のユーザーに対してのみ作成およびインストールされ、ディスクがデスクトップにアタッチされた場合、アプリのショートカットは［スタート］メニューに表示されません。

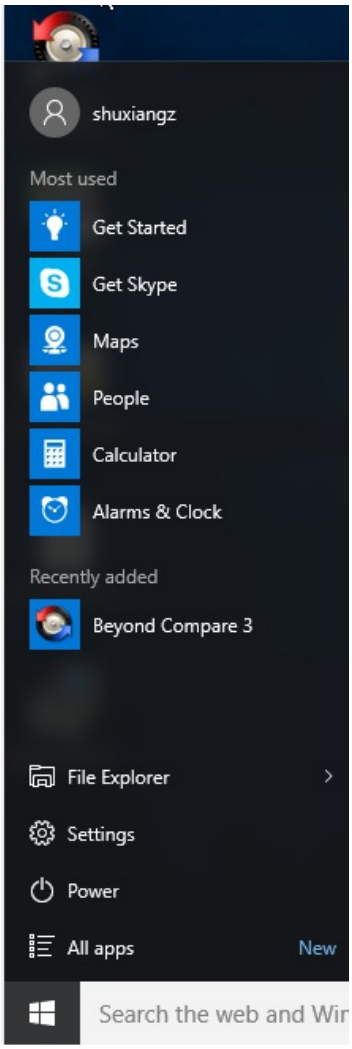
たとえば、新しいアプリを作成して、それをすべてのユーザーが利用できるようにします。

1. AppDiskにアプリをインストールします（たとえば、*Beyond Compare*が選択されたアプリだとします）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



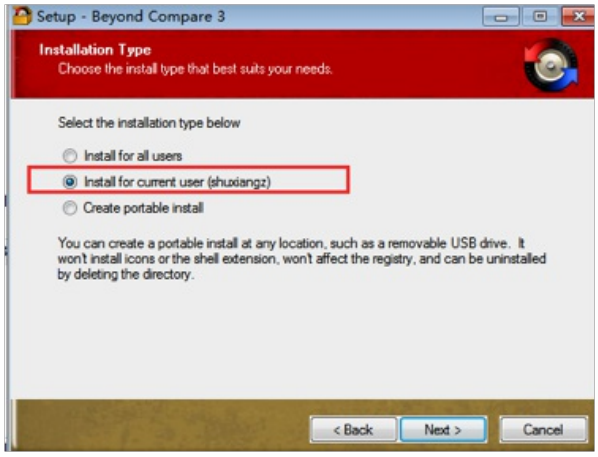
2. デスクトップにディスクをアタッチします。新しくインストールされたアプリ（*Beyond Compare*）のショートカットが、次のように［スタート］メニューに表示されます。



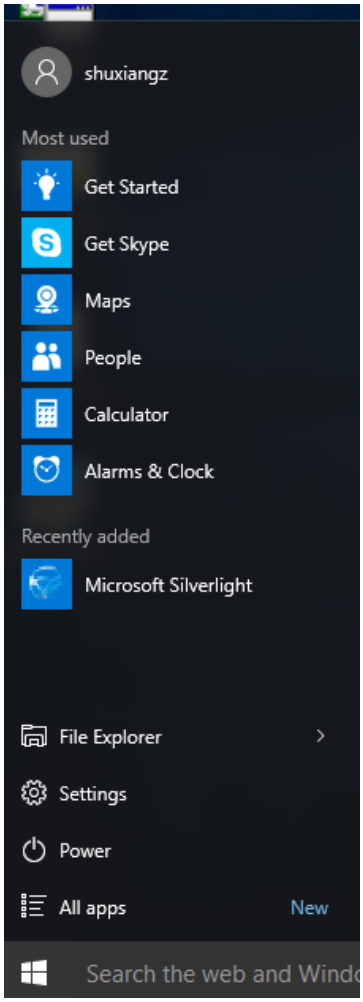
現在のユーザー用にのみアプリケーションをインストールするには：

1. AppDiskにアプリをインストールし、現在のユーザーが利用できるようにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. デスクトップにディスクをアタッチします。ショートカットが［スタート］メニューに表示されないことに注意してください。



AppDiskログの更新

このリリースでAppDiskのログとサポートのパラダイムが強化されました。このアップデートによって、AppDiskユーザー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

は、診断情報を取得して、任意でCIS（Citrix Insight Services）のWebサイトにアップロードできるようになりました。

この新機能で使用されるスクリプトベースのPowerShellツールによって、AppDiskやPVDが作成するログファイルをすべて洗い出し、システム（およびプロセス）に関する情報を含むPowerShellコマンドの出力を収集して、すべての情報を整理された単一のファイルに圧縮し、最終的に圧縮されたフォルダーをローカルに保存するか、CISにアップロードするかを選択できます。

> ### 注意
>
> CISでは匿名の診断情報を収集し、AppDiskやPVDの機能強化に役立てています。Citrix CISのWebサイトにアクセスして、手動で診断バンドルをアップロードしてください。このサイトへのアクセスには、お手持ちのCitrix資格情報でログインする必要があります。

PowerShellスクリプトを使用してAppDiskやPVDのログファイルを収集する

AppDiskおよびPVDのインストーラーに診断データ収集のためのスクリプトが新たに2つ追加されました。

- Upload-AppDDiags.ps1 – AppDiskの診断データ収集を実行します
- Upload-PvDDiags.ps1 – PvDの診断データ収集を実行します

> ### 注意
>
> これらのスクリプトは、C:\Program Files\Citrix\personal vDisk\bin\scriptsに追加されています。これらのPowerShellスクリプトは管理者として実行する必要があります。

このスクリプトを使ってAppDiskの診断データ収集を開始し、任意で手動によりCISのWebサイトにデータをアップロードします。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
SYNTAX

    Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

        -OutputFile

            Local path for zip file instead of uploading to CIS

 EXAMPLES

    Upload-AppDDiags

        Upload diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-AppDDiags -OutputFile C:\MyDiags.zip

        Save AppDisk diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

> ## ヒント
>
> **–OutputFile**引数を指定しない場合、アップロードが実行されます。**–OutputFile**を指定した場合は、スクリプトによってzipファイルが作成され、後から手動でアップロードできます。

このスクリプトを使ってPvDの診断データ収集を開始し、任意で手動によりCISのWebサイトにデータをアップロードします。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
SYNTAX

 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

    -OutputFile

        Local path for zip file instead of uploading to CIS

 EXAMPLES

    Upload-PvDDiags

        Upload PvD diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-PvDDiags -OutputFile C:\MyDiags.zip

        Save PvD diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

ヒント

–OutputFile引数を指定しない場合、アップロードが実行されます。**–OutputFile**を指定した場合は、スクリプトによってzipファイルが作成され、後から手動でアップロードできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp Secure Browser

Dec 05, 2017

アプリケーションのWebへの移行が進むにつれて、Webベースのアプリケーションに対応するために、ユーザーは複数のベンダーおよびバージョンのブラウザーを使用する必要があります。 アプリケーションを社内でホストしていると、多くの場合、組織はリモートユーザーにアクセスを提供するために複雑なVPNソリューションをインストールして構成する必要があります。一般的なVPNソリューションには、クライアント側のエージェントが必要ですが、このエージェントもさまざまなオペレーティングシステムで維持する必要があります。

XenApp Secure Browserを使用すると、ユーザーにWebベースのアプリケーションのエクスペリエンスをシームレスに提供することができます。ホストしているWebベースのアプリケーションは、ユーザーが希望するローカルブラウザーに表示されます。 たとえば、ユーザーがブラウザーにMozilla Firefoxを希望しても、アプリケーションが対応しているのはMicrosoft Internet Explorerのみという場合があります。 XenApp Secure Browserを使用すると、Internet Explorerに対応するアプリケーションが、Firefoxブラウザーのタブに表示されます。

XenApp Secure Browser Editionの展開

XenApp Secure Browser用のCitrix Smart Toolsブループリントを活用して展開を簡素化することをお勧めします。

XenApp Secure Browserブループリントには、以下のタスクを自動化するスクリプトが含まれています。

- Citrixライセンスサーバーおよび StoreFrontを含むXenAppのインストール
- XenAppデリバリーサイトの作成
- 既存ドメインへのプロビジョニングされたマシンの追加

Citrix Smart Toolsブループリントを使用するには

1. Citrix Cloudホームページから［Services］に移動して、［Request Trial for Citrix Smart Tools］をクリックします。試用を申請すると、試用サービスを利用できるようになった時点でメールでの通知を受信します。通常、これには5～10分程度かかります。
2. 試用を申請して受信したメールで［Manage］をクリックし、Citrix Smart Toolsホームページを表示します。
3. Citrixのダウンロードサイトから、Citrix XenApp Secure Browser Edition ISOをダウンロードします。

Secure Browser Edition ISOのダウンロード後、以下を検討します。

- 『XenApp Secure Installation with a Citrix Smart Tools blueprint』で指定した手順に従って、XenApp Secure Browserブループリントの使用を開始します。
- インストールの完了後、『XenApp Secure Browser展開ガイド』で指定した構成手順を使用して、Webappデリバリー用の環境をさらに最適化します。

XenApp Secure Browser Versionを手動でインストールするには

1. Citrixのダウンロードサイトから、Citrix XenApp Secure Browser Edition ISOをダウンロードします。
2. XenAppのさまざまなコンポーネントのインストールの手順に従います。
3. インストール後、次の追加手順を実行して、Secure Browserエディションのエディションとライセンスモードを構成しま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。

a. Delivery Controllerで、タスクバーの青色のアイコンをクリックするか、［スタート］ボタンをクリックし、［すべてのプログラム］>［アクセサリ］>［Windows PowerShell］>［Windows PowerShell］の順に選択して、PowerShellセッションを起動します。

注： 64ビットシステムでは、64ビット版が起動します。32ビット版と64ビット版の両方がサポートされます。

b. Asnp Citrix*と入力し、Enterキーを押してCitrix固有のPowerShellモジュールをロードします。

注： 「Asnp」はAdd-PSSnapinを表します。

c. Get-ConfigSiteコマンドレットを実行して、現在のサイト設定とライセンスモードを確認します。

d. Set-ConfigSite -ProductCode XDT -ProductEdition BASを実行して、ライセンスモードをXenApp Secure Browserエディションに設定します。

e. Get-BrokerSiteコマンドレットを実行して、XenApp Secure Browserのエディションとライセンスモードが正しく設定されていることを確認します。

注意

インストールの完了後、『XenApp Secure Browser展開ガイド』で指定した構成手順を使用して、Webappデリバリー用の環境をさらに最適化します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コンテンツの公開

Dec 05, 2017

Microsoft WordドキュメントやWebリンクなどのリソースへのURLまたはUNCパスを、アプリケーションとして公開できます。この機能は、コンテンツの公開と呼ばれています。コンテンツの公開機能を使用することで、ユーザーへのコンテンツの配信をより柔軟に行うことができるようになります。既存のアプリケーションのアクセス制御と管理機能を使用できるというメリットもあります。さらに、コンテンツを開くのにローカルアプリケーションと公開アプリケーションのどちらを使用するかも指定できます。

公開コンテンツは、StoreFrontやCitrix Receiverの他のアプリケーションと同じように表示されます。アクセス方法はアプリケーションへアクセスするときと同じです。クライアントでは、リソースは通常どおりに開かれます。

- ローカルにインストールされているアプリケーションが適している場合は、こうしたアプリケーションが起動されリソースが開かれます。
- ファイルタイプの関連付けが定義されている場合は、公開アプリケーションが起動されリソースが開かれます。

コンテンツの公開にはPowerShell SDKを使用します（Studioを使用してコンテンツを公開することはできませんが、アプリケーションの公開後にStudioを使用してそのプロパティを編集することはできます）。

構成の概要と準備

コンテンツの公開では、New-BrokerApplicationコマンドレットに以下のキープロパティを指定して使用します（すべてのコマンドレットプロパティの説明についてはこのコマンドレットのヘルプを参照してください）。

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable <location> -Name <app-name>
-DesktopGroup <delivery-group-name>
```

ApplicationTypeプロパティにはPublishedContentを指定する必要があります。

CommandLineExecutableプロパティでは、公開するコンテンツの場所を指定します。以下の形式を使用でき、最大文字数は255文字です。

- HTML Webサイトアドレス（例：http://www.citrix.com）
- Webサーバー上の文書ファイル（例：https://www.citrix.com/press/pressrelease.doc）
- FTPサーバー上のディレクトリ（例：ftp://ftp.citrix.com/code）
- FTPサーバー上の文書ファイル（例：ftp://ftp.citrix.com/code/Readme.txt）
- UNCディレクトリパス（例：file://myServer/myShareまたは\\myServer\myShare）
- UNCファイルパス（例：file://myServer/myShare/myFile.asfまたは\\myServer\myShare\myFile.asf）

適切なSDKがあることを確認します。

- 展開環境がXenAppおよびXenDesktop Serviceの場合は、XenAppとXenDesktop用のRemote PowerShell SDKをダウンロードしてインストールします。
- 展開環境がオンプレミスのXenAppおよびXenDesktopの場合は、Delivery Controllerとともにインストールされている PowerShell SDKを使用します。公開コンテンツアプリケーションの追加にはDelivery Controllerのバージョン7.11以上が必要です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下の手順ではサンプルを利用しています。このサンプルの詳細は次のとおりです。

- マシンカタログを作成しています。
- PublishedContentAppsという名前のデリバリーグループを作成しています。このデリバリーグループでは、カタログのサーバーOSマシンを使用しています。このデリバリーグループには、ワードパッドアプリケーションが追加されています。
- デリバリーグループ名、CommandLineExecutableの場所、およびアプリケーション名用の変数を作成しています。

導入

PowerShell SDKをインストール済みのマシンでPowerShellを開きます。

次のコマンドレットにより、適切なPowerShellスナップインを追加し、返されたデリバリーグループレコードを変数に代入します。

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

XenAppおよびXenDesktop Serviceを使用している場合は、Citrix Cloud資格情報を入力して認証を行います。ユーザーが複数存在する場合は1人を選択します。

URLの公開

次のコマンドレットでは、場所とアプリケーション名を変数に代入してからCitrixホームページをアプリケーションとして公開します。

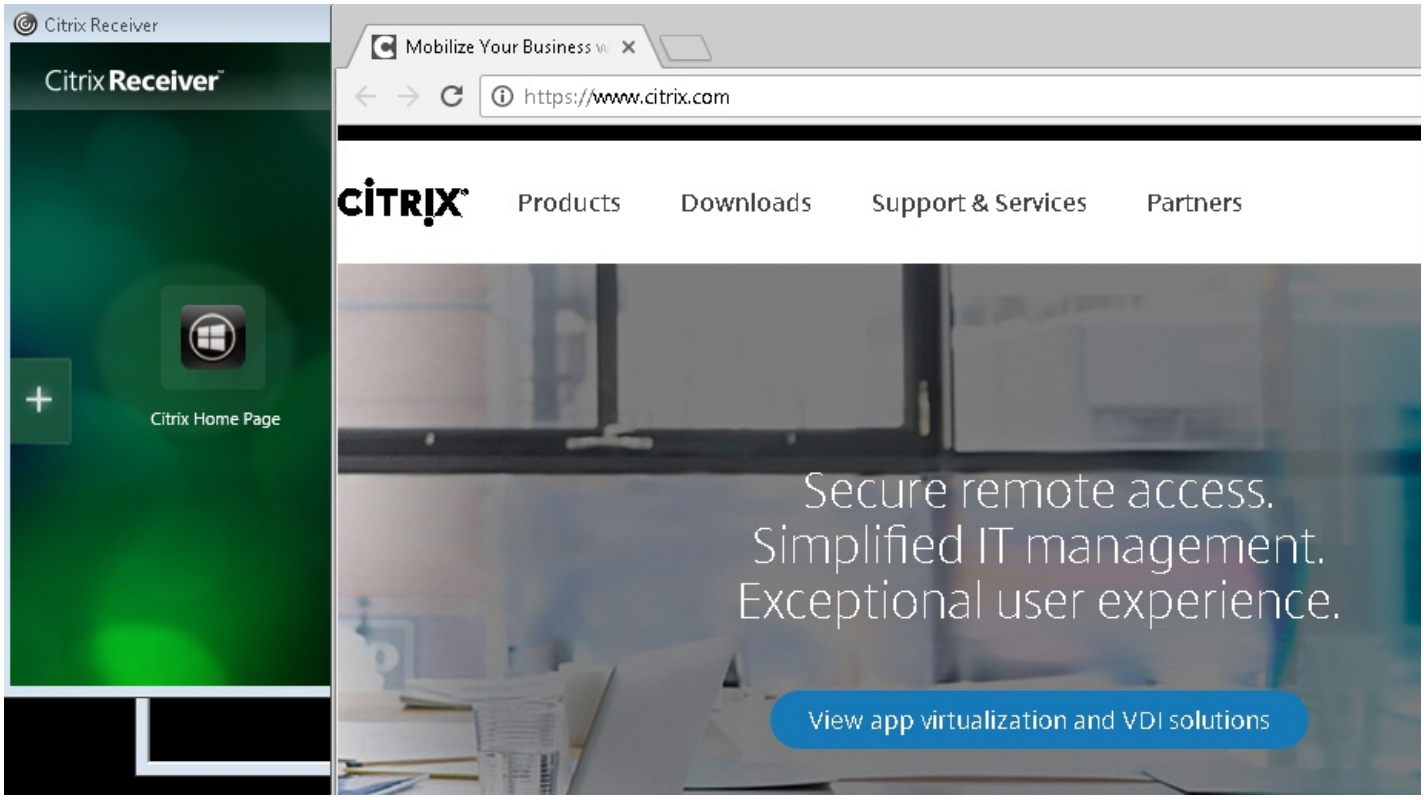
```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $citrixURL –Name $appName
–DesktopGroup $dg.Uid
```

次の手順を実行して、成功したことを確認します。

- StoreFrontを開き、PublishedContentAppsデリバリーグループのアプリケーションにアクセスできるユーザーとしてログオンします。新しく作成したアプリケーションが、デフォルトのアイコンで表示されます。アイコンのカスタマイズ方法について詳しくは、https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/を参照してください。
- Citrix Home Pageアプリケーションをクリックします。ローカルで実行されているデフォルトブラウザーのインスタンスの新しいタブで、指定したURLが開かれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



UNCパスに配置されているリソースの公開

この例では、管理者が共有名PublishedResourcesをすでに作成しています。次のコマンドレットで、場所とアプリケーション名を変数に代入してから、この共有に含まれるRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

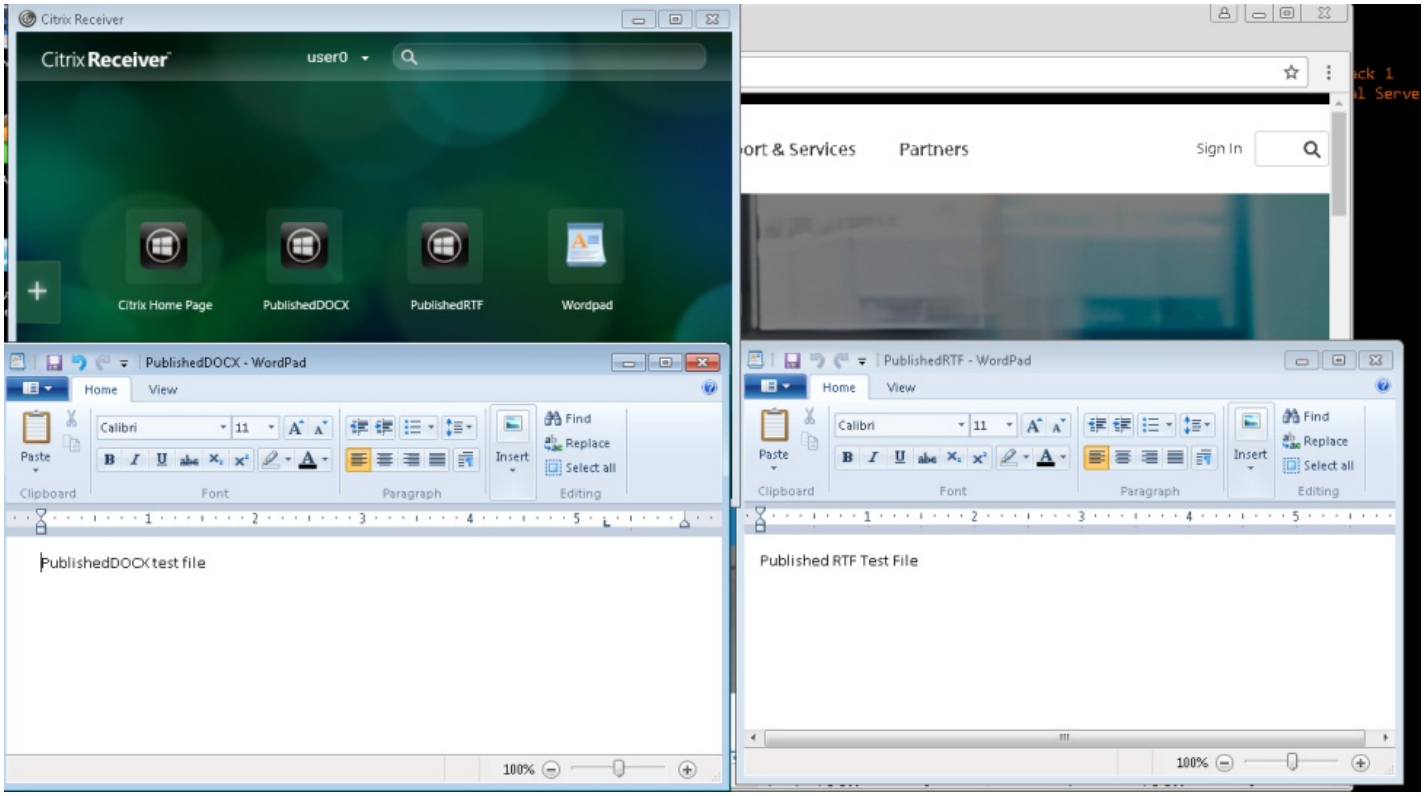
次の手順を実行して、成功したことを確認します。

- StoreFrontウィンドウを更新して、新しく公開したドキュメントが表示されることを確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



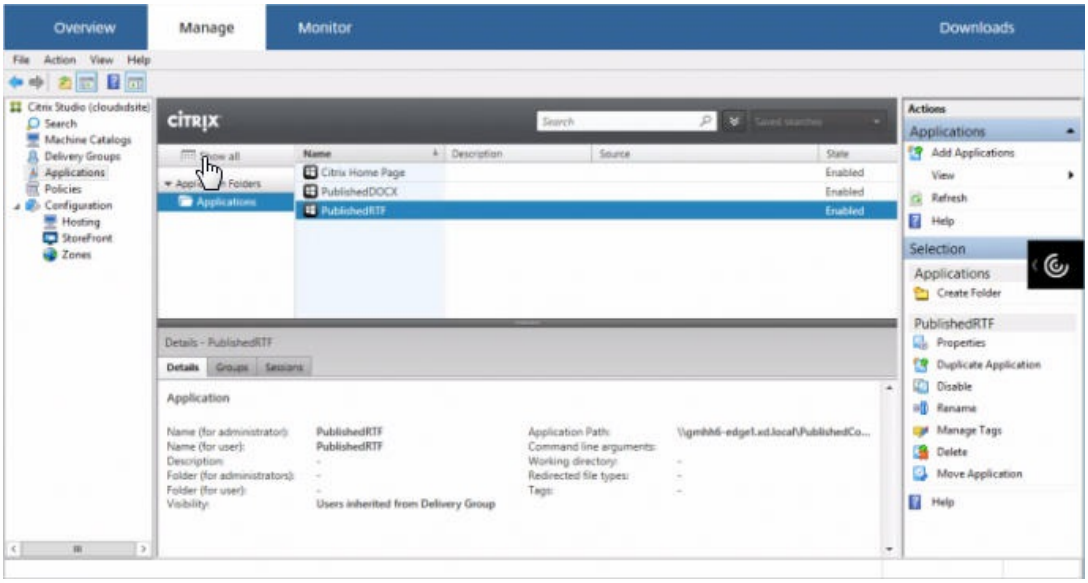
- PublishedRTFアプリケーションおよびPublishedDOCXアプリケーションをクリックします。各ドキュメントが、ローカルで実行されるワードパッドで開きます。



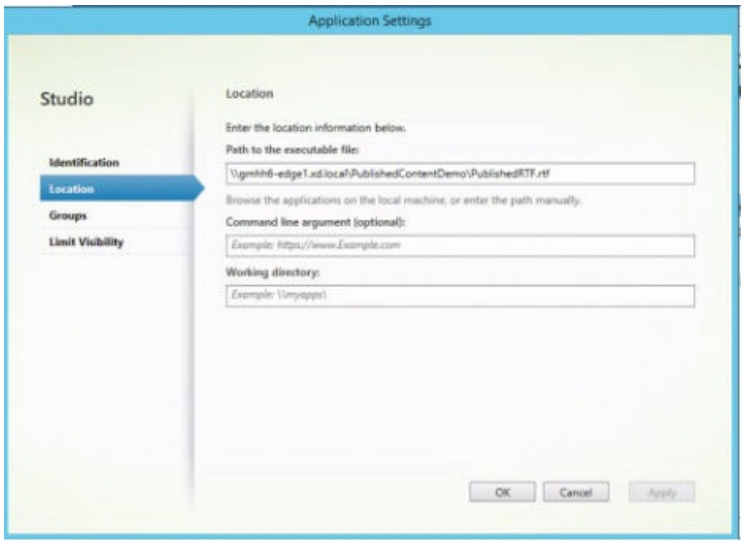
PublishedContentアプリケーションの確認と編集

© 1999-2017 Citrix Systems, Inc. All rights reserved.

公開コンテンツは、他の種類のアプリケーションと同じ方法で管理できます。公開されたコンテンツアイテムはStudioのアプリケーション一覧に表示され、Studioで編集できます



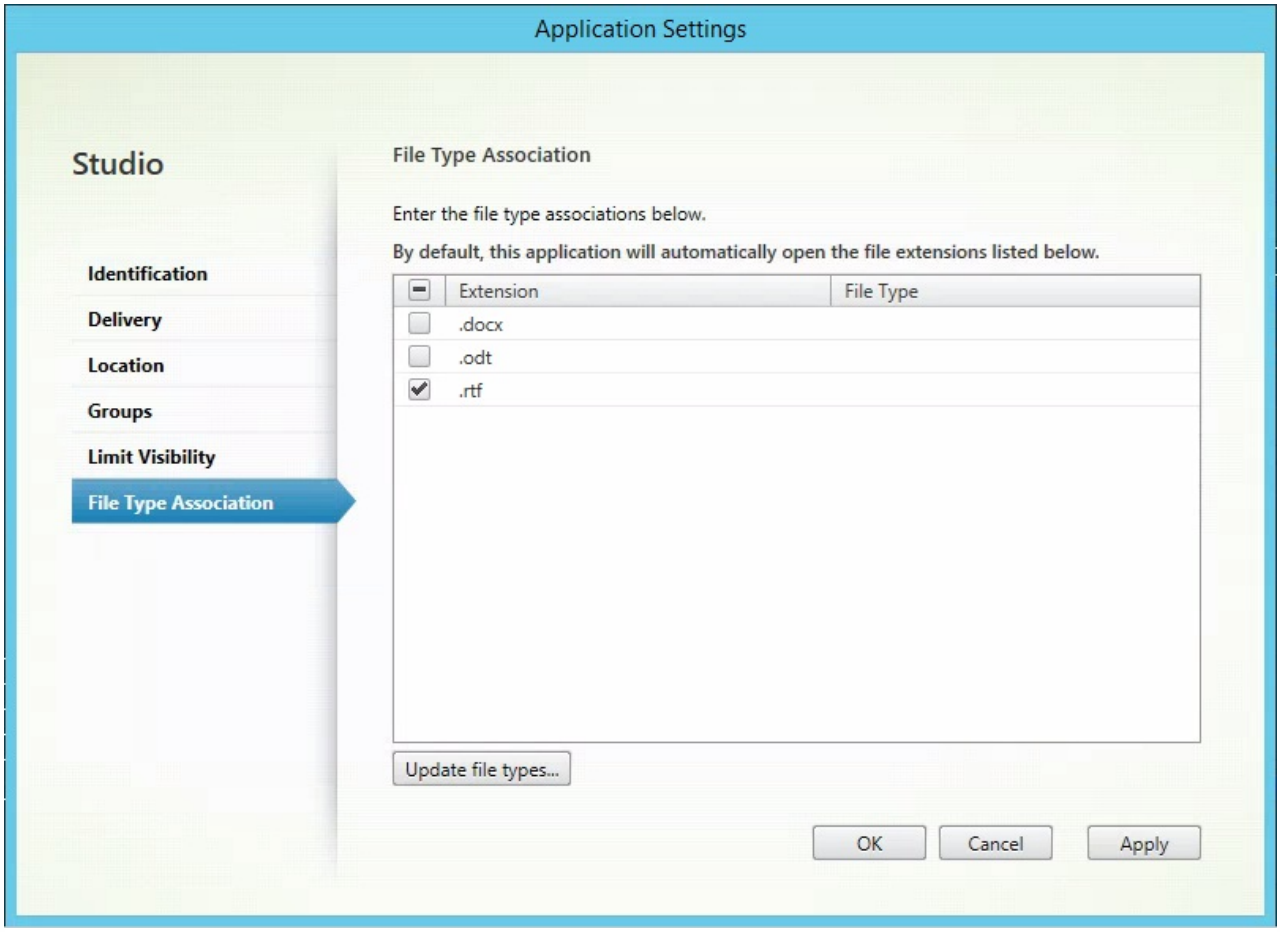
公開コンテンツには、アプリケーションのプロパティ（表示できるユーザー、グループ割り当て、ショートカットなど）が適用されます。ただし、 **[場所]** ページでコマンドライン引数や作業ディレクトリプロパティを変更することはできません。ソースを変更するには、［場所］ページの［実行可能ファイルのパス］を変更します。



PublishedContentアプリケーションを開くのに（ローカルアプリケーションではなく）公開アプリケーションを使用するには、該当する公開アプリケーションのファイルタイプの関連付けプロパティを編集します。この例では、公開済みのワードパッドアプリケーションを編集して、.rtfファイルに対するファイルタイプの関連付けを作成しています。

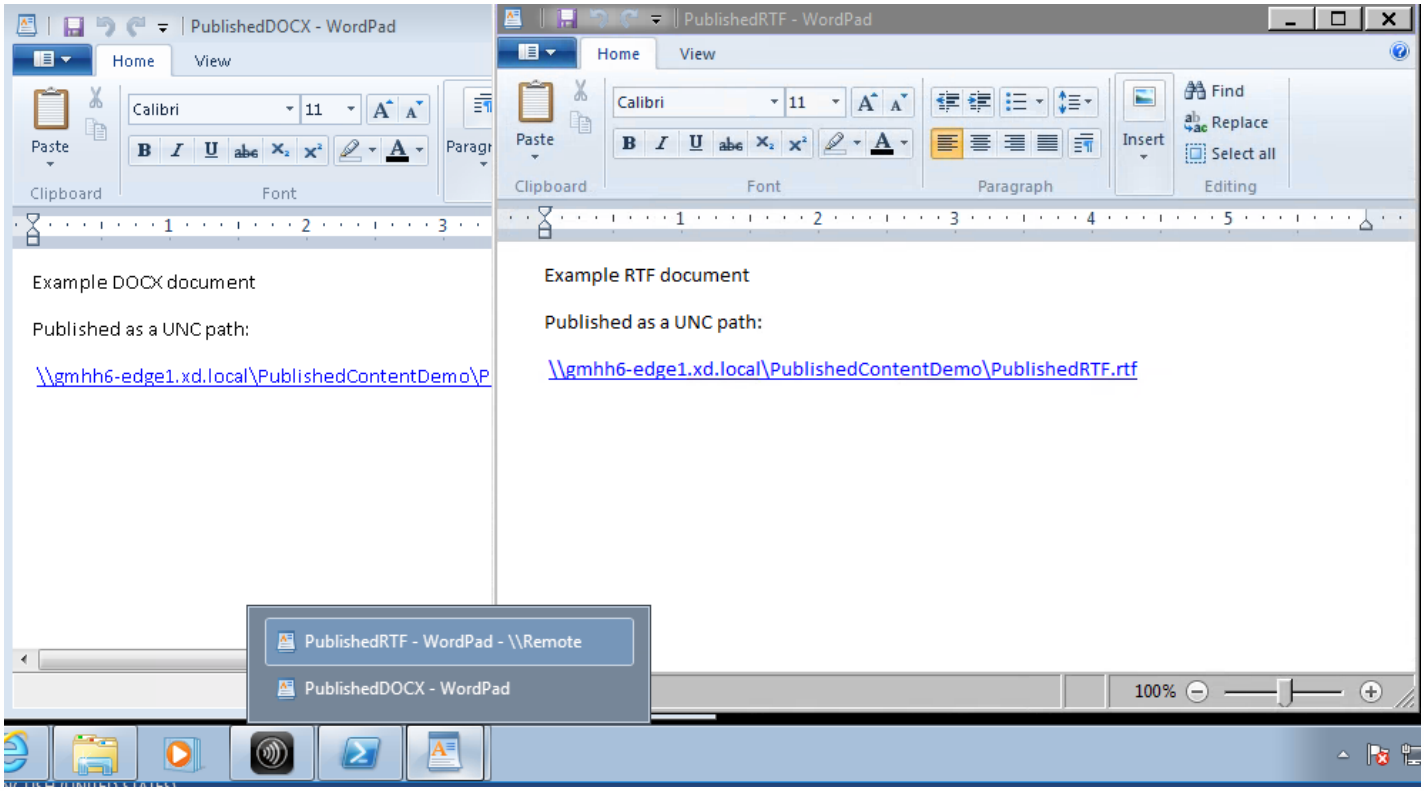
重要：ファイルタイプの関連付けを編集する前にデリバリーグループのメンテナンスモードを有効にしてください。編集が完了したらメンテナンスモードはオフにしてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



StoreFrontを更新してファイルタイプの関連付けに対する変更を反映させ、PublishedRTFアプリケーションおよびPublishedDOCXアプリケーションをクリックします。違いに注目してください。PublishedDOCXは以前と同様にローカルのワードパッドで開かれますが、PublishedRTFは、ファイルタイプの関連付けが変更されたため公開済みのワードパッドアプリケーションで開かれるようになりました。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



詳しい情報の参照先

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サーバーVDI

Dec 05, 2017

サーバーVDI（Virtual Desktop Infrastructure）機能を使用すると、サーバーオペレーティングシステムからユーザーにデスクトップを配信できます。

- エンタープライズ管理者は、エンジニアやデザイナーなどのユーザーにサーバーオペレーティングシステムをVDIデスクトップとして配信できます。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement（SPLA）に準拠します。

デスクトップエクスペリエンス拡張のCitrixポリシー設定を使用すると、サーバーオペレーティングシステムでデスクトップオペレーティングシステムの外観を提供できます。

サーバーVDIでは、次の機能を使用できません。

- Personal vDisk
- ホストされるアプリケーション
- ローカルアプリケーションアクセス
- 直接（非仲介）デスクトップ接続
- リモートPCアクセス

スキャナのようなTWAINデバイスと連携するサーバーVDIには、Windows Serverのデスクトップエクスペリエンス機能をインストールする必要があります。これは、Windows Server 2012のオプション機能であり、［管理ツール］>［サーバー マネージャ］>［機能］>［機能の追加］>［デスクトップ エクスペリエンス］でインストールします。

サーバーVDIは、VDA for Windows Server OSと同じサーバーオペレーティングシステムでサポートされます。

サーバーVDIをインストールするには

手順1： Windowsサーバーでのインストールの準備

- Windowsサーバーマネージャーを使って、リモートデスクトップサービスの役割サービスがインストールされていないことを確認します。既にインストールされている場合は、それを削除します。（これらの役割サービスがインストールされていると、VDAのインストールに失敗します。）
- ［1ユーザーにつき1セッションに制限する］プロパティが有効であることを確認します。

  Windows Server 2008 R2では、［管理ツール］>［リモートデスクトップサービス］>［リモートデスクトップセッションホストの構成］の順に選択します。［設定の編集］>［全般］で、［1ユーザーにつき1セッションに制限する］設定が［はい］であることを確認します。

  Windows Server 2012R2またはWindows Server 2016で、レジストリを編集してターミナルサーバー設定を設定します。レジストリキー、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServerの DWORD fSingleSessionPerUserを1に設定します。

手順2： Windows Server 2008 R2では、VDAをインストールする前に、サーバー上にMicrosoft .NET Framework 3.5 SP1をインストールします。

手順3：インストーラーのコマンドラインインターフェイスで/quietおよび/servervdiオプションを指定して、VDAをサーバーまたはサーバーマスターイメージ上にインストールします。（デフォルトでインストーラーのグラフィカルユーザーインタ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フェイスでは、サーバーオペレーティングシステム上のWindowsデスクトップOSのVDAはブロックされます。コマンドラインを使うことで、この動きを無効にします。）

オンプレミスXenAppおよびXenDesktop環境：XenDesktopVdaSetup.exe /quiet /servervdi

オンプレミスXenAppおよびXenDesktopまたはXenDesktopサービス環境：VDAWorkstationSetup.exe /quiet /servervdi

Delivery ControllerまたはCloudコネクタを/controllersオプションで指定できます。

ファイアウォールが手動で構成されていない限りは、/enable_hdx_portsオプションを使ってファイアウォールでポートを開きます。

イメージにVDAをインストールしており、MCSを使用してそのイメージからサーバー仮想マシンを作成する場合は、/masterimageオプションを追加します。

/baseimageなど、サーバーVDIでサポートされてない機能のオプションを指定しないでください。

手順4：サーバーVDIのマシンカタログを作成します。

- **[オペレーティング システム]** ページで、［デスクトップ OS］を選択します。
- **[概要]** ページで、管理者がサーバーVDI用のマシンカタログを識別できるようにマシンカタログ名と説明を指定します。これは、StudioにおいてそのマシンカタログがサーバーVDI用であることを示す唯一のインジケーターになります。
- VDAはサーバー上にインストールされていますが、Studioで検索すると、このサーバーVDIカタログは［デスクトップOSマシン］タブに表示されます。

手順5：デリバリーグループを作成し、前の手順で作成したサーバーVDIカタログを割り当てます。

VDAのインストール中にDelivery ControllerまたはCloudコネクタを指定しなかった場合、Citrixポリシー設定やActive Directoryを使って、あるいはVDAマシンのレジストリ値を編集して、あとから指定します。「VDA登録」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personal vDisk

Dec 05, 2017

Personal vDisk 機能を使用すると、プールされるデスクトップやストリーム配信されるデスクトップ を単一のイメージで管理でき、しかもユーザーによるアプリケーションのインストールやデスクトップ設定の変更が可能になります。従来の仮想デスクトップインフラストラクチャ（VDI）では、 仮想デスクトップでユーザーが設定を変更したりアプリケーション をインストールしたりしても、管理者がマスターイメージを更新するたびにそれらの変更が破棄されてしまいます。Personal vDiskを使用すると、ユーザーによる変更がそのまま保持されます。管理者は、ユーザーによる デスクトップのカスタマイズや個人設定を許可しながら、マスターイメージを容易に一元 管理できます。

Personal vDisk では、ユーザーの仮想マシンに対するすべての変更をその仮想マシンに割り当てられた 別ディスク（Personal vDisk）にリダイレクトすることにより、変更内容を保持します。Personal vDiskに保存された 内容はデスクトップの実行時にマスターイメージの内容と統合され、ユーザーに一貫した操作環境が提供されます。この方法では、管理者がマスターイメージでプロビジョニングしたアプリケーションにもユーザーは引き続き アクセスできます。

Personal vDiskは、デフォルトで同じ容量の 2つの領域で構成されます。

- ユーザープロファイル： ここには、ユーザーデータ、ドキュメント、およびユーザープロファイルが格納されます。デフォルトでは ドライブ文字「P」が割り当てられますが、マシンカタログ を作成するときに別のドライブ文字を選択することもできます。使用されるドライブの設定は、レジストリキー EnableUserProfileRedirectionにも依存します。
- 仮想ハードディスク （VHD）ファイル：ここには、そのほかのすべてのファイル（ C:\Program Filesにインストールされたアプリケーションなど）が格納されます。この部分はWindows Explorerには表示されず、 Version 5.6.7以降ではドライブ文字は必要ありません。

Personal vDisk では、個々のユーザーがダウンロードしてインストールする アプリケーションに加えて、部門レベルでプロビジョニングするアプリケーションがサポートされます。これには ドライバー（Phase 1ドライバーを除く）やデータベースを必要とするアプリケーション、およびマシン管理ソフトウェアなどがあります。ユーザーによる変更と管理者による変更が競合する場合でも、Personal vDisk の機能を使って簡単かつ自動的に解決できます。

さらに、ローカルで管理されるアプリケーション （ローカルのIT 部門によりプロビジョニングされて管理されるアプリケーションなど）をユーザーの環境にプロビジョニングすることもできます。Personal vDiskを使用する場合でも、ユーザーの 操作性は変更されません。ユーザーが変更した設定 やインストールしたアプリケーションは、自動的にPersonal vDisk上に格納されます。Personal vDisk上のアプリケーションがマスターイメージ上のものとまったく同じである場合、 Personal vDisk上のアプリケーションが破棄されます。これにより、その アプリケーションは使用可能なままPersonal vDiskの容量が節約されます。

物理的には、Personal vDiskをハイパーバイザーに格納します。 ただし、仮想デスクトップにアタッチされているほかのディスクと同じ 場所に配置する必要はありません。これにより、Personal vDiskストレージの コストを削減できます。

サイトの作成中、コネクションを作成するときに、仮想マシンで使用されるディスクの ストレージを指定します。Personal vDiskは、 オペレーティングシステム用のディスクとは異なるストレージに配置できます。各仮想マシンは、 どちらのストレージにもアクセスできる必要があります。これらのディスクをローカルストレージに配置する場合は、 同じハイパーバイザーからアクセスできる必要があります。このため、これらの条件を満たす ストレージのみが表示されます。後で、Personal vDiskとそのストレージを既存のホストに追加することもできます（マシン カタログには追加できません）。これを行うにはStudioで［構成］の［ホスト］を選択します。

Personal vDiskは、適切な方法で定期的にバックアップしてください。vDiskはハイパーバイザーのストレージ層の標準のボリュームであるため、 ほかのボリュームと同様の方法でバックアップできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意

PvDのレポート、メッセージ、および既知の問題については、「トラブルシューティング」の記事を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

インストールとアップグレード

Dec 05, 2017

Personal vDisk 7.xは、XenDesktop Version 5.6以降でサポートされています。XenDesktopの各バージョンの「システム要件」のトピックを参照して、サポートされるVirtual Delivery Agent（VDA）のオペレーティングシステム、ホスト（仮想化リソース）、およびProvisioning Servicesについて確認してください。Provisioning Servicesの操作について詳しくは、現行のProvisioning Servicesのドキュメントを参照してください。

マシン上にVDA for Desktop OSをインストールしたりアップグレードしたりするときに、Personal vDiskをインストールして有効化できます。これらの操作は、インストールウィザードの**[追加コンポーネント]**と**[機能]**ページでそれぞれ選択します。詳しくは、「Install Capture」を参照してください。

VDAのインストール後にPersonal vDiskをアップデートする場合は、ここで提供されているPersonal vDiskのMSIファイルをXenAppまたはXenDesktopのインストールメディアで使用してください。

Personal vDiskは、以下の状況で有効になります。

- Machine Creation Services（MCS）を使用している場合、Personal vDisk用のデスクトップOSマシンカタログの作成時にPersonal vDiskが自動的に有効になります。
- Provisioning Services（PVS）を使用している場合、マスター（基本）イメージ作成時に管理者がインベントリを実行したとき、および自動更新によるインベントリ実行時にPersonal vDiskが自動的に有効になります。

そのため、VDAのインストール中にPersonal vDiskコンポーネントをインストールしたのに有効化しなかったとしても、カタログ作成時にPersonal vDiskが有効になるため、同じイメージを使用してPersonal vDiskが有効なデスクトップおよびPersonal vDiskが無効なデスクトップを作成できます。

新しいサイトを構成するときに、Personal vDiskをホストに追加します。ホスト上の同じ ストレージを仮想マシンとPersonal vDisk用に使用したり、Personal vDisk用に専用の ストレージを使用したりできます。

その後で、Personal vDiskとそのストレージを既存のホスト（接続）に 追加することもできます（ マシンカタログには追加できません）。

1. Studioのナビゲーション ペインで ［構成］> ［ホスト］の順に選択します。
2. ［操作］ペインの ［ Personal vDiskストレージの追加］ を選択し、ストレージの場所を指定します。

Personal vDisk Version 7.xを簡単にアップグレードするには、VDA for Desktop OSを最新のXenDesktopレベルにアップグレードします。その後で、Personal vDiskのインベントリを実行します。

Personal vDiskソフトウェアをアンインストールするには、以下のいずれかの方法を使用します。

- VDAをアンインストールします。これにより、Personal vDiskソフトウェアもアンインストールされます。
- Personal vDiskのMSIファイルを使用してPersonal vDiskをアップデートした場合は、コントロールパネルを使用してアンインストールできます。

Personal vDiskをアンインストールして同じまたは新しいバージョンを再インストールする場合は、事前にレジストリキーHKEY_LOCAL_MACHINE\Software\Citrix\personal vDisk\configをバックアップしておいてください。このレジストリキーに

© 1999-2017 Citrix Systems, Inc. All rights reserved.

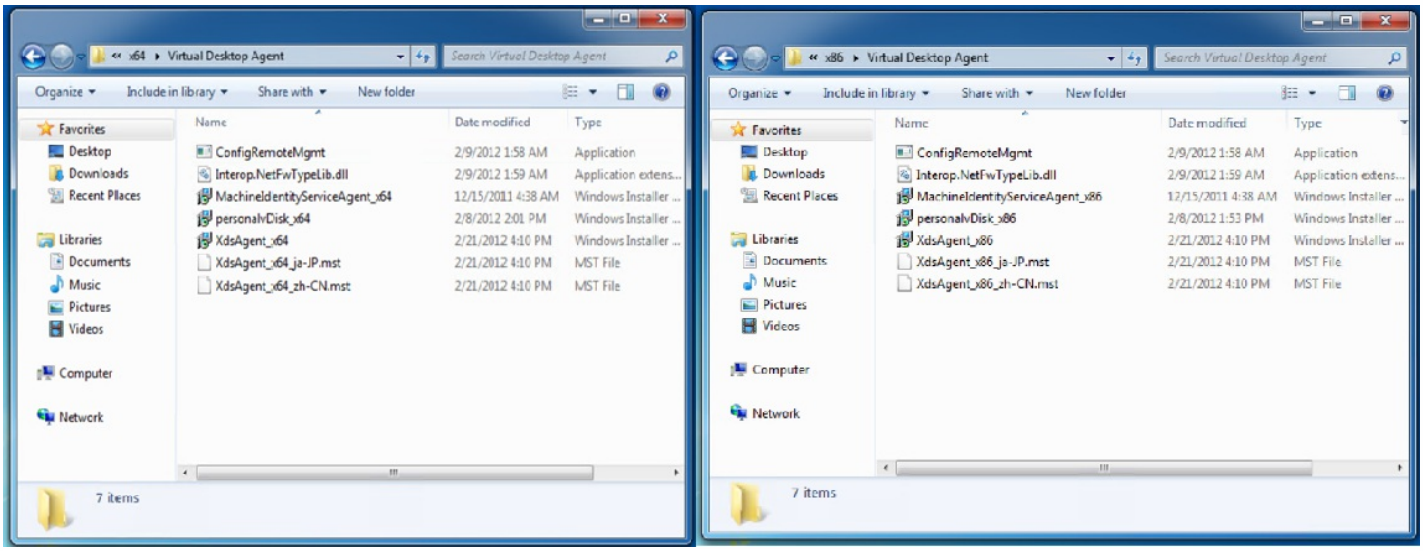
は、変更された環境構成設定が含まれています。Personal vDiskを再インストールしたら、バックアップしたレジストリ情報を使用して、必要に応じて値を変更してください。

Personal vDiskをアンインストールする時の重要な考慮事項

Personal vDiskがWindows 7（64ビット）で基本イメージにインストールされていると、アンインストールできないことがあります。この問題を解決するには、以下の手順でPersonal vDiskを削除してからアップグレードしてください。

1. XenAppおよびXenDesktopメディアからvDiskインストーラーの適切なコピーを選択します。次のいずれかの場所（アップグレードされた仮想マシンが32ビットか64ビットかによる）のXenAppおよびXenDesktop ISOから最新のPersonal vDiskのMSIインストーラーを見つけます。

- 32ビット：XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
- 64ビット：XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi

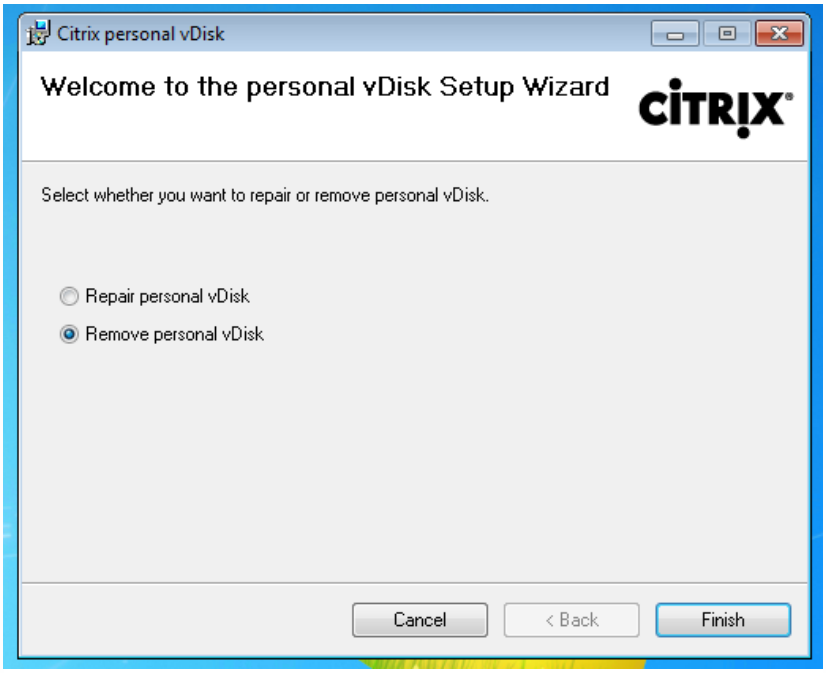


2. 既存のPersonal vDiskインストールを削除します。手順1で見つけたPersonal vDiskのMSIインストーラーパッケージを選択します。Personal vDiskのセットアップ画面が開きます。

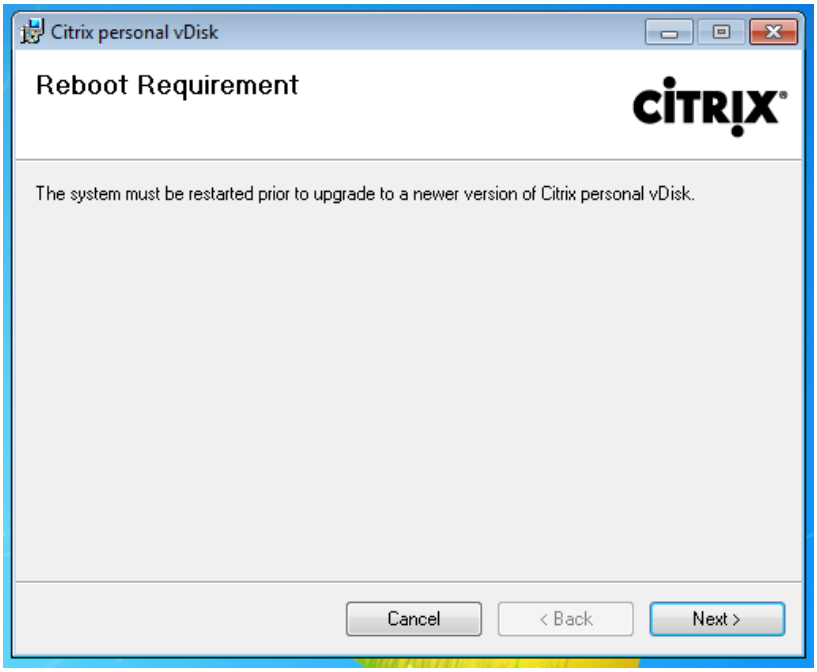
3. ［Remove personal vDisk］を選択します。

4. **［完了］**をクリックします。

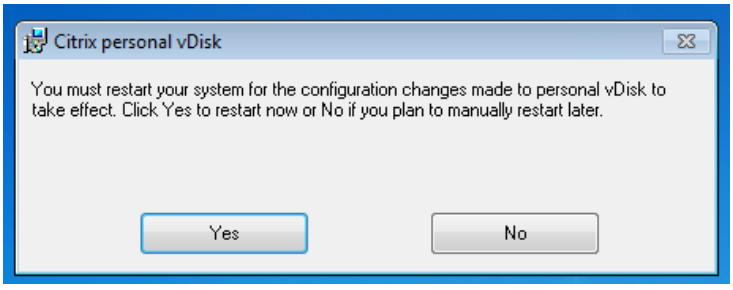
© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. ［再起動してください］ページが開きます。 **[Next]** をクリックします。



6. **[Yes]** をクリックしてシステムを再起動し、構成の変更を適用します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

構成と管理

Dec 05, 2017

このトピックでは、Personal vDisk（PvD）環境を構成したり管理したりするときに考慮すべき内容について説明します。また、推奨される構成やタスクについても説明します。

Windowsレジストリの編集が必要な操作を行う場合の注意事項。
注意： レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、 Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による 障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、 レジストリを編集してください。

メインのPersonal vDiskのサイズを決定するときは、以下の要因について考慮します。

- **ユーザーがPersonal vDisk上にインストールするアプリケーションのサイズ**
  Personal vDiskでは、再起動時にアプリケーション領域（UserData.v2.vhd）の空き容量が確認されます。空き容量が全体の10%未満になると、未使用のプロファイル領域（デフォルトではPドライブの使用可能領域）を使ってアプリケーション領域が拡張されます。このときアプリケーション領域に追加されるスペースは、アプリケーション領域とプロファイル領域で使用可能な合計空き容量の約50%です。

  たとえば、10GBのPersonal vDisk上のアプリケーション領域が5GBでプロファイル領域の空き容量が3GBの場合、アプリケーション領域の4.7GBが消費されたときに自動的に追加されるスペースは以下の式で算出されます。

  追加されるスペース = （5.0 – 4.7）÷2 + 3.0÷2 = 1.65GB

  アプリケーション領域に追加されるスペースのサイズは概算値です。これは、ログやオーバーヘッド用にわずかな余分スペースが追加されるためです。この計算およびサイズ調整は、各再起動時に行われます。

- **ユーザープロファイルのサイズ（ほかのプロファイル管理ツールを使用しない場合）**
  アプリケーションに必要な容量に加えて、ユーザープロファイルの格納に十分な容量がPersonal vDisk上にあることを確認してください。また、リダイレクトされないユーザーフォルダー（マイドキュメントやマイミュージックなど）の容量についても考慮する必要があります。既存のプロファイルのサイズを確認するには、コントロールパネルから［システムのプロパティ］（sysdm.cpl）を開きます。

  プロファイルをリダイレクトする一部のツールを使用すると、実際のプロファイルデータの代わりにスタブファイル（センチネルファイル）が格納されます。これらのプロファイル管理ツールでは初期状態でディスクが消費されていないように見えますが、各スタブファイルについて1ファイルディレクトリエントリがファイルシステム上に作成されます（通常、各ファイルについて4KB程度）。このようなプロファイル管理ツールを使用する場合は、スタブファイルではなく実際のプロファイルデータのサイズを考慮する必要があります。

  エンタープライズクラスのファイル共有アプリケーション（ShareFile、Dropboxなど）により、Personal vDisk上のユーザープロファイル領域がデータの同期に使用される場合があります。このようなアプリケーションを使用する場合は、同期データのサイズも考慮する必要があります。

- **Personal vDiskインベントリを含んでいるテンプレートVHDで使用される容量**
  テンプレートVHDには、Personal vDiskインベントリデータ（マスターイメージの内容に対応するセンチネルファイル）が含まれています。Personal vDiskのアプリケーション領域はこのVHDから作成されます。各センチネルファイルやフォルダーによりファイルディレクトリエントリが構成されるため、ユーザーがアプリケーションをインストールしていなくても、Personal vDiskのアプリケーション領域がテンプレートVHDの内容により消費されます。テンプレートVHDのサイズは、イ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンベントリを実行した後でマスターイメージを参照すると確認できます。または、以下の式でおおよそのサイズを算出でき
ます。

テンプレートVHDのサイズ＝マスターイメージ上のファイル数×4KB

マスターイメージ上のファイルおよびフォルダーの数を確認するには、そのイメージのCドライブを右クリックして[プロパティ]を選択します。たとえば、イメージに250,000個のファイルがある場合、テンプレートVHDのサイズはおよそ1,024,000,000バイト（ちょうど1GB）になります。つまり、Personal vDiskのアプリケーション領域のうち1GB弱のディスクスペースには、アプリケーションをインストールできません。

- **Personal vDiskイメージの更新時に使用される容量**
  Personal vDiskイメージを更新するときには、イメージの2つのバージョンの差分やユーザーによるPersonal vDiskの変更内容を統合するために十分な空き領域が、Personal vDisk（デフォルトでPドライブ）のルートに必要になります。通常、Personal vDiskの200～300MBがこの目的で予約されます。ただし、Pドライブに追加されるデータの量によっては、イメージの更新に必要な容量を確保できなくなることがあります。Personal vDiskプール統計スクリプト（XenDesktopインストールメディアの Support/Tools/Scriptsフォルダー）またはPersonal vDiskイメージ更新監視ツール（Support/Tools/Scripts\PvdToolフォルダー）を使用して、更新対象のカタログから空き領域が少ないPersonal vDiskディスクを特定できます。

  アンチウイルス製品をインストールすると、インベントリや更新に時間がかかる場合があります。CtxPvD.exeおよびCtxPvDSvc.exeをアンチウイルス製品の除外の一覧に追加すると、パフォーマンスを向上させることができます。これらのファイルは、C:\Program Files\Citrix\personal vDisk\binにあります。ウイルスチェックの対象からこれらの実行可能ファイルを除外すると、インベントリおよびイメージ更新の処理パフォーマンスが最大で10倍に向上することがあります。

- **予定外の追加容量（計画外のアプリケーションのインストールなど）**
  ユーザーが追加のアプリケーションをインストールできるように、（特定サイズまたは全体に対する割合で）追加領域を加算することを検討してください。

管理者は、 Pドライブに対するVHDの 相対的なサイズを決定するときの自動サイズ変更アルゴリズムを手動で調整できます。これを行うには、VHDの初期サイズを設定します。たとえば、 ユーザーがインストールするアプリケーションの数が多いために、 デフォルトのアルゴリズムで決定されるサイズでは足りなくなることがわかっている場合などには、この機能が役に立ちます。 この場合、アプリケーションをインストールするための領域が足りなくならないように、 アプリケーション領域の初期サイズを増やします。

可能な場合は、 マスターイメージ上でVHDの初期サイズを調整します。または、仮想デスクトップ上でVHDのサイズを調整して、 ユーザーのアプリケーションのインストールに必要な領域 を確保することもできます。ただし、この方法では各仮想デスクトップ上で 個別に調整する必要があります。作成済みのマシンカタログで VHDの初期サイズを調整することはできません。

VHDには、 アンチウイルス定義ファイルを保存するのに十分なサイズを設定してください。通常、アンチウイルス定義ファイルのサイズは小さくありません。

HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\personal vDisk\Configで、以下のレジストリキーを設定します（これ以外のレジストリキーは変更しないでください）。 MinimumVHDSizeInMBを除き、 すべての値はマスターイメージ上で設定します（MinimumVHDSizeInMBは マシン単位で変更できます）。マスターイメージ上で設定された値は、 次回イメージ更新時に適用されます。

- **MinimumVHDSizeMB**
  Personal vDiskのアプリケーション領域（Cドライブ）の最小サイズをMB単位で指定します。 新しいサイズは、既存のサイズよりも大きなものにする必要がありますが、ディスクのサイズからPvDReservedSpaceMBの値を差し引いたものよりも小

© 1999-2017 Citrix Systems, Inc. All rights reserved.

さくする必要があります。

この値を大きくすると、Personal vDisk上のプロファイル領域からCドライブに空き領域が割り当てられます。 この設定は、Cドライブの現在の使用サイズよりも小さい値を指定したり、EnableDynamicResizeOfAppContainerに0を設定したりすると無視されます。

デフォルト値：2048

- EnableDynamicResizeOfAppContainer
  動的サイズ変更アルゴリズムを有効または無効にします。
  - 1を設定すると、アプリケーション領域（Cドライブ上）の空き容量が10%未満になったときにその領域のサイズが自動的に調整されます。1または0を設定できます。変更後、仮想マシンの 再起動が必要です。
  - 0を設定すると、XenDesktop 7.x以前 で使用されていた方法でVHDのサイズが決定されます。

  デフォルト値=1

- EnableUserProfileRedirection
  ユーザープロファイルのPersonal vDiskへのリダイレクトを有効または無効にします。
  - 1を設定すると、ユーザーのプロファイルがPersonal vDiskドライブ（デフォルトでPドライブ）にリダイレクトされます。 通常、各プロファイルは、P:\Usersフォルダーの、標準 Windowsプロファイルに対応するサブフォルダーにリダイレクトされます。これにより、ユーザーの デスクトップのリセットが必要になった場合でもプロファイルが保持されます。
  - 0を設定すると、Personal vDisk上のPvDReservedSpaceMBのサイズを差し引いた全領域がCドライブ（Personal vDiskのアプリケーション領域）に割り当てられ、Personal vDiskドライブ（Pドライブ）は Windowsエクスプローラーに表示されなくなります。Citrix Profile managementやほかの移動プロファイル管理ツールを使用する場合は、この値に 0を設定してプロファイルのリダイレクトを無効にすることをお勧めします。
    この 設定により、プロファイルはPersonal vDiskにリダイレクトされずにC:\Users内に保持されます。このため、Profile managementなどの移動プロファイル管理ツールでプロファイルを管理できるようになります。

    この設定 により、Pドライブの領域がすべてアプリケーションに割り当てられます。

    移動 プロファイル管理ツールを使用する環境でのみ 0を設定してください。移動プロファイル管理ツールを使用 しない環境でこのレジストリ設定を使用すると、Personal vDiskをリセットしたときに プロファイルが削除されてしまいます。

  この設定は、イメージの更新時には変更しないでください。イメージ更新時に設定値を1から0に変更すると既存のプロファイルが移動されないままPersonal vDiskの全領域がCドライブに割り当てられ、Personal vDiskが非表示になってしまいます。

  この値は、マシンカタログを展開する前に設定してください。 マシンカタログを展開した後で値を変更することはできません。

  重要：XenDesktop 7.1以降では、イメージの更新時にこの値の変更が適用されなくなっています。 このレジストリキーは、プロファイルの元になるカタログを最初に作成するときに設定してください。 この設定を後で変更することはできません。

  デフォルト値=1

- PercentOfPvDForApps
  Personal vDiskのアプリケーション領域（Cドライブ）とプロファイル領域との割合を指定します。 この値は新しい仮想マシンの作成時に適用され、またEnableDynamicResizeOfAppContainerが0の場合はイメージの更新時にも適用されます。

  PercentOfPvDForApps設定に対する変更を適用するには、EnableDynamicResizeOfAppContainerを0に設定する必要があります。 EnableDynamicResizeOfAppContainerは、デフォルトで1（有効）に設定されています。このため、アプリケーショ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ン領域（AppContainer。表示上はCドライブ）は空き領域が10%未満になった時点で動的に拡張されます。

PercentOfPvDForAppsの値を増やしても、AppContainerの拡張が許可される最大領域が増えるだけです。 設定した値がすぐに適用されるわけではありません。また、この割り当て比率の設定はマスターイメージ内で構成する必要があります。これにより、次回イメージ更新時に設定が反映されます。

EnableDynamicResizeOfAppContainerを1に設定したままマシンカタログを生成した場合は、マスターイメージ内でこの値を0に変更して、適切な割り当て比率を構成してください。 構成する割り当て比率は、Cドライブの現在の割り当てサイズよりも大きな値である必要があります。

この値を0に設定すると、管理者が割り当て比率を完全に制御できます。 つまり、ユーザーが消費する領域サイズにかかわらずCドライブのサイズを完全に制御でき、動的なサイズ調整は行われません。

デフォルト値：50%（2つの領域に同じサイズが割り当てられます）

- **PvDReservedSpaceMB**
  Personal vDiskログおよびほかのデータ用に予約されるPersonal vDisk上の領域をMB単位で指定します。

  XenApp 6.5（またはそれ以前のバージョン）が動作する環境でアプリケーションのストリーム配信機能を使用する場合は、Rade Cacheのサイズに応じてこの値を増やしてください。

  デフォルト値=512

- **PvDResetUserGroup**
  Citrix XenDesktop 5.6にのみ適用され、Personal vDiskのリセットを許可するユーザーのグループを指定します。 これ以降のバージョンのXenDesktopでは、管理権限の委任機能を使用します。

そのほかの設定：

- **Windows Updateサービス** ：マスターイメージでは、Windows Updateのオプションとして ［更新プログラムを確認 しない］を選択し、Windows Updateサービスを ［無効］に設定します。Windows Updateサービスを実行する必要がある場合でも、 ［更新プログラムを 確認しない］を選択することで更新プログラムがマシン上にインストールされることを防ぐことができます。
  たとえば、WindowsストアからWindowsストアアプリをインストールする場合は、このサービスを実行しておく必要があります。

- **Windowsの更新プログラム**：Internet Explorerを 含むWindowsの更新プログラムをマスターイメージに適用しておきます。
- **再起動が必要な更新プログラム** ：Windowsの更新プログラムの中には、インストールを完了するために何回かの再起動が必要になるものがあります。 Personal vDiskインベントリを収集する前に、 マスターイメージを正しく再起動して、適用した更新プログラムが完全にインストールされたことを 確認してください。
- **アプリケーションの更新プログラム**：マスターイメージ上のアプリケーションに必要な更新プログラムを適用しておくと、ユーザーの vDiskに必要なディスク領域を節約できます。また、各ユーザーのvDisk上のアプリケーションを個別に更新する 手間も省けます。

一部のアプリケーションでは 、Personal vDiskによるユーザー環境で問題が発生する場合があります。このような問題を避けるには、 管理者がそれらのアプリケーションを個々のマシン上ではなくマスターイメージ上に インストールする必要があります。さらに、Personal vDisk環境で正しく動作する場合でも、 特定の種類のアプリケーションについてはマスターイメージ上にインストール することをお勧めします。

マスターイメージ上 へのインストールが必須のアプリケーションは次のとおりです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- エージェントおよび クライアントソフトウェア（System Center Configuration Managerエージェント、App-V Client、Citrix Receiverなど）
- 早期起動ドライバーをインストールまたは変更する アプリケーション
- プリンターやスキャナーのソフトウェアやドライバーをインストールする アプリケーション
- Windowsネットワークスタックを変更する アプリケーション
- VMware ToolsやXenServer Toolsなどの 仮想マシンツール

マスターイメージ上へのインストールが推奨される アプリケーションは次のとおりです。
- 多くのユーザーに配信する アプリケーション。以下のアプリケーションは、 更新機能を無効にしてから配信します。
  - ボリュームライセンスを使用する、 Microsoft OfficeやMicrosoft SQL Serverなどのエンタープライズアプリケーション。
  - Adobe Reader、Firefox、Chromeなど、ユーザーに共通の アプリケーション。
- SQL Server 、Visual Studio、アプリケーションフレームワーク（ .NETなど）などのサイズの大きなアプリケーション。

Personal vDiskのマシンに ユーザーがインストールするアプリケーションについて、以下の 推奨事項および制限事項があります。ただし、管理者権限を持つユーザーに対しては、 一部の項目を強制できない場合があります。
- ユーザーが マスターイメージからアプリケーションをアンインストールして、そのアプリケーションを自分の Personal vDisk上にインストールすることは避けてください。
- 管理者が マスターイメージのイメージ上のアプリケーションを更新したりアンインストールしたりするときは、十分に注意してください。管理者が マスターイメージ上にアプリケーションをインストールした後で、そのアプリケーションバージョン用の アドオンソフトウェア（プラグインソフトウェアなど）をユーザーがインストールしている場合があります。このような 依存関係が存在する場合、そのイメージ上のアプリケーションを更新したりアンインストールしたりすると、ユーザーのアドオンソフトウェアが正しく動作しなくなることがあります。たとえば、マスターイメージ上に インストールされているMicrosoft Office 2010に対応するVisio 2010をユーザーが自分のPersonal vDisk上にインストールした場合、マスターイメージ上のOfficeを更新すると ローカルのVisioが動作しなくなることがあります。
- ハードウェア 依存のライセンスを使用するソフトウェア（ドングルを使用したり署名ベースの ハードウェアを使用したりするもの）はサポートされません。

Provisioning ServicesとPersonal vDiskを併用する場合は、以下の考慮事項があります。
- Studioの［管理者］ノードで、Soap Serviceアカウントを追加してマシン管理者以上の役割を割り当てます。これにより、Provisioning Services（PVS）のvDiskを実稼働段階に昇格するときにPersonal vDiskデスクトップが準備中の状態になります。
- Personal vDiskを更新するには、Provisioning Serviceのバージョン機能を使用する必要があります。更新したバージョンが実稼働段階に昇格するときに、Soap ServiceによりPersonal vDiskデスクトップが準備中状態になります。
- Personal vDiskのサイズは、Provisioning Serviceの書き込みキャッシュディスクよりも常に大きくなくてはなりません。Personal vDiskがProvisioning Serviceの書き込みキャッシュより小さいと、Personal vDiskディスクが書き込みキャッシュとして使用されてしまう場合があります。
- デリバリーグループを作成した後では、Personal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）またはサイズ変更とプール統計のスクリプト（personal-vdisk-poolstats.ps1）を使用してPersonal vDiskを監視することができます。

書き込みキャッシュディスクのサイズを正しく設定してください。Personal vDiskがアクティブな場合、ユーザーによる多くの書き込み処理（変更内容）がPersonal vDisk上にリダイレクトされます。このため、Provisioning Servicesの書き込みキャッシュディスクのサイズを小さく設定できる場合があります。ただし、Personal vDiskがアクティブでないとき（イメージ更新時など）にProvisioning Services書き込みキャッシュディスクのサイズが足りなくなり、マシンがクラッシュすることがあります。

Provisioning Servicesのベストプラクティスに従ってProvisioning Services書き込みキャッシュディスクのサイズを設定し、さら

© 1999-2017 Citrix Systems, Inc. All rights reserved.

にマスターイメージ上のテンプレートVHDの2倍のサイズを統合（マージ）処理用に追加することをお勧めします。マージ処理ですべての領域が使用されることはまれですが、可能性はあります。

Personal vDiskが有効なマシンのカタログをProvisioning Servicesで展開する場合は、以下の点に注意してください。

- Provisioning Servicesのドキュメントの手順に従います。
- Studioのホスト接続の設定を編集して、同時操作を制限することができます。方法については、後述の説明を参照してください。
- アプリケーションやほかのソフトウェアをインストールまたはアップデートしてProvisioning Services vDiskを再起動した後でそのvDiskを更新した場合は、Personal vDiskインベントリを実行して仮想マシンをシャットダウンしてください。その後で、新しいバージョンを実稼働モードに昇格させます。そのカタログ内のPersonal vDiskデスクトップが自動的に準備中の状態になります。準備中にならない場合は、Soap ServiceアカウントにControllerのマシン管理者またはそれ以上の権限が付与されていることを確認してください。

Provisioning Servicesのテストモード機能を使用すると、更新済みのマスターイメージを使用するマシンのテストカタログを作成できます。このテストカタログで実用性をテストしてから、それを実稼働用に昇格させることができます。

Personal vDiskが有効なマシンのカタログをMachine Creation Services（MCS）で展開する場合は、以下の点に注意してください。

- XenDesktopのドキュメントの手順に従います。
- マスターイメージ作成後にPersonal vDiskインベントリを実行し、仮想マシンの電源を切ります（仮想マシンの電源を切らないとPersonal vDiskが正しく機能しません）。次に、マスターイメージのスナップショットを作成します。
- マシンカタログの作成ウィザードで、Personal vDiskのサイズとドライブ文字を指定します。
- デリバリーグループを作成した後では、Personal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）またはサイズ変更とプール統計のスクリプト（personal-vdisk-poolstats.ps1）を使用してPersonal vDiskを監視することができます。
- Studioのホスト接続の設定を編集して、同時操作を制限することができます。方法については、後述の説明を参照してください。
- マスターイメージを更新する場合は、マスターイメージ上のアプリケーションやほかのソフトウェアをアップデートした後でPersonal vDiskインベントリを実行し、仮想マシンの電源を切ります。次に、マスターイメージのスナップショットを作成します。
- Personal vDisk Image Update Monitoring Toolまたはpersonal-vdisk-poolstats.ps1スクリプトを使用して、更新したマスターイメージが展開される各仮想マシン上に十分な領域があることを確認します。
- マシンカタログを更新すると、各Personal vDiskデスクトップが準備中の状態になり、マスターイメージの更新内容が適用されます。各デスクトップは、マシン更新時に指定したロールアウト方法に基づいて更新されます。
- Personal vDisk Image Update Monitoring Toolまたはpersonal-vdisk-poolstats.ps1スクリプトを使用して、「準備中」状態のPersonal vDiskを監視します。

vDiskから ファイルやフォルダーを除外するには、以下の規則ファイルを使用します。この方法は、展開済みの Personal vDiskで使用できます。この規則ファイルの名前は custom_*_rules.template.txtで、configフォルダーに格納されています。これらの ファイルの使用方法については、各規則ファイルのコメントを参照してください。

Personal vDiskを有効にしてマスターイメージを更新したら、ディスクのインベントリを更新し（この操作は「インベントリの実行」と呼ばれます）、新しいスナップショットを作成することが重要です。

マスターイメージを管理するのは（ユーザーではなく）管理者であるため、管理者がアプリケーションをインストールしたと

© 1999-2017 Citrix Systems, Inc. All rights reserved.

きにその管理者のプロファイルにバイナリファイルが配置されると、共有された仮想デスクトップ（プールされたマシンカタログおよびプールされたPersonal vDiskマシンカタログのデスクトップも含む）のユーザーがそのアプリケーションを使用できなくなります。このようなアプリケーションは、ユーザーが自分でインストールする必要があります。

以下の各手順を実行した後で、イメージのスナップショットを作成することをお勧めします。

1. マスターイメージを更新します。つまり、オペレーティングシステムの更新プログラムや必要なアプリケーションをインストールして、マシンのシステム構成を実行します。
   Personal vDiskを使用するWindows XPベースのマスターイメージの場合は、ソフトウェアインストールの確認メッセージや未署名のドライバーの使用に対するメッセージなど、何らかのダイアログボックスが開いていないことを確認します。この環境のマスターイメージでダイアログボックスが開いていると、VDAをDelivery Controllerに登録できません。未署名のドライバーに対するメッセージは、コントロールパネルで無効にすることができます。たとえば、［システム］、［ハードウェア］、［ドライバの署名］の順に選択し、警告メッセージを無視するオプションを選択します。
2. マシンをシャットダウンします。Windows 7マシンの場合は、Citrix Personal vDiskがシャットダウンをブロックするときに［キャンセル］をクリックします。
3. ［Citrix Personal vDisk］ダイアログボックスの［インベントリの更新］をクリックします。この処理が完了するまで数分間かかることがあります。
   重要： この処理の後のシャットダウンを中断すると、（軽微なイメージ更新であっても）Personal vDiskのインベントリがマスターイメージと一致しなくなります。これによりPersonal vDiskが機能しなくなります。シャットダウンを中断した場合は、マシンを再起動してから再度シャットダウンし、メッセージが表示されたら［インベントリの更新］をもう一度クリックします。
4. インベントリ操作によりマシンがシャットダウンしたら、マスターイメージのスナップショットを作成します。

インベントリをネットワーク共有上にエクスポートして、それをマスターイメージ上にインポートできます。詳しくは、「Personal vDiskインベントリのエクスポートとインポート」を参照してください。

デスクトップや アプリケーションを提供するマシンの電源状態は、Citrix Broker Serviceにより制御されます。このBroker Serviceは、 Delivery Controllerを介していくつかのハイパーバイザーを制御することもできます。Broker Serviceの電源操作機能により、Controllerとハイパーバイザー 間の相互操作が制御されます。ハイパーバイザーに過剰な負荷がかかること を防ぐため、マシンの電源状態に対する変更操作に優先度が割り当てられ、これにより ハイパーバイザーの同時操作が制御されます。これを設定するには、 次の手順に従います。これらの値を変更するには、 Studioの［ホスト］ノードで［接続の編集］ダイアログボックスを開き、［詳細設定］ページを使用します。

ホスト 接続の同時操作を制御するには、次の手順に従います。

1. Studioのナビゲーションペインで ［構成］>［ホスト］の順に選択 します。
2. 接続を選択し、［操作］ペインの ［接続の 編集］を選択します。
3. 必要に 応じて、以下の値を変更します。
   - **同時操作（すべての 種類）** - 同時に実行可能な電源操作の上限値を 指定します。この値は、絶対値およびハイパーバイザーへの接続に対する パーセンテージで指定できます。2つの設定値のうちより小さい値が 適用されます。
     デフォルト値 ：絶対値100、20%
   - **Personal vDiskストレージインベントリの同時更新** - 同時に実行可能なPersonal vDiskの 電源操作の上限値を指定します。この値は、絶対値および接続に対する パーセンテージで指定できます。2つの設定値のうちより小さい値が適用されます。
     デフォルト値 ：絶対値50、25%

     絶対値を 計算するには、エンドユーザーのストレージでサポートされる 合計IOPS（1秒あたりの読み取り/書き込み回数）を使用します。 さらに、各仮想マシンのIOPS（IOPS/VM）を350として、ストレージで同時に アクティブにできる

© 1999-2017 Citrix Systems, Inc. All rights reserved.

仮想マシン数を計算します。合計 IOPS値をIOPS/VM値で除算するとこの値が算出されます。

たとえば 、エンドユーザーのストレージのIOPSが14000の場合、同時にアクティブにできる仮想マシン数は40（14000÷350＝40）になります。

- **1分あたりの最大新規 操作** - ハイパーバイザーに送信可能な新規電源操作の1分あたりの 上限値を指定します。この値は、設定値で指定します。
  デフォルト値 ：10

これらの設定について 最適な値を確認するには、以下の操作を行います。

1. デフォルトの値を 使用して、テストカタログの単一イメージ更新にかかる合計応答時間を 計測します。つまり、イメージ更新の開始時刻（T1）から カタログ内の最後のマシンでのVDAのControllerへの登録時刻 （T2）までの時間を計測します（合計応答時間＝T2－T1）。
2. イメージ更新時の ハイパーバイザーストレージのIOPS（1秒あたりの読み取り/書き込み回数）を 計測します。この値を最適化の基準値として使用します。通常は デフォルトの設定値を使用しますが、 IOPSの限界まで達する場合はより小さい値を設定します。
3. 以下の手順に従って ［Personal vDiskストレージインベントリの同時更新］ の値を変更します（ほかのすべての設定値はそのまま保持します）。
   1. 値を 10ずつ増やし、そのたびに合計応答時間を計測します。合計 応答時間が低下または一定化するまでこれを 繰り返します。
   2. 値を 10ずつ増やしても合計応答時間が改善されない場合は、値を10ずつ 減らし、そのたびに合計応答時間を 計測します。合計応答時間が一定化し、改善されなくなるまで これを繰り返します。これにより、最適なPersonal vDisk電源操作値を求めます。
4. 最適な Personal vDisk電源操作値を確認したら、 ［同時操作 （すべての種類）］ および［1分あたりの最大新規操作］の設定値を1つずつ調整します。これらの 設定でも、上記の（値を10ずつ増減させる）方法で値を変更して 効果を確認します。

System Center Configuration Manager（Configuration Manager）2012を使用する場合は特別な 構成が不要で、ほかのマスターイメージ アプリケーションと同じ方法でインストールできます。以下の説明は、System Center Configuration Manager 2007にのみ適用されます。Configuration Manager 2007より 前のバージョンはサポートされません。

Personal vDisk環境で Configuration Manager 2007エージェントソフトウェアを使用するには、 以下の操作を行います。

1. マスターイメージに クライアントエージェントをインストールします。
   1. マスターイメージに Configuration Managerクライアントをインストールします。
   2. ccmexec service （SMS Agent）を停止して、さらに無効に設定します。
   3. ローカルコンピューターの 証明書ストアから、SMSまたはクライアント証明書を削除します。これを行うには、 以下の手順に従います。
      - 混在モード：証明書（ローカルコンピューター）\SMS\証明書
      - ネイティブモード
        - 証明書（ローカルコンピューター）\個人\証明書
        - 証明機関（通常は内部の公開キー基盤）により 発行されたクライアント証明書を削除します。
   4. C:\Windows\smscfg.iniを削除するか、 名前を変更します。
2. クライアント固有の 情報を削除します。
   1. C:\Windows\System32\CCM\Logsの ログファイルを削除または移動します（オプション）。
   2. Virtual Delivery Agentが インストールされていない場合はインストールして、Personal vDiskの インベントリを実行します。
   3. マスターイメージを シャットダウンしてスナップショットを作成し、この スナップショットを使用してマシンカタログを作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Personal vDiskを 検証して、サービスを起動します。各Personal vDisk デスクトップの初回起動時に、以下の手順を1回実行します。ドメインのグループポリシーオブジェクトを 使用してこれを実行することもできます。
   - Personal vDiskが アクティブであることを確認します。これを行うには、レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\personal vDisk\config\virtualが存在することを確認します。
   - ccmexec service （SMSエージェント）を［自動］にして、このサービスを起動します。 Configuration Managerクライアントが Configuration Managerサーバーと通信して、 新しい固有の証明書および GUIDが取得されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ツール

Dec 05, 2017

以下のツールおよびユーティリティを使ってPersonal vDiskの機能を構成、管理、および監視できます。

Personal vDiskに付属の規則 を使用して、Personal vDiskイメージの以下のデフォルトの動作を 変更できます。

- Personal vDisk上の ファイルの表示/非表示
- ファイルに対する変更内容のマージ方法
- ファイルの書き込みの 許可/禁止

カスタムの規則ファイルおよびコピーオンライトについて 詳しくは、各ファイル内に記述されている コメントを参照してください。これらのファイルは、Personal vDiskをインストールした マシンのC:\ProgramData\Citrix\personal vDisk\Configにあります。「custom_*」という名前のファイルには、 規則の説明と規則を有効にする方法が記述されています。

Personal vDiskのサイズを監視したり管理したりするための2つのスクリプトが 用意されています。これらのスクリプトは、XenDesktopインストールメディアの Support\Tools\Scriptsフォルダーに収録されています。また、Support\Tools\Scripts\PvdToolフォルダーに収録されているPersonal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）を 使用することもできます。詳しくは、 http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ を参照してください。

resize-personalvdisk-pool.ps1スクリプトでは、カタログ内のすべての デスクトップのPersonal vDiskのサイズを増やすことができます。このスクリプトを使用するには、Studioが動作するマシン上に、使用するハイパーバイザーに対応する以下のスナップインまたはモジュールをインストールする 必要があります。

- XenServer ：XenServerPSSnapin
- vCenter： vSphere PowerCli
- System Center Virtual Machine Manager：VMMコンソール

personal-vdisk-poolstats.ps1スクリプトでは、複数のPersonal vDiskに対してアプリケーション 領域とユーザープロファイル領域の容量を確認したり、イメージの更新状態を確認したりできます。イメージを更新する前にこの スクリプトを実行すると、更新の失敗の原因となる 空き容量不足のデスクトップを特定することができます。このスクリプトを使用するには、Personal vDisk デスクトップのファイアウォールで、 Windows Management Instrumentationからの受信規則（WMI受信）が有効になっている必要があります。この規則は、マスターイメージまたはGPOを使用して有効にできます。

イメージの更新に 失敗すると、［Update］列にその原因が表示されます。

問題のあるアプリケーションのインストールなどが原因でユーザーのデスクトップが 破損した場合は、 管理者がPersonal vDiskのアプリケーション領域を工場出荷時のデフォルト （つまり空の状態）にリセットできます。この領域をリセットしても、ユーザープロファイルには影響しません。

Personal vDiskの アプリケーション領域をリセットするには、以下のいずれかを行います。

- ユーザーのデスクトップに管理者としてログオンします。コマンドラインで C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Resetを実行します。
- Citrix Directorでユーザーの デスクトップを選択します。 ［Personal vDiskを リセット］をクリックして ［OK］をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

イメージの更新 プロセスは、Personal vDiskデスクトップに新しいイメージをロールアウトする操作に組み込まれています。これにより、新しい基本イメージで既存のPersonal vDiskを使用できるようになります。 Machine Creations Services（MCS）を使用する展開環境では、アクティブな仮想マシンから インベントリをネットワーク共有上にエクスポートして、それを マスターイメージ上にインポートできます。マスター イメージでは、このインベントリ情報に基づいて差分が計算されます。インベントリのエクスポート/インポート機能を使用することは必須ではありませんが、これによりイメージ更新プロセスの全体的なパフォーマンスが 向上します。

インベントリの エクスポート/インポート機能を使用するには、管理者権限が必要です。必要に応じて、「net use」コマンドを実行して、エクスポート/インポート機能で使用するファイル共有に対して認証します。このとき、 エクスポートまたはインポートで使用するすべてのファイル共有にユーザー環境からアクセスできることが必要です。

- インベントリをエクスポートするには、Personal vDisk（Version 7.6以降）が有効な VDAのマシン上で、管理者として次のエクスポートコマンドを実行します。
  Ctxpvdsvc.exe exportinventory “<path-to-export-location>”

  現在のインベントリの場所が検出され、で指定した場所のExportedPvdInventoryフォルダーにインベントリがエクスポートされます。 このコマンドにより、以下のようなメッセージが出力されます。
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory
  \\share location\ExportedInventory
  Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS
  ...
  Exporting current inventory to location \\ ….
  ...
  Deleting any pre-existing inventory folder at \\ ….
  .Successfully exported current inventory to location \\ …. Error code = OPS
- エクスポートしたインベントリを マスターイメージにインポートするには、管理者としてインポートコマンドを実行します。

インベントリをインポートするには

マスターイメージ上で、管理者として次のインポート コマンドを実行します。

Ctxpvdsvc.exe importinventory “<path-to-exported-inventory>”

<path to exported inventory>には、インベントリーファイルのフルパスを指定します。 通常は、<network location\ExportedPvdInventory>です。

exportinventoryオプションでエクスポートされたインベントリが 取得され、それが マスターイメージ上のインベントリストアにインポートされます。このコマンドにより、以下のようなメッセージが出力されます。
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
\\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \\share location\ExportedInventory\ExportedPvdInventory
…
Successfully added inventory \\share location\ExportedInventory\ExportedPvdInventory to the store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
インベントリのエクスポート先には、以下のファイルが出力されます。 これらのファイルは、マスターイメージ上の インベントリストアに同じ名前でインポートされます。

- Components.DAT
- files_rules
- folders_rules

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

© 1999-2017 Citrix Systems, Inc. All rights reserved.

表示、メッセージ、およびトラブルシューティング

Dec 05, 2017

レポートを介したPvDのモニター

Personal vDiskのユーザーデータ領域およびアプリケーション領域に対するユーザーによる変更は、Personal vDiskの診断ツールを使って監視できます。これらの変更には、ユーザーがインストールしたアプリケーションや修正したファイルが含まれます。変更内容はいくつかのレポートに保存されます。

1. 監視するマシン上で、**C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe**を実行します。
2. レポートとログを保存する場所を参照し、生成するレポートを選択して**[OK]** をクリックします。 以下のレポートを利用できます。

SOFTWAREハイブレポート：このレポートは次の2つのファイルを生成します。 Software.Dat.Report.txtとSoftware.Dat.delta.txtです。

Software.Dat.Report.txtファイルには、HKEY_LOCAL_MACHINE\Softwareハイブに対してユーザーが行った変更が記録されます。以下のセクションがあります。

- List of Applications installed on the base — レイヤー0にインストールされたアプリケーション
- List of user installed software - Personal vDiskのアプリケーション領域にユーザーがインストールしたアプリケーション
- List of software uninstalled by user - レイヤー0からユーザーが削除したアプリケーション

Software.Dat.delta.txtに記録される情報については、この表の「ハイブデルタレポート」を参照してください。

SYSTMハイブレポート：生成されるSYSTEM.CurrentControlSet.DAT.Report.txtファイルには、HKEY_LOCAL_MACHINE\Systemハイブに対してユーザーが行った変更が記録されます。以下のセクションがあります。

- List of user installed services - ユーザーがインストールしたサービスおよびドライバー
- Startup of following services were changed - ユーザーが起動の種類を変更したサービスおよびドライバー

SECURITYハイブレポート：生成されるSECURITY.DAT.Report.txtファイルにより、HKEY_LOCAL_MACHINE\Securityハイブでユーザーが行ったすべての変更が監視されます。

SAMハイブレポート：生成されるSAM.DAT.Report.txtファイルにより、HKEY_LOCAL_MACHINE\SAMハイブでユーザーが行ったすべての変更が監視されます。

ハイブデルタレポート：生成されるSoftware.Dat.delta.txtファイルにより、追加または削除されたすべてのレジストリキーおよび値と、HKEY_LOCAL_MACHINE\Softwareハイブでユーザーが変更したすべての値が記録されます。

Personal vDiskのログ： ログファイルPud-IvmSupervisor.log、PvDActivation.log、PvDSvc.log、PvDWMI.log、SysVol-IvmSupervisor.log、およびvDeskService-<#>.logは、デフォルトではP:\Users\\AppData\Local\Temp\PVDLOGSに生成されますが、選択した場所に移動されます。

Windowsオペレーティングシステムのログ：

- EvtLog_App.xmlおよびEvtLog_System.xmlは、Personal vDiskボリュームから生成されるXML形式のアプリケーションおよびシステムイベントログです。
- Setupapi.app.logおよびsetuperr.logには、Personal vDiskのインストールでmsiexec.exeを実行したときからのログメッセー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ジが記録されます。
- Setupapi.dev.logには、デバイスインストールログメッセージが記録されます。
- Msinfo.txtには、msinfo32.exeからの出力が記録されます。詳しくは、Microsoft社のドキュメントを参照してください。

ファイルシステムレポート：生成されるFileSystemReport.txtファイルにより、ユーザーがファイルシステムに対して行った変更が以下のセクションに記録されます。

- Files Relocated - ユーザーがPersonal vDiskに移動したレイヤー0のファイル。レイヤー0のファイルは、Personal vDiskが接続されたマシンによりマスターイメージから継承されます。
- Files Removed — ユーザーの操作（アプリケーションの削除など）によって非表示になったレイヤー0のファイル。
- Files Added（MOF、INF、SYS） — Personal vDiskに追加された拡張子.mof、.inf、または.sysを持つファイル（Visual Studio 2010などのアプリケーションのインストールにより登録された自動回復用のMOFファイルなど）。
- Files Added Other — Personal vDiskに追加されたそのほかのファイル（アプリケーションのインストールにより追加されたファイルなど）。
- Base Files Modified But Not Relocated — 変更されたレイヤー0のファイルで、Personal vDiskカーネルモードドライバーにより移動されないもの。

イメージの更新

Personal vDiskが有効なマシンをStudioのマシンカタログで選択すると、［PvD］タブにイメージ更新時の監視状態や推定完了時間、および進行状況が表示されます。イメージ更新時には、準備完了、準備中、待機中、失敗、および要更新のいずれかの状態が表示されます。

イメージの更新は、ディスクの空き容量不足やPersonal vDiskが見つからないなど、さまざまな要因で失敗することがあります。Studioでイメージ更新に失敗したことが示されると、トラブルシューティングに役立つエラーコードおよび説明が表示されます。Personal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）またはpersonal-vdisk-poolstats.ps1スクリプトを使用すると、イメージの更新状況を監視して、問題が生じた場合はそのエラーコードを取得できます。

イメージ更新に失敗した場合は、以下のログファイルを参照してトラブルシューティングを行います。
- Personal vDiskサービスログ：C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Personal vDiskアクティブ化ログ：P:\PVDLOGS\PvDActivation.log.txt

最新の情報は、これらのログファイルの末尾に記録されます。

Personal vDisk 7.6およびそれ以降では、以下のエラーメッセージが生成されます。
- **内部エラーが発生しました。詳しくは、Personal vDiskのログを参照してください。エラーコード %d（%s）**
  このメッセージは未分類のエラーに対して生成され、特定のエラーコードは提供されません。インベントリ作成またはPersonal vDisk更新時に予期されないエラーが発生すると、このメッセージが生成されます。
  - ログファイルを収集してCitrixのサポート担当者に問い合わせてください。
  - カタログ更新時にこのエラーが発生した場合は、カタログをロールバックして以前のマスターイメージの状態に戻してください。
- **規則ファイルに構文エラーがあります。詳しくは、ログを参照してください。**
  エラーコードは、2です。規則ファイルに構文エラーが含まれています。Personal vDiskのログファイルに、規則ファイルの名前と構文エラーの行番号が記録されます。規則ファイルの構文エラーを修正して再試行してください。
- **前のバージョンのマスターイメージに対応しているPersonal vDisk上のインベントリが破損しているか、読み取ることができません。**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

エラーコードは、3です。最新のインベントリは、\ProgramData\CitrixPvD\Settings\Inventory\VER-LASTのUserData.V2.vhdに格納されます。正常なPersonal vDiskマシンから「VER-LAST」フォルダーをインポートして、マスターイメージの最終バージョンに相当するインベントリを復元してください。

- **前のバージョンのマスターイメージに対応しているPersonal vDisk上のインベントリは、より新しいバージョンです。**
  エラーコードは、4です。前回のマスターイメージと新しいマスターイメージでPersonal vDiskのバージョンが異なるとこの問題が発生します。マスターイメージに最新バージョンのPersonal vDiskをインストールしてからカタログ更新を再試行してください。

- **変更ジャーナルのオーバーフローが検出されました。**
  エラーコードは、5です。インベントリ作成時にマスターイメージに加えられた変更の数が多いと、USNジャーナルのオーバーフローが発生します。何回か再試行してもこのエラーが発生する場合は、procmonを使用して、インベントリ作成時にサードパーティソフトウェアが大量のファイルを作成したり削除したりしていないかどうかを確認してください。

- **Personal vDiskで、ユーザー データの格納用にシステムにアタッチされたディスクが見つかりません。**
  エラーコードは、6です。まず、ハイパーバイザーのコンソールでPersonal vDisk用のディスクが仮想マシンにアタッチ（接続）されていることを確認してください。一般的に、このエラーはデータの漏洩を防ぐソフトウェアによりPersonal vDisk用ディスクへのアクセスが阻止されると発生します。Personal vDisk用のディスクが仮想マシンにアタッチされている場合は、データ漏洩を防ぐソフトウェアにそのディスクに対する除外規則を追加してください。

- **インストール後にシステムが再起動されていません。変更内容を実装するために再起動してください。**
  エラーコードは、7です。デスクトップを再起動してから再試行してください。

- **インストールが破損しています。Personal vDiskを再インストールしてください。**
  エラーコードは、8です。Personal vDiskを再インストールしてから再試行してください。

- **Personal vDiskのインベントリが最新の状態ではありません。マスターイメージ内でインベントリを更新してから再試行してください。**
  エラーコードは、9です。デスクトップのシャットダウン前にマスターイメージ内でPersonal vDiskインベントリが更新されていないとこのエラーが発生します。マスターイメージを再起動して、［Personal vDiskの更新］オプションを使用してデスクトップをシャットダウンし、その後で新しいスナップショットを作成してください。このスナップショットを使用してカタログを更新します。

- **Personal vDiskの起動時に内部エラーが発生しました。詳しくは、Personal vDiskのログを参照してください。**
  エラーコードは、10です。このエラーは、内部エラーまたはPersonal vDiskの破損により、Personal vDiskドライバーで仮想化セッションの起動に失敗すると発生します。Controllerを介してデスクトップを再起動してください。引き続き問題が発生する場合は、ログファイルを収集してCitrixのサポート担当者に問い合わせてください。

- **ユーザーのパーソナル設定を格納するディスクの検索時にPersonal vDiskでタイムアウトが発生しました。**
  エラーコードは、11です。このエラーは、再起動後30秒以内にPersonal vDiskドライバーでPersonal vDisk用のディスクを検出できない場合に発生します。通常、サポートされない種類のSCSIコントローラーを使用したり、ストレージで遅延が発生したりすると検出に失敗します。マシンカタログ内のすべてのデスクトップでこのエラーが発生する場合は、テンプレート仮想マシンやマスター仮想マシンのSCSIコントローラーの種類をPersonal vDiskでサポートされるものに変更してください。このエラーがマシンカタログ内の一部のデスクトップのみで発生する場合は、多くのデスクトップの同時起動などで一時的にストレージに遅延が発生していることが考えられます。ホスト接続の設定で、最大電源操作数を制限することを検討してください。

- **システムが正しくシャットダウンされなかったためPersonal vDiskが無効になっています。マシンを再起動してください。**
  エラーコードは、12です。このエラーは、Personal vDiskが有効なデスクトップで起動プロセスを完了できない場合に発生

© 1999-2017 Citrix Systems, Inc. All rights reserved.

します。デスクトップを再起動してください。問題が解決しない場合は、ハイパーバイザーのコンソールでデスクトップの起動状況を監視して、デスクトップがクラッシュしているかどうかを確認します。デスクトップが起動中にクラッシュする場合は、バックアップ（バックアップがある場合）からPersonal vDiskを復元するか、Personal vDiskをリセットしてください。

- **Personal vDiskをマウントするためのドライブ文字を使用できません。**
  エラーコードは、13です。このエラーは、管理者により指定されたマウントポイントにPersonal vDisk用のディスクをマウントできない場合に発生します。指定されたドライブ文字がほかのハードウェアにより使用されていると、Personal vDisk用ディスクのマウントに失敗します。Personal vDisk用にほかのマウントポイントを指定してください。

- **Personal vDiskカーネルモードドライバーのインストールに失敗しました。**
  エラーコードは、14です。Personal vDiskをインストールした後の初回インベントリ更新時に、ドライバーがインストールされます。一部のアンチウイルス製品では、インストーラーコンテキスト外のドライバーのインストールがブロックされることがあります。初回インベントリ作成時にアンチウイルス製品のリアルタイムスキャン機能を一時的に無効にするか、例外規則を追加してください。

- **システムボリュームのスナップショットを作成できません。Volume Shadow Copyサービスが有効になっていることを確認してください。**
  エラーコードは、15です。このエラーは、Volume Shadow Copyサービスが無効になっていると発生します。Volume Shadow Copyサービスを有効にしてからインベントリ操作を再試行してください。

- **変更ジャーナルのアクティブ化に失敗しました。数分待ってから再試行してください。**
  エラーコードは、16です。Personal vDiskでは、マスターイメージに対する変更を追跡するために「変更ジャーナル」が使用されます。インベントリ更新時に変更ジャーナルが無効になっていることが検出されると、有効化が試行され、有効化に失敗するとこのエラーが発生します。しばらくしてから再試行してください。

- **システムボリュームに十分な空き領域がありません。**
  エラーコードは、17です。デスクトップのCドライブにイメージの更新操作に必要な空き領域がない場合にこのエラーが発生します。システムボリュームを拡張するか、不要なファイルを削除して空き領域を確保してください。十分な空き領域を確保すると、次回再起動時にイメージ更新が開始されます。

- **Personal vDiskストレージに十分な空き領域がありません。Personal vDiskストレージを拡張して空き領域を増やしてください。**
  エラーコードは、18です。イメージの更新時にPersonal vDisk用のドライブに十分な空き領域がない場合にこのエラーが発生します。Personal vDiskストレージを拡張するか、不要なファイルを削除して空き領域を確保してください。十分な空き領域を確保すると、次回再起動時にイメージ更新が再開されます。

- **Personal vDiskストレージがオーバーコミットされました。Personal vDiskストレージを拡張して空き領域を増やしてください。**
  エラーコードは、19です。シックプロビジョニングされたUserData.V2.vhdを格納するための空き領域がPersonal vDisk用のドライブにない場合にこのエラーが発生します。Personal vDiskストレージを拡張するか、不要なファイルを削除して空き領域を確保してください。

- **システムレジストリが破損しています。**
  エラーコードは、20です。システムレジストリが破損または欠落しているか、読み取り不能になっています。Personal vDiskをリセットするか、作成済みのバックアップから復元してください。

- **Personal vDiskのリセット時に内部エラーが発生しました。詳しくは、Personal vDiskのログを参照してください。**
  エラーコードは、21です。このメッセージは、Personal vDiskのリセット時に発生したすべてのエラーに対して生成されます。ログファイルを収集してCitrixのサポート担当者に問い合わせてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Personal vDiskのリセットに失敗しました。Personal vDiskストレージに十分な空き領域がありません。**
  エラーコードは、22です。リセット時にPersonal vDisk用のドライブに十分な空き領域がない場合にこのエラーが発生します。Personal vDiskストレージを拡張するか、不要なファイルを削除して空き領域を確保してください。

Version 7.6より前のPersonal vDisk 7.xでは、以下の エラーメッセージが生成されます。

- **スタートアップに失敗しました。Personal vDiskは、ユーザーの個人設定用のストレージディスクを見つけることができませんでした。**
  このエラーメッセージは、Personal vDiskソフトウェアでPersonal vDisk（デフォルトでPドライブ）が見つからない場合、または管理者がカタログ作成時に指定したマウントポイントにそのディスクをマウントできない場合に表示されます。
  - この問題が発生した場合は、 Personal vDiskサービスログで 「PvD 1 status --> 18:183」を検索します。
  - Version 5.6.12よりも古いバージョンのPersonal vDiskを 使用している場合は、最新 バージョンにアップグレードすることでこの問題を解決できます。
  - Version 5.6.12またはそれ以降のバージョンを 使用している場合は、ディスクの管理ツール（diskmgmt.msc）を使用してPドライブが不明なボリュームとして存在することを確認してください。Pドライブが 存在する場合は、そのボリューム上でchkdskを実行します。ボリュームが破損していることが検出された場合は、chkdskを使用して 修復してください。
- **スタートアップに失敗しました。Citrix Personal vDiskを起動できませんでした。 詳細は .... 状態コード：7、エラーコード0x70**
  「状態コード7」はPersonal vDisk更新時のエラーを示します。 次のいずれかのエラーコードが表示されます。

エラーコード	説明
0x20000001	差分パッケージの保存に失敗しました。VHDの 空き領域不足が考えられます。
0x20000004	Personal vDiskの更新に必要な特権の取得に失敗しました。
0x20000006	Personal vDiskイメージまたはPersonal vDiskインベントリからのハイブのロードに失敗しました。Personal vDiskイメージまたはインベントリの破損が考えられます。
0x20000007	ファイルシステムインベントリのロードに失敗しました。 Personal vDiskイメージまたはインベントリの破損が考えられます。
0x20000009	ファイルシステムインベントリを含んでいるファイルを開くことができません。 Personal vDiskイメージまたはインベントリの破損が考えられます。
0x2000000B	差分パッケージの保存に失敗しました。VHDの 空き領域不足が考えられます。
0x20000010	差分パッケージのロードに失敗しました。
0x20000011	規則ファイルがありません。
0x20000021	Personal vDiskインベントリが破損しています。
0x20000027	カタログ「MojoControl.dat」が破損しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

エラーコード	説明
0x2000002B	Personal vDiskインベントリが破損または欠落しています。
0x2000002F	更新時に、ユーザーによりインストールされたMOFの登録に失敗しました。 Version 5.6.12にアップグレードすることで解決できます。
0x20000032	PvDactivation.log.txtで、最後の Win32エラーコードエントリを確認してください。
0x20	イメージ更新用のアプリケーションコンテナーのマウントに失敗しました。 Version 5.6.12にアップグレードすることで解決できます。
0x70	ディスク上に十分な領域がありません。

- **スタートアップに失敗しました。Citrix Personal vDiskを起動できませんでした。（または「Personal vDiskで内部エラーが発生しました。」） 詳細は ... 状態コード： 20、エラーコード0x20000028**
  このメッセージは、Personal vDiskが見つかったにもかかわらずPersonal vDiskセッションを作成できなかったことを示します。

  ログを収集して、SysVol-IvmSupervisor.logにセッションの作成の失敗が記録されていないかどうかを確認してください。
  1. 「IvmpNativeSessionCreate: failed to create native session, status 」というエントリ を検索します。
  2. が0xc00002cfの場合は、カタログに新しいバージョンのマスター イメージを追加することで解決できます。この状態コードは、 インベントリ更新後の変更数が多いためにUSNジャーナルのオーバーフローが発生したことを示します。
  3. 問題が発生した仮想デスクトップを再起動します。問題が解決されない場合は、Citrixのテクニカル サポートに問い合わせてください。
- **スタートアップに失敗しました。安全ではないシステムシャットダウンが検出されたため、Citrix Personal vDiskが非アクティブ化されています。 もう一度実行するには、［再試行］をクリックします。問題が解決しない場合は、システム管理者に連絡してください。**
  このメッセージは、プールされた仮想マシンを、Personal vDiskを有効にしたまま起動できないことを示します。 まず、起動に失敗した原因を調べます。 考えられる原因として、以下の理由によるブルースクリーンエラーが挙げられます。
  - 互換性のないアンチウィルスソフトウェア（古いバージョンのTrend Microなど）がマスターイメージ上にインストールされている。
  - Personal vDiskと互換性のないソフトウェアがユーザーにより インストールされている。これが原因となることはまれですが、マシンカタログに新しいマシンを追加して、そのマシンが正しく 再起動するかどうかを 確認してください。
  - Personal vDisk イメージが破損している（この問題はVersion 5.6.5で確認されています）。

  プールされた仮想マシンでブルースクリーンエラーが発生するかどうか、または不完全な状態で起動するかどうかを確認するには、以下の操作を行います。
  - ハイパーバイザーのコンソールを使用して、仮想 マシンにログオンします。
  - ［再試行］をクリックして、仮想マシンがシャットダウンするまで待ちます。
  - Studioを使用して、 仮想マシンを起動します。
  - ハイパーバイザーのコンソールを使用して、仮想マシンの起動時に問題が発生するかどうかを確認します。

  また、以下の解決方法があります。
  - 仮想マシンから メモリダンプを収集して、 それをCitrix社のテクニカルサポート部門に送ります。
  - 次の手順で、Personal vDiskのイベントログに エラーが記録されているかどうかを確認します。
    1. DiskMgmt.mscを起動して、［操作］メニューの［VHDの接続］を選択して、Pドライブのルートにある UserData.V2.vhdをマウントします。
    2. Eventvwr.mscを起動します。
    3. ［操作］メニューの［保存されたログを開く］を選択して、UserData.V2.vhdのシステムイベントログ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

（Windows\System32\winevt\logs\system.evtx）を開きます。

4. ［操作］メニューの［保存されたログを開く］を選択して、UserData.V2.vhdのアプリケーションイベントログ（Windows\System32\winevt\logs\application.evtx）を開きます。

- Personal vDiskを開始できません。**インベントリが更新されていないため、Personal vDiskを開始できませんでした。 マスターイメージのインベントリを更新してから再試行してください。状態コード： 15、エラーコード： 0x0**
  このメッセージは、管理者がPersonal vDiskカタログを作成するときに不適切なスナップショットを選択した（つまりスナップショット作成時にマスターイメージが ［Update Personal vDisk］でシャットダウンされなかった）ことを示します。

Personal vDiskが無効な場合は、Windowsイベント ビューアーで以下のイベントを確認できます。Personal vDisk関連のイベントは ［アプリケーション］ノードに表示されます（ソースは「Citrix Personal vDisk」）。Personal vDiskが有効な場合、 これらのどのイベントも表示されません。

イベントのIDが1のものは情報メッセージを意味し、IDが2のものはエラーを 意味しています。Personal vDiskのバージョンによっては、一部のイベントが発生しない場合があります。

イベントID	説明
1	Personal vDisk状態：インベントリの更新を開始しました。
1	Personal vDisk状態：インベントリの更新が完了しました。GUID：%s。
1	Personal vDisk状態：イメージ更新を開始しました。
1	Personal vDisk状態：イメージ更新が完了しました。
1	リセット中です。
1	OK。
2	Personal vDisk状態：%s により、インベントリの更新に失敗しました。
2	Personal vDisk状態：%s により、イメージ更新に失敗しました。
2	Personal vDisk状態：内部エラーにより、イメージ更新に失敗しました。
2	Personal vDiskの状態： 内部 エラーにより、インベントリ更新に失敗しました。
2	正しくシャットダウンされなかったため Personal vDiskが無効になっています。
2	イメージ更新に失敗しました。エラーコードは %d です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

イベントID	説明
2	Personal vDiskで内部エラーが発生しました。状態コード[%d]、 エラーコード[0x%X]
2	Personal vDiskのリセットに失敗しました。
2	ユーザーのパーソナル設定を格納するためのディスクが見つかりません。
2	このストレージディスクには Personal vDiskコンテナーの作成に必要な領域がありません。

バージョンに依存しない既知の問題

次のPvDの問題が確認されています。

- Personal vDisk上にインストールされたアプリケーションがマスターイメージ上にインストールされた同一バージョンのアプリケーションと関連付けられている場合、イメージの更新後にPersonal vDisk上のアプリケーションが動作しなくなることがあります。この問題は、マスターイメージ上のアプリケーションをアンインストールしたりアップグレードしたりしたために、Personal vDisk上のアプリケーションで必要なファイルがマスターイメージから削除されると発生します。この問題を回避するには、マスターイメージ上のアプリケーションを保持しておきます。

  たとえば、マスターイメージ上にOffice 2007をインストールして、Personal vDisk上にVisio 2007をインストールします。その後で管理者がマスターイメージ上のOffice 2007をOffice 2010にアップグレードして、そのイメージを使用してマシンを更新すると、Visio 2007が動作しなくなります。この問題を避けるには、Office 2007をマスターイメージ上にインストールしたままにしておきます。 [#320915]

- Personal vDiskを使用するデスクトップにMcAfee Virus Scan Enterprise（VSE）を展開する場合は、マスターイメージ上にVersion 8.8 Patch 4以降をインストールしてください。 [#303472]
- マスターイメージ内で作成されたファイルのショートカットが動作しなくなった場合（そのショートカットのリンク先の名前がPersonal vDisk内で変更された場合など）は、ショートカットを作成し直してください。 [#367602]
- マスターイメージ内で絶対/ハードリンクを使用しないでください。 [#368678]
- Windows 7のバックアップと復元機能は、Personal vDiskでサポートされていません。 [#360582]
- 更新したマスターイメージを適用した後で、ローカルユーザーおよびグループのコンソールがアクセス不能になったり不正なデータが表示されたりすることがあります。この問題を解決するには、仮想マシン上でユーザーアカウントをリセットします。これを行うには、セキュリティハイブのリセットが必要です。この問題はVersion 7.1.2で解決されており、Version 7.1.2以降で作成された仮想マシンは正しく処理されます。ただし、アップグレード前に作成された仮想マシンでの問題は解決されません。 [#488044]
- ESXハイパーバイザー環境でプールされた仮想マシンを使用する場合、SCSIコントローラーの種類として［VMware Paravirtual］を選択すると再起動を確認するメッセージがユーザーに表示されます。この問題を避けるには、SCSIコントローラーの種類としてLSIを使用してください。 [#394039]
- Provisioning Servicesで作成されたデスクトップ上でPersonal vDiskをリセットすると、ログオンしたユーザーに再起動を確認するメッセージが表示されることがあります。この問題が発生した場合は、デスクトップを再起動してください。 [#340186]
- Windows 8.1のデスクトップを使用するユーザーがPersonal vDiskにログオンできなくなることがあります。この問題が発生すると、「システムが正しくシャットダウンされなかったためPersonal vDiskが無効になっています」というメッセージが管理者に表示され、PvDActivation.logに「Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]」というメッセージが記録されます。この問題は、ユーザーの仮想マシンを正しくシャットダウンできなかった場合に発生します。この問題を解決するには、Personal vDiskをリ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セットしてください。 [#474071]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コンポーネントの削除

Dec 05, 2017

製品のコンポーネントを削除するには、プログラムの削除（アンインストール）や変更を行うWindowsの機能を使用するこ
をお勧めします。または、コマンドラインや、インストールメディアに収録されているスクリプトを使用してコンポーネン
をアンインストールすることもできます。

コンポーネントをアンインストールしても、そのコンポーネントと一緒にインストールされたサードパーティ製ソフトウェ
はアンインストールされず、ファイアウォール設定も変更されません。Controllerをアンインストールしても、SQL Serverソ
フトウェアおよびデータベースは削除されません。

Controllerをアンインストールする前に、サイトからそのControllerを削除してください。StudioやDirectorをアンインスト
ールする場合は、それらを閉じておくことをお勧めします。

Controllerをアップグレードする前の環境でWeb Interfaceを使用していた場合は、Web Interfaceコンポーネントを別途アン
インストールする必要があります。この製品のインストーラーを使ってWeb Interfaceをアンインストールすることはできま
せん。

VDAを削除すると、削除後にデフォルトでマシンが自動的に再起動します。

プログラムの削除や変更を行うWindowsの機能を使用してコンポーネントをアンインストールする

プログラムの削除や変更を行うためのWindows機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作
を行います。

- Controller、Studio、Director、ライセンスサーバー、またはStoreFrontをアンインストールするには、［Citrix XenApp <*version*>］または［Citrix XenDesktop <*version*>］を選択してから右クリックし、**［アンインストール］**を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。StoreFrontは、**［Citrix StoreFront］**を右クリックしてから**［アンインストール］**を選択して削除することもできます。
- VDAをアンインストールするには、**［Citrix Virtual Delivery Agent** <*version*>］を選択し、右クリックしてから**［アンインストール］**を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。
- Universal Print Serverをアンインストールするには、**［Citrix Universal Print Server］**を選択してから右クリックし、**［アンインストール］**を選択します。

コマンドラインを使ってコアコンポーネントをアンインストールする

インストールメディアの\x64\XenDesktop Setupディレクトリから、**XenDesktopServerSetup.exe**コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、/removeおよび/componentsオプションを使用します。
- すべてのコンポーネントをアンインストールするには、/removeallオプションを使用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コマンドおよびパラメーターについて詳しくは、「コマンドラインを使ったインストール」を参照してください。

たとえば、Studioをアンインストールするには次のコマンドを実行します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

コマンドラインを使ってVDAをアンインストールする

インストールメディアの\x64\XenDesktop Setupディレクトリから、**XenDesktopVdaSetup.exe**コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、/removeおよび/componentsオプションを使用します。
- すべてのコンポーネントをアンインストールするには、/removeallオプションを使用します。

コマンドおよびパラメーターについて詳しくは、「コマンドラインを使ったインストール」を参照してください。

たとえば、VDAおよびCitrix Receiverをアンインストールするには次のコマンドを実行します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Active Directoryのスクリプトを使用してVDAを削除するには、「スクリプトを使ったVirtual Delivery Agentのインストールまたは削除」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アップグレードと移行

Dec 05, 2017

アップグレード

新しいバージョンのマシンやサイトをセットアップしなくても、既存の環境をアップグレードすることで最新バージョンのコンポーネントを使用できます。これをインプレースアップグレードと呼びます。次のバージョンから現在のバージョンにアップグレードできます。

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

XenApp 6.5ワーカーのサーバーを最新のVDA for Windows Server OSにアップグレードすることもできます。これは、XenApp 6.5からの移行時に補足的に行います。「XenApp 6.5ワーカーのVDA for Windows Server OSへのアップグレード」を参照してください。

アップグレードするには

1. コアコンポーネントおよびVDAのインストール先のマシン上でインストーラーを実行します。アップグレードが可能かどうかが検出され、新しいバージョンのソフトウェアがインストールされます。
2. アップグレードしたStudioを使用して、データベースとサイトをアップグレードします。

*XenDesktop 5.6からアップグレードするには、まず最新のCUを使用して7.6 LTSRにアップグレードしてから、7.15 LTSRにアップグレードします。

詳しくは、「環境のアップグレード」を参照してください。

Controller Hotfixのインストールについて詳しくは、CTX201988を参照してください。

移行

以前のバージョンの環境から、最新バージョンの環境にデータを移行できます。XenApp 6の環境を移行できます。移行処理により、XenApp/XenDesktopコンポーネントのインストール、新しいサイトの作成、既存のファームからのデータのエクスポート、および新しいサイトへのデータのインポートが行われます。

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

ヒント： 7.xリリースで導入されたアーキテクチャ、コンポーネントおよび機能変更について詳しくは、「7.xでの変更点」を参照してください。

XenApp 6.5からの移行では、以下の操作を行います。

1. コアコンポーネントをインストールして、新しいXenAppサイトを作成します。
2. XenApp 6.5コントローラーで、PowerShellコマンドレットを実行してポリシーやファームのデータをXMLファイルとしてエクスポートします。エクスポートしたXMLファイルは、必要に応じてインポート用に編集できます。
3. 新しいXenAppのサイトで、PowerShellコマンドレットを実行してXMLファイルからポリシーやアプリケーションのデータをサイトにインポートします。
4. 新しいサイトで移行後のタスクを完了します。

詳しくは、「XenApp 6.xからの移行」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.xでの変更点

Jan 03, 2018

7.xリリース以降で、XenAppおよびXenDesktopのアーキテクチャ、用語、および機能が変更されました。ここでは、旧（7.xより前の）バージョンしか詳しくないユーザーに必要な変更情報を提供します。

ヒント：7.xバージョンに移行した後、それより後のバージョンへの変更については、「新機能」で説明されています。

特記しない限り、*7.x*はXenApp Version 7.5以降、およびXenDesktop Version 7以降を指します。

この記事に概要を示します。7.xより前のバージョンから最新バージョンへの移行の包括的な情報については、「XenApp 7へのアップグレード」を参照してください。

XenApp 6と現在のバージョンのXenAppとの相違点

XenApp 6.5以前のバージョンとXenApp/XenDesktop 7.x以降との機能や用語の対応は次の表のとおりです。ただし、これらは単なる名前の置き換えではなく、機能的にも更新されていることに注意してください。アーキテクチャ上の相違点の説明が続きます。

XenApp 6.5以前の機能	対応するXenApp/XenDesktop 7.x以降の機能
Independent Management Architecture（IMA）	FlexCast Management Architecture（FMA）
ファーム	サイト
ワーカーグループ	マシンカタログ デリバリー グループ
ワーカー	Virtual Delivery Agent（VDA） サーバーOSマシン、サーバーOS VDA デスクトップOSマシン、デスクトップOS VDA
リモートデスクトップサービス（RDS）またはターミナルサービスマシン	サーバーOSマシン、サーバーOS VDA
ゾーンとデータコレクター	Delivery Controller
デリバリーサービスコンソール	Citrix StudioとCitrix Director
アプリケーションの公開	アプリケーションの配信

© 1999-2017 Citrix Systems, Inc. All rights reserved.

データストア	データベース
負荷評価基準	負荷管理のポリシー
管理者	委任管理者 役割 スコープ

アーキテクチャの相違

XenApp/XenDesktop 7.x以降は、「FlexCast Management Architecture（FMA）」と呼ばれるアーキテクチャに基づいています。FMAは、Citrixテクノロジ間の相互運用性と管理モジュール性を可能にする、サービス指向のアーキテクチャです。FMAにより、アプリケーション配信、モビリティ、サービス、フレキシブルなプロビジョニング、およびクラウド管理のためのプラットフォームが提供されます。

FMAは、XenApp 6.5以前で使用されていたIMA（Independent Management Architecture）を置き換えるものです。

FMAの主要要素とXenApp 6.5以前のバージョンとの違いは以下のとおりです。

- **デリバリーサイト**： XenApp 6.5以前のバージョンでは、最上位レベルのオブジェクトが「ファーム」と呼ばれていました。XenApp/XenDesktop 7.xでの最上位レベルは「サイト」です。デリバリーサイトでは、ユーザーのグループにアプリケーションやデスクトップが提供されます。FMAでは、サイトを展開する管理者がドメインに属している必要があります。たとえばサーバーをインストールするには、アカウントにローカル管理者権限があり、Active Directoryのドメインユーザーである必要があります。
- **マシンカタログとデリバリーグループ**: XenApp 6.5以前のバージョンでは、アプリケーションやサーバーソフトウェアを効率的に管理するため、ホストマシンがワーカーグループとしてグループ化されました。管理者は、ワーカーグループ内のすべてのマシン上のアプリケーションや負荷分散を単一エンティティとして管理できました。また、アプリケーションやマシンをフォルダーで分類することもできました。XenApp/XenDesktop 7.xでは、マシンカタログ、デリバリーグループ、およびアプリケーショングループを使用して、マシン、負荷分散、およびアプリケーションやデスクトップを管理します。また、アプリケーションフォルダーを使用することもできます。
- **VDA**： XenApp 6.5以前のバージョンでは、ワーカー グループ内のワーカーマシンがユーザーのアプリケーションをホストして、データコレクターと通信しました。XenApp/XenDesktop 7.xでは、VDAがDelivery Controllerと通信して、Delivery Controllerがユーザー接続を管理します。
- **Delivery Controller** XenApp 6.5以前のバージョンでは、ユーザーからの接続要求とハイパーバイザーとの通信をゾーンマスターが担当していました。XenApp/XenDesktop 7.xでは、接続要求はサイト内の各Controllerに分散されて処理されます。XenApp 6.5以前のバージョンでは、ゾーンによりWAN接続を介したサーバー集約およびデータ複製が提供されていました。XenApp/XenDesktop 7.xにはこのようなゾーンに正確に対応するものがありませんが、7.xでのゾーンとゾーン優先度機能を使用して、リモートのユーザーがWANの大規模セグメントを経由する接続を必ずしも必要とせず、リソースに接続できるようにサポートできます。
- **StudioとDirector**： Studioコンソールでは、環境を構成したり、ユーザーにアプリケーションやデスクトップへのアクセスを提供したりできます。Studioは、XenApp 6.5以前のバージョンのデリバリーサービスコンソールに相当するもので

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。また、管理者はDirectorを使用して環境の監視、ユーザーセッションのシャドウ、およびトラブルシューティングを行います。ユーザーのセッションをシャドウするには、Windowsリモートアシスタンスが有効になっている必要があります（VDAのインストール時に自動的に有効になります）。

- **アプリケーションの配信**： XenApp 6.5以前のバージョンでは、アプリケーションの公開ウィザードを使用してアプリケーションをユーザーに公開しました。XenApp/XenDesktop 7.xでは、Studioを使ってアプリケーションを作成および追加して、配信先のユーザーのデリバリーグループ（およびオプションでアプリケーショングループ）を選択します。Studioでは、最初にサイトを構成し、マシンカタログを作成および指定してから、そのカタログのマシンを使用するデリバリーグループを作成します。デリバリーグループでは、アプリケーションへのアクセスを許可するユーザーを指定します。必要な場合は、複数のデリバリーグループを作成する代わりに、アプリケーショングループを作成することを選択できます。
- **データベース**： XenApp 7.xとXenDesktop 7.xの構成情報は、IMAデータストアに格納されません。代わりに、構成情報およびセッション情報のデータストアとしてMicrosoft SQL Serverデータベースが使用されます。
- **負荷管理のポリシー**： XenApp 6.5以前のバージョンの負荷評価基準では、事前定義された値に基づいてマシンの負荷が評価されていました。これにより、より負荷の軽いマシンにユーザー接続が割り当てられました。XenApp/XenDesktop 7.xでは、負荷管理ポリシーを使用してマシン間の負荷を管理します。
- **管理権限の委任**： XenApp 6.5以前のバージョンでは、カスタム管理者を作成してフォルダーやオブジェクト単位で管理権限を割り当てることができました。XenApp/XenDesktop 7.xでは、役割とスコープのペアを使用してカスタム管理者の権限を定義します。役割はその管理者が担当する管理タスクに対応しており、それらに割り当てられた権限を使用して管理業務を委任できます。スコープは、接続、マシン カタログ、デリバリー グループなど、その管理者が管理できるオブジェクトをグループ化したものです。組み込みの役割には、ヘルプデスク、アプリケーション、ホスト、カタログなど特定の権限が事前定義されています。たとえば、ヘルプデスク管理者は特定のサイト上の個々のユーザーのみを対象としますが、すべての管理権限を実行できる管理者は展開全体を監視して、システム全体の問題を解決できます。

機能比較

FMAへの移行により、XenApp 6.5以前のバージョンで提供されていたいくつかの機能の実装が変更されたり、ほかの機能、コンポーネント、またはツールに置き換えられたりしています。

XenApp 6.5以前の機能	対応するXenApp/XenDesktop 7.x以降の機能
セッションの事前起動とセッション残留はポリシーで構成します。	セッションの事前起動とセッション残留はデリバリーグループを編集して構成します。 これらの機能では、セッションが要求される前にセッションを開始したり（セッションの事前起動）、ユーザーがすべてのアプリケーションを閉じた後もセッションをアクティブな状態で保持したり（セッション残留）できます。これにより、ユーザーがアプリケーションにすばやくアクセスできるようになります。XenApp 6.5以前のバージョンでは、ポリシーを使用してこれらの機能を構成していました。XenApp/XenDesktop 7.xでは、既存のデリバリーグループを編集することでこれらの機能を有効にします。この設定は、そのデリバリーグループに含まれているユーザーに適用されます。「セッションの事前起動およびセッション残留の構成」を参照してください。
認証が不要なユーザー（匿名ユーザー）のサポートは公開アプリケーションのプロパティを設定して構成します。	認証が不要なユーザー（匿名ユーザー）のサポートはデリバリーグループのユーザープロパティを設定して構成します。「ユーザー」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ローカルホストキャッシュにより、データストアに接続できない状態でもワーカーサーバーが正しく動作します。	ローカルホストキャッシュを使用すると、Controllerとサイトデータベースの間の接続が失敗しても、接続仲介操作を続行できます。この実装は、より頑強で、必要なメンテナンスも少なくなります。「ローカルホストキャッシュ」を参照してください。 ローカルホストキャッシュを使用する代わりに、接続リースにより、サイトデータベースに接続できない状態でも、ユーザーが最近使用していたアプリケーションやデスクトップに接続および再接続できます。「接続リース」を参照してください。
アプリケーションのストリーム配信	Citrix App-Vによるアプリケーションのストリーム配信をStudioで管理できます。
Web Interface	StoreFrontへの移行をお勧めします。
ユーザーセッションの画面上アクティビティを録画するSmartAuditor。	7.6 Feature Pack 1以降、この機能はSession Recordingにより提供されます。また、構成ログを使用して、すべてのセッションアクティビティを管理の視点から記録することもできます。
節電やサーバー能力の管理に役立つ電源能力管理。	Microsoft Configuration Managerを使用します。

機能のサポートと変更

以下の機能は、現在提供されていないか、もうサポートされていないか、7.x以降のXenAppまたはXenDesktopで大幅に変更されました。

128ビット未満のSecureICA暗号化： 7.xより前のリリースでは、SecureICAにより基本レベル、40ビット、56ビット、および128ビットの暗号化でクライアント接続を保護できました。このリリースのSecureICAでは、128ビットの暗号化のみを使用できます。

従来の印刷機能： 以下の印刷機能は、7.xでサポートされなくなりました。

- Dosクライアントと16ビットプリンターに対する後方互換性。
- 強化された拡張プリンタープロパティおよびWin32FavorRetainedSettingを含む、Windows 95およびWindows NTオペレーティングシステムに接続されたプリンターのサポート。
- 自動保持および自動復元プリンターを有効または無効にする機能
- 自動保持および自動復元プリンターを有効または無効にするサーバーのレジストリ設定であるDefaultPrnFlag。サーバー」のユーザープロファイルに保存されます。

注：従来のクライアントプリンター名は使用できます。

Secure Gateway： 7.xより前のリリースでは、Secure Gatewayを使用してサーバーとユーザーデバイス間の接続を保護で

© 1999-2017 Citrix Systems, Inc. All rights reserved.

きました。このリリースでは、外部接続をセキュリティで保護するためのオプションとして、NetScaler Gatewayを使用します。

ユーザーのシャドウ：7.xより前のリリースでは、管理者はポリシーを設定してユーザー間のシャドウを制御しました。このリリースでは、エンドユーザーのシャドウ機能がDirectorコンポーネントに統合されています。管理者は、DirectorからWindowsリモートアシスタンスを使用してユーザーのアプリケーションや仮想デスクトップをシャドウして、問題のトラブルシューティングを行います。

第1世代のFlashリダイレクト：第2世代Flashリダイレクトをサポートしないクライアント（Citrix Receiver for Windows 3.0より前のバージョン、Citrix Receiver for Linux 11.100より前のバージョン、およびCitrix Online Plug-in 12.1）では、従来のFlashリダイレクトが機能しないためにサーバー側でのレンダリングにフォールバックされます。このリリースに含まれるVDAは、第2世代のFlashリダイレクト機能をサポートします。

ローカルテキストエコー：この機能は、以前の形式のWindowsアプリケーション上で入力文字列を高速に表示するために使用されました。このリリースではHDX SuperCodecおよびグラフィックサブシステムが改善されたため、この機能は削除されています。

Single Sign-On：パスワードセキュリティを提供するこの機能は、Windows 8、Windows Server 2012、および新しくサポートされたWindowsオペレーティングシステムのバージョンではサポートされません。Windows 2008 R2およびWindows 7環境ではサポートされますが、このリリースには含まれていません。ただし、CitrixのダウンロードWebサイト（http://citrix.com/downloads）から入手することができます。

Oracleデータベースのサポート：このリリースでは、SQLデータベースを使用します。

サーバーヘルスの監視および復元（HMR）：7.xより前のリリースでは、この機能を使用してサーバーファーム内のサーバーでテストを実行し、サーバーの状態を監視したり、サーバーヘルスのリスクを発見したりできました。このリリースでは、Directorのコンソールを使用して、インフラストラクチャ全体のシステム状態を一元的に管理および監視できます。

カスタムICAファイル：7.xより前のリリースでは、カスタムのICAファイルを使用して、ユーザーデバイスから特定のマシンへの直接接続が可能でした。このリリースでは、この機能はデフォルトでは無効になっていますが、ローカルグループを使用する標準的な使用においては有効にできます。また、Controllerが使用できなくなった場合に高可用性モードで使用することもできます。

Management Pack for System Center Operations Manager (SCOM) 2007：SCOMを使ってXenAppファームのアクティビティを監視する管理パックは、7.xリリースに対応していません。最新のCitrix SCOM Management Pack for XenApp and XenDesktopを参照してください。

CNAME機能：7.xより前のリリースでは、CNAME機能はデフォルトで有効になっていました。このため、CNAMEレコードに依存するFQDNの再ルーティングやNetBIOS名の使用に失敗することがありました。このリリースでは、Controllerの自動更新機能によりControllerの一覧が動的に更新され、サイトのControllerが追加または削除されるとVDAに自動的に通知されます。この自動更新機能はCitrixポリシーのデフォルトで有効になっていますが、無効にできます。または、レジストリでCNAME機能を有効にして、従来のFQDNの再ルーティングやNetBIOS名の使用を許可することもできます。詳しくは、CTX137960を参照してください。

簡易展開ウィザード：7.xより前のリリースのXenDesktopでは、このStudioオプションを選択してすべてが構成済みのXenDesktop展開をすばやく作成することができました。このリリースではインストールおよび構成のワークフローが簡素化されたため、簡易展開ウィザードが不要になりました。

自動管理用のリモートPCサービス構成ファイルおよびPowerShellスクリプト：リモートPCアクセスは、StudioおよびControllerに統合されました。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow Studio：7.xより前のリリースでは、XenDesktopのワークフロー構成用のグラフィカルインターフェイスとしてWorkflow Studioを使用しました。このリリースでは、この機能はサポートされません。

クライアント接続での非公開アプリケーションの起動：7.xよりも前のリリースでは、このCitrixポリシー設定は、サーバー上のICAまたはRDPを介して開始アプリケーションまたは公開アプリケーションを起動するかどうかを指定しました。7.xリリースでは、サーバー上のRDPを介して開始アプリケーションまたは公開アプリケーションを起動するかどうかのみを指定します。

デスクトップの起動：7.xよりも前のリリースでは、このCitrixポリシー設定は非管理者ユーザーがデスクトップセッションに接続できるかどうかを指定しました。7.xリリースでは、VDA上のセッションに接続するため、非管理者ユーザーがVDAマシンのDirect Access Usersグループのメンバーである必要があります。デスクトップの起動設定により、VDAのDirect Access Usersグループの非管理者ユーザーは、ICAコネクションを使ってVDAに接続できます。デスクトップの起動設定は、RDP接続には影響を与えません。VDAのDirect Access Usersグループのユーザーは、この設定が有効であるかどうかにかかわらず、RDP接続を使ってVDAに接続できます。

色数：リリース7.6以前のStudioでは、デリバリーグループのユーザー設定で色数を指定していました。バージョン7.6以降、デリバリーグループの色数はNew-BrokerDesktopGroupまたはSet-BrokerDesktopGroup PowerShellコマンドレットを使って設定できます。

タッチパネルでの操作に最適化されたデスクトップを起動：この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは使用できません。詳しくは、「モバイルデバイスでの動作のポリシー設定」を参照してください。

COMポートマッピング：COMポートのマッピング機能により、ユーザーデバイス上のCOMポートへのアクセスが許可または禁止されます。この機能は、以前のリリースのデフォルトでは有効になっていました。このリリースでは、COMポートマッピングがデフォルトで無効になります。詳しくは、「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

LPTポートマッピング：LPTポートのマッピング機能により、LPTポートへのレガシーアプリケーションのアクセスが制御されます。この機能は、以前のリリースのデフォルトでは有効になっていました。このリリースでは、LPTポートマッピングがデフォルトで無効になります。

PCMオーディオコーデック：7.xリリースでは、HTML5クライアントでのみPCMオーディオコーデックがサポートされます。

Microsoft ActiveSyncのサポート

以前のバージョンのプロキシサポート：以下が含まれます。

- Microsoft Internet Security and Acceleration（ISA）2006（Windows Server 2003）。
- Oracle iPlanet Proxy Server 4.0.14（Windows Server 2003）。
- Squid Proxy Server 3.1.14（Ubuntu Linux Server 11.10）。

詳しくは、使用しているバージョンのCitrix Receiverのドキュメントを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

環境のアップグレード

Feb 22, 2018

ここでは次のことについて説明します。

- はじめに
- アップグレードの順序
- アップグレードできる製品コンポーネントのバージョン
- 準備と制限
- 混在環境に関する考慮事項
- Windows XPまたはWindows Vista上のVDA
- Windows 8.xおよびWindows 7上のVDA
- VDAの混在環境のサポート
- アップグレード手順
- データベースとサイトのアップグレード

はじめに

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。このプロセスはインプレースアップグレードと呼ばれます。アップグレード可能なバージョンの一覧は、「アップグレード」を参照してください。

最新のXenAppインストーラーでは、XenApp 6.5ワーカーサーバーを最新のVDA for Windows Server OSにアップグレードすることもできます。これは、XenApp 6.5からの移行時に補足的に行います。「XenApp 6.5ワーカーのVDA for Windows Server OSへのアップグレード」を参照してください。

アップグレードを開始するには、新しいバージョンのインストーラーを実行して、既存のコアコンポーネント（Delivery Controller、Citrix Studio、Citrix Director、Citrixライセンスサーバー）とVDAをアップグレードします。その後、データベースとサイトをアップグレードします。

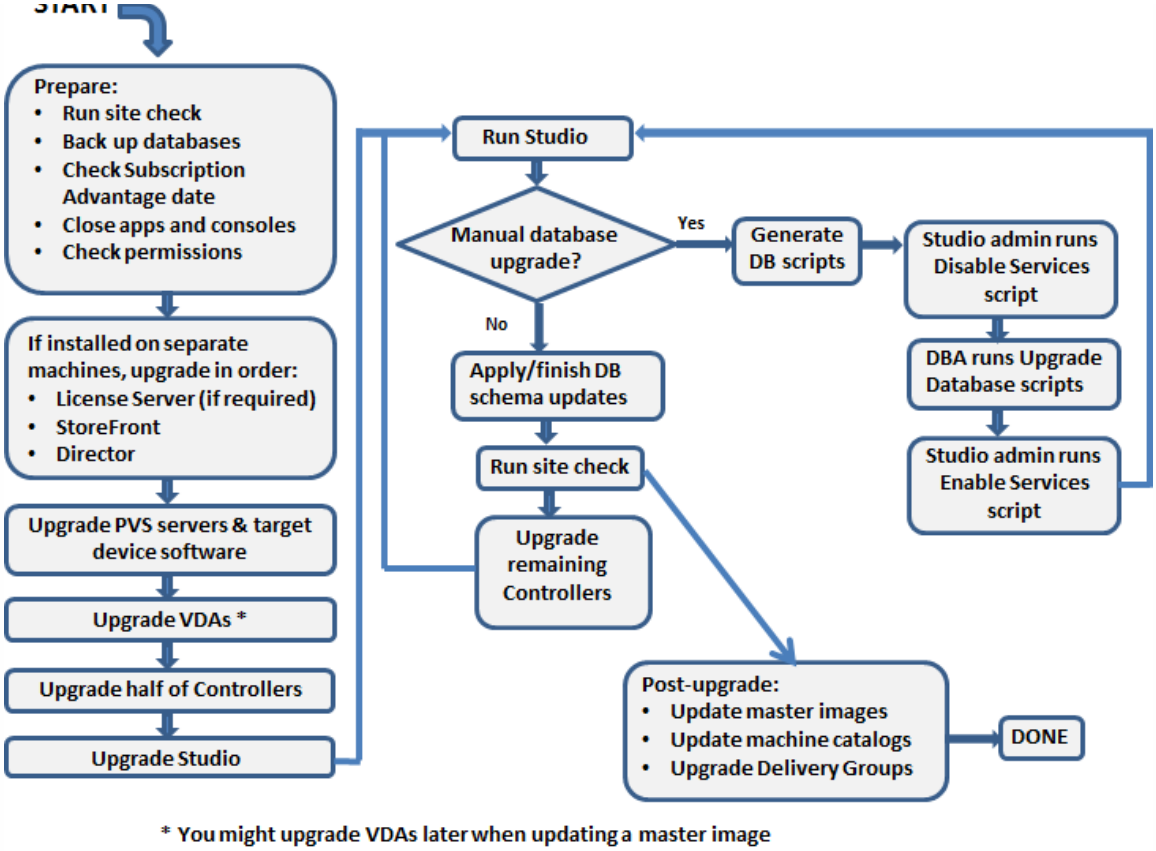
アップグレードを開始する前に、この記事の情報をすべて確認するようにしてください。

（7.16以降のリリースにアップグレードする場合は、「環境のアップグレード」のガイダンスを参照してください）。

アップグレードの順序

次の図に、アップグレードの順序の概要を示します。詳細については、下記「アップグレード手順」で説明します。サーバーに複数のコアコンポーネントがインストールされている場合、このサーバーマシンでインストーラーを実行すると、新しいバージョンが存在するすべてのコンポーネントがアップグレードされます。マスターイメージで使用されているVDAをアップグレードしてから、このマスターイメージを更新することもできます。その後、このマスターイメージを使用するカタログと、このカタログを使用するデリバリーグループを更新します。手順の詳細では、サイトデータベースとサイトを自動または手動でアップグレードする方法についても説明します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



アップグレードできる製品コンポーネントのバージョン

製品のインストーラーを使って、以下のコンポーネントをアップグレードできます。

- Citrixライセンスサーバー、Studio、StoreFront
- Delivery Controller 5.6以降
- VDA 5.6以降
  - 以前のVDAリリースとは異なり、VDAをアップグレードするには製品のインストーラーを使用する必要があります。MS
    は使用できません。
  - マシンでReceiver for Windows（Receiver.exe）が検出された場合は、製品のインストールメディアに含まれているバー
    ジョンにアップグレードされます。
  - VDA 5.6～VDA 7.8：マシンでReceiver for Windows Enterprise（CitrixReceiverEnterprise.exe）が検出された場合は、
    Receiver for Windows Enterprise 3.4にアップグレードされます。
- Director 1以降
- データベース： スキーマがアップグレードされ、サイトデータベースのデータが移行されます（Version 7.xからのアップ
  グレードでは、構成ログデータベースと監視データベースのデータも移行されます）
- Personal vDisk

注：XenDesktop 5.6からアップグレードするには、まず最新のCUを使用して7.6 LTSRにアップグレードしてから、このリリ-
スにアップグレードします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

適切なドキュメントの指示に従って、次の機能または製品を必要に応じてアップグレードします。

- Provisioning Services（XenApp 7.xおよびXenDesktop 7.xでは最新リリースのバージョンを使用することをお勧めします。Provisioning Services 7.0以降がサポートされます）。
  - ローリングアップグレードを使用してProvisioning Servicesサーバーをアップグレードし、vDiskのバージョン管理機能を使用してクライアントをアップグレードします。
  - Provisioning Services 7.xはXenDesktop 5でのデスクトップの作成をサポートしていません。既存のデスクトップは引き続き使用できますが、XenDesktopをアップグレードするまではProvisioning Services 7.xで新しいデスクトップを作成することはできません。このため、XenDesktop 7.xとXenDesktop 5.6のサイトを同時に運用する場合は、Provisioning Services 7にアップグレードしないでください。
- ホストハイパーバイザーのバージョン。
- StoreFront。
- Profile Management。

制限事項

アップグレードには以下の制限があります。

選択的なコンポーネントインストール

新しいバージョンのコンポーネントをインストールしたりアップグレードしたりする場合、別のマシン上のほかのコンポーネントをアップグレードしないと、Studioにメッセージが表示されます。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれるとします。Controllerをアップグレードしますが、Studioがインストールされているマシン上でインストーラーを実行しません。Studioをアップグレードするまではサイトを管理できません。

VDAをアップグレードする必要はありませんが、利用できる機能をすべて使用できるようにするために、すべてのVDAをアップグレードすることをお勧めします。

7.5よりも前のバージョンのXenApp

7.5より前のバージョンのXenAppからアップグレードすることはできません。XenApp 6.xの環境を移行できます。「XenApp 6.xからの移行」を参照してください。

XenApp 6.5ファームはアップグレードできませんが、Windows Server 2008 R2マシン上のXenApp 6.5ソフトウェアを、最新のVDA for Server OSに交換できます。「XenApp 6.5ワーカーから新しいVDAへのアップグレード」を参照してください。

5.6よりも前のバージョンのXenDesktop

5.6より前のバージョンのXenDesktopからアップグレードすることはできません。

XenDesktop Express Edition

XenDesktop Express Editionをアップグレードすることはできません。現在サポートされているエディションのライセンスを入手してインストールしてからアップグレードしてください。

Early Release版またはTechnology Preview版

XenAppまたはXenDesktopのEarly Release版やTechnology Preview版からアップグレードすることはできません。

Windows XPまたはWindows Vista

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAがWindows XPまたはWindows Vistaのマシンにインストールされている場合は、「Windows XPまたはWindows Vistaを実行しているマシンのVDA」を参照してください。

製品の選択

7.x以前のバージョンからアップグレードする場合は、製品（XenAppまたはXenDesktop）の選択も指定もしません（初回インストール時に設定されています）。

混在環境/サイト

以前のバージョンのサイトを引き続き運用する必要がある場合は、「混在環境に関する考慮事項」を参照してください。

準備

アップグレードを始める前に：

使用するインストーラーとインターフェイスを決定する

XenAppまたはXenDesktop ISOで提供される全製品インストーラーを使用して、コアコンポーネントをアップグレードできます。全製品インストーラーまたはスタンドアロンのVDAインストーラーを使用して、VDAをアップグレードできます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。詳しくは、「インストーラー」を参照してください。

アップグレードできるバージョンからデータをインポートまたは移行することによってアップグレードすることはできません（注： 非常に古いバージョンは、アップグレードするのではなく移行する必要があります。どのバージョンをアップグレードできるかは、「アップグレードと移行」を参照してください）。

デスクトップVDAの最初のインストールにVDAWorkstationCoreSetup.exeインストーラーを使用した場合は、アップグレードするときもそのインストーラーを使用することを推奨しています。VDAの全製品インストーラーまたはVDAWorkstationSetup.exeインストーラーを使用してVDAをアップグレードする場合、もともと除外されていたコンポーネントが、アップグレードから明示的に削除または除外しない限り、インストールされる可能性があります。

たとえば、VDAWorkstationCoreSetup.exeを使ってVDAバージョン7.13をインストールし、全製品インストーラーを使ってVDAをバージョン7.14にアップグレードするときにデフォルト設定をそのまま使用するか、/excludeコマンドラインオプションを使用しない場合、最初のインストールから除外されたコンポーネント（Profile ManagementやPersonal vDiskなど）が、このアップグレードでインストールされることがあります。

サイトのヘルスをチェックする

アップグレードを開始する前に、サイトが安定して機能している状態であることを確認してください。サイトに問題がある場合、アップグレードでは解決されず、サイトが複雑で修復が困難な状態になる可能性があります。サイトをテストするには、Studioのナビゲーションペインの **[サイト]** エントリをクリックします。中央ペインのサイト構成の部分で、 **[サイトのテスト]** をクリックします。

サイトデータベース、監視データベース、構成ログデータベースのバックアップ

CTX135207の指示に従います。アップグレード後に問題を検出した場合は、バックアップを回復できます。

必要な場合は、テンプレートをバックアップしてハイパーバイザーをアップグレードします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

他の準備タスクが事業継続計画に記載されていれば、それも完了します。

Citrixライセンスが最新であることを確認する

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantage日が新しい製品バージョンに対して有効であることを確認してください。製品のVersion 7.xからのアップグレードでは、この日付が2017.0801以降である必要があります。（この日付は7.15 LTSRリリースに適用され、以降の累積更新プログラム（CU）には適用されません。）

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルのロックの原因になりうるすべてのプログラムを終了してください。（マシンを再起動すると、ロックされているファイルや保留中のWindows更新プログラムがない状態になります。）

重要： アップグレードの開始前に、サードパーティの監視エージェントサービスを停止し、無効にしてください。

適切な権限があることを確認する

製品コンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。

サイトデータベースとサイトは、自動でも手動でもアップグレードできます。データベースの自動アップグレードでは、SQL Serverデータベーススキーマを更新できる権限（db_securityadminまたはdb_ownerデータベースロールなど）がStudioユーザーに必要です。詳しくは、「データベース」を参照してください。Studioユーザーにこれらの権限がない場合は、データベースの手動アップグレードで生成されるスクリプトを使用します。生成されるスクリプトの一部をStudioユーザーがStudioから実行して、ほかスクリプトをデータベース管理者がSQL Server Management Studioなどのツールを使って実行します。

混在環境に関する考慮事項

環境内に異なる製品バージョンのSites/farmsがある場合（混在環境）、StoreFrontを使って異なる製品バージョンのアプリケーションやデスクトップ（XenDesktop 7.13サイトとXenDesktop 7.14サイトがある場合など）を集約することをお勧めします。詳しくは、StoreFrontのドキュメントを参照してください。

- 混在環境では、異なるバージョンのStudioやDirectorを同一マシン上にインストールすることはできません。
- Provisioning Servicesを使用するXenDesktop 7.xおよびXenDesktop 5.6のサイトを同時に運用する場合は、XenDesktop 7.xサイト用に新しいProvisioning Servicesを展開するか、Provisioning Servicesを最新バージョンにアップグレードし、XenDesktop 5.6サイトでのワークロードのプロビジョニングを無効にしてください。

各サイト内ですべてのコンポーネントをアップグレードすることをお勧めします。コンポーネントによっては以前のバージョンを使用できますが、最新バージョンの機能を一部使用できない場合があります。たとえば、以前のバージョンのControllerを含む環境で最新のVDAを使用できますが、最新リリースの新機能を使用できない場合があります。最新でないバージョンを使用すると、VDA登録で問題が発生する可能性もあります。

- Version 5.xのControllerとVersion 7.xのVDAとの混在環境は、アップグレードに伴う一時的な構成としてのみ運用してください。可能な限り、環境内のすべてのコンポーネントのアップグレードを早急に完了してください。
- スタンドアロンのStudioは、新しいバージョンを使用する準備ができるまでアップグレードしないでください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows XPまたはWindows Vista上のVDA

Windows XPまたはWindows Vistaが動作するマシンにインストールされているVDAをVersion 7.xにアップグレードすることはできません。特定のHotfixが適用されたVDA 5.6 FP1を使用する必要があります。手順については、CTX140941を参照してください。以前のバージョンのVDAをVersion 7.xのサイトで実行することは可能ですが、次のような多くの機能を使用できません。

- 新しいバージョンのVDAを必要とするStudioの機能。
- Studioを使ったApp-Vアプリケーションの構成。
- Studioを使ったStoreFrontのアドレスの構成。
- Machine Creation Servicesを使用する場合のMicrosoft Windows KMSライセンスの自動サポート。CTX128580を参照してください。
- Directorでの情報の表示：
  - ［ダッシュボード］、［傾向］、および［ユーザーの詳細］ビューでログオン処理時間を算出するためのログオン時間およびログオン終了イベント。
  - HDX接続時間および認証時間のログオン処理時間ブレークダウンの詳細と、プロファイルロード、GPOロード、ログオンスクリプト、および対話型セッション確立の期間の詳細。
  - マシンおよび接続の障害率のいくつかのカテゴリ。
  - ［ヘルプデスク］ビューおよび［ユーザーの詳細］ビューのアクティビティマネージャー。

Windows XPとWindows Vistaのマシンは、サポートされているオペレーティングシステムで再イメージ化して最新のVDAをインストールすることをお勧めします。

Windows 8.xおよびWindows 7上のVDA

Windows 8.xまたはWindow 7を実行しているマシン上にインストールされたVDAをWindows 10にアップグレードするには、Windows 7およびWindows 8.xマシンをWindows 10に再イメージ化して、Windows 10用にサポートされているVDAをインストールすることを推奨します。再イメージ化がオプションではない場合は、オペレーティングシステムをアップグレードする前にVDAをアンインストールします。これを実行しない場合、VDAは未サポート状態となります。

VDAの混在環境のサポート

製品バージョンをアップグレードするときには、すべてのコアコンポーネントおよびVDAをアップグレードすることをお勧めします。これにより、そのエディションで追加されたり強化されたりした機能をすべて使用できるようになります。

環境のすべてのVDAを同時にアップグレードできない場合は、マシンカタログを作成するときに、マシンにインストールされているVDAのバージョンを指定できます。デフォルトでは、推奨される最新バージョンが指定されます。したがって、ここで変更が必要になるのは、以前のバージョンのVDAがインストールされているマシンがマシンカタログに含まれている場合だけです。ただし、マシンカタログで複数のバージョンのVDAを混在させることは推奨されていません。

マシンカタログを作成するときにVDAのバージョンとして推奨バージョンを指定する場合、そのカタログに以前のバージョンのVDAが含まれていると、それらのマシンはControllerに登録されず、機能しなくなります。

詳しくは、「VDAバージョンと機能レベル」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アップグレード手順

製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、インストールメディアまたはISOファイルの **[AutoSelect]** をダブルクリックします。コマンドラインインターフェイスを使用する場合は、「コマンドラインを使ったインストール」を参照してください。

手順1： アップグレード可能な複数のコアコンポーネント（Controller、Studio、ライセンスサーバーなど）が同じサーバーにインストールされている場合、インストーラーによりそれらがすべてアップグレードされます。

コアコンポーネントがController以外のマシンにインストールされている場合は、各マシン上でインストーラーを実行します。推奨される順番は次のとおりです。 License Server、StoreFront、Director。

手順2： Provisioning Servicesを使用する場合、Provisioning Servicesのドキュメントの指示に従って、PVSサーバーとクライアントをアップグレードします。

手順3： アップグレードするVDAのマシン上で製品インストーラーを実行します（マスターイメージおよびMachine Creation Servicesを使用する場合は、手順12を参照してください）。

手順4： 半数のController上で製品のインストーラーを実行します（これにより、これらのサーバー上にインストールされたほかのコアコンポーネントもアップグレードされます）。たとえば、サイトにControllerが4つある場合は2つのControllerを先にアップグレードします。

- 半分のControllerをそのまま残すことで、ユーザーはそのサイトを引き続き使用できます。VDAはこれらの残りのControllerに登録されます。動作するControllerの数が減少するため、サイトの処理能力が低下する場合があります。データベースのアップグレードの最終段階で新しいクライアント接続を確立するときに、ほんの短い間だけサイトの動作が中断されます。サイト全体がアップグレードされるまでは、アップグレード済みのControllerでは要求を処理できません。
- サイトにControllerが1つしかない場合、アップグレード中はサイトが動作しなくなります。

手順5： 既にアップグレードしたControllerとは別のマシンにStudioがインストールされている場合は、そのマシン上でインストーラーを実行します。

手順6： アップグレードしたStudioを使ってサイトデータベースをアップグレードします。詳しくは、「データベースとサイトのアップグレード」を参照してください。

手順7： アップグレードしたStudioのナビゲーションペインで **[Citrix Studio**（*<サイト名>*）**]** を選択し、 **[よく使用するタスク]** タブの **[残りのDelivery Controllerのアップグレード]** を選択します。

手順8： 残りのControllerでのアップグレードが完了したら、Studioをいったん閉じてから再度開きます。Studioに、Controllerのサービスをサイトに登録するため、またはゾーンIDがまだ存在しない場合は作成するために、追加のサイトアップグレードを要求するメッセージが表示されることがあります。

手順9： ［よく使用するタスク］ページの［サイト構成］セクションで、**[登録の実行]** を選択します。Controllerを登録すると、サイトで使用できるようになります。

手順10： アップグレードの完了時に **[完了]** を選択すると、Citrixの利用統計情報プログラムに登録するかどうかを選択できるページが表示されます。このプログラムでは、使用環境に関する情報が収集されます。収集された情報は、弊社製品の品質、信頼性、およびパフォーマンスの向上のために使用させていただきます。

手順11： コンポーネント、データベース、およびサイトのアップグレードが完了したら、新しくアップグレードされたサイトをテストします。Studioのナビゲーションペインで **[Citrix Studio**（*<サイト名>*）**]** を選択し、 **[よく使用するタスク]** タブ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

の **[サイトのテスト]** を選択します。これらのテストはデータベースのアップグレード後に自動的に実行されますが、必要に応じて再実行できます。

> ControllerをWindows Server 2016にインストールして、サイトデータベースにローカルのSQL Server Expressを使用している場合、SQL Server Browserが開始されてないと、サイトのテスト機能でエラーが発生する可能性があります。これを回避するには、以下のタスクを行います。
>
> 1. （必要に応じて）SQL Server Browserサービスを有効にして開始します。
> 2. SQL Server（SQLEXPRESS）サービスを再開始します。

手順12： Machine Creation Servicesを使用しておりアップグレード後のVDAを使用する必要がある場合：アップグレードと環境のテスト後に、マスターイメージで使用するVDAを更新します（まだ更新していない場合）。これらのVDAを使用するマスターイメージを更新します。「マスターイメージの更新または新しいマスターイメージの作成 を参照してください。 次に、これらのマスターイメージを使用するマシンカタログを更新し、さらにこれらのカタログを使用するデリバリーグループをアップグレードします。

コアコンポーネントとVDAをアップグレードしたら、アップグレードしたStudioを使ってデータベースとサイトの自動または手動アップグレードを開始します。

そのほかの注意事項： 権限要件に関して上記の「準備」セクションを確認してください。

- データベースの自動アップグレードでは、SQL Serverデータベーススキーマを更新できる権限がStudioユーザーに必要です。
- 手動アップグレードの場合、StudioユーザーはStudioが生成したスクリプトをいくつか実行します。データベース管理者は、SQLCMDユーティリティ、またはSQL Server Management StudioをSQLCMDモードで使用し、そのほかのスクリプトを実行します。このようにしないと、エラーが発生することがあります。

重要： アップグレードを実行する前に、データベースをバックアップしておくことを強く推奨します。CTX135207を参照してください。
データベースのアップグレード中は製品サービスが無効になります。その間はControllerでサイトへの接続要求を仲介できなくなるため、慎重な計画が必要です。

データベースのアップグレードが完了し、製品サービスが有効になると、Studioにより環境と構成がテストされてHTMLレポートが生成されます。問題が見つかった場合は、データベースのバックアップを復元できます。問題を解決した後で、データベースのアップグレードを再試行します。

データベースとサイトの自動アップグレード：

アップグレードしたStudioを起動します。［サイトの自動アップグレードを開始する］を選択して準備内容を確認すると、データベースとサイトのアップグレードが開始されます。

データベースとサイトの手動アップグレード：

手順1： 新たにアップグレードしたStudioを起動します。［このサイトを手動でアップグレードする］を選択すると、ウィザードによってライセンスサーバーの互換性がチェックされて確認メッセージが表示されます。データベースをバックアップしてあることを確認すると、スクリプトとアップグレード手順のチェックリストが生成されて表示されます。

手順2： 以下のスクリプトを順番に実行します。

スクリプト	説明

© 1999-2017 Citrix Systems, Inc. All rights reserved.

DisableServices.ps1	Controller上でStudioユーザーが実行するPowerShellスクリプト。製品サービスを無効にします。
UpgradeSiteDatabase.sql	サイトデータベースを格納しているサーバー上でデータベース管理者が実行するSQLスクリプト。
UpgradeMonitorDatabase.sql	モニターデータベースを格納しているサーバー上でデータベース管理者が実行するSQLスクリプト。
UpgradeLoggingDatabase.sql	構成ログデータベースを格納しているサーバー上でデータベース管理者が実行するSQLスクリプト。このスクリプトは、このデータベースが変更された場合にのみ実行します（Hotfixの適用後など）。
EnableServices.ps1	Controller上でStudioユーザーが実行するPowerShellスクリプト。製品サービスを有効にします。

手順3：チェックリストのタスクを完了したら、**[アップグレードを完了する]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp 6.5ワーカーから新しいVDAへのアップグレード

Dec 05, 2017

XenAppp6.5ファームに移行した後は、以前のソフトウェアを削除し、新しいVDA for Server OSをインストールすることで、セッションホスト専用モード（セッションホストモードまたはワーカーとも呼ばれます）で構成されたXenApp6.5サーバーを使用できます。

注：XenApp 6.5ワーカーサーバーはアップグレードできますが、クリーンなマシンに最新のVDAソフトウェアをインストールする方が、セキュリティは優れています。

XenApp 6.5ワーカーから新しいVDAにアップグレードするには、以下の操作を行います。

1. hotfix readmeの説明に従って、XenApp 6.5のHotfix Rollup Pack 7を削除します。CTX202095を参照してください。
2. 「役割やコンポーネントを削除する」の説明に従って、XenApp 6.5を削除します。このプロセスでは再起動が数回必要です。アンインストール時にエラーが発生した場合は、エラーメッセージに従ってアンインストールエラーログを参照してください。ログファイルは、%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\フォルダーに生成されます。
3. このリリースで提供されるインストーラーを使って、VDA for Server OSをインストールします。「VDAのインストール」または「コマンドラインを使ったインストール」を参照してください。

新しいVDAをインストールした後、新しいXenAppサイトのStudioを使用して、アップグレードされたワーカーのマシンカタログを作成（または既存のマシンカタログを編集）します。

トラブルシューティング

問題：XenApp 6.5ソフトウェアのアンインストールに失敗し、アンインストールログにメッセージ「Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct.」が記録される。

原因：この問題は、元のXenApp 6.5のインストール時にCitrix XML Service（CtxHttp.exe）とIISとのポート共有を無効にしたシステム、および.NET Framework 3.5.1がインストールされたシステムで発生します。

解決策：

1. Windowsのサーバーの役割の削除ウィザードを使用して［Webサーバー（IIS）の役割］を削除します。Webサーバー（IIS）の役割は必要に応じて後で再インストールできます。
2. サーバーを再起動します。
3. ［プログラムの追加と削除］を使って、Citrix XenApp 6.5とMicrosoft Visual C++ 2005 Redistributable（x64）バージョン8.0.56336をアンインストールします。
4. サーバーを再起動します。
5. VDA for Windows Server OS をインストールします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp 6.xからの移行

Dec 05, 2017

注：Citrix Smart Migrate製品をこのバージョンのXenAppおよびXenDesktopとともに使用することはできません。移行ツールは使用できます。

XenApp 6.x移行ツール

XenApp 6.xの移行ツールでは、いくつかのPowerShellスクリプトが実行されます。これらのスクリプトにより、XenApp 6.x（6.0または6.5）のポリシーおよびファームデータを移行するためのコマンドレットが実行されます。XenApp 6.xのコントローラーサーバー上でエクスポートコマンドレットを実行して、データをXMLファイルにエクスポートします。その後でXenApp 7.6 Controller上でインポートコマンドレットを実行して、エクスポートされたデータに基づいてオブジェクトを作成します。

移行ツールの概要ビデオについてはここを参照してください。

移行プロセスの主な手順は以下のとおりです。詳しい説明については後述します。

1. XenApp 6.0または6.5のコントローラー上で、以下の操作を行います。
   1. PowerShellのエクスポートモジュールをインポートします。
   2. エクスポートコマンドレットを実行して、ポリシーとファームのデータをXMLファイルにエクスポートします。
2. エクスポートしたXMLファイルおよびアイコンフォルダー（エクスポート時にアイコンをXMLファイルに埋め込まなかった場合）をXenApp 7.6のControllerにコピーします。
3. XenApp 7.6のController上で、以下の操作を行います。
   1. PowerShellのインポートモジュールをインポートします。
   2. インポートコマンドレットを実行して、ポリシーとファーム（アプリケーション）のデータをXMLファイルからインポートします。
4. 移行後のタスクを完了します。

実際に移行を実行する前に、XenApp 6.xの設定をエクスポートしてからXenApp 7.6サイトでプレビューインポートを実行できます。これにより、問題が発生する可能性がある箇所を特定して、実際にインポートを実行する前に問題を修正できます。たとえば、新しいXenApp 7.6サイトに同じ名前のアプリケーションが既に存在していることが検出される場合があります。プレビューによって生成されるログファイルを実際の移行を実行するためのガイドとして使用することもできます。

特に明記されている場合を除き、6.xはXenApp 6.0または6.5を指します。

2014年12月の リリース（Version 20141125）には、以下の更新が含まれています。

- XenApp 6.0ファームで移行ツールを使用するときに問題が 発生する場合は、 サポートフォーラム （http://discussions.citrix.com/forum/1411-xenapp7x/）までご報告ください。 このツールのアップデート開発にあたり、調査させていただきます。
- 新しいパッケージ - XAMigration.zipファイルには、ReadIMA.zipとImportFMA.zipという2つのパッケージが含まれています。 ReadIMA.zipおよびImportFMA.zip。XenApp 6.xサーバーからのエクスポートでは、ReadIMA.zip のみが必要です。XenApp 7.6サーバーへのインポートでは、ImportFMA.zip のみが必要です。
- Export-XAFarmコマンドレットにEmbedIconDataパラメーターが追加されました。これを使用すると、アイコンデータを別個のファイルとしてコピーする 必要がなくなります。
- Import-XAFarmコマンドレットに以下の3つのパラメーターが追加されました。
  - MatchServer - 条件に一致する名前のサーバーからアプリケーションをインポートします。
  - NotMatchServer - 条件に 一致しない名前のサーバーからアプリケーションをインポートします。
  - IncludeDisabledApps - 無効に設定されたアプリケーションをインポートします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 事前起動 アプリケーションはインポートされません。
- Export-Policyコマンドレットは、XenDesktop 7.x上で機能します。

移行ツールのパッケージは、Citrix社のダウンロードサイトから入手できます。XAMigration.zipファイルには、以下の2つのパッケージが含まれています。

- ReadIMA.zip - XenApp 6.xファームからデータをエクスポートするためのファイルと、共有モジュールが含まれています。

モジュールまたはファイル	説明
ExportPolicy.psm1	XenApp 6.xのポリシーをXMLファイルにエクスポートするPowerShellスクリプトモジュール。
ExportXAFarm.psm1	XenApp 6.xのファーム設定をXMLファイルにエクスポートするPowerShellスクリプトモジュール。
ExportPolicy.psd1	スクリプトモジュールExportPolicy.psm1のPowerShellマニフェストファイル。
ExportXAFarm.psd1	スクリプトモジュールExportXAFarm.psm1のPowerShellマニフェストファイル。
LogUtilities.psm1	ログ機能を含んでいる共有PowerShellスクリプトモジュール。
XmlUtilities.psd1	スクリプトモジュールXmlUtilities.psm1のPowerShellマニフェストファイル。
XmlUtilities.psm1	XML機能を含んでいる共有PowerShellスクリプトモジュール。

- ImportFMA.zip - XenApp 7.6ファームにデータをインポートするためのファイルと、共有モジュールが含まれています。

モジュールまたはファイル	説明
ImportPolicy.psm1	ポリシーをXenApp 7.6サイトにインポートするPowerShellスクリプトモジュール。
ImportXAFarm.psm1	アプリケーションをXenApp 7.6サイトにインポートするPowerShellスクリプトモジュール。
ImportPolicy.psd1	スクリプトモジュールImportPolicy.psm1のPowerShellマニフェストファイル。
ImportXAFarm.psd1	スクリプトモジュールImportXAFarm.psm1のPowerShellマニフェストファイル。
PolicyData.xsd	ポリシーデータのXMLスキーマ。
XAFarmData.xsd	XenAppファームデータのXMLスキーマ。
LogUtilities.psm1	ログ機能を含んでいる共有PowerShellスクリプトモジュール。
XmlUtilities.psd1	スクリプトモジュールXmlUtilities.psm1のPowerShellマニフェストファイル。
XmlUtilities.psm1	XML機能を含んでいる共有PowerShellスクリプトモジュール。

- 一部のポリシー設定はインポートされません。「インポートされないポリシー設定」を参照してください。サポートされない設定は無視され、ログファイルに記録されます。
- エクスポートによりすべてのアプリケーションの詳細がXMLファイルにエクスポートされますが、サーバー上にインストールされたアプリケーションだけがXenApp 7.6サイトにインポートされます。つまり、公開アプリケーション、公開コンテンツ、および多くのストリーム配信アプリケーション

© 1999-2017 Citrix Systems, Inc. All rights reserved.

インポートされません。例外については、「手順：データのインポート」のImport-XAFarmコマンドレットのパラメーターを参照してください。
- アプリケーションサーバーはインポートされません。
- XenApp 6.xのIndependent Management Architecture（IMA）とXenApp 7.6のFlexCast Management Architecture（FMA）ではアーキテクチャが異なるため、アプリケーションプロパティの多くはインポートされません（「アプリケーションプロパティの対応」参照）。
- インポートによりデリバリーグループは作成されません。インポートする項目を制限するためのパラメーターの使用については、高度な使用方法」を参照してください。
- AppCenterで作成されたCitrixポリシーの設定だけがインポートされます。Windowsグループポリシーオブジェクト（GPO）で作成されたCitrixポリシーはインポートされません。
- 移行スクリプトは、XenApp 6.xからXenApp 7.6への移行のみを対象としています。
- Studioは複数階層で5レベルよりも深いフォルダーはサポートされず、インポートされません。アプリケーションフォルダー構造に5レベルより深いフォルダーがある場合、インポートを実行する前にフォルダーレベルの階層数を減らすことを検討してください。

エクスポートスクリプトによって 作成されるXMLファイルには 環境と組織に関する機密情報（ユーザー名、サーバー名、および XenAppファーム、アプリケーション、ポリシーの構成データなど）が含まれることがあるため、 安全な取り扱いが必要です。

ポリシーと アプリケーションをインポートする前に、 XMLファイルが不正に変更されていないことを確認してください。

ポリシーの 適用方法は、オブジェクトへのポリシーの 割り当て（ポリシーフィルター）によって制御されます。ポリシーをインポートしたら、 各ポリシーのオブジェクト割り当てをよく調べて、 インポートに起因するセキュリティ上の脆弱性がないことを確認してください。インポートしたポリシー別のユーザー、IPアドレス、またはクライアント名が 割り当てられていることがあります。許可/拒否の設定の意味が 変わることもあります。

スクリプトにより、コマンドレットのすべての実行、情報 メッセージ、実行結果、警告、およびエラーについてのログが 記録されます。
- ほとんどのCitrix PowerShellコマンドレットでログが生成されます。インポートスクリプトで新しいサイトオブジェクトを 作成するために実行されるすべてのPowerShellコマンドレットでもログが生成されます。
- スクリプトの 実行状況（処理中のオブジェクトなど）についてのログが記録されます。
- 処理フローの状態に 影響する主な操作のログが記録されます。これには、 コマンドラインからのフローも含まれます。
- コンソールに 出力されるすべてのメッセージがログに記録されます。これには、警告やエラーも含まれます。
- ログの各行には、ミリ秒までの タイムスタンプが記録されます。

エクスポートおよびインポートのコマンドレットを実行するときは、常に個別のログファイルを 指定することをお勧めします。

ログファイルの名前を 指定しない場合、実行ユーザーの既存のホーム フォルダー（PowerShell $HOME変数で指定される）にログファイルが格納されます。ホームフォルダーが存在しない 場合は、スクリプトの現在の実行フォルダーに格納されます。デフォルトでは、「XFarm<YYYYMMDDHHmmSS-xxxxxx>」という ログファイルが生成されます。ここで、「xxxxxx」はランダムな数字で 構成されます。

デフォルトでは、すべての 進捗情報が表示されます。表示されないようにするには、エクスポートコマンドレットとインポートコマンドレットで NoDetailsパラメーターを指定します。

通常、 スクリプトでエラーが発生すると処理がそこで停止します。エラー状態を解決した後で、コマンドレットを 再実行できます。

エラーとして みなされない状態も多くは警告としてログに記録され、スクリプトの 実行は続行されます。たとえば、アプリケーションの種類がサポートされない場合は 警告として記録され、インポートから除外されます。XenApp 7.6サイトに既に存在するアプリケーションはインポートされません。XenApp 7.6でサポートされなくなったポリシー設定はインポート されません。

移行 スクリプトでは多くのPowerShellコマンドレットが使用され、一部のエラーが ログに記録されない場合があります。ログに記録される情報を追加するには、PowerShellのログ機能を使用してください。 たとえば、PowerShellで 画面上に出力されるすべての情報をログに記録できます。詳しくは、Start-Transcriptおよび Stop-Transcriptコマンドレットのヘルプを参照してください。

移行には、Citrix XenApp 6.5 SDKを使用する必要があります。SDKは、https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.htmlからダウンロードできます。

重要：移行を開始する前に、このトピック全体をよくお読みください。
PowerShellの実行ポリシー、モジュール、スクリプトなどについての基本的な理解が必要です。スクリプトを作成するための専門知識は必要ありませんが、実行するコマンドレットについて理解しておく必要があります。事前にGet-Helpコマンドレットを使用して、各移行コマンドレットのヘルプを確認しておいてください。例：
Get-Help -full Import-XAFarm
コマンドラインでログファイルを指定して、コマンドレットの実行後にそのログファイルを確認してください。スクリプトの処理に失敗した場合は、ログファイルを参照してエラーを解決し、コマンドレットを再実行してください。

ヒント：
- 2つの環境（XenApp 6.xファームと新しいXenApp 7.6サイト）を実行している間のアプリケーション配信を容易にするには、StoreFrontまたはWeb Interfaceで両方の環境を集約します。eDocsで、使用するStoreFrontまたはWeb Interfaceのドキュメント（「管理」>「ストアの作成」）を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- アプリケーションのアイコンデータは、以下のいずれかの方法で処理されます。
  - EmbedIconDataパラメーターを指定してExport-XAFarmコマンドレットを実行すると、アプリケーションのアイコンデータが埋め込まれたXMLファイルがエクスポートされます。
  - EmbedIconDataパラメーターを指定せずにExport-XAFarmコマンドレットを実行すると、エクスポートされたXMLファイルのベース名に「-icons」を追加した名前のフォルダーにアプリケーションのアイコンデータが格納されます。たとえば、XmlOutputFileパラメーターで「FarmData.xml」を指定した場合は、「FarmData-icons」というフォルダーが作成され、そこにアプリケーションアイコンが格納されます。
    このフォルダーに格納されるアイコンデータファイルは、その公開アプリケーションの表示名に基づく名前のTXTファイルです。これらのファイルにはエンコードされたバイナリアイコンデータが記述されており、インポートスクリプトがこれを読み込んでアプリケーションアイコンを再作成します。インポート時にXMLファイルと同じフォルダー内にアイコンフォルダーが見つからない場合、インポートした各アプリケーションで標準的なアイコンが使用されます。

- スクリプトモジュール、マニフェストファイル、共有モジュール、およびコマンドレットには類似した名前が付けられています。Tabキーによる補完機能を使用して、入力エラーを避けることができます。たとえば、Export-XAFarmはコマンドレット名です。ExportXAFarm.psd1およびExportXAFarm.psm1には似たファイル名が付いていますが、コマンドレットとは異なり実行不能です。
- 後述の手順説明で、<string>パラメーターの値は二重引用符で囲んであります。値にスペースが含まれない場合、二重引用符で囲まなくても正しく処理されます。

XenApp 6.xサーバーからのエクスポート:
- エクスポートは、コントローラーモードとセッションホストモード（通常コントローラーと呼ばれます）で構成されたXenApp 6.xサーバー上で実行する必要があります。
- エクスポートコマンドレットを実行するには、オブジェクトの読み取り権限を持つXenApp管理者である必要があります。また、PowerShellスクリプトを実行するためのWindows権限も必要です。設定方法は、後述の手順説明に記載されています。
- エクスポートを開始する前に、XenApp 6.xファームのヘルス状態が良好であることを確認します。ファームデータベースをバックアップします。Citrix IMA Helperツール（CTX137461）を使用してファームの整合性を確認します。［IMA Datastore］タブでMaster Checkを実行します（実行後、DSCheckオプションを使用して無効なエントリを解決します）。移行前に問題を解決しておくと、エクスポートエラーを避けることができます。たとえば、ファームから不適切に削除されたサーバーがあると、データベースにそのサーバーのデータが残ってしまい、エクスポートスクリプトのコマンドレット（Get-XAServer-ZoneNameなど）の処理が失敗することがあります。コマンドレットの処理が失敗すると、スクリプトの処理も失敗します。
- ファームにユーザーが接続している状態でもエクスポートコマンドレットを実行できます。エクスポートスクリプトでは、静的なファーム構成とポリシーデータのみが読み取られます。

XenApp 7.6サーバーへのインポート:
- XenApp 7.6環境（およびそれ以降の移行可能なバージョン）にデータをインポートできます。XenApp 6.xファームからエクスポートしたデータをインポートする前に、XenApp 7.6のControllerとStudioをインストールしてサイトを作成しておく必要があります。設定をインポートするためにVDAをインストールしておく必要はありませんが、インストールしておくとアプリケーションのファルタイプが使用可能になります。
- インポートコマンドレットを実行するには、オブジェクトの読み取り権限および作成権限を持つXenApp管理者である必要があります。すべての管理権限を実行できる管理者には必要な権限が付与されています。また、PowerShellスクリプトを実行するためのWindows権限も必要です。設定方法は、後述の手順説明に記載されています。
- インポート時にほかのユーザーが接続していないことを確認してください。インポートスクリプトにより多くのオブジェクトが作成されるため、ほかのユーザーが同時に構成を変更すると環境が正しく機能しなくなることがあります。

エクスポートしたデータを事前にテストするために、インポートコマンドレットに-Previewパラメーターを指定して実行することができます。これにより、実際にインポートを行う前に、インポート内容を確認することができます。このパラメーターでは、実際のインポートにより実行される処理がログとして出力されます。ここでエラーが発生した場合は、それを解決してからインポートを行います。

エクスポート処理のビデオについてはここを参照してください。

XenApp 6.xのコントローラーからXMLファイルにデータをエクスポートするには、次の手順に従います。

1. Citrixのダウンロードサイトから、移行ツールのパッケージXAMigration.zipをダウンロードします。XenApp 6.xファームおよびXenApp 7.6サイトの両方からアクセスできるネットワーク上の共有フォルダーにパッケージをダウンロードすると便利です。ネットワーク上の共有フォルダーでXAMigration.zipを展開します。ReadIMA.zipおよびImportFMA.zipの2つのZIPファイルが展開されます。
2. ファームに対する読み取り以上の権限と、PowerShellスクリプトを実行できるWindows権限を持つXenApp管理者としてXenApp 6.xのコントローラーにログオンします。
3. 共有フォルダーのReadIMA.zipをXenApp 6.xのコントローラーにコピーします。コントローラー上のReadIMA.zipを展開し、新規フォルダー（C:\XAMigrationなど）にスクリプトを展開します。
4. PowerShellコンソールを開き、カレントディレクトリをスクリプトの場所に移動します。例：
   cd C:\XAMigration
5. Get-ExecutionPolicyを実行して、スクリプトの実行ポリシーを確認します。
6. スクリプトを実行するには、実行ポリシーをRemoteSignedまたはそれ以上に設定する必要があります。例：
   Set-ExecutionPolicy RemoteSigned
7. 以下のコマンドを実行して、モジュール定義ファイルExportPolicy.psd1およびExportXAFarm.psd1をインポートします。
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

   ヒント：
   - 移行するデータがポリシーデータのみの場合は、モジュール定義ファイルExportPolicy.psd1のみをインポートできます。同様に、移行するデータがファームデータのみの場合は、ExportXAFarm.psd1のみをインポートできます。
   - モジュール定義ファイルをインポートすると、必要なPowerShellスナップインも追加されます。
   - スクリプトモジュールファイル（*.psm1）をインポートしないでください。
8. Export-Policyコマンドレットを実行して、ポリシーデータをエクスポートします。

パラメーター	説明
-XmlOutputFile "<string>.xml"	出力するXMLファイルの名前です。このファイルにエクスポートされたデータが記述されます。拡張子として「.xml」を指定する必要があります。既存のファイル名を指定しないでください。ただし、パスを指定する場合は既存のパスを指定してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

パラメーター	説明
	デフォルト：なし。必須パラメーターです。
-LogFile "<string>"	ログファイルの名前です。必要に応じて拡張子を指定します。指定したファイルが存在しない場合は新規に作成されます。ファイルが存在し、-NoClobberパラメーターも指定した場合はエラーが発生します。-NoClobberパラメーターを指定しない場合は既存のファイルが上書きされます。 デフォルトは以下のとおりです。 「ログとエラー処理」を参照
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFileパラメーターが無視されます。 デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFileパラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。 デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。 デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。 デフォルト：False。上記のメッセージがコンソールに表示されます。

例：次のコマンドレットを実行すると、MyPolicies.xmlという名前のXMLファイルにポリシー情報がエクスポートされます。この処理は、MyPolicies.logという名前のログファイルに記録されます。
Export-Policy -XmlOutputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"

9. Export-XAFarmコマンドレットを実行して、ファームデータをエクスポートします。

パラメーター	説明
-XmlOutputFile "<string>.xml"	出力するXMLファイルの名前です。このファイルにエクスポートされたデータが記述されます。拡張子として「.xml」を指定する必要があります。既存のファイル名を指定しないでください。ただし、パスを指定する場合は既存のパスを指定してください。 デフォルト：なし。必須パラメーターです。
-LogFile "<string>"	ログファイルの名前です。必要に応じて拡張子を指定します。指定したファイルが存在しない場合は新規に作成されます。ファイルが存在し、-NoClobberパラメーターも指定した場合はエラーが発生します。-NoClobberパラメーターを指定しない場合は既存のファイルが上書きされます。 デフォルトは以下のとおりです。 「ログとエラー処理」を参照
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFileパラメーターが無視されます。 デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFileパラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。 デフォルト：False。既存のファイルが上書きされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

パラメーター	説明
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。 デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。 デフォルト：False。上記のメッセージがコンソールに表示されます。
-IgnoreAdmins	管理者情報をエクスポートから除外します。使用方法については、「高度な使用方法」を参照してください。 デフォルト：False。管理者情報がエクスポートされます。
-IgnoreApps	アプリケーション情報をエクスポートから除外します。使用方法については、「高度な使用方法」を参照してください。 デフォルト：False。アプリケーション情報がエクスポートされます。
-IgnoreServers	サーバー情報をエクスポートから除外します。 デフォルト：False。サーバー情報がエクスポートされます。
-IgnoreZones	ゾーン情報をエクスポートから除外します。 デフォルト：False。ゾーン情報がエクスポートされます。
-IgnoreOthers	そのほかの情報（構成ログ、負荷評価基準、負荷分散ポリシー、プリンタードライバー、およびワーカーグループ）をエクスポートから除外します。 デフォルト：False。上記の情報がエクスポートされます。 注： IgnoreOtherスイッチの目的は、エクスポートまたはインポートに使用中の実データには影響がないエラーが生じた場合に、エクスポート処理を可能にすることです。
-AppLimit <integer>	エクスポートするアプリケーションの数を指定します。使用方法については、「高度な使用方法」を参照してください。 デフォルト：すべてのアプリケーションがエクスポートされます。
-EmbedIconData	アプリケーションのアイコンデータをXMLファイル内に埋め込みます。 デフォルト：アイコンデータは埋め込まれず、別フォルダー内に格納されます。詳細は、「要件、準備、およびベストプラクティス」を参照してください。
-SkipApps <integer>	エクスポートを省略するアプリケーションの数を指定します。使用方法については、「高度な使用方法」を参照してください。 デフォルト：アプリケーションは省略されません。

例：次のコマンドレットを実行すると、MyFarm.xmlという名前のXMLファイルにファーム情報がエクスポートされます。この処理は、MyFarm.logという名前のログファイルに記録されます。MyFarm.XMLと同じフォルダー内に「MyFarm-icons」という名前のフォルダーが作成され、そこにアプリケーションのアイコンデータが格納されます。

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"
```

エクスポートスクリプトの処理が完了すると、コマンドラインで指定したXMLファイルにポリシーとXenAppファームのデータが含まれています。アプリケーションアイコンファイルにはアイコンデータが含まれ、ログファイルにはエクスポート処理の内容が記述されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

インポート処理のビデオについてはここを参照してください。

エクスポートしたデータを事前にテストするために、Import-PolicyまたはImport-XAFarmコマンドレットに-Previewパラメーターを指定して実行することができます。これにより、実際にインポートを行う前に、インポート内容をログファイルで確認することができます。

エクスポートで生成されたXMLファイルの情報をXenApp 7.6サイトにインポートするには、次の手順に従います。

1. サイトに対する読み取り/書き込み権限と、PowerShellスクリプトを実行できるWindows権限を持つ管理者としてXenApp 7.6のControllerにログオンします。
2. 移行ツールのパッケージXAMigration.zipをネットワーク上の共有フォルダーに展開します。共有フォルダーのImportFMA.zipをXenApp 7.6のControllerにコピーします。Controller上のImportFMA.zipを展開し、新規フォルダー（C:\XAMigrationなど）にスクリプトを展開します。
3. XenApp 6.xのコントローラーでエクスポートされたXMLファイルを、XenApp 7.6 ControllerのImportFMA.zipの展開先フォルダー（つまりC:\XAMigrationなど）にコピーします。
   Export-XAFarmコマンドレット実行時にアプリケーションのアイコンデータをXMLファイルに埋め込まなかった場合は、アイコンデータのフォルダーおよびファイルをXMLファイルのコピー先フォルダー（つまりC:\XAMigrationなど）にコピーします。
4. PowerShellコンソールを開き、カレントディレクトリをスクリプトの場所に移動します。
   cd C:\XAMigration
5. Get-ExecutionPolicyを実行して、スクリプトの実行ポリシーを確認します。
6. スクリプトを実行するには、実行ポリシーをRemoteSignedまたはそれ以上に設定する必要があります。例：
   Set-ExecutionPolicy RemoteSigned
7. 以下のコマンドを実行して、PowerShellモジュール定義ファイルImportPolicy.psd1およびImportXAFarm.psd1をインポートします。
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   ヒント：
   - 移行するデータがポリシーデータのみの場合は、モジュール定義ファイルImportPolicy.psd1のみをインポートできます。同様に、移行するデータがファームデータのみの場合は、ImportXAFarm.psd1のみをインポートできます。
   - モジュール定義ファイルをインポートすると、必要なPowerShellスナップインも追加されます。
   - スクリプトモジュールファイル（*.psm1）をインポートしないでください。
8. Import-Policyコマンドレットを実行して、ポリシーデータをインポートします。

パラメーター	説明
-XmlInputFile "<string>.xml"	入力するXMLファイルの名前です。Export-Policyコマンドレットで収集されたデータが記述されています。拡張子として「.xml」を指定する必要があります。 デフォルト：なし。必須パラメーターです。
-XsdFile "<string>"	XSDファイルの名前です。インポートスクリプトでは、このファイルにより入力XMLファイルの構文が検証されます。使用方法については、「高度な使用方法」を参照してください。 デフォルト：PolicyData.XSD。
-LogFile "<string>"	ログファイルの名前です。エクスポート時に生成されたログファイルもController上にコピーしてある場合は、異なるログファイル名を指定してください。 デフォルトは以下のとおりです。「ログとエラー処理」を参照
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFileパラメーターが無視されます。 デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFileパラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。 デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

パラメーター	説明
	デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。 デフォルト：False。上記のメッセージがコンソールに表示されます。
-Preview	プレビューインポートを実行します。この処理では、入力XMLファイルからデータが読み込まれますが、サイトへのオブジェクトのインポートは実行されません。プレビューインポートにより、実際のインポートで実行される処理内容がログファイルおよびコンソールに出力されます。これにより、管理者はインポートの問題を事前に解決できます。 デフォルト：False。実際のインポートが実行されます。

例：次のコマンドレットを実行すると、MyPolicies.xmlという名前のXMLファイルからポリシーデータがインポートされます。この処理は、MyPolicies.logという名前のログファイルに記録されます。
Import-Policy -XmlInputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"

9. Import-XAFarmコマンドレットを実行して、アプリケーションデータをインポートします。

パラメーター	説明
-XmlInputFile "<string>.xml"	入力するXMLファイルの名前です。Export-XAFarmコマンドレットで収集されたデータが記述されています。拡張子として「.xml」を指定する必要があります。 デフォルト：なし。必須パラメーターです。
-XsdFile "<string>"	XSDファイルの名前です。インポートスクリプトでは、このファイルにより入力XMLファイルの構文が検証されます。使用方法については、「高度な使用方法」を参照してください。 デフォルト：XAFarmData.XSD。
-LogFile "<string>"	ログファイルの名前です。エクスポート時に生成されたログファイルもController上にコピーしてある場合は、異なるログファイル名を指定してください。 デフォルトは以下のとおりです。「ログとエラー処理」を参照
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFileパラメーターが無視されます。 デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFileパラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。 デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。 デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。 デフォルト：False。上記のメッセージがコンソールに表示されます。
-Preview	プレビューインポートを実行します。この処理では、入力XMLファイルからデータが読み込まれますが、サイトへのオ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

パラメーター	説明
	オブジェクトのインポートは実行されません。プレビューインポートにより、実際のインポートで実行される処理内容がログファイルおよびコンソールに出力されます。これにより、管理者はインポートの問題を事前に解決できます。 デフォルト：False。実際のインポートが実行されます。
-DeliveryGroupName "<string>"	インポートされるすべてのアプリケーションのデリバリーグループです。使用方法については、 高度な使用方法」を参照してください。 デフォルトは以下のとおりです。 "<xenapp-farm-name> - デリバリー グループ
-MatchFolder "<string>"	にマッチする名前のフォルダー内のアプリケーションのみをインポートします。使用方法については、 高度な使用方法」を参照してください。 デフォルト：の指定なし。
-NotMatchFolder "<string>"	にマッチしない名前のフォルダー内のアプリケーションのみをインポートします。使用方法については、 高度な使用方法」を参照してください。 デフォルト：の指定なし。
-MatchServer "<string>"	にマッチする名前のサーバーからのアプリケーションのみをインポートします。使用方法については、 高度な使用方法」を参照してください。
-NotMatchServer "<string>"	にマッチしない名前のサーバーからのアプリケーションのみをインポートします。使用方法については、 高度な使用方法」を参照してください。 デフォルト：の指定なし。
-MatchWorkerGroup "<string>"	にマッチする名前のワーカーグループに公開されたアプリケーションのみをインポートします。使用方法については、「高度な使用方法」を参照してください。 デフォルト：の指定なし。
-NotMatchWorkerGroup "<string>"	にマッチしない名前のワーカーグループに公開されたアプリケーションのみをインポートします。使用方法については、「高度な使用方法」を参照してください。 デフォルト：の指定なし。
-MatchAccount "<string>"	にマッチする名前のユーザーアカウントに公開されたアプリケーションのみをインポートします。使用方法については、「高度な使用方法」を参照してください。 デフォルト：の指定なし。
-NotMatchAccount "<string>"	にマッチしない名前のユーザーアカウントに公開されたアプリケーションのみをインポートします。使用方法については、「高度な使用方法」を参照してください。 デフォルト：の指定なし。
-IncludeStreamedApps	種類が「StreamedToClientOrServerInstalled」のアプリケーションのみをインポートします。ほかの種類のストリーム配信アプリケーションはインポートされません。 デフォルト：ストリーム配信アプリケーションはインポートされません。
-IncludeDisabledApps	無効に設定されたアプリケーションをインポートします。 デフォルト：無効に設定されたアプリケーションはインポートされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

パラメーター	説明

例：次のコマンドレットを実行すると、MyFarm.xmlという名前のXMLファイルからアプリケーションデータがインポートされます。この処理は、MyFarm.logという名前のログファイルに記録されます。

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

10. インポート処理が正しく完了したら、移行後のタスクを行います。

XenApp 6.xのポリシーおよびファール設定をXenApp 7.6サイトにインポートしたら、以下のタスクを行ってインポート内容を確認します。

- **ポリシーおよびポリシーの設定項目**
  ポリシーのインポートでは、ポリシー情報が単にコピーされます。ただし。廃止予定のポリシーや設定項目はコピーされません。移行後の検証タスクは、本質的に移行前後の比較になります。

  1. ログファイルには、インポートされたり無視されたりしたすべてのポリシーおよび設定項目が記録されます。まず、ログファイルを参照してインポートされなかったポリシーおよび設定項目を確認します。
  2. XenApp 6.xのポリシーとXenApp 7.6にインポートされたポリシーを比較します。同じ設定値が保持されていることを確認します（次の手順で説明する廃止予定の設定項目を除く）。
     - 移行したポリシーの数が多くない場合は、XenApp 6.xのAppCenterとXenApp 7.6のStudioの両方でポリシーを並べて表示して視覚的に比較できます。
     - ポリシーの数が多い場合、視覚的に比較することは困難です。この場合、ポリシーのエクスポートコマンドレット（Export-Policy）を使用してXenApp 7.6のポリシーを別名のXMLファイルにエクスポートして、テキストファイルの比較ツール（windiffなど）を使用してXenApp 6.xからエクスポートしたファイルと比較します。
  3. 「インポートされないポリシー設定」セクションを参照して、インポート時に変更された可能性のある設定項目を確認します。XenApp 6.xのポリシーに廃止予定の設定項目のみが含まれる場合、そのポリシーはインポートされません。たとえば、XenApp 6.xで［サーバーヘルス監視テスト］設定のみが構成されたポリシーがある場合、対応する設定項目がXenApp 7.6にないため、そのポリシーは無視されます。
     一部のXenApp 6.xポリシー設定はサポートされなくなりましたが、同等の機能がXenApp 7.6に実装されています。たとえば、XenApp 7.6では、デリバリーグループを編集してサーバーOSマシンの再起動スケジュールを構成できます。この機能は、以前はポリシー設定で実装されていました。
  4. XenApp 7.6サイトとXenApp 6.xファームでのポリシーの適用フィルターの動作について確認します。XenApp 6.xファームとXenApp 7.6サイトとのフィルターの違いについては、次のセクションを参照してください。

- **フィルター**
  各ポリシーに適用されるフィルター（割り当て先）を慎重に確認してください。XenApp 6.xでの元のフィルター設定がXenApp 7.6でも正しく適用するようにするには、設定の変更が必要になる場合があります。

フィルター	注意事項
アクセス制御	XenApp 6.xからインポートしたアクセス制御フィルターには元の設定と同じ値が適用されており、変更は不要です。
Citrix CloudBridge	単純なブール値なので変更は不要です。（この製品は現在NetScaler SD-WANと呼ばれています。）
クライアントのIPアドレス	接続が許可または拒否されるクライアントIPアドレスの範囲の一覧です。インポートしたフィルターには元の設定と同じ値が適用されていますが、XenApp 7.6のVDAマシンに接続するクライアントが異なる場合は変更が必要です。
クライアント名	クライアントのIPアドレスと同様、インポートしたフィルターには元の設定と同じ値が適用されていますが、XenApp 7.6のVDAマシンに接続するクライアントが異なる場合は変更が必要です。
組織単位	インポート時に組織単位の解決が可能な場合は元の設定と同じ値が保持されます。特にXenApp 6.xとXenApp 7.6のマシンが異なるドメインに属している場合は、このフィルターの内容を確認してください。適切な値が設定されていない場合、ポリシーが不正な組織単位に適用されてしまいます。 組織単位は名前でのみ解決されます。このため、XenApp 6.xドメインの組織単位とは異なるメンバーシップを持つ組織単位に解決される可能性もあります。組織単位フィルターのいくつかの値が保持されている場合も、すべての値を確認してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フィルター	注意事項
ユーザーまたはグループ	インポート時にアカウントの解決が可能な場合は元の設定と同じ値が保持されます。 組織単位フィルターと同様、アカウントは名前でのみ解決されます。このため、XenApp 7.6サイトに同名のドメインおよびユーザーが存在する場合、XenApp 6.xドメインのユーザーとは異なるユーザーに解決される場合があります。フィルターの値を確認して適切に変更しないと、ポリシーが不正なアカウントに適用されてしまいます。
ワーカーグループ	XenApp 7.6では、ワーカーグループはサポートされません。XenApp 7.6サイトでは、デリバリーグループ、デリバリーグループの種類、およびタグを使用してポリシーを割り当ててください（これらのフィルターはXenApp 6.xでは使用できません）。 • デリバリーグループ：ポリシーを適用するデリバリーグループを指定します。このフィルターでは、既存のデリバリーグループを選択して許可または禁止を指定します。 • デリバリーグループの種類：ポリシーを適用するデリバリーグループの種類を指定します。このフィルターでは、デリバリーグループの種類を選択して許可または禁止を指定します。 • タグ：ポリシーを適用するVDAマシンのタグを指定します。このフィルターでは、既存のタグを選択して許可または禁止を指定します。

XenApp 6.xファームとXenApp 7.6サイトのドメインが異なる場合は、特にドメインユーザーの変更による影響を受けるフィルターについて詳細に確認してください。インポートスクリプトでは、ドメインやユーザーの名前が文字列でのみ解決され、移行先ドメインのユーザーが決定されます。このため、一部のアカウントが正しく解決されない場合があります。異なるドメインでドメイン名やユーザー名が同一であることはまれですが、これらのフィルターの値が正しく移行されていることを確認してください。

- **アプリケーション**
  アプリケーションをインポートするスクリプトでは、アプリケーションだけではなく、デリバリーグループなどのオブジェクトも作成されます。アプリケーションを複数回に分けてインポートすると、元のアプリケーションフォルダーの構造が大幅に変更されている場合があります。
  1. まず、移行ログファイルを確認して、インポートおよび除外されたアプリケーションと、アプリケーションの作成に使用されたコマンドレットの詳細を確認します。
  2. 各アプリケーションについて、以下を確認します。
     - 基本的なプロパティが正しく保持されていることを視覚的に確認します。「アプリケーションプロパティの対応」セクションを参照して、変更されずにインポートされるプロパティ、インポートから除外されるプロパティ、またはXenApp 6.xのアプリケーションデータで初期化されるプロパティについて確認します。
     - ユーザーの一覧を確認します。インポートスクリプトにより、指定ユーザーの一覧がXenApp 7.6の「表示の制限」のユーザー一覧としてインポートされます。この一覧で各ユーザーが正しく保持されていることを確認してください。
  3. アプリケーションサーバーはインポートされません。このため、インポートした直後のアプリケーションにユーザーがアクセスすることはできません。ユーザーがアクセスできるようにするには、これらのアプリケーションを含んでいるデリバリーグループを、アプリケーションの実行可能イメージを含んでいるマシンカタログに割り当てる必要があります。各アプリケーションについて、以下を確認します。
     - 実行可能ファイルの名前と作業ディレクトリが、そのデリバリーグループのマシンカタログで割り当てられているマシン上に存在すること。
     - コマンドラインパラメーター（ファイル名、環境変数、または実行可能ファイル名など）。そのデリバリーグループのマシンカタログで割り当てられているすべてのマシン上で、それらのパラメーターが有効である必要があります。
- **ログファイル**
  ログファイルには、エクスポートおよびインポートの処理に関する重要な情報が記録されています。既存のログファイルがデフォルトで上書きされず、固有のファイル名で生成される仕様になっているのはこのためです。

  前の「ログとエラー処理」で説明したように、PowerShellのStart-TranscriptおよびStop-Transcriptコマンドレットを使って入出力のすべてを記録した場合は、その記録とログファイルを参照することでエクスポートおよびインポートの詳細を確認することができます。

  ログファイルに記録されるタイムスタンプは、特定の問題について診断するときに便利です。たとえば、エクスポートまたはインポートに時間がかかった場合は、データベース接続に問題があったかどうか、またはユーザーアカウントの解決に時間がかかったのかどうかを確認できます。

  ログファイルに記録されたコマンドにより、移行するオブジェクトがどのように読み取られ、作成されたかを判断できます。たとえば、デリバリーグループを作成するときにはいくつかのコマンドが実行され、デリバリーグループオブジェクト自体だけでなく、そのデリバリーグループにアプリケーションオブジェクトを割り当てるためのアクセスポリシー規則などのオブジェクトも作成されます。

  エクスポートやインポートに失敗した場合もログファイルが役に立ちます。通常、ログファイルの最後の行を参照すると問題の原因が判断できる場合があります。ログファイルには、エラーメッセージも記録されます。XMLファイルとログファイルを参照して、問題発生時に処理されていたオブジェクトを特定できます。

移行内容を確認してテストした後で、以下のタスクを行います。

1. XenApp 6.5のワーカーサーバーを最新のVirtual Delivery Agent（VDA）にアップグレードします。これを行うには、ワーカーサーバー上でXenApp 7.6のインストーラーを実行します。これにより、XenApp 6.5がアンインストールされ、最新のVDAがインストールされます。手順については、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「XenApp 6.5ワーカーのVDA for Windows Server OSへのアップグレード」を参照してください。
XenApp 6.0のワーカーサーバーでは、手作業でXenApp 6.0をアンインストールします。その後でXenApp 7.6のインストーラーを使用して最新のVDAをインストールします。XenApp 7.6のインストーラーを実行してXenApp 6.0をアンインストールすることはできません。

2. 新しいXenAppサイトのStudioを使用して、そのワーカーのマシンカタログを作成（または既存のマシンカタログを編集）します。
3. そのマシンカタログを使用してデリバリーグループを作成し、アップグレードしたマシンおよびそれらのマシン上のアプリケーションをユーザーに供します。

デフォルトでは、Export-Policyコマンドレットによりすべてのポリシーデータ がXMLファイルにエクスポートされます。同様に、Export-XAFarmコマンドレットによりすべてのファームデータ がXMLファイルにエクスポートされます。ここでは、コマンドラインパラメーターを使用してエクスポートおよびインポートするオブジェクトを制御する方法について説明します。

- **一部のアプリケーションのみのエクスポート** - 移行するアプリケーションの数が多い場合は、1つのXMLファイルにエクスポートするアプリケーションの数を制御できます。これを行うには、以下のパラメーターを使用します。
  - AppLimit - エクスポートするアプリケーションの数を指定します。
  - SkipApps - 指定した数のアプリケーションのエクスポートが省略され、その数以降のアプリケーションからエクスポートされます。

  これらのパラメーターを使用して、アプリケーションをいくつかのグループに分けてエクスポートできます。たとえば、1回目のExport-XAFarmの実行時に最初の200個のアプリケーションをエクスポートするには、AppLimitパラメーターを次のように指定します。

  Export-XAFarm -XmlOutputFile "Apps1-200.xml"
  -AppLimit "200"

  2回目のExport-XAFarmの実行時に残りのアプリケーションのうちの100個をエクスポートするには、エクスポート済みの200個のアプリケーションをエクスポートから除外するためのSkipAppsパラメーターと、その後の100個をエクスポートするためのAppLimitパラメーターを次のように指定します。

  Export-XAFarm -XmlOutputFile "Apps201-300.xml"
  -AppLimit "100" -SkipApps "200"
- **エクスポートから除外するオブジェクト**の指定 - インポートされないオブジェクトなど、一部のオブジェクトはエクスポート時に無視されます。これらのオブジェクトについては、「インポートされないポリシー設定」および「アプリケーションプロパティの対応」を参照してください。以下のパラメーターを使用すると、特定の種類のオブジェクトをエクスポートから除外できます。
  - IgnoreAdmins - 管理者オブジェクトをエクスポートから除外します。
  - IgnoreServers - サーバーオブジェクトをエクスポートから除外します。
  - IgnoreZones - ゾーンオブジェクトをエクスポートから除外します。
  - IgnoreOthers - そのほかのオブジェクト（構成ログ、負荷評価基準、負荷分散ポリシー、プリンタードライバー、ワーカーグループ）をエクスポートから除外します。
  - IgnoreApps - アプリケーションオブジェクトをエクスポートから除外します。アプリケーション以外のデータとアプリケーションを別のXMLファイルにエクスポートする場合に使用します。

  これらのパラメーターは、エクスポート時の問題を回避するときに使用することもできます。たとえば、ゾーン内に不適切なサーバーがあるとエクスポートが失敗する場合があります。この場合は、IgnoreZonesパラメーターを使用してほかのオブジェクトをエクスポートできます。

- **デリバリーグループ名** - インポートするアプリケーションを複数のデリバリーグループ内に分けて追加する場合（異なるユーザーグループに提供する場合や異なるサーバーグループで公開する場合など）、Import-XAFarmコマンドレットを複数に分けて実行し、異なるアプリケーションとデリバリーグループを指定します。移行後にPowerShellコマンドレットを使ってアプリケーションをほかのデリバリーグループに移動することもできますが、インポート時にデリバリーグループを指定しておくと、後でアプリケーションを移動する手間が省けます。
  1. DeliveryGroupNameパラメーターを指定してImport-XAFarmコマンドレットを実行します。これにより、指定されたデリバリーグループが存在しない場合は作成されます。
  2. 以下のパラメーターで正規表現を使用して、アプリケーションを特定のフォルダー、ワーカーグループ、ユーザーアカウント、サーバー名に基づいて特定のデリバリーグループにインポートします。正規表現の部分を引用符または二重引用符で囲むことをお勧めします。正規表現について詳しくは、http://msdn.microsoft.com/ja-jp/library/hs600312(v=vs.110).aspxを参照してください。
     - MatchWorkerGroupおよびNotMatchWorkerGroup - たとえば、ワーカーグループに公開されたアプリケーションに対して次のコマンドレットを実行すると、ワーカーグループ「Productivity Apps」内のアプリケーションがXenApp 7.6の同じ名前のデリバリーグループにインポートされます。

       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchWorkerGroup ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’
     - MatchFolderおよびNotMatchFolder - たとえば、アプリケーションフォルダーで分類されたアプリケーションに対して次のコマンドレットを実行すると、フォルダー「Productivity Apps」内のアプリケーションがXenApp 7.6の同じ名前のデリバリーグループにインポートされます。

       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’

       たとえば、次のコマンドレットを実行すると、「MS Office Apps」という文字列を含んでいる名前のフォルダーからすべてのアプリケーションがデフォルトのデリバリーグループにインポートされます。

       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- MatchAccountおよびNotMatchAccount - たとえば、Active Directoryのユーザーまたはユーザーグループに公開されたアプリケーションに対して次のコマンドレットを実行すると、ユーザーグループ「Finance Group」に公開されたアプリケーションがXenApp 7.6のデリバリーグループ「Finance」にインポートされます。
  Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
  –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
- MatchServerおよびNotMatchServer - たとえば、サーバー単位で公開されたアプリケーションに対して次のコマンドを実行すると、名前が「Current」でないサーバーに関連付けられたアプリケーションが「Legacy」という名前のXenAppデリバリーグループにインポートされます。
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
  -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'

- **カスタマイズ** - PowerShellのプログラミング知識がある場合は、カスタムのツールを作成できます。たとえば、エクスポートスクリプトをインベントリツールとして使用して、XenApp 6.xファームの変更履歴を追跡できます。また、XSDファイルを編集したり新しく作成したりして、XMLファイルに記述されるデータを追加したり、記述形式を変更したりできます。各インポートコマンドレットに非デフォルトのXSDファイルを指定できます。
  注： 特定の移行要件に応じてスクリプトファイルを編集することができますが、その場合はサポート対象外になります。Citrixのテクニカルサポートは、スクリプトを元の状態に戻したうえで正しい動作を確認することを推奨し、必要な場合サポートを提供します。

- PowerShell Verison 2.0を使用する環境で、Add-PSSnapInコマンドレットを使用してCitrix Group Policy PowerShellプロバイダースナップインまたはCitrix Common Commandsスナップインを追加した場合、エクスポートまたはインポートコマンドレットの実行時に「オブジェクト参照がオブジェクトインスタンスに設定されていません」というエラーメッセージが表示されることがあります。このエラーメッセージはスクリプトの実行に影響せず、無視して構いません。
- Citrix Group Policy PowerShellプロバイダースナップインはエクスポートおよびインポートのスクリプトモジュールにより自動的に追加されるため、これらのスクリプトモジュールを使用するコンソールセッション上にこのスナップインを追加したり削除したりすることは避けてください。このスナップインを事前に追加したり削除したりすると、以下のエラーメッセージが表示されることがあります。
  - 「名前 'LocalGpo' のドライブは既に存在しています。」このエラーメッセージは、スナップインを2回追加すると表示されます。スナップインのロード時にドライブ「LocalGpo」のマウントが試行されるため、このメッセージが表示されます。
  - 「パラメーター名 'Controller' に一致するパラメーターが見つかりません。」このエラーメッセージは、スナップインが追加されていないにもかかわらずドライブのマウントが試行されると表示されます。この問題は、スナップインが事前に削除されていると発生します。コンソールを閉じて新しいセッションを起動してください。新しいセッションでスクリプトモジュールをインポートします。事前にスナップインを追加したり削除したりしないでください。
- モジュールをインポートするときにPSD1ファイルを右クリックして［開く］または［PowerShellで開く］を選択すると、プロセスを終了するまでPowerShellコンソールのウィンドウが高速に開いたり閉じたりします。この問題を避けるには、PowerShellコンソールのウィンドウにPowerShellスクリプトモジュールの名前を直接入力してください（「Import-Module .\ExportPolicy.psd1」など）。
- エクスポートまたはインポートの実行時にアクセス権に関するエラーが発生した場合は、オブジェクトの読み取り権限（エクスポート時）または読み取りおよび作成権限（インポート）を持つXenApp管理者アカウントを使用していることを確認してください。また、PowerShellスクリプトを実行するためのWindows権限も必要です。
- エクスポートに失敗した場合は、XenApp 6.xファームのヘルス状態が良好であることを確認してください。これを行うには、XenApp 6.xのコントローラーサーバー上でDSMAINTおよびDSCHECKコマンドを使用します。
- プレビューインポートを実行した後で実際のインポートを実行しても何もインポートされない場合は、インポートコマンドレットから-Previewパラメーターを削除したことを確認してください。

以下の コンピューターポリシー設定とユーザーポリシー設定は、 サポートされていないためインポートされません。フィルターを適用していないポリシーはインポートされないことに注意してください。これらの設定項目をサポートする機能 やコンポーネントが新しい テクノロジやコンポーネントに き換えられたか、アーキテクチャ やプラットフォームの変更によって適用されなくなりました。

インポートされないコンピューターポリシー設定

- 接続の アクセス制御
- サーバーのCPU最適化レベル
- DNSアドレス 解決
- ファーム名
- アイコンの完全 キャッシュ
- サーバーヘルス 監視、サーバーヘルス監視テスト
- ライセンスサーバーの ホスト名、ライセンスサーバーポート
- ユーザー セッションの制限、管理者アカウントの接続も制限する
- 負荷評価基準 名
- ログオン数制限のログ
- ログオン制御できる最大 サーバー数（%）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- メモリの 最適化、メモリ最適化のアプリケーション除外一覧、メモリの 最適化の間隔、メモリの最適化のスケジュール：月間、メモリの 最適化のスケジュール：週間、メモリの最適化のスケジュール：時間
- オフラインアプリケーションへの 再認証なしでの再接続、オフラインアプリケーションのログ、オフラインライセンスの有効期間、オフライン アプリケーションユーザー
- パスワードの入力を要求
- カスタムの再起動 警告、カスタムの再起動警告メッセージ、再起動前のログオンの無効化、再起動スケジュールの 頻度、再起動スケジュールのランダム化間隔、再起動スケジュールの開始日、 再起動スケジュールの時間、再起動警告の間隔、再起動警告の開始時間、 ユーザーへの再起動警告、スケジュールによる再起動
- シャドウ機能 *
- XML 要求を信頼する（StoreFrontで構成）
- 仮想IP アダプターアドレスフィルター、仮想IP互換プログラム一覧、仮想IP 拡張互換性、仮想IPアダプターアドレスフィルタープログラム一覧
- ワークロード名
- XenApp製品 エディション、XenApp製品モデル
- XML Serviceの ポート

* Windowsリモートアシスタンス機能に置き換えられています

インポートされないユーザーポリシー 設定
- クライアントCOMポートを自動接続する、クライアントLPTポートを自動接続する
- クライアントCOMポート リダイレクト、クライアントLPTポートリダイレクト
- クライアントプリンター 名
- 同時 接続数の制限
- シャドウする側からの入力 *
- 残留セッションの 切断タイマー、残留セッションの終了タイマー
- シャドウイベント をログに記録する *
- シャドウ要求をシャドウされる側のユーザーに通知する *
- 事前起動セッションの 切断タイマー、事前起動セッションの終了タイマー
- セッションの 重要度
- Single Sign-On、 Single Sign-On中央ストア
- ほかのユーザーを シャドウできるユーザー、ほかのユーザーをシャドウできないユーザー *

* Windowsリモートアシスタンス機能に置き換えられています

以下の種類の アプリケーションはインポートされません。
- サーバーのデスクトップ
- 公開コンテンツ
- ストリーム配信 アプリケーション（アプリケーションのストリーム配信にはApp-Vを使用します）

ファームデータのインポートスクリプトでは、アプリケーションのみがインポートされます。以下のアプリケーションプロパティは変更されずにインポートされます。

IMAのプロパティ	FMAのプロパティ
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
説明	説明

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IMAのプロパティ	FMAのプロパティ
DisplayName	PublishedName
有効	有効
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

注： IMAとFMAでは、フォルダー名の長さの制限が異なります。IMAでのフォルダー名は256文字以下、FMAでは64文字以下である必要があります。フォルダーパスに64文字を超えるフォルダー名が含まれる場合、そのフォルダー内のアプリケーションはインポートされません。この制限はフォルダーパスに含まれるフォルダー名に対するもので、フォルダーパス全体に対するものではありません。アプリケーションが正しくインポートされるように、アプリケーションのフォルダー名の長さを確認し、必要な場合は短くしてからエクスポートしてください。

以下のアプリケーションプロパティには、デフォルトで初期化されるものと初期化されないものがあります。また、XenApp 6.xのデータで指定された値が設定されるものもあります。

FMAのプロパティ	値
名前	フルパス名に初期化されます。フルパスには、IMAプロパティのFolderPathおよびDisplayNameが含まれ、先頭の「Applications\」の部分は削除されます。
ApplicationType	HostedOnDesktop
CommandLineArguments	XenApp 6.xのコマンドライン引数で初期化されます。
IconFromClient	初期化されずにデフォルト値のfalseになります。
IconUid	XenApp 6.xアイコンデータで作成されたアイコンオブジェクトに初期化されます。
SecureCmdLineArgumentsEnabled	初期化されずにデフォルト値のtrueになります。
UserFilterEnabled	初期化されずにデフォルト値のfalseになります。
UUID	読み取り専用でControllerにより割り当てられます。
表示可能	初期化されずにデフォルト値のtrueになります。

以下のアプリケーションプロパティは、一部のみ移行されます。

IMAのプロパティ	コメント
FileTypes	新しいXenAppサイトに存在するファイルタイプのみが移行されます。新しいサイトに存在しないファイルタイプは無視されます。ファイルタイプは、新しいサイトのファイルタイプが更新された後でインポート可能になります。
IconData	エクスポートされたアプリケーションのアイコンデータが提供されている場合は新しいアイコンオブジェクトが作成されます。
アカウント	アプリケーションのユーザーアカウントはデリバリーグループとアプリケーションのユーザー一覧に分類されます。指定ユーザーのアカウントはアプリケーションのユーザー一覧を初期化するために使用されます。さらに、ユーザーアカウントが属するドメインのDomain Usersアカウントがデリバリーグループのユーザー一覧に追加されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下のXenApp 6.xプロパティはインポートされません。

IMAのプロパティ	コメント
ApplicationType	無視されます。
HideWhenDisabled	無視されます。
AccessSessionConditions	デリバリーグループのアクセスポリシーに置き換えられます。
AccessSessionConditionsEnabled	デリバリーグループのアクセスポリシーに置き換えられます。
ConnectionsThroughAccessGatewayAllowed	デリバリーグループのアクセスポリシーに置き換えられます。
OtherConnectionsAllowed	デリバリーグループのアクセスポリシーに置き換えられます。
AlternateProfiles	FMAはストリーム配信アプリケーションをサポートしません。
OfflineAccessAllowed	FMAはストリーム配信アプリケーションをサポートしません。
ProfileLocation	FMAはストリーム配信アプリケーションをサポートしません。
ProfileProgramArguments	FMAはストリーム配信アプリケーションをサポートしません。
ProfileProgramName	FMAはストリーム配信アプリケーションをサポートしません。
RunAsLeastPrivilegedUser	FMAはストリーム配信アプリケーションをサポートしません。
AnonymousConnectionsAllowed	認証が不要なユーザー（匿名ユーザー）の接続は、FMAでは別の方法でサポートされています。
ApplicationId、SequenceNumber	IMA固有のデータです。
AudioType	FMAはクライアント接続の詳細オプションをサポートしません。
EncryptionLevel	SecureICAの有効/無効はデリバリーグループで設定します。
EncryptionRequired	SecureICAの有効/無効はデリバリーグループで設定します。
SslConnectionEnabled	FMAでは別の方法でTLSが実装されています。
ContentAddress	FMAは公開コンテンツをサポートしません。
ColorDepth	FMAはウィンドウ表示の詳細オプションをサポートしません。
MaximizedOnStartup	FMAはウィンドウ表示の詳細オプションをサポートしません。
TitleBarHidden	FMAはウィンドウ表示の詳細オプションをサポートしません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IMAのプロパティ	コメント
WindowsType	FMAはウィンドウ表示の詳細オプションをサポートしません。
InstanceLimit	FMAはアプリケーション数の制限をサポートしません。
MultipleInstancesPerUserAllowed	FMAはアプリケーション数の制限をサポートしません。
LoadBalancingApplicationCheckEnabled	負荷分散は、FMAでは別の方法でサポートされています。
PreLaunch	セッションの事前起動は、FMAでは別の方法でサポートされています。
CachingOption	セッションの事前起動は、FMAでは別の方法でサポートされています。
ServerNames	FMAでは別の方法が使用されています。
WorkerGroupNames	FMAはワーカーグループをサポートしません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セキュア

Dec 05, 2017

XenAppおよびXenDesktopでは、セキュリティニーズに合わせて環境をカスタマイズできる、セキュアバイデザイン（セキュリティに配慮した設計）ソリューションが提供されます。

モバイルワーカーへの対応でIT部門が直面するセキュリティ上の問題に、データの紛失や盗難があります。XenAppおよびXenDesktopでは、アプリケーションとデスクトップがホストされ、すべてのデータがデータセンターに保持されるため、機密データや知的財産がエンドポイントデバイスから安全に分離されます。データ転送を許可するポリシーを有効にしている場合でも、すべてのデータが暗号化されます。

また、XenDesktopおよびXenAppのデータセンターでは、一元的な監視と管理サービスを利用できるため、インシデント対応が容易になります。Directorでは、ネットワーク経由でアクセスされたデータを監視して分析できます。また、Studioではデータセンターにパッチを適用して多くの脆弱性を解決できるため、エンドユーザーデバイスごとにローカルで問題を解決する必要がありません。

XenAppおよびXenDesktop では、 一元化された監査記録を使用して、どのアプリケーションやデータにどのユーザーがアクセスしたかを判別できるため、監査と法規制順守も簡素化されます。Directorでは、構成ログとOData APIにアクセスして、システムに適用された更新とユーザーのデータ 使用状況に関する履歴データが収集されます。

委任 管理によって、管理者の役割を設定して、 XenDesktopおよびXenAppへのアクセスを詳細に制御できます。これにより、ほかの管理者のアクセス権は制限したままで、特定の管理者に対してタスク、操作、およびスコープへの完全なアクセス権を組織内で柔軟に付与できます。

XenAppおよびXenDesktopでは、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用してユーザーを制御できます。このポリシー制御によって、ユーザー、デバイス、またはユーザーやデバイスのグループが実行できる操作（接続、印刷、コピーと貼り付け、ローカルドライブのマップ）を指定できるため、社外作業者に対するセキュリティ上の問題を最小限に抑えることができます。Desktop Lock機能を使用すると、エンドユーザーデバイスのローカルのオペレーティングシステムにアクセスできないようにして、エンドユーザーによる使用を仮想デスクトップのみに制限することも可能です。

管理者は、Controllerで、またはエンドユーザーとVDA（Virtual Delivery Agent）間でTLS（Transport Layer Security）プロトコルが使用されるように構成して、XenAppまたはXenDesktopのセキュリティを強化できます。このプロトコルを有効にして、TCP/IP接続に対してサーバー認証、データストリームの暗号化、およびメッセージの整合性チェックが行われるようにすることもできます。

さらに、XenAppおよびXenDesktopでは、Windowsや特定のアプリケーションでの複数要素認証が サポートされています。複数要素認証を使用して、 XenAppおよびXenDesktopで配信されるすべてのリソースを管理することもできます。以下の認証方法を使用できます。

- トークン
- スマートカード
- RADIUS
- kerberos
- 生体認証

XenDesktopは、ID管理からウイルス対策ソフトウェアまで、さまざまなサードパーティセキュリティソリューションを統合できます。サポートされている製品の一覧については、http://www.citrix.com/readyを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenAppおよびXenDesktopの一部リリースは、情報セキュリティ国際評価基準（コモンクライテリア）の認定を受けています。これらの基準の一覧については、 http://www.commoncriteriaportal.org/cc/を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セキュリティに関する考慮事項およびベストプラクティス

Apr 10, 2018

このドキュメントでは次のことを説明しています。

- このリリースを使用するときの一般的なセキュリティに関する推奨事項、およびこのリリースと従来のコンピューター環境でのセキュリティに関する相違点
- ユーザーアカウントの管理
- ユーザー権限の管理
- ログオン権限の管理
- ユーザー権利の構成
- サービス設定の構成
- 展開シナリオとそのセキュリティ設定
- リモートPCアクセスのセキュリティに関する考慮事項

組織によっては、法的規制の要件を満たすために特定のセキュリティ基準への準拠が要求される場合があります。このようなセキュリティ基準は変更されることがあるため、ここでは説明しません。セキュリティ基準とCitrix製品に関する最新情報については、http://www.citrix.com/security/を参照してください。

セキュリティに関する推奨事項

セキュリティパッチを適用して、環境内にあるすべてのマシンを最新の状態にします。この製品の利点の1つは、シンクライアントをターミナルとして使用することによってこの作業を簡略化できることです。

環境内にあるすべてのマシンを、アンチウイルスソフトウェアで保護します。

WindowsマシンむけのMicrosoft Enhanced Mitigation Experience Toolkit（EMET）のような、プラットフォーム特有のアンチマルウェアソフトウェアの使用を検討してください。一部の専門家は、規制された環境でMicrosoftがサポートするEMETの最新バージョンを使用することを勧めています。Microsoft社によると、EMETは一部のソフトウェアと互換性がないことがあるため、実稼働環境で展開する前にアプリケーションとのテストを十分に行う必要があることに注意してください。XenAppおよびXenDesktopは、EMET 5.5のデフォルトの構成でテスト済みです。現在、Virtual Delivery Agent（VDA）がインストールされたマシンでのEMETの使用は、お勧めしません。

環境内にあるすべてのマシンを、境界ファイアウォール（必要に応じてエンクレーブ境界を含む）で保護します。

従来の環境を新しいバージョンに移行する場合は、既存の境界ファイアウォールを移動するか、新しい境界ファイアウォールを追加する必要があります。たとえば、従来のクライアントとデータセンター内のデータベースサーバーとの間に境界ファイアウォールがあるとします。このリリースを使用するときは、仮想デスクトップおよびユーザーデバイスと、データセンター内のデータベースサーバーおよびDelivery Controllerとの間に境界ファイアウォールを設定する必要があります。したがって、データベースサーバーとControllerを含むエンクレーブをデータセンター内に作成することを検討します。また、ユーザーデバイスと仮想デスクトップ間のセキュリティについても考慮する必要があります。

環境内にあるすべてのマシンは、パーソナルファイアウォールで保護する必要があります。コアコンポーネントとVDAをインストールするときにWindows Firewallサービスが検出された場合は（ファイアウォールが無効であったとしても）、コンポーネントと機能の通信に必要なポートが自動的に開放されるように設定できます。また、それらのファイアウォールポートを手

© 1999-2017 Citrix Systems, Inc. All rights reserved.

作業で構成することもできます。Windows以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。

注： TCPポート1494および2598はICAおよびCGPに使用され、ファイアウォールで開放されているため、データセンター外のユーザーはこれらのポートにアクセスできます。管理インターフェイスが不注意で開いたままになって攻撃を受ける可能性を避けるため、これらのTCPポートをほかの目的で使用しないでください。ポート1494および2598は、Internet Assigned Number Authority（http://www.iana.org/）に正規登録されています。

すべてのネットワーク通信が正しく保護され、セキュリティポリシーに従って暗号化されている必要があります。IPSecを使用して、Microsoft Windowsコンピューターの間でのすべての通信を保護できます。その方法について詳しくは、使用するオペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、デフォルトで128ビット暗号化を行うCitrix SecureICAで保護できます。SecureICAは、デリバリーグループの作成または更新時に設定できます。

Windowsベストプラクティスをアカウント管理に適用します。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、アカウントをテンプレートやイメージに作成しないでください。保存された、権限が付与されているドメインアカウントを使用して、タスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。こうすることにより、ローカルの永続アカウントのパスワードがマシンへの攻撃によって取得され、他者所有のMCS/PVS共有イメージへのログオンに使用されるのを阻止することができます。

ユーザー権限の管理

ユーザーには、必要な権限だけを付与します。デスクトップのユーザーには、Microsoft Windowsでの権限（グループポリシーの［ユーザー権利の割り当て］およびグループメンバーシップ）がそのまま適用されます。このリリースの利点の1つは、仮想デスクトップが格納されているコンピューターに対する物理的な制御を許可せずに、デスクトップに対するユーザーの管理権限を付与できることです。

デスクトップに対する管理権限を計画するときは、以下の点に注意してください。

- デフォルトでは、権限を持たないユーザーがデスクトップに接続すると、ユーザーデバイスのタイムゾーンではなく、そのデスクトップを実行しているシステムのタイムゾーンが表示されます。デスクトップの使用時にローカルの時刻が表示されるようにする方法については、「基本設定の変更」を参照してください。
- デスクトップの管理者権限を持つユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールデスクトップの場合、管理者権限を持つユーザーはそのデスクトップのすべてのユーザー（将来のユーザーを含む）に信頼されている必要があります。このため、プールデスクトップのすべてのユーザーは、この状況によってデータのセキュリティに永続的な危険性が存在することを認識する必要があります。これは、単一ユーザーに対してのみ割り当てられるデスクトップには当てはまりません。つまり、このユーザーはほかのデスクトップの管理者になることはできません。
- 通常、デスクトップの管理者であるユーザーはそのデスクトップにソフトウェアをインストールできます。インストールできるソフトウェアには悪意のあるものも含まれます。またユーザーが、そのデスクトップに接続しているすべてのネットワーク上のトラフィックを監視または制御することも可能です。

一部のアプリケーションでは、管理者ではなくユーザー向けであってもデスクトップ権限が必要です。こうしたユーザーはセキュリティリスクを認識していない可能性があります。

これらのアプリケーションは、たとえデータに機密性がない場合でも、機密性の高いアプリケーションとして扱います。セキュリティリスクを軽減するために、以下のアプローチを検討してください。

- 二要素認証を適用し、すべてのアプリケーションのシングルサインオンメカニズムを無効にする
- コンテキストアクセスポリシーを適用する

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 専用のデスクトップにアプリケーションを公開する。ホストされた共有デスクトップにアプリケーションを公開する必要がある場合は、その共有デスクトップに他のアプリケーションを公開しない
- デスクトップ権限がそのデスクトップにのみ適用され、他のコンピューターには適用されないようにする
- アプリケーションのセッションの録画を有効にする。また、アプリケーション内およびWindows内の他のセキュリティ記録機能も有効にする
- XenAppおよびXenDesktopを構成して、アプリケーションで使用される機能（クリップボード、プリンター、クライアントドライブ、USBリダイレクトなど）を制限する
- アプリケーションのセキュリティ機能を有効にする。厳密にユーザーの要件のみに一致するように制限する
- Windowsのセキュリティ機能を厳密にユーザーの要件に合わせて構成する。これは単一のアプリケーションだけがデスクトップに公開されている場合、より簡単な構成を意味する。例：制限のあるAppLocker構成の使用。ファイルシステムへのアクセスを制御する
- 将来のデスクトップ権限が不要になるように、アプリケーションの再構成、アップグレード、または置き換えを計画する

これらのアプローチは、デスクトップ権限を必要とするアプリケーションからすべてのセキュリティリスクを排除するわけではありません。

ログオン権限の管理

ユーザーアカウントとコンピューターアカウントの両方にログオン権限が必要です。 Microsoft Windowsの権限では、ログオン権限は引き続き、［ユーザー権限の割り当て］で権限を設定し［グループポリシー］でグループメンバーシップを設定するという通常の方法で、デスクトップに適用されます。

Windowsのログオン権限には次の種類があります。ローカルログオン、リモートデスクトップサービスを使ったログオン、ネットワーク経由でのログオン（ネットワーク経由でコンピューターへアクセス）、バッチジョブとしてログオン、サービスとしてログオン。

コンピューターアカウントでは、必要なログオン権限だけをコンピューターに付与します。次のアカウントに、ログオン権限「ネットワーク経由でコンピューターへアクセス」が必要です。

- VDAで、Delivery Controllerのコンピューターアカウント
- Delivery Controllerで、VDAのコンピューターアカウント。「Active Directory OUベースのController検出」を参照してください。
- StoreFrontサーバーで、同じStoreFrontサーバーグループ内の他のサーバーのコンピューターアカウント

ユーザーアカウントでは、必要なログオン権限だけをユーザーに付与します。

Microsoftによると、デフォルトでRemote Desktop Usersグループに［リモート デスクトップ サービスを使ったログオンを許可］でログオン権限が付与されています（ドメインコントローラを除く）。

組織のセキュリティポリシーによっては、このグループがこのログオン権限から除外されることを明示的に設定している場合もあります。 次の方法を検討してください。

- Virtual Delivery Agent（VDA）for Server OSはMicrosoftリモートデスクトップサービスを使用します。 Remote Desktop Usersグループを制限されたグループとして構成し、Active Directoryグループポリシー経由でグループのメンバーシップを制御できます。 詳しくは、Microsoft社のドキュメントを参照してください。
- VDA for Desktop OSを含むXenAppおよびXenDesktopの他のコンポーネントでは、Remote Desktop Usersグループは必要ありません。 このため、これらのコンポーネントではRemote Desktop Usersグループにログオン権限［リモート デスクトップ サービスを使ったログオンを許可］の必要はなく、削除できます。さらに、以下を確認します。
  - リモートデスクトップサービスでこれらのコンピューターを管理する場合、すべての必要な管理者が既にAdministrator

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

グループのメンバーであることを確認してください。
- リモートデスクトップサービスでこれらのコンピューターを管理しない場合、コンピューター上でリモートデスクトップサービスを無効にすることを検討してください。

ユーザーとグループをログオン権限［リモートデスクトップサービスによるログオンを拒否］に追加することは可能ですが、ログオン権限の拒否の使用は、通常推奨されません。 詳しくは、Microsoft社のドキュメントを参照してください。

ユーザー権利の構成

Delivery Controllerをインストールすると、次のWindowsサービスが作成されます。

- Citrix AD Identity Service（NT SERVICE\CitrixADIdentityService）：仮想マシンのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics（NT SERVICE\CitrixAnalytics）：Citrixが使用するサイト構成の使用状況情報の収集がサイト管理者によって承認されている場合、この情報を収集します。 その後、製品の改善に役立てるために、この情報をCitrixに送信します。
- Citrix App Library（NT SERVICE\CitrixAppLibrary）：AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service（NT SERVICE\CitrixBrokerService）：ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。
- Citrix Configuration Logging Service（NT SERVICE\CitrixConfigurationLogging）：すべての構成の変更と、管理者がサイトに対して行ったそのほかの状態の変更を記録します。
- Citrix Configuration Service（NT SERVICE\CitrixConfigurationService）：共有される構成のサイト全体のリポジトリです。
- Citrix Delegated Administration Service（NT SERVICE\CitrixDelegatedAdmin）：管理者に与えられた権限を管理します。
- Citrix Environment Test Service（NT SERVICE\CitrixEnvTest）：そのほかのDelivery Controllerサービスのセルフテストを管理します。
- Citrix Host Service（NT SERVICE\CitrixHostService）：XenAppまたはXenDesktop環境で使用されているハイパーバイザーインフラストラクチャに関する情報を保存します。また、コンソールで使用される、ハイパーバイザープールのリソース列挙する機能を提供します。
- Citrix Machine Creation Service（NT SERVICE\CitrixMachineCreationService）：デスクトップ仮想マシンの作成をオーケストレーションします。
- Citrix Monitor Service（NT SERVICE\CitrixMonitor）：XenAppまたはXenDesktopの測定基準を収集し、履歴情報を保存して、トラブルシューティングのためのクエリインターフェイスと各種のレポートツールを提供します。
- Citrix Storefront Service（NT SERVICE\ CitrixStorefront）：StoreFrontの管理をサポートします （StoreFrontコンポーネント自体には含まれていません）。
- Citrix Storefront Privileged Administration Service（NT SERVICE\CitrixPrivilegedService）：StoreFrontの特権管理操作をサポートします（StoreFrontコンポーネント自体には含まれていません）。
- Citrix Configuration Logging Service（NT SERVICE\CitrixConfigSyncService）：メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service（NT SERVICE\CitrixHighAvailabilityService）：メインサイトデータベースが使用できない場合に、ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。

Delivery Controllerをインストールすると、次のWindowsサービスも作成されます。 これらは、そのほかのCitrixコンポーネントをインストールしたときにも作成されます。

- Citrix Diagnostic Facility COM Server（NT SERVICE\CdfSvc）：Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service（NT SERVICE\CitrixTelemetryService）：Citrixが分析するための診断情報を収集することで、管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.

者が分析結果と推奨事項を確認してサイトの問題解決に役立てることができるようにします。

Delivery Controllerをインストールすると、次のWindowsサービスも作成されます。これは現在使用されていません。有効だった場合、無効にしてください。

- Citrix Remote Broker Provider（NT SERVICE\XaXdCloudProxy）

Delivery Controllerをインストールすると、次のWindowsサービスも作成されます。 これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- Citrix 信頼サービス (NT SERVICE\CitrixTrust)

Citrix Storefront Privileged Administration Serviceを除く、これらのサービスには、［サービスとしてログオン］のログオン権限と［プロセスのメモリクォータの増加］、［セキュリティ監査の生成］、［プロセスレベルトークンの置き換え］の権限が付与されます。通常、これらのユーザー権利を変更する必要はありません。これらの権限はDelivery Controllerでは使用されないため、自動的に無効にされています。

サービス設定の構成

Citrix Storefront Privileged Administration ServiceとCitrix Telemetry Serviceを除く、上述の「ユーザー権利の構成」セクションに示すDelivery Controller Windowsサービスは、ネットワークサービスIDでログオンするように構成されます。このサービス設定は変更しないでください。

Citrix Storefront Privileged Administration Serviceは、ローカルシステム（NT AUTHORITY\SYSTEM）にログオンするように構成されます。 これは、通常はサービスで実行できないDelivery Controller StoreFront操作（Microsoft IISサイトの作成など）に必要な構成です。 このサービス設定は変更しないでください。

Citrix Telemetry Serviceは、このサービス自体のサービス固有のIDでログオンするように構成されます。

Citrix Telemetry Serviceは、無効にすることができます。このサービスと、既に無効にされているサービス以外のそのほかのDelivery Controller Windowsサービスは、無効にしないでください。

レジストリ設定の構成

VDAファイルシステムで8.3ファイル名およびフォルダーの作成を有効にする必要はなくなりました。レジストリキー**NtfsDisable8dot3NameCreation**は、8.3ファイル名およびフォルダーの作成が無効になるように構成できます。 これは、**fsutil.exe behavior set disable8dot3**コマンドを使用しても構成できます。

展開シナリオのセキュリティ

ユーザー環境は、組織に管理されずにユーザーにより完全に制御されるユーザーデバイス、または組織により管理されたユーザーデバイスで構成できます。通常、これら2つの環境に対するセキュリティ上の考慮事項は異なります。

管理されるユーザーデバイス

「管理されるユーザーデバイス」とは、管理者または信頼されたほかの組織によって管理されるユーザーデバイスを指します。この場合、ユーザーデバイスを管理者が構成してユーザーに直接提供したり、全画面のみを実行するモードで単一のデス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クトップを実行する端末を提供したりできます。管理されるユーザーデバイスに対しては、前述の一般的なセキュリティ構成を実装します。この製品の長所は、ユーザーデバイス上に最低限のソフトウェアしか必要としないという点です。

管理されるユーザーデバイスでは、仮想デスクトップの実行モードとして、全画面のみを実行するモードまたはウィンドウモードを構成できます。

- 全画面のみを実行するモード：ユーザーは通常の［Windowsへのログオン］画面からユーザーデバイスにログオンします。すると、同じユーザー資格情報で自動的にこのリリースへのログオンが実行されます。
- 一方、ウィンドウモードを使用する場合、ユーザーは最初にユーザーデバイスにログオンし、次にこのリリースで提供されたWebサイトを介してこの製品にログオンします。

管理されていないユーザーデバイス

「管理されていないユーザーデバイス」とは、管理者または信頼された組織によって管理されていないユーザーデバイスを指します。たとえば、ユーザーが自分のデバイスを使用する場合、上記のセキュリティ上の推奨事項にユーザーが従わないことがあります。このリリースでは、このような管理されていないユーザーデバイスにも、デスクトップを安全に配信できます。ただし、これらのユーザーデバイスでも、キーロガーやそれに類似した入力攻撃を阻止するための基本的なウイルス対策が施されている必要があります。

データストレージの考慮事項

このリリースを使用しているときに、ユーザーが自分のユーザーデバイスにデータを保存できないように構成できます。ただし、ユーザーが仮想デスクトップにデータを保存することを許可するかどうかも考慮する必要があります。ユーザーによるデスクトップ上へのデータ保存は推奨されません。データはファイルサーバー、データベースサーバー、またはデータが適切に保護されるそのほかのリポジトリに保存する必要があります。

デスクトップ環境は、プールデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールデスクトップなど、複数のユーザーで共有されるデスクトップ上にデータを保存するべきではありません。また、専用デスクトップでも、そのデスクトップをほかのユーザーが使用することになった場合に、保存されているデータを削除する必要があります。

バージョン混在環境

アップグレード処理のある時点においては、バージョンが混在する環境は不可避なものです。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが同時に存在する時間を最短化させます。たとえばバージョン混在環境ではセキュリティポリシーが一律には適用されない可能性があります。

注： これは、ほかのソフトウェア製品では一般的な問題です。Active Directoryの以前のバージョンを使用すると、最近のバージョンのWindowsにはグループポリシーが部分的にしか適用されません。

次のシナリオでは、特定のバージョン混在Citrix環境で発生する可能性があるセキュリティ問題について説明します。XenAppおよびXenDesktop 7.6 Feature Pack 2のVirtual Delivery Agentを実行している仮想デスクトップへの接続にCitrix Receiver 1.7が使用されている場合、ポリシー設定「**デスクトップとクライアント間におけるファイル転送の許可**」はサイトでは有効ですが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerによっては無効にできません。製品のより新しいバージョンでリリースされたポリシーの設定は認識されません。このポリシーにより、ユーザーはファイルを自分の仮想デスクトップにアップロードしてダウンロードできます – セキュリティ問題。この問題を回避するには、Delivery ControllerあるいはStudioのスタンドアロンインスタンスをバージョン7.6 Feature Pack 2にアップグレードし、その後でグループポリシーを使ってポリシーを無効にします。または、すべての該当する仮想デスクトップでローカルポリシーを使用します。

リモートPCアクセスのセキュリティに関する考慮事項

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リモートPCアクセスでは、次のセキュリティ機能がサポートされます。

- スマートカードの使用がサポートされます。
- リモートセッションの間、社内のPCのモニターは非表示になります。
- リモートPCアクセスでは、すべてのキーボードおよびマウスの入力がリモートセッションにリダイレクトされます（Ctrl+Alt+Delキー入力、およびUSB対応スマートカードや生体認証デバイスを除く）。
- SmoothRoamingは単一ユーザーに対してのみサポートされます。
- リモートセッションで接続していた社内のPCにローカルでアクセスを再開できるのはそのユーザーのみです。ローカルでのアクセスを再開するには、ローカルのキーボードでCtrl+Alt+Delキーを押して、リモートセッションと同じ資格情報を使ってログオンします。システムに適切なサードパーティ製の資格情報プロバイダー統合が構成されている場合は、スマートカードを挿入したり生体認証を使用したりしてローカルアクセスを再開することもできます。グループポリシーオブジェクト（GPO）やレジストリキーでユーザーの簡易切り替え機能を有効にして、このデフォルトの動作設定を上書きすることができます。

注： VDA管理者特権を一般のセッションユーザーに割り当てないことをお勧めします。

自動割り当て

リモートPCアクセスでは、デフォルトで単一VDAへの複数ユーザーの自動割り当てがサポートされます。XenDesktop 5.6 Feature Pack 1では、PowerShellスクリプトRemotePCAccess.ps1を使ってこの動作を上書きできました。このリリースでは、レジストリキーを使って複数ユーザーの自動割り当てを許可または禁止できます。この設定はサイト全体に適用されます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

自動割り当てを単一ユーザーのみに制限するには、以下の手順に従います。

サイト上の各Controllerで、以下のレジストリエントリを設定します。

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

値の名前：AllowMultipleRemotePCAssignments

種類：REG_DWORD

値のデータ：0（複数ユーザーの割り当て無効）、1（デフォルト。複数ユーザーの割り当て有効）

既存のユーザー割り当てを削除するには、SDKコマンドを使用します。これにより、VDAに単一ユーザーが割り当てられるようになります。

- 割り当てられているすべてのユーザーをVDAから削除するには、$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machineを実行します。
- デリバリーグループからVDAを削除するには、$machine | Remove-BrokerMachine -DesktopGroup $desktopGroupを実行します。

社内の物理PCを再起動します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

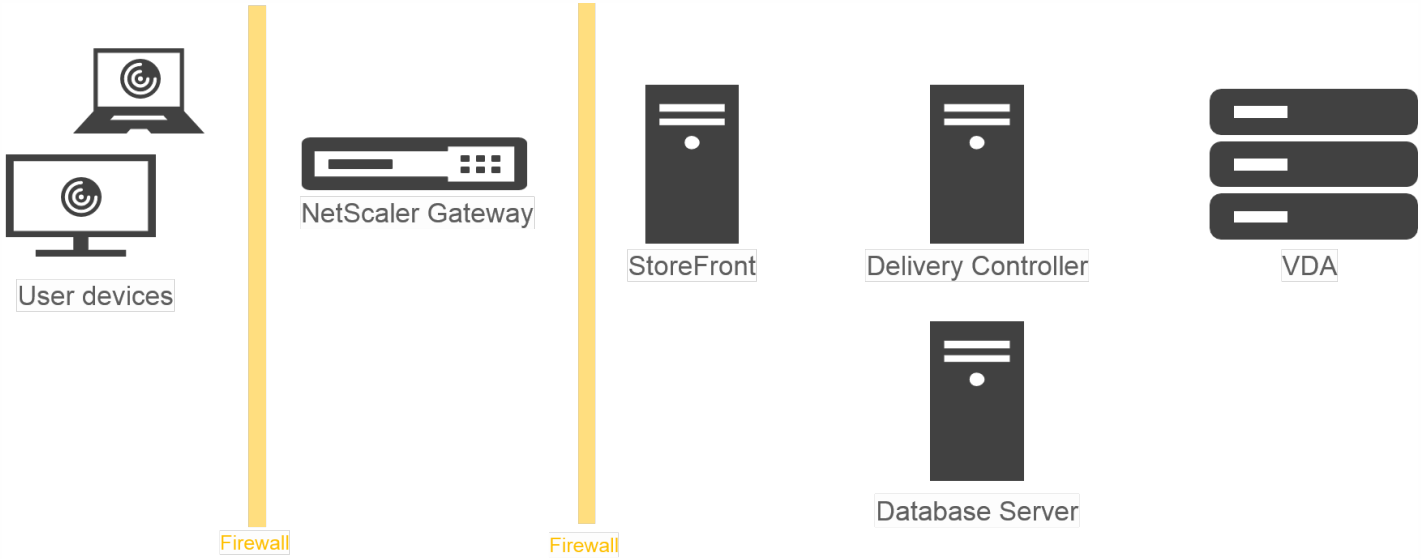
XenAppおよびXenDesktopのNetScaler Gatewayとの統合

Dec 05, 2017

公開リソースおよびデータへのアクセスを管理するには、StoreFrontサーバーを展開および構成します。リモートアクセスの場合は、NetScaler GatewayをStoreFrontの前に追加することをお勧めします。

> **注意**
>
> XenAppおよびXenDesktopをNetScaler Gatewayと統合する構成手順については、StoreFrontのドキュメントを参照してください。

次の図は、NetScaler Gatewayを含む簡略化されたCitrixの展開例を示しています。NetScaler GatewayはStoreFrontと通信して、 XenAppおよびXenDesktopが配信するアプリやデータを保護します。ユーザーデバイスはCitrix Receiverを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。



ユーザーは、NetScaler Gatewayを使用してログオンおよび認証を行います。NetScaler Gatewayは、DMZで展開およびセキュリティ保護されます。2要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します（図には表示されていません）。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理権限の委任

Dec 05, 2017

委任管理モデルにより、役割やオブジェクトベースの制御により、組織の管理業務の分担に基づいて柔軟に管理権限を委任することができます。あらゆる規模のサイトで委任管理機能を使用でき、展開環境が複雑化するにつれてより詳細な権限の分担を構成できます。管理権限の委任機能では、管理者、役割、およびスコープという3つの概念が使用されます。

- **管理者** — 管理者は、Active Directoryアカウントにより識別される、管理権限を持つ個人またはそのグループを示します。各管理者には、1つまたは複数の役割とスコープのペアが割り当てられます。
- **役割** — 役割は管理ジョブの機能を表し、それぞれ定義された権限が割り当てられています。たとえば、［デリバリーグループ管理者］の役割には、「デリバリーグループの作成」および「デリバリーグループからのデスクトップの削除」などの権限があります。管理者は、サイトに対して複数の役割を有することができ、1人の管理者がデリバリーグループ管理者とマシンカタログ管理者を兼ねることができます。役割には、組み込みの役割とカスタムの役割があります。
  組み込みの役割は、次のとおりです。

役割	権限
すべての管理権限を実行できる管理者	すべてのタスクと操作を実行できます。［すべての管理権限を実行できる管理者］の役割は、常に［すべて］のスコープとペアになります。
読み取り専用管理者	全体的な情報に加えて、指定されたスコープのすべてのオブジェクトを表示できますが、変更することはできません。たとえば、「大阪」というスコープを作成して読み取り専用管理者に割り当てると、構成ログなどのグローバルオブジェクトと、大阪支社用のデリバリーグループなど、［大阪］スコープのオブジェクトを表示できます。ただし、この管理者は「ニューヨーク」スコープのオブジェクトを表示できません。
ヘルプデスク管理者	デリバリーグループを表示して、関連付けられているセッションとマシンを管理できます。デリバリーグループのマシンカタログやホスト情報を表示したり、デリバリーグループのマシンのセッションや電源を管理したりできます。
マシンカタログ管理者	マシンカタログを作成および管理したり、マシンカタログにマシンをプロビジョニングしたりできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンを使用してマシンカタログを作成できます。この役割では、基本イメージを管理したりソフトウェアをインストールしたりできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信したり、それらのセッションを管理したりできます。ポリシーや電源管理設定など、アプリケーションおよびデスクトップの構成を管理することもできます。
ホスト管理者	ホスト接続およびその関連リソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

この製品の一部のエディションでは、必要に応じてカスタムの役割を作成して、より詳細な権限を委任することができます。カスタムの役割では、コンソールにおける操作またはタスク単位で権限を割り当てることができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **スコープ** — 接続、マシン カタログ、デリバリーグループなど、その管理者が管理できるオブジェクトをグループ化したものです。スコープでは、組織の要件に基づいてオブジェクトをグループ化します（営業チームで使用されるデリバリーグループのセットなど）。オブジェクトを複数のスコープに含めることができます。つまり、1つまたは複数のスコープでオブジェクトをラベル付けすることができます。組み込みのスコープである「すべて」には、すべてのオブジェクトが含まれています。［すべての管理権限を実行できる管理者］の役割は、常にこのスコープとペアになります。

例

XYZ社 は自社の部署 （経理、営業、倉庫）およびそのデスクトップオペレーティングシステム（Windows 7 またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各 デリバリーグループに2つのスコープ（部署を表すスコープと 使用するオペレーティングシステムを表すスコープ）を割り当てました。

次の 管理者を作成しました。

管理者	役割	スコープ
ドメイン/fred	すべての管理権限を実行できる管理者	すべて（［すべての管理権限を実行できる管理者］の役割は、常に［すべて］スコープとペアになります）
ドメイン/rob	読み取り専用管理者	すべて
ドメイン/heidi	読み取り専用管理者 ヘルプデスク管理者	すべて 営業
ドメイン/warehouseadmin	ヘルプデスク管理者	倉庫
ドメイン/peter	デリバリーグループ管理者 マシンカタログ管理者	Win7

- Fredは「すべての 管理権限を実行できる管理者」で、システム内のすべてのオブジェクトを表示、編集、および削除できます。
- Robはサイト内の すべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidiは すべてのオブジェクトを表示でき、［営業］ スコープのデリバリーグループでヘルプデスクタスクを実行できます。これにより、［営業］スコープのデリバリーグループに割り当てられているセッションとマシンを管理できます。ただし、これらの デリバリーグループに（マシンの追加や 削除などの）変更を加えることはできません。
- Active Directoryセキュリティグループwarehouseadminのすべての メンバーは、［倉庫］スコープのマシンに対するヘルプデスクタスクを表示および 実行できます。
- Peterは Windows 7の専門家で、すべてのWindows 7マシンカタログを管理でき、所属している 部署のスコープに関係なくWindows 7アプリケーション、デスクトップ、およびマシンを 配信できます。当初、管理者はPeterを［Win7］スコープの「すべての 管理権限を実行できる管理者」にしようとしましたが、考え直しました。これは、「 すべての管理権限を実行できる管理者」には、そのスコープに含まれていないオブジェクト （「サイト」や「管理者」など）に対する全権限が付与されるためです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

委任管理の使用方法

一般的に、 管理者数およびその権限の細分性は 展開のサイズおよびその複雑度に応じて異なります。

- 小規模または 検証用の展開サイトでは、1人または少数の管理者ですべてを管理し、 委任管理者は存在しません。この場合、組み込みの ［すべての管理権限を実行できる管理者］役割（および［すべて］スコープ）の管理者を作成します。
- より多くの マシン、アプリケーション、およびデスクトップがあるサイトでは、委任管理者の配置 が必要になります。何人かの管理者に、より専門的な 管理責任（役割）を付与できます。たとえば、2人の「 すべての管理権限を実行できる管理者」を設定して、残りをヘルプデスク管理者にします。さらに、マシンカタログなど、 特定グループ（スコープ）のオブジェクトの管理を1人の管理者に委任することもできます。この場合、 新しいスコープを作成して、組み込みの役割とそのスコープをペアにした管理者を作成します。
- 大規模サイトにおいても、 より多くの（またはより詳細な）スコープと、 特殊な役割を持つさまざまな管理者が必要になることがあります。この場合は、 追加のスコープを作成または編集して、カスタムの役割を作成し、 組み込みまたはカスタムの役割と既存または新しいスコープを持つ各管理者を作成します。

新しいスコープは、 管理者を作成するときに作成できます。また、マシン カタログやホスト接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカルの管理者アカウントを使用してサイトを作成するときは、すべてのオブジェクトに対する完全な 管理権限を持つ管理者としてそのアカウントが設定されます。ただし、サイトを作成した後では、 ローカル管理者には特別な特権は与えられません。

すべての 管理タスクの実行権限を持つ管理者には、常に［すべて］のスコープが割り当てられます。これを変更することはできません。

デフォルトでは、 管理者は有効になります。 新しい管理者を作成するときに、 その管理者が実際に作業を始めるまで管理者を無効にしておく必要が生じる場合があります。また、 オブジェクトやスコープを 再構成するときに、既存の管理者を一時的に無効にすることもできます。 完全な管理権限を持つ管理者が1人しかいない環境では、その管理者を無効にすることはできません。管理者の有効/無効は、管理者を作成、コピー、または編集するときの［管理者を有効にする］チェック ボックスで設定できます。

管理者を編集したりコピーしたりするときのダイアログボックスで スコープ/役割ペアを削除すると、その管理者とスコープ/役割ペアとの関連付けが 削除され、個々のスコープや役割は削除されません。また、同じスコープ/役割ペアが割り当てられている 管理者がいる場合でも、その関連付けは削除されません。

管理者を管理するには、Studioのナビゲーションペインで ［構成］>［管理者］の順にクリックし、 中央ペインの上部の ［管理者］タブをクリックします。

- 管理者を作成するには、［操作］ペインの ［管理者の作成］をクリックします。 ユーザーアカウント名を入力するか参照し、スコープを選択または作成して、 役割を選択します。新しい管理者はデフォルトで有効になりますが、無効にすることもできます。
- 管理者をコピーするには、中央ペインで管理者を選択し、［操作］ペインの ［管理者の コピー］をクリックします。 ユーザーアカウント名を入力するか参照します。必要に応じて、スコープ/役割 ペアを編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になりますが、 無効にすることもできます。
- 管理者を編集するには、中央ペインで管理者を選択し、［操作］ペインの ［管理者の 編集］をクリックします。必要に応じて、スコープ/役割 ペアを編集または削除したり、新しいペアを追加したりできます。
- 管理者を削除するには、中央ペインで管理者を選択し、［操作］ペインの ［管理者の削除］をクリックします。 完全な管理権限を持つ管理者が1人しかいない環境では、その管理者を 削除することはできません。

役割の作成と管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.

役割には、 64文字までのUnicode文字で名前を付けることができます。ただし、次の 文字は使用できません。 バックスラッシュ（\）、スラッシュ（/）、セミコロン（;）、 コロン（:）、番号記号（# ）、コンマ（,）、アスタリスク（*）、疑問符、（?）、等号（=）、小なり記号（<） 、大なり記号（>）、パイプ（|）、角かっこ（[ ]）、丸かっこ（( )）、 二重引用符（"）、およびアポストロフィ（'）。 説明には、256文字までのUnicode文字を入力できます。

組み込みの役割を 編集または削除することはできません。いずれかの管理者が 使用しているカスタムの役割は削除できません。

注： カスタムの役割を作成するには、 特定の製品エディションが必要です。カスタムの 役割をサポートしないエディションでは、［操作］ペインに関連エントリが表示されません。
役割を管理するには、 Studioの ナビゲーションペインで ［構成］>［管理者］の順にクリックし、中央ペインの上部の ［役割］タブをクリックします。

- 役割の 詳細を表示するには、中央ペインでその役割を選択します。中央 ペインの下部に、その役割のオブジェクトの種類および許可される権限が表示されます。ここで ［管理者］タブをクリックすると、その役割が割り当てられている 管理者が表示されます。
- カスタムの役割を作成するには、 ［操作］ペインの ［役割の作成］をクリックします。名前 と説明を入力します。この役割に割り当てるオブジェクトの種類と権限を選択します。
- 役割をコピーするには、中央ペインで役割を選択し、 ［操作］ペインの ［役割の コピー］をクリックします。必要に応じて、役割の名前、説明、 および権限を変更します。
- カスタムの役割を編集するには、中央ペインで役割を選択し、 ［操作］ペインの ［役割の 編集］をクリックします。必要に応じて、役割の名前、説明、 および権限を変更します。
- カスタムの役割を削除するには、中央ペインで役割を選択し、 ［操作］ペインの ［役割の削除］をクリックします。確認のメッセージが表示されたら、 ［削除］をクリックします。

スコープの作成と 管理

サイトを作成すると、 ［すべて］のスコープが使用可能になります。このスコープは削除できません。

スコープを作成するには、次の手順を使用します。 管理者を作成するときにスコープを作成することもできます。すべての管理者は、少なくとも1つの役割と スコープのペアが割り当てられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成したり編集したりするときに、それらを既存のスコープに追加できます。ただし、特定のスコープに 追加しない場合でも、自動的に［すべて］のスコープに追加されます。

サイトの作成および委任管理オブジェクト（スコープおよび役割）をスコープに 含めることはできません。 ただし、スコープに含めることができないオブジェクトも ［すべて］のスコープには含まれています。（すべての 管理タスクの実行権限を持つ管理者には、常に ［すべて］のスコープが割り当てられます）。 マシン、電源操作、デスクトップ、および セッションはスコープに含まれません。管理者にこれらのオブジェクトに対する 権限を関連するマシンカタログまたは デリバリーグループによって割り当てることができます。

スコープには、 64文字までのUnicode文字で名前を付けることができます。ただし、次の 文字は使用できません。 バックスラッシュ（\）、スラッシュ（/）、セミコロン（;）、 コロン（:）、番号記号（# ）、コンマ（,）、アスタリスク（*）、疑問符、 （?）、等号（=）、小なり記号（<） 、大なり記号（>）、パイプ（|）、角かっこ（[ ]）、丸かっこ（( )）、 二重引用符（"）、およびアポストロフィ（'）。 説明には、256文字までのUnicode文字を入力できます。

スコープをコピーまたは 編集するときにオブジェクトをスコープから削除すると、管理者がその オブジェクトにアクセスできなくなる可能性があることに注意してください。編集するスコープに いくつかの役割が関連付けられている場合は、編集により スコープと役割のペアが使用できなくならないかどうかを確認してください。

スコープを管理するには、Studioのナビゲーションペインで ［構成］>［管理者］の順にクリックし、 中央ペインの上部の［スコープ］タブをクリックします。

- スコープを作成するには、 ［操作］ペインの ［スコープの作成］をクリックします。名前 と説明を入力します。オブジェ

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

クトの種類（［デリバリーグループ］チェックボックスなど）を選択すると、その種類のすべてのオブジェクトがスコープに追加されます。特定のオブジェクトを追加するには、オブジェクトの 種類を開き、個々のオブジェクトを選択します（営業部で使用される特定のデリバリーグループを選択する場合など）。

- スコープをコピーするには、中央ペインでスコープを選択し、［操作］ペインの ［スコープの コピー］をクリックします。名前と説明を入力します。必要に応じて、 オブジェクトの種類とオブジェクトを変更します。
- スコープを編集するには、中央ペインでスコープを選択し、［操作］ペインの ［スコープの 編集］をクリックします。必要に応じて、名前、説明、オブジェクトの 種類、およびオブジェクトを変更します。
- スコープを削除するには、中央ペインでスコープを選択し、［操作］ペインの ［スコープの削除］をクリックします。確認のメッセージが表示されたら、 ［削除］をクリックします。

レポートの作成

次の2種類の委任管理レポートを作成できます。

- 管理者に関連付けられているスコープ/役割ペアと各種類のオブジェクト（デリバリー グループ、マシンカタログなど）に対する 個々の権限の一覧についてのHTML レポート。Studioで生成できます。
  このレポートを作成するには、ナビゲーションペインで ［構成］ > ［管理者］の順に選択します。 中央ペインで管理者を選択し、操作ペインで ［レポートの作成］をクリックします。

  このレポートは、管理者の作成、コピー、および編集時に作成することもできます。

- 組み込みおよびカスタムの役割とそれらに関連付けられた権限を一覧表示するHTMLまたは CSVレポート。 このレポートは、PowerShellスクリプトOutputPermissionMapping.ps1を実行して生成します。
  このスクリプトを実行するには、すべての管理権限を実行できる管理者、読み取り専用管理者、または役割の読み取り権限を持つ管理者である必要があります。 このスクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\にインストールされています。

  構文：

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

パラメーター	説明
-Help	スクリプトのヘルプを表示します。
-Csv	CSVレポートを作成します。デフォルト値：HTML
パスstring	出力先を指定します。デフォルト値：stdout
-AdminAddress <string>	接続先のDelivery ControllerのIPアドレスまたはホスト名を指定します。 デフォルト値：localhost
-Show	（-Pathパラメーターを指定した場合のみ有効）ファイルに 出力する場合に-Showを指定すると、レポートが 適切なアプリケーションプログラム（Webブラウザーなど）で表示されます。
	Verbose、Debug、ErrorAction、ErrorVariable、WarningAction、 WarningVariable、OutBuffer、およびOutVariable。詳しくは、Microsoft社の ドキュメントを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

次の 例では、Roles.htmlという名前のファイルにHTMLテーブルが出力され、 Webブラウザーで表示されます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
```

次の 例では、Roles.csvという名前のファイルにCSVテーブルが出力されます。このテーブルは自動的には 表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
–CSV -Path Roles.csv
```

上の例をWindows コマンドプロンプトから実行する場合は、次のコマンドを実行します。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

スマートカード

Dec 05, 2017

スマートカードおよび同等のテクノロジは、このアーティクルに記載されているガイドライン内でサポートされています。 XenAppまたはXenDesktopでスマートカードを使用するには、以下を行う必要があります。

- 所属する組織における、スマートカードの使用に関するセキュリティポリシーを理解します。たとえば、スマートカードがどのように発行され、ユーザーがそれをどのように保護するかについてこれらのポリシーで規定してあることがあります。XenAppおよびXenDesktopの環境では、これらのポリシーの一部の変更が必要になる場合があります。
- どのユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションがスマートカードとともに使用されるかを決定します。
- スマートカードテクノロジ全般および選択したスマートカードベンダーのハードウェアとソフトウェアについて理解します。
- 分散環境でのデジタル証明書の展開管理方法について理解します。

スマートカードの種類

エンタープライズ向けとコンシューマー向けのスマートカードは、寸法も電気コネクタも同じで、同じスマートカードリーダーを使用できます。

エンタープライズ向けのスマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートしていて、ドキュメントや電子メールのデジタル署名と暗号化のためのアプリケーションと連携して使用できます。 XenAppとXenDesktopは、これらの用途をサポートしています。

コンシューマー向けのスマートカードにはデジタル証明書は含まれていませんが、共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名、チップとPINクレジットカードなど）をサポートできます。これらのスマートカードは、Windowsログインや一般的なWindowsアプリケーションをサポートしていません。これらのスマートカードと合わせて使用するには、特別なWindowsアプリケーションと、適切なソフトウェアインフラストラクチャ（支払いカードネットワークへの接続など）が必要です。XenAppまたはXenDesktopでのこのような特別なアプリケーションのサポートについて詳しくは、Citrix担当者にお問い合わせください。

エンタープライズ向けスマートカードには、互換性のある同等のものが存在し、類似した方法で使用できます。

- スマートカードと同等のUSBトークンはUSBポートに直接接続します。これらのUSBトークンは通常USBフラッシュドライブのサイズですが、携帯電話で使用されるSIMカードと同じくらい小さいものもあります。それらは、スマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windowsトラステッド プラットフォーム モジュール（TPM）を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Receiver 4.3以上を使用して、Windows 8およびWindows 10でサポートされます。
  - XenAppおよびXenDesktopの7.6 FP3よりも前のバージョンは、仮想スマートカードをサポートしていません。
  - 仮想スマートカードについて詳しくは、「Virtual Smart Card Overview」を参照してください。

  注：「仮想スマートカード」という用語は、単にユーザーコンピューターに保存されたデジタル証明書についても使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

XenAppおよびXenDesktopのスマートカードのサポートは、MicrosoftのPC/SC（Personal Computer/Smart Card）標準仕様に基づいています。スマートカードおよびスマートカードデバイスは、使用するWindowsオペレーティングシステムでサポ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

トされており、Microsoft WHQL（Windows Hardware Quality Lab）により承認されている必要があります。PC/SCに準拠しているハードウェアについては、Microsoft社のドキュメントを参照してください。 その他のタイプのユーザーデバイスは、PS/SC標準に準拠していることがあります。 詳しくは、http://www.citrix.com/ready/でCitrix Readyプログラムについて参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、別々のデバイスドライバーが必要です。ただし、スマートカードがNIST Personal Identity Verification（PIV）標準などの標準に準拠している場合、一定範囲のスマートカードに単一のデバイスドライバーを使用できる場合があります。デバイスドライバーをユーザーデバイスとVirtual Delivery Agent（VDA）の両方にインストールする必要があります。多くの場合、デバイスドライバーはCitrixパートナーから入手可能なスマートカードミドルウェアパッケージの一部として提供されます。スマートカードミドルウェアパッケージにより、高度な機能が提供されます。デバイスドライバーは、暗号化サービスプロバイダー（CSP）、キーストレージプロバイダー（KSP）、ミニドライバーとして説明されることもあります。

Windowsシステムでは、以下のスマートカードとミドルウェアでの動作確認が行われています。ただし、そのほかのスマートカードおよびミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアについて詳しくは、http://www.citrix.com/ready/jaを参照してください。

ミドルウェア	スマートカード
ActivClient 7.0（DoDモード有効）	DoD CACカード
PIVモードのActivClient 7.0	NIST PIVカード
Microsoftミニドライバー	NIST PIVカード
GemAlto Mini Driver for .NETカード	GemAlto .NET v2+
Microsoftネイティブドライバー	仮想スマートカード（TPM）

他の種類のデバイスでのスマートカード使用法について詳しくは、そのデバイスに関するCitrix Receiverのドキュメントを参照してください。XenDesktopによるPIV使用法について詳しくは、『Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV Smart Card Authentication』を参照してください。

他の種類のデバイスでのスマートカード使用法について詳しくは、そのデバイスに関するCitrix Receiverのドキュメントを参照してください。

リモートPCアクセス

オフィスで動作する、物理的なWindow 10、Windows 8、またはWindows 7マシンにリモートアクセスする場合は、スマートカードがサポートされます。Windows XPマシンへのリモートアクセスでは、スマートカードはサポートされません。

以下のスマートカードが、リモートPCアクセス機能でテストされています。

ミドルウェア	スマートカード

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gemalto .NETミニドライバー	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoftミニドライバー	NIST PIV
Microsoftネイティブドライバー	仮想スマートカード

スマートカードリーダーの種類

スマートカードリーダーはユーザーデバイス内に作成されることもありますし、別にユーザーデバイスに（通常はUSBまたはBluetoothで）接続することもあります。 USB Chip/Smart Card Interface Devices（CCID）仕様に準拠する接触カードリーダーがサポートされます。これらのカードリーダーでは、ユーザーがスマートカードをスロットに挿入したりスワイプしたりします。Deutsche Kreditwirtschaft（DK）標準は、接触カードリーダーの4つのクラスを定義しています。

- Class 1スマートカードリーダーは最も一般的で、通常1つのみのスロットを備えています。Class 1スマートカードリーダーは通常、オペレーティングシステム付属の標準CCIDデバイスドライバーでサポートされます。
- Class 2スマートカードリーダーには、ユーザーデバイスがアクセスできない安全なキーパッドも含まれています。 Class 2スマートカードリーダーは、内蔵の安全なキーパッドがあるキーボードに搭載される場合があります。Class 2スマートカードリーダーについては、Citrixの担当者に連絡してください。安全なキーパッドの機能を有効化するには、リーダー固有のデバイスドライバーが必要になる場合があります。
- Class 3スマートカードリーダーには、安全なディスプレイも含まれます。 Class 3スマートカードリーダーはサポートされません。
- Class 4スマートカードリーダーには、安全なトランザクションモジュールも含まれます。Class 4スマートカードリーダーはサポートされません。

注： スマートカードリーダーのクラスは、USBデバイスのクラスには無関係です。

スマートカードリーダーは、対応するデバイスドライバーとともにユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Receiverのマニュアルを参照してください。サポートされているバージョンは、通常、Citrix Receiverのドキュメントでスマートカードの記事でまたはシステム要件に関する記事に掲載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、デフォルトで有効な特定のICA/HDXスマートカード仮想チャネルを使用して、XenAppおよびXenDesktopに統合されています。

重要：スマートカードリーダーでは一般のUSBリダイレクションを使用しないでください。 一部のスマートカードリーダーではこれはデフォルトで無効にされており、有効化した場合サポートされなくなります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

同一ユーザーデバイス上で、複数のスマートカードやスマートカードリーダーを使用することは可能ですが、パススルー認証を使用する場合は1枚のスマートカードを挿入した状態で仮想デスクトップまたはアプリケーションを開始する必要があります。 アプリケーション内でスマートカードを使用する場合（デジタル署名または暗号化機能など）、スマートカードの挿入またはPINの入力を求めるメッセージが表示されることがあります。 これは、同時に複数のスマートカードが挿入されている場合に発生します。

- 適切なスマートカードを挿入しているにもかかわらずスマートカードの挿入を求めるメッセージが表示された場合は、［キャンセル］をクリックするよう通知します。
- ただし、PINの入力が求められた場合は、PINを再入力する必要があります。

Microsoft社のベーススマートカード暗号化サービスプロバイダー（CSP）によるスマートカードを使用する場合、Windows Server 2008または2008 R2が動作するサーバー上のアプリケーションにユーザーがアクセスすると、ほかのユーザーがスマートカードでログオンできなくなります。これについての詳細および修正プログラムについては、http://support.microsoft.com/kb/949538を参照してください。

カード管理システムまたはベンダーのユーティリティを使ってPINをリセットできます。

> **Important**
>
> XenAppまたはXenDesktopセッションでは、Microsoftリモートデスクトップ接続アプリケーションでのスマートカードの使用はサポートされません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前の確認事項

- スマートカードリーダーのデバイスドライバーを入手して、ユーザーデバイスにインストールする必要があります。Microsoftにより提供されるCCIDデバイスドライバーは、多くのスマートカードリーダーで使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手して、ユーザーデバイスと仮想デスクトップの両方にインストールします。このドライバーとCSPソフトウェアは、XenAppやXenDesktopと互換性がある必要があります。詳しくは、ベンダーのドキュメントを参照してください。ミニドライバーモデルのスマートカードを使用する仮想デスクトップでは、スマートカードミニドライバーが自動的にダウンロードされます。また、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。さらに、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要：Citrixソフトウェアをインストールする前に、物理的なコンピューターにドライバーとCSPソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10で実行するInternet Explorerでスマートカードを実行するユーザーの信頼済みサイトの一覧にCitrix Receiver fo Web URLを追加します。Windows 10では、Internet Explorerは信頼済みサイトのデフォルトで保護モードでは実行しません。
- PKI（Public Key Infrastructure：公開キー基盤）が適切に構成されていることを確認します。つまり、アカウントマッピングのための証明書がActive Directory環境に対して正しく構成されており、ユーザー証明書の検証を正しく実行できることを確認します。
- Citrix ReceiverやStoreFrontなど、スマートカードで使用するほかのCitrixコンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーにアクセスできることを確認します。
  - スマートカード上のログオン証明書に関連付けられているユーザーアカウント用のActive Directoryドメインコントローラー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Delivery Controller
- Citrix StoreFront
- Citrix NetScaler Gateway/Citrix Access Gateway 10.x
- VDA
- Microsoft Exchange Server（リモートPCアクセスの場合はオプション）

スマートカード使用の有効化

手順1： カードの発行ポリシーに従って、ユーザーにスマートカードを発行します。

手順2： 必要に応じて、ユーザーがリモートPCアクセスを実行できるようにスマートカードをセットアップします。

手順3： Delivery ControllerとStoreFrontをインストールして（未インストールの場合）、スマートカードのリモート処理用に構成します。

手順4： StoreFrontで、スマートカードの使用を有効にします。詳しくは、StoreFrontドキュメントの「スマートカード認証の構成」を参照してください。

手順5： NetScaler Gateway/Access Gatewayで、スマートカードの使用を有効にします。詳しくは、NetScalerドキュメントの「認証と承認の構成」および「Web Interfaceでのスマートカードアクセスの構成」を参照してください。

手順6： VDAでスマートカードの使用を有効にします。

- VDAに必要なアプリケーションおよび更新がインストール済みであることを確認します。
- ミドルウェアをインストールします。
- ユーザーデバイス上のCitrix Receiverと仮想デスクトップセッション間でスマートカードデータ通信が行われるように、スマートカードのリモート処理をセットアップします。

手順7： ユーザーデバイス（ドメインに属しているマシンと属していないマシンを含む）でスマートカードの使用を有効にします。詳しくは、StoreFrontドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書とその証明機関の証明書をデバイスのキーストア内にインポートします。
- ベンダーが提供するスマートカードミドルウェアをインストールします。
- Citrix Receiver for Windowsをインストールおよび構成して、グループポリシー管理コンソールを使ってicaclient.admをインポートします。また、スマートカード認証を有効にします。

手順8： 展開をテストします。テストユーザーのスマートカードで仮想デスクトップを起動して、展開が正しく構成されていることを確認します。すべてのアクセス方法（たとえば、Internet ExplorerおよびCitrix Receiverを介したデスクトップアクセスなど）をテストします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スマートカード展開

Dec 05, 2017

この製品バージョンおよびこのバージョンと以前のバージョンとの混在環境では、以下の種類のスマートカード展開がサポートされます。そのほかの構成でも使用できる場合がありますが、サポートの対象外です。

公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「	StoreFrontへの接続
ローカルのドメイン参加コンピューター	直接接続
ドメイン参加コンピューターからのリモートアクセス	NetScaler Gateway経由の接続
ドメイン不参加コンピューター	直接接続
ドメイン不参加コンピューターからのリモートアクセス	NetScaler Gateway経由の接続
デスクトップアプライアンスサイトにアクセスするドメイン不参加コンピューターおよびシンクライアント	デスクトップアプライアンスサイト経由の接続
XenApp Servicesサイト経由でStoreFrontにアクセスするドメイン参加コンピューターおよびシンクライアント	XenApp Servicesサイト経由の接続

展開の種類は、スマートカードリーダーが接続されているユーザーデバイスの特徴により定義されます。

- デバイスがドメインに参加しているか参加していないか。
- デバイスがStoreFrontにどのように接続するか。
- 仮想デスクトップやアプリケーションの表示にどのソフトウェアを使用するか。

これらの展開では、Microsoft WordやMicrosoft Excelなど、スマートカード対応のアプリケーションを使用できます。ユーザーは、これらのアプリケーションを使用してドキュメントにデジタル署名を追加したり、ドキュメントを暗号化したりできます。

2モード認証

これらの各展開で可能な箇所では、 スマートカードを使用するのか、ユーザー名およびパスワードを入力するのかをユーザーに選択させる 2方式認証をReceiverがサポートします。この機能は、 ユーザーがスマートカードを使用できない場合 （スマートカードを自宅に忘れた場合や資格情報の有効期限が切れた場合など）に便利です。

ドメイン不参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。 2モード認証を構成した場合、ユーザーは最初にスマートカードとPINを使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

NetScaler Gatewayを使用する環境では、ユーザーはデバイスにログオンし、NetScaler Gatewayの認証を受けるようにReceiver for Windowsから要求されます。 これはドメイン参加デバイスとドメイン不参加デバイスの両方に適用されます。ユーザーは、スマートカードとPINを使って、または指定ユーザーの資格情報を使ってNetScaler Gatewayにログオンできます。 これにより、 NetScaler Gatewayにログオンするときの2モード認証をユーザーに提供できます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gateway に委任します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

複数Active Directoryフォレストでの考慮事項

Citrix環境では、スマートカードは単一の フォレスト内でサポートされます。フォレスト間でのスマートカード認証には、すべてのユーザーアカウントに対する直接の双方向の信頼関係が必要です。より複雑なマルチフォレスト展開（一方向のみまたはそのほかの信頼関係が設定された複数フォレスト展開）はサポートされていません。

リモート デスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、（スマートカードが接続されるユーザーデバイス上に）ローカルにインストールしたり、（ユーザーデバイスが接続するリモートデスクトップ上に）リモートにインストールしたりできます。

スマートカード取り出し時の動作ポリシー

スマートカード取り出し時の動作ポリシーの設定により、セッション中にスマートカードリーダーからカードを取り出したときの処理が制御されます。 このポリシーは、Windowsオペレーティングシステムで設定します。

ポリシー設定	デスクトップの動作
何もしない	何もしません。
ワークステーションをロック	デスクトップセッションは切断され、仮想デスクトップはロックされます。
ログオフを強制する	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効な場合、セッションはログオフされてユーザーのデータは消失します。
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

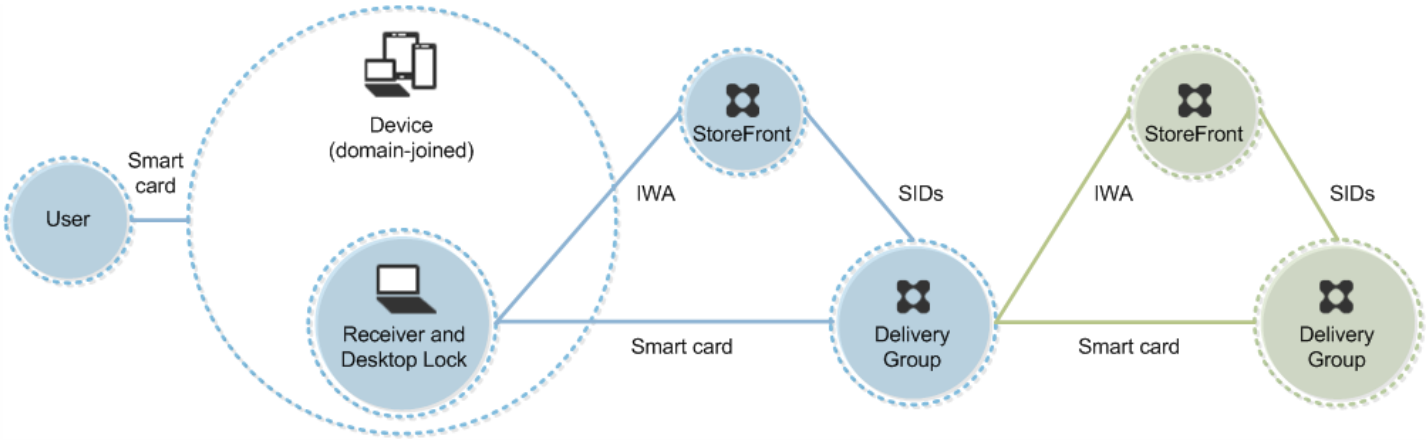
証明書失効のチェック

証明書失効のチェックが有効な場合、スマートカードの証明書が有効かどうか検出されます。証明書が無効な場合、ユーザー認証に失敗したり、その証明書に関連付けられているデスクトップやアプリケーションへのアクセスが拒否されたりします。たとえば、メールの復号化用の証明書が無効な場合、暗号化されたメールを復号化できなくなります。 同じスマートカードに有効なほかの証明書がある場合、その機能については有効なままとなります。たとえば、認証用の証明書が有効な場合、ユーザー認証に成功します。

展開例：ドメイン参加コンピューター

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続する、ドメインに参加しているユーザーデバイスが含まれています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

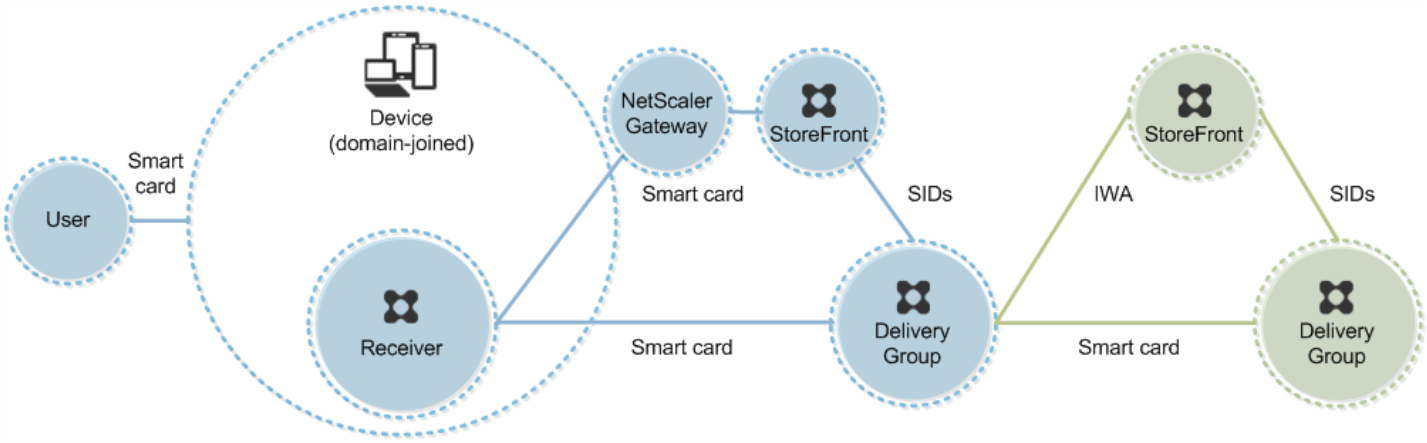


ユーザーは、スマートカードとPINを使ってデバイスにログオンします。Receiver は、StoreFrontサーバーにアクセスするユーザーを統合Windows 認証（IWA）で認証します。StoreFrontにより、ユーザーのセキュリティ識別子（SID）が XenAppまたはXenDesktopに渡されます。Receiverでシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要はありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン参加コンピューターからのリモートアクセス

この展開には、Desktop Viewerを実行し、NetScaler Gateway/Access Gatewayを介してStoreFrontに接続する、ドメインに参加しているユーザーデバイスが含まれています。



ユーザーはスマートカードとPINを使ってデバイスにログオンし、次にNetScaler Gateway/Access Gatewayにもう一度ログオンします。 この展開ではReceiverで2モード認証を使用できるため、この2つ目のログオンではスマートカードとPINを使用したりユーザー名とパスワードを入力したりできます。

ユーザーは自動的にStoreFrontにログオンし、ユーザーセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。 Receiverでシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要はありません。

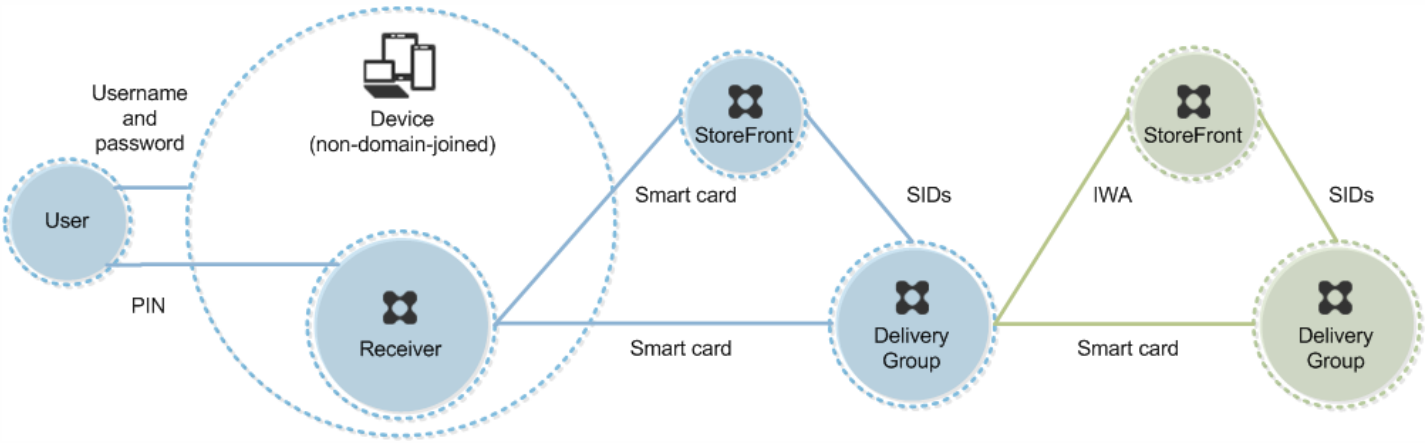
この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張でき

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

展開の例： ドメイン不参加コンピューター

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続する、ドメイン不参加のユーザーデバイスが含まれています。



ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。 この展開では2モード認証を使用できるため、Receiverではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。 その後、ReceiverがStorefrontへの認証を実行します。

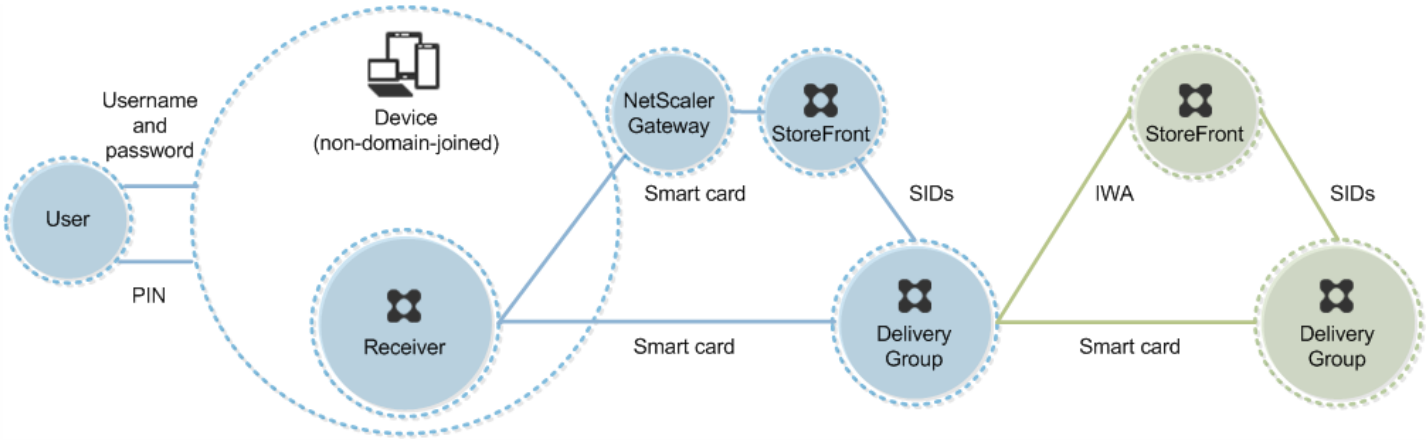
StoreFrontにより、ユーザーのセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。 この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要があります。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

展開例： ドメイン不参加コンピューターからのリモートアクセス

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続する、ドメイン不参加のユーザーデバイスが含まれています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。 この展開では2モード認証を使用できるため、Receiverではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。 その後、ReceiverがStorefrontへの認証を実行します。

StoreFrontにより、ユーザーのセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。 この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要があります。

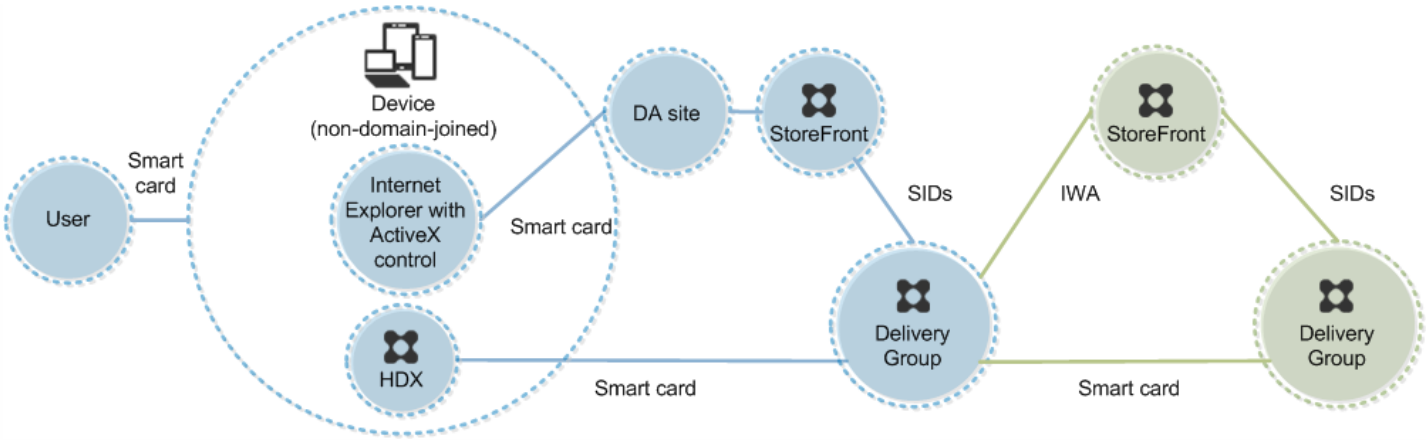
この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

展開の例： デスクトップアプライアンス サイトにアクセスするドメイン不参加コンピューターおよびシンクライアント

この展開には、 Desktop Lockを実行し、デスクトップアプライアンスサイトを介してStoreFrontに接続する、ドメイン不参加のユーザーデバイスが含まれています。

Desktop Lockは、XenApp、 XenDesktop、およびCitrix VDI-in-a-Boxと一緒にリリースされる個別のコンポーネントです。 Desktop Viewerの代替として使用でき、主に再目的化されたWindowsコンピューターおよびWindowsシンクライアント向けに設計されています。 Desktop Lockはユーザーデバイス上のWindows Shellとタスクマネージャーを置き換えるもので、 これによりユーザーはそのデバイスに直接アクセスできなくなります。Desktop Lockにより、 ユーザーにはWindows ServerおよびWindows Desktopのデスクトップが提供されます。 Desktop Lockのインストールは必須ではありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



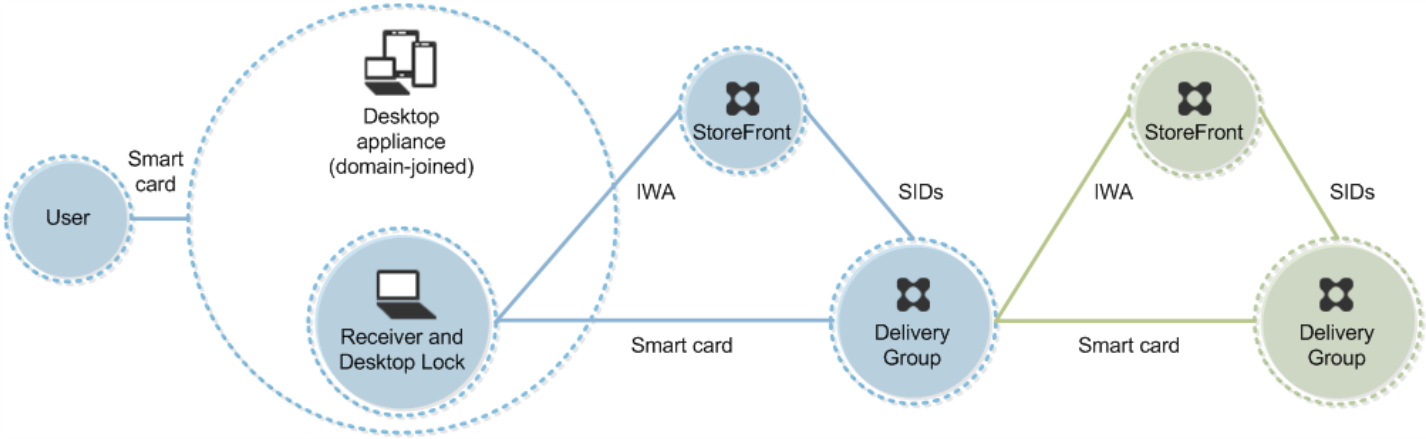
ユーザーは、スマートカードを使ってデバイスにログオンします。Desktop Lockを実行するデバイスは、 キオスクモードで動作するInternet Explorerを介してデスクトップアプライアンスサイトを起動するように構成されます。 サイトのActiveXコントロールによりPINの入力が求められ、それがStoreFrontに送信されます。 StoreFrontにより、 ユーザーのセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。割り当てられたデスクトップグループ一覧で使用可能な（アルファベット順で）最初のデスクトップが起動します。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

展開例：XenApp Servicesサイト経由でStoreFrontにアクセスするドメイン参加コンピューターおよびシンクライアント

この展開には、 Desktop Lockを実行し、XenApp Services URLを介してStoreFrontに接続する、ドメインに参加しているユーザーデバイスが含まれています。

Desktop Lockは、XenApp、 XenDesktop、およびCitrix VDI-in-a-Boxと一緒にリリースされる個別のコンポーネントです。 Desktop Viewerの代替として使用でき、主に再目的化されたWindowsコンピューターおよびWindowsシンクライアント向けに設計されています。 Desktop Lockはユーザーデバイス上のWindows Shellとタスクマネージャーを置き換えるもので、 これによりユーザーはそのデバイスに直接アクセスできなくなります。Desktop Lockにより、 ユーザーにはWindows ServerおよびWindows Desktopのデスクトップが提供されます。 Desktop Lockのインストールは必須ではありません。



ユーザーは、スマートカードとPINを使ってデバイスにログオンします。デバイス上でDesktop Lockが動作している場合は、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFrontサーバーでのユーザー認証に統合Windows認証（IWA） が使用されます。StoreFrontにより、ユーザーの セキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。Receiverでシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップを起動するときにPINを再入力する必要はありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。 仮想デスクトップのReceiverは、2つ目のStoreFrontサーバーへの認証を実行します。 この2つ目の接続では任意の認証方法を使用できます。 最初の接続で使用した認証方法を2つ目の接続で再使用したり、または2つ目の接続で異なる方法を使用したりできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スマートカードを使用したパススルー認証とシングルサインオン

Dec 05, 2017

パススルー認証

仮想デスクトップへのスマートカードによるパススルー認証は、Windows 10、Windows 8、Windows 7 Service Pack 1 Enterpriseエディション、およびProfessionalエディションが動作するユーザーデバイスでサポートされます。

ホストされるアプリケーションへのスマートカードによるパススルー認証は、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、およびWindows Server 2008 R2 SP1が動作するサーバーでサポートされます。

サーバーでホストされるアプリケーションへのスマートカードパススルー認証を使用するには、サイトの認証方法としてスマートカードパススルーを構成するときにKerberosを有効にする必要があります。

注： スマートカードによるパススルー認証を使用できるかどうかは、次の要因を含むさまざまな要因により決定されます。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFront上で構成します。詳しくは、StoreFrontのドキュメントを参照してください。

Single Sign-On

「シングルサインオン」とは、仮想デスクトップやアプリケーションの起動時にパススルー 認証を実行する機能を指します。この 機能を「ドメイン参加のStoreFront直接アクセス」および「ドメイン参加の NetScaler経由のStoreFrontアクセス」のスマートカード展開で使用して、 ユーザーがPINを入力する回数を減らすことができます。これらの種類の展開でシングルサインオンを使用するには、 StoreFrontサーバー上default.icaで以下のパラメーターを編集します。

- ドメイン参加の StoreFront直接アクセス — DisableCtrlAltDelをOffに設定します。
- ドメイン参加の NetScaler経由のStoreFrontアクセス — UseLocalUserAndPasswordを Onに設定します。

これらのパラメーター設定について詳しくは、StoreFront またはNetScaler Gatewayのドキュメントを参照してください。

シングルサインオン機能を使用できるかどうかは、 以下を含むさまざまな要因により決定されます。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

注： 注：スマートカードリーダーが接続された マシン上のVirtual Delivery Agent（VDA）にユーザーがログオンすると、 前回使用された認証方法（スマートカード またはパスワードなど）の画面が開く場合があります。この結果、シングルサインオンが有効な場合はシングルサインオン用の 画面が開きます。この画面では シングルサインオンが機能しないため、ユーザーは ［ユーザーの切り替え］をクリックしてほかの画面を開く必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Transport Layer Security（TLS）

Jan 05, 2018

XenAppまたはXenDesktopのサイトのTLS（Transport Layer Security）プロトコルを構成するには、以下の手順が必要です。

- サーバー証明書を入手して、すべてのDelivery Controller上にインストールして登録します。さらに、TLS証明書のポート構成を行います。詳しくは、「TLSサーバー証明書のControllerへのインストール」を参照してください。
  必要な場合は、ControllerでHTTPおよびHTTPSトラフィック用に使用されるポートを変更することもできます。

- ユーザーとVirtual Delivery Agent（VDA）間のTLS接続を有効にします。これを行うには、以下のタスクが必要です。
  - VDAがインストールされたマシン上でTLSを構成します（便宜上、VDAがインストールされたマシンをここでは「VDA」と呼びます）。提供されているPowerShellスクリプトを使用したり、手作業で構成したりすることができます。全般的な情報については、「VDA上のTLS設定について」を参照してください。詳しくは、「VDA上のTLS構成：PowerShellスクリプトの使用」および「VDA上のTLS構成：手作業による構成」を参照してください。
  - VDAが追加されているデリバリーグループでTLSを構成します。これを行うには、Studioでいくつかの PowerShellコマンドレットを実行します。詳しくは、「デリバリーグループのTLSの構成」を参照してください。

  以下の要件および考慮事項があります。
  - ユーザーとVDA間のTLS接続を有効にするのは、XenApp 7.6サイト、XenDesktop 7.6サイト、およびこれ以降のリリースでのみ必要です。
  - デリバリーグループおよびVDA上のTLSは、コンポーネントのインストール、サイトの作成、およびマシンカタログとデリバリーグループの作成を行った後で構成します。
  - デリバリーグループでTLSを構成するには、Controllerのアクセス規則を変更するための権限が必要です。すべての管理権限を実行できる管理者には必要な権限が付与されています。
  - VDA上のTLSを構成するには、そのマシン上のWindows管理者権限が必要です。
  - VDAを以前のバージョンからアップグレードしてTLSを構成する場合は、アップグレード前にすべてのSSLリレーソフトウェアをアンインストールしておく必要があります。
  - PowerShellスクリプトでは、静的に割り当てられるVDA上のTLSを構成できます。Machine Creation ServicesまたはProvisioning Servicesでプロビジョニングされてプールされる VDAは再起動時にマシンイメージがリセットされるため、PowerShellスクリプトでTLSを構成することはできません。

> ### 警告
>
> Windowsレジストリの編集を含むタスクの場合：レジストリの編集を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

サイトデータベース接続のTLSを有効にする方法については、CTX137556を参照してください。

> ### 注意
>
> TLS とUDTが両方ともVDAで有効な場合：
>
> - Citrix Directorは、VDAへの直接アクセスに常にTLS over TCP（UDP やUDTではなく）を使用します。
> - NetScaler Gatewayを使用してVDAに間接的にアクセスする場合、Citrix Receiverは、NetScaler Gatewayとの通信にDTLS over UDPを使用します。NetScaler GatewayとVDA間の通信には、DTLSなしのUDPが使用されます。 UDTが使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TLSサーバー証明書のControllerへのインストール

HTTPS接続を使用する場合、XML ServiceはサーバーTLS証明書を使用したTLS機能をサポートしますが、クライアント証明書はサポートしません。サーバー証明書を入手してController上にインストールおよび登録し、TLS証明書のポート構成を行うには、以下のタスクが必要です。

ControllerにIISがインストールされている場合は、https://technet.microsoft.com/ja-jp/library/cc771438%28v=ws.10%29.aspxの手順に従います。

ControllerにIISがインストールされていない場合は、以下の方法で証明書を構成します。

1. http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspxを参照し、TLSサーバー証明書を取得してController上にインストールします。証明書要求ツール（Certreq）については、http://technet.microsoft.com/ja-jp/library/cc736326(WS.10).aspxを参照してください。
   PowerShellスクリプトを使用してVDA上のTLSを構成するときにTLS証明書の拇印を指定しない場合は、証明書ストアの［ローカルコンピューター］>［個人］>［証明書］に適切な証明書が配置されていることを確認してください。この場所に複数の証明書が配置されている場合、最初に検出されたものが使用されます。
2. 証明書でのポートの構成については、http://msdn.microsoft.com/ja-jp/library/ms733791%28v=vs.110%29.aspxを参照してください。

ControllerをWindows Server 2016にインストールし、StoreFrontをWindows Server 2012にインストールする場合は、TLSの暗号の組み合わせ順を変更するために、Controllerで構成を変更する必要があります。

> **注意**
>
> この構成の変更は、他のバージョンのWindows Serverの組み合わせのControllerとStoreFrontでは必要ありません。

暗号の組み合わせの順序一覧には、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384またはTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256の暗号の組み合わせ（またはこの両方）を含める必要があります。また、これらの暗号の組み合わせをTLS_DHE_の暗号の組み合わせより前に配置する必要があります。

> **注意**
>
> Windows Server 2012では、GCMの暗号の組み合わせTLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384またはTLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256はサポートされません。

1. Microsoftのグループポリシーエディターを使用して、［コンピューターの構成］>［管理用テンプレート］>［ネットワーク］>［SSL構成設定］の順に参照します。
2. 「SSL暗号の順位」というポリシーを編集します。デフォルトでは、このポリシーは［未構成］に設定されています。このポリシーを［有効］に設定します。
3. 暗号の組み合わせを適切な順序に並び替え、使用しない暗号の組み合わせを削除します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384またはTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256のどちらかがすべてのTLS_DHE_暗号の組み合わせより前に配置されていることを確認します。

Microsoft MSDNの「Prioritizing Schannel Cipher Suites」も参照してください。

HTTPまたはHTTPSポートの変更

デフォルトでは、XML ServiceはHTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443を使用します。これらのポート番号を変更することもできますが、信頼されないネットワークにControllerを露出させる場合のセキュリティ上のリスクについて考慮してください。デフォルト構成を変更する場合は、スタンドアロンのStoreFrontサーバーを使用することをお勧めします。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioで次のコマンドを実行します。

BrokerService.exe -WIPORT <*http-port*> -WISSLPORT <*https-port*>

ここで、*<http-port>*はHTTPトラフィックのポート番号で、*<https-port>*はHTTPSトラフィックのポート番号です。

> ## 注意
>
> ポートが変更されると、ライセンスの互換性およびアップグレードに関するメッセージがStudioに表示されます。この問題を解決するには、以下のPowerShellコマンドレットを順に実行してサービスインスタンスを再登録してください。
>
> Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |
>
> Unregister-ConfigRegisteredServiceInstance
>
> Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" | Register-ConfigServiceInstance

HTTPSトラフィックのみに制限する

HTTPトラフィックがXML Serviceで無視されるように構成するには、Controller上のHKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\で以下のレジストリ設定を作成してからBroker Serviceを再起動します。

HTTPトラフィックを無視するには、DWORD XmlServicesEnableNonSslを作成して0に設定します。

同様に、HTTPSトラフィックを無視するために作成できるレジストリのDWORD値も存在します：DWORD XmlServicesEnableSsl これは0に設定しないでください。

VDA上のTLS設定

TLSを構成したVDAと構成していないVDAを同一デリバリーグループ内で混在させることはできません。デリバリーグループのTLSを構成する前に、そのグループに属しているすべてのVDA上でTLS構成を完了しておく必要があります。

VDA上にTLSを構成すると、インストールされているTLS証明書の権限が変更され、その証明書の秘密キーに対する読み取り権限がICA Serviceに付与されます。ICA Serviceには、以下の情報が提供されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **証明書ストア内のどの証明書がTLS**で使用されるのか。
- **どのTCPポートがTLS接続**で使用されるのか。

Windowsファイアウォールを使用する環境では、このTCPでの着信接続が許可されている必要があります。PowerShellスクリプトを使用する場合は、このファイアウォール規則が自動的に構成されます。

- **どのバージョンのTLSプロトコルが許可されるのか。**

> ## Important
>
> SSLv3の使用状況を確認し、必要に応じ、それらの展開を再構成してSSLv3のサポートを削除することをお勧めします。CTX200238を参照してください。

サポートされるTLSプロトコルのバージョンは、低いものからSSL 3.0、TLS 1.0、TLS 1.1、およびTLS 1.2です。サポートされるSSLプロトコルを指定するときは、許可する最低バージョンを指定します。

たとえば、最低バージョンとしてTLS 1.1を指定すると、TLS 1.1およびTLS 1.2のプロトコルを使用した接続が許可されます。最低バージョンとしてSSL 3.0を指定すると、サポートされるSSLプロトコルのすべてのバージョンが許可されます。最低バージョンとしてTLS 1.2を指定すると、TLS 1.2の接続のみが許可されます。

- **どのTLS暗号の組み合わせが許可されるのか。**

暗号スイートが、この接続において使用する暗号化を選択します。 クライアントとVDAは、暗号スイートの異なる組み合わせをサポートできます。クライアント（Citrix ReceiverまたはStoreFront）がVDAに接続するときは、そのクライアントがサポートするTLS暗号スイートの一覧をVDAに送信します。VDA側では、構成済みの暗号スイートの独自の一覧内にクライアントのいずれかの暗号スイートと一致するものがあるかどうかがチェックされ、あった場合にのみ接続が確立されます。一致する暗号スイートがない場合、その接続はVDAにより拒否されます。

VDAがサポートしている暗号スイート（コンプライアンスモードとも呼ばれます）は、GOV（ernment）、COM（mercial）、およびALLの3つです。確立できる暗号スイートは、WindowsのFIPSモードによっても異なります。WindowsのFIPSモードについては、http://support.microsoft.com/kb/811833を参照してください。次の表は、それぞれの組み合わせにある暗号スイートを示しています。

TLS暗号スイート	GOV	COM	すべて	GOV	COM	すべて
FIPSモード	電源 - オフ	オフ	オフ	オン	オン	オン
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	○		○	○		○
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	○		○	○		○
TLS_RSA_WITH_AES_256_GCM_SHA384	○		○	○		○
TLS_RSA_WITH_AES_128_GCM_SHA256	○	○	○	○	○	○

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TLS_RSA_WITH_AES_256_CBC_SHA256	○		○	○		○
TLS_RSA_WITH_AES_256_CBC_SHA	○		○	○		○
TLS_RSA_WITH_AES_128_CBC_SHA		○	○		○	○
TLS_RSA_WITH_RC4_128_SHA		○	○			
TLS_RSA_WITH_RC4_128_MD5		○	○			
TLS_RSA_WITH_3DES_EDE_CBC_SHA	○		○	○		x

Important

VDAが、Windows Server 2012 R2、Windows Server 2016、Windows 10 Anniversary Edition、または以降のサポートリリースにインストールされている場合は、追加の手順が必要になります。これは、Citrix Receiver for Windows（バージョン4.6～4.9）、Citrix Receiver for HTML5、およびCitrix Receiver for Chromeからの接続に影響します。これには、NetScaler Gatewayを介した接続も含まれます。

この手順は、NetScaler GatewayとVDA間のTLSが設定されている場合、すべてのVDAバージョンでNetScaler Gatewayを使用するすべての接続にも必要です。これはCitrix Receiverのすべてのバージョンに影響します。

グループポリシーエディターを使用するVDA（Windows Server 2016またはWindows 10 Anniversary Edition以降）上で、［コンピューターの構成］>［管理用テンプレート］>［ネットワーク］>［SSL構成設定］>［SSL暗号の順位］と移動します。以下の順に選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
、TLS_RSA_WITH_AES_256_GCM_SHA384
、TLS_RSA_WITH_AES_128_GCM_SHA256
、TLS_RSA_WITH_AES_256_CBC_SHA256
、TLS_RSA_WITH_AES_256_CBC_SHA
、TLS_RSA_WITH_AES_128_CBC_SHA
、TLS_RSA_WITH_RC4_128_SHA
、TLS_RSA_WITH_3DES_EDE_CBC_SHA

注意

最初の4つの項目は、楕円曲線、P384、またはP256も指定します。［curve25519］が選択されていないことを確認します。FIPSモードは、「curve25519」の使用を妨げません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

このグループポリシー設定が構成されると、VDAは、暗号の組み合わせを、グループポリシーの一覧と選択されたコンプライアンスモード（COM、GOVまたはALL）の一覧の両方に表示されている場合のみ選択します。また、暗号スイートは、クライアント（Citrix ReceiverまたはStoreFront）が送信する一覧にも記載されている必要があります。

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、このグループポリシーの一覧に追加する必要がある場合があります。

> **Important**
>
> グループポリシーの変更が適用されたときに表示されても、TLS構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。したがって、プールデスクトップの場合、TLS構成のグループポリシーの変更は基本イメージに適用してください。

VDA上のTLS構成：PowerShellスクリプトの使用

VDA上でEnable-VdaSSL.ps1スクリプトを実行すると、そのVDAでのTLSリスナーを有効または無効にできます。このスクリプトは、インストールメディアのSupport > Tools > SslSupportフォルダーに収録されています。

スクリプトでTLSを有効にする場合、指定したTLS TCPポートについての既存のWindowsファイアウォール規則がすべて無効になります。その後で、ICA Serviceがそのポートで着信接続を受け入れるための新しい規則が追加されます。また、スクリプトにより以下のWindowsファイアウォール規則が無効になります。

- Citrix ICA（デフォルトで1494）
- Citrix CGP（デフォルトで2598）
- Citrix WebSocket（デフォルトで8008）

この影響として、TLSを使用した場合のみ接続が可能になります。TLSを使用しないと、ICA/HDX、セッション画面を保持したICA/HDX、WebSocketを介したHDXを使用することはできません。

「ネットワークポート」を参照してください。

このスクリプト内には、以下の構文および使用例が記載されています。Notepad++などのツールを使用してこれらを参照できます。

> **Important**
>
> EnableまたはDisableパラメーターとCertificateThumbPrintパラメーターを指定します。その他のパラメータはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint ""[–SSLPort ] [-SSLMinVersion ""] [-SSLCipherSuite""]
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parameter	Description
有効化	TLSリスナーをVDA上にインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかを指定する必要があります。
無効化	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかを指定する必要があります。このパラメーターを指定した場合、ほかのパラメーターは無視されます。
CertificateThumbPrint ""	証明書ストア内のTLS証明書の拇印を二重引用符で囲んで指定します。スクリプトは、指定された拇印によって使用する証明書を選択します。このパラメーターは必須です。このパラメーターがないと、不正な証明書が選択されます。
SSLPort	TLSポート指定します。デフォルトは以下のとおりです。 443
SSLMinVersion ""	許可されるTLSプロトコルの最低バージョンを二重引用符で囲んで指定します。有効な値は次のとおりです。 • "SSL_3.0" • "TLS_1.0" • "TLS_1.1" • "TLS_1.2" デフォルト："TLS_1.0" **重要：**SSLv3の使用状況を確認し、必要に応じ、展開を再構成してSSLv3のサポートを削除する措置をとることをお勧めします。CTX200238を参照してください。
SSLCipherSuite ""	TLS暗号スイートを二重引用符で囲んで指定します。有効な値は次のとおりです。 • "GOV" • "COM" • "ALL" デフォルト："ALL"

例

次のスクリプトでは、TLS 1.2プロトコルバージョン値をインストールして有効にします。拇印（この例の場合、「12345678987654321」）を指定して、使用する証明書を選択します。

```
Enable-VdaSSL –Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトでは、TLSリスナーをインストールして有効化し、TLSポートとして400、暗号スイートGOV、およびSSLプロトコルの最低バージョンとしてTLS 1.2を設定します。拇印（この例の場合、「12345678987654321」）を指定して、使用する証明書を選択します。

```
Enable-VdaSSL – Enable
-CertificateThumbPrint "12345678987654321"
–SSLPort 400 'SSLMinVersion "TLS_1.2"
–SSLCipherSuite "GOV"
```

次のスクリプトでは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL –Disable
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA上のTLS構成：手作業による構成

VDA上のTLSを手作業で構成するには、TLS証明書の秘密キーに対する読み取り権限をVDA上のNT SERVICE\PorticaService（VDA for Windows Desktop OSの場合）またはNT SERVICE\TermService（VDA for Windows Server OSの場合）に付与します。VDAがインストールされたマシン上で、以下の手順を行います。

手順1：Microsoft管理コンソール（MMC）を起動します： ［スタート］>［ファイル名を指定して実行］> mmc.exe。

手順2：MMCに証明書スナップインを追加します。

1. ［ファイル］>［スナップインの追加と削除］の順に選択します。
2. ［証明書］を選択して［追加］をクリックします。
3. ［このスナップインで管理する証明書］で［コンピューターアカウント］をクリックし、［次へ］をクリックします。
4. ［このスナップインで管理するコンピューター］で［ローカルコンピューター］をクリックし、［完了］をクリックします。

手順3：コンソールツリーの［証明書（ローカルコンピューター）］>［個人］>［証明書］で証明書を右クリックして、［すべてのタスク］>［秘密キーの管理］の順に選択します。

手順4：アクセス制御リストエディターで［（FriendlyName）プライベートキーのアクセス許可］ダイアログボックスが開きます。ここで（FriendlyName）は、TLS証明書の名前です。以下のいずれかのサービスを追加して、［読み取り］アクセスを許可します。

- VDA for Windows Desktop OSでは「PORTICASERVICE」
- VDA for Windows Server OSでは「TERMSERVICE」

手順5：インストールしたTLS証明書をダブルクリックします。［証明書］ダイアログボックスの［詳細］タブをクリックして、一番下までスクロールします。［拇印］をクリックします。

手順6：regeditを実行して、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawdを開きます。

1. SSL Thumbprintキーを編集して、TLS証明書の拇印の値をバイナリ値にコピーします。［バイナリ値の編集］ダイアログボックスでは、不明な項目（「0000」や特殊文字など）は無視して構いません。
2. SSLEnabledキーを編集して、DWORD値を1に変更します（このDWORD値を0にするとSSLが無効になります）。
3. このレジストリパスでは、必要に応じて以下のデフォルト値を変更できます。

    SSLPortのDWORD値 – SSLポート番号。デフォルト：443。

    SSLMinVersionのDWORD値 – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2。デフォルト：2（TLS 1.0）。

    SSLCipherSuiteのDWORD値 – 1 = GOV、2 = COM、3 = ALL。デフォルト：3（ALL）。

手順7：デフォルトの443以外のTLS TCPポートを使用する場合は、そのポートがWindowsファイアウォールで開放されていることを確認します（Windowsファイアウォールで受信規則を作成するときは、［接続を許可する］および［有効］が選択されていることを確認してください）。

手順8：ほかのアプリケーションやサービスなど（IISなど）がそのTLS TCPポートを使用していないことを確認します。

手順9：VDA for Windows Server OSの場合は、変更を適用するためのマシンを再起動します。VDA for Windows Desktop OSのマシンを再起動する必要はありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デリバリーグループのTLSの構成

TLS接続を構成したVDAを含んでいるすべてのデリバリーグループで、以下の手順を行います。

1. StudioからPowerShellコンソールを開きます。
2. **asnp Citrix.***を実行してCitrix製品のコマンドレットをロードします。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '<*delivery-group-name*>' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true**を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Citrix Receiver for WindowsでTLS関連の接続エラー（1030など）が発生した場合は、Desktop Viewerを無効にしてから再試行してください。接続エラーは解決されませんが、TLSの問題についての情報が表示される場合があります。たとえば、証明機関に証明書を要求したときに正しくないテンプレートを使用したなどがあります。

ControllerとVDAの間の通信

ControllerとVDA間の通信は、Windows Communication Framework（WCF）のメッセージレベルの保護によってセキュリティ保護されています。TLSを使用した追加の移送レベルの保護は必要ありません。WCF構成では、ControllerとVDA間の相互認証にKerberosが使用されます。暗号化には、CBCモードでのAESが256ビットキーで使用されます。メッセージの整合性にはSHA-1が使用されます。

Microsoftによると、WCFで使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）による標準に準拠しています。 さらに、WCFはSecurity Policy 1.2に表記されているアルゴリズムスイートすべてをサポートしていることも明言されています。

ControllerとVDA間の通信には、上述のアルゴリズムによるbasic256アルゴリズムスイートが使用されます。

TLSおよびHTML5ビデオリダイレクション

HTML5ビデオリダイレクションを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されたJavaScriptは、VDAで動作するCitrix HDX HTML5ビデオリダイレクションサービス（WebSocketService.exe）へのTLS接続を確立する必要があります。これを達成するために、VDAの証明書ストアで2つのカスタム証明書が生成されます。

HTML5ビデオリダイレクションポリシーはデフォルトで無効になっています。

HTML5ビデオリダイレクションについて詳しくは、「マルチメディアのポリシー設定」を参照してください。

> **注意**
>
> HTML5ビデオリダイレクションを使用しない場合、ローカルコンピューターの証明書ストアから生成された2つの証明書を削除することをお勧めします。
>
> 次の証明書です。
>
> - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
> 場所：［証明書 - ローカルコンピューター］>［信頼されたルート証明機関］>［証明書］。
> - エンドエンティティ（リーフ）：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
場所： [証明書 - ローカルコンピューター] > [個人] > [証明書] 。

Citrix HDX HTML5ビデオリダイレクションサービスが自動的に開始しないように設定することをお勧めします。
このサービスを停止すると、証明書も削除されます。

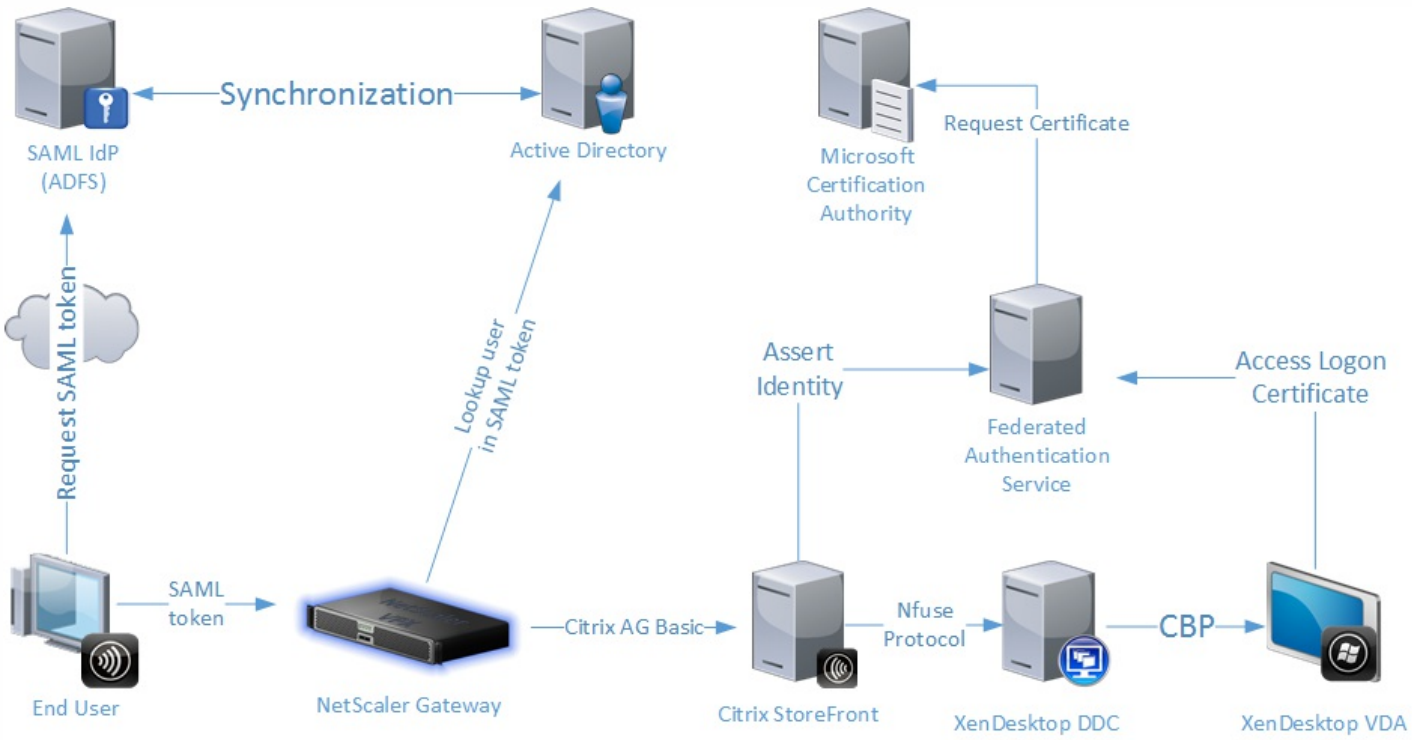
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated 認証サービス

Dec 05, 2017

Citrix Federated Authentication Serviceは、Active Directory証明書サービスと統合するように設計されている、権限が付与されたコンポーネントです。 Citrix Federated Authentication Serviceではユーザー向けの証明書が動的に発行され、ユーザーはスマートカードを持っている場合と同じようにActive Directory環境にログオンできます。 これにより、StoreFrontで、SAML（Security Assertion Markup Language）アサーションなどの広範な認証オプションを使用できます。SAMLは、インターネット上で従来のWindowsユーザーアカウントに代わるものとして一般的に使用されています。

以下の図に、Microsoft証明機関と統合したFederated Authentication Serviceによる、StoreFrontとXenAppおよびXenDesktop Virtual Delivery Agent（VDA）へのサポートサービスの提供について示します。



ユーザーがCitrix環境へのアクセスを要求すると、信頼済みのStoreFrontサーバーがFederated Authentication Service （FAS）にアクセスします。 FASは、単一のXenAppまたはXenDesktopセッションがそのセッションの証明書で認証できるようにするチケットを付与します。VDAでユーザーを認証する必要がある場合、VDAはFASにアクセスしてチケットを使用します。ユーザー証明書の秘密キーにアクセスできるのはFASだけです。VDAは、証明書を使用して実行する必要のあるすべての署名処理および暗号化解除処理を、FASに送信しなければなりません。

要件

Federated Authentication ServiceはWindowsサーバー（(Windows Server 2008 R2以降）でサポートされます。

- FASは、ほかのCitrixコンポーネントを含まないサーバーにインストールすることをお勧めします。
- Windowsサーバーはセキュリティ保護されている必要があります。 Windowsサーバーには登録機関の証明書および秘密キーへのアクセス権限があり、ドメインユーザーに対して自動的に証明書を発行できます。また、これらのユーザー証明書

© 1999-2017 Citrix Systems, Inc. All rights reserved.

および秘密キーへのアクセス権限もあります。

XenAppまたはXenDesktopのサイトでの要件は次のとおりです。

- Delivery Controllerのバージョンは7.9以上である必要があります。
- VDAのバージョンは7.9以上である必要があります。マシンカタログを通常どおりに作成する前に、Federated Authentication Serviceのグループポリシー構成が適切にVDAに適用されていることを確認してください。詳しくは、「グループポリシーの構成」セクションを参照してください。
- StoreFrontサーバーのバージョンは3.6（XenAppおよびXenDesktop 7.9 ISOで提供されるバージョン)以上である必要があります。

このサービスの展開を計画する場合は、「セキュリティに関する考慮事項」セクションを参照してください。

参照先ドキュメント：

- Active Directory証明書サービス

  https://technet.microsoft.com/en-us/library/hh831740.aspx

- 証明書ログオン用のWindowsの構成

  http://support.citrix.com/article/CTX206156

インストールとセットアップの順序

1. Federated Authentication Serviceのインストール
2. StoreFrontサーバーでのFederated Authentication Serviceプラグインの有効化
3. グループポリシーの構成
4. Federated Authentication Serviceの管理コンソールを使用した作業：（a）提供されたテンプレートの展開、（b）証明機関のセットアップ、および（c）Federated Authentication Serviceへの証明機関の使用権限の付与
5. ユーザールールの構成

Federated Authentication Serviceのインストール

セキュリティ上の理由により、FASは、ドメインコントローラーや証明機関と同様にセキュリティ保護されている専用サーバーにインストールすることをお勧めします。 FASは、ISOの挿入時に自動実行されるスプラッシュスクリーンの［**Federated Authentication Service**］ボタンからインストールできます。

以下のコンポーネントがインストールされます。

- Federated 認証サービス
- Federated Authentication Serviceをリモートで構成するPowerShellスナップインコマンドレット
- Federated Authentication Serviceの管理コンソール
- Federated Authentication Serviceのグループポリシーテンプレート（CitrixFederatedAuthenticationService.admx/adml）
- 証明機関の簡易構成用の証明書テンプレートファイル
- パフォーマンスカウンターおよびイベントログ

StoreFrontストアでのFederated Authentication Service

© 1999-2017 Citrix Systems, Inc. All rights reserved.

プラグインの有効化

StoreFrontストアでFederated Authentication Serviceの統合を有効にするには、管理者アカウントで以下のPowerShellコマンドレットを実行します。複数のストアがある場合、またはストアの名前が異なる場合は、以下のパスのテキストが異なる可能性があります。

-command コピー

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
$StoreVirtualPath = "/Citrix/Store"
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "FASLogonDataProvider"
```

FASの使用を停止するには、以下のPowerShellスクリプトを使用します。

-command コピー

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
$StoreVirtualPath = "/Citrix/Store"
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

Delivery Controllerの構成

Federated Authentication Serviceを使用するには、接続可能なStoreFrontサーバーを信頼するようにXenAppまたはXenDesktop Delivery Controllerを構成します。PowerShellコマンドレット**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**を実行します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

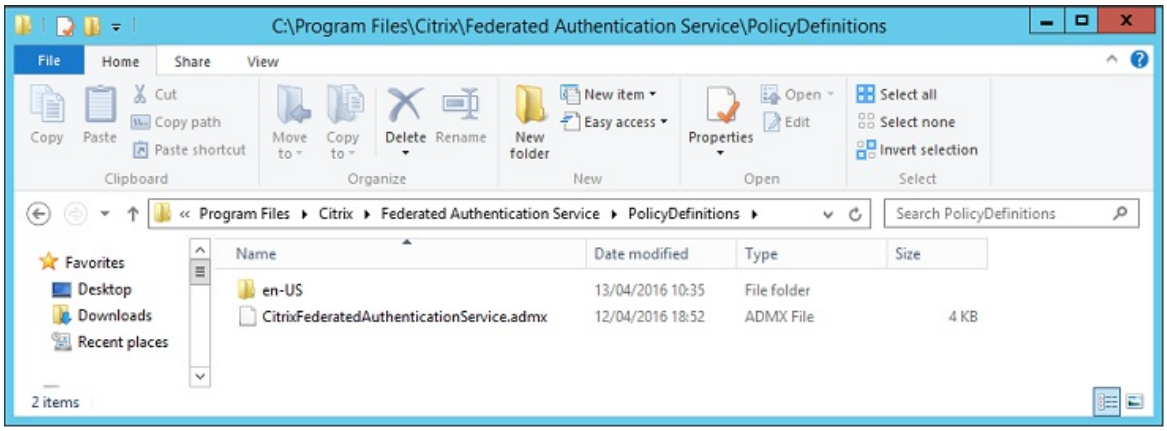
グループポリシーの構成

Federated Authentication Serviceのインストール後は、インストールで提供されたグループポリシーテンプレートを使用して、グループポリシー内のFASサーバーの完全なDNSアドレスを指定する必要があります。

重要： チケットを要求するStoreFrontサーバーおよびチケットを使用するVDAに、グループポリシーオブジェクトによって適用されるサーバーの自動番号設定を含む、同じDNSアドレス構成を行う必要があります。

説明をシンプルにするために、以下の例ではすべてのマシンに適用されるドメインレベルで単一のポリシーを構成していますが、これは必須ではありません。 StoreFrontサーバー、VDA、およびFAS管理コンソールを実行しているマシンで同じDNSアドレスの一覧が参照されている限り、FASは機能します。グループポリシーオブジェクトによって各エントリにインデックス番号が追加されることに注意してください。このインデックス番号は、複数のオブジェクトを使用する場合も一致する必要があります。

手順1： FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admxファイルおよびen-USフォルダーを見つけます。

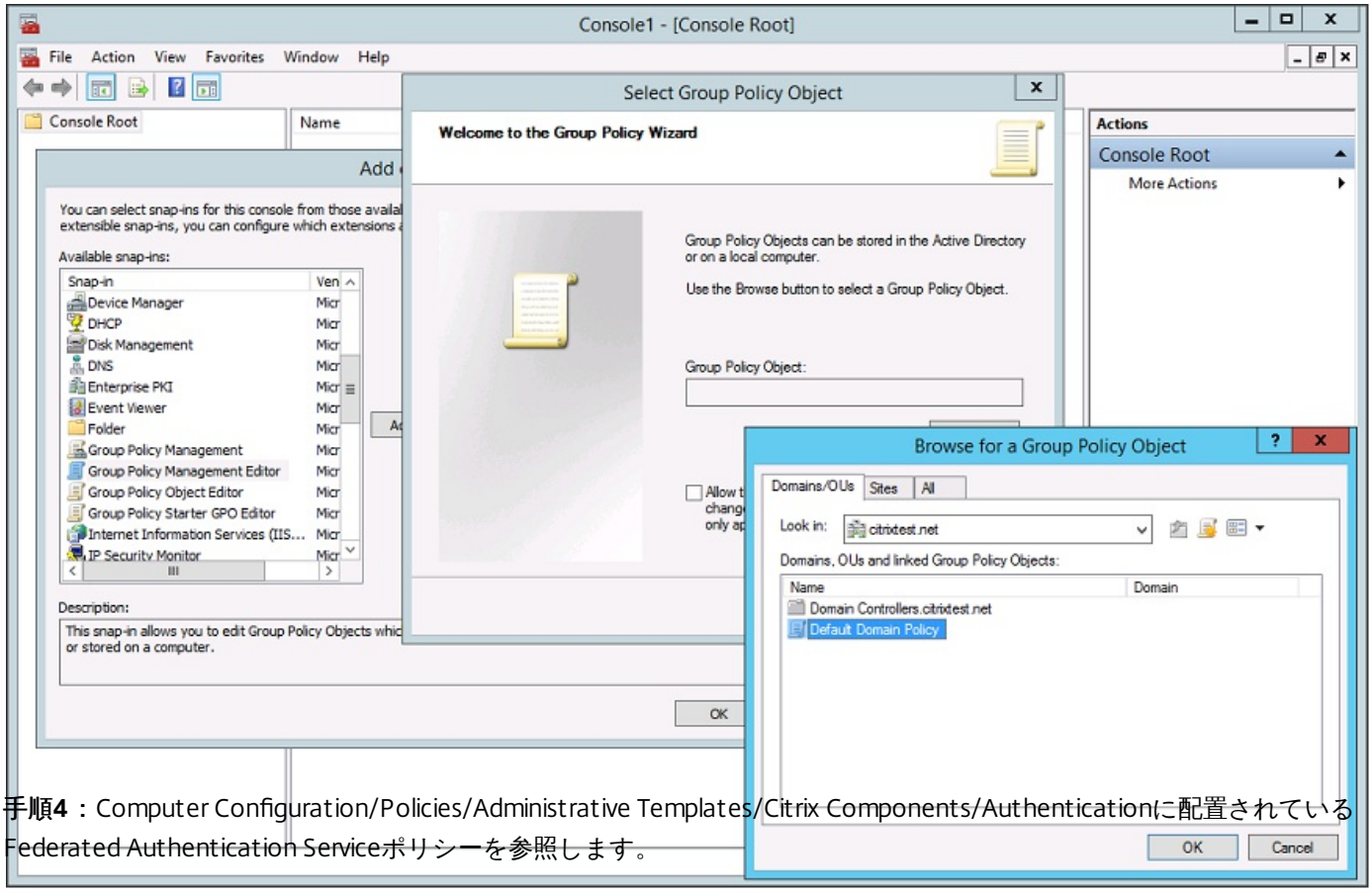


手順2：これらをドメインコントローラーにコピーして、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

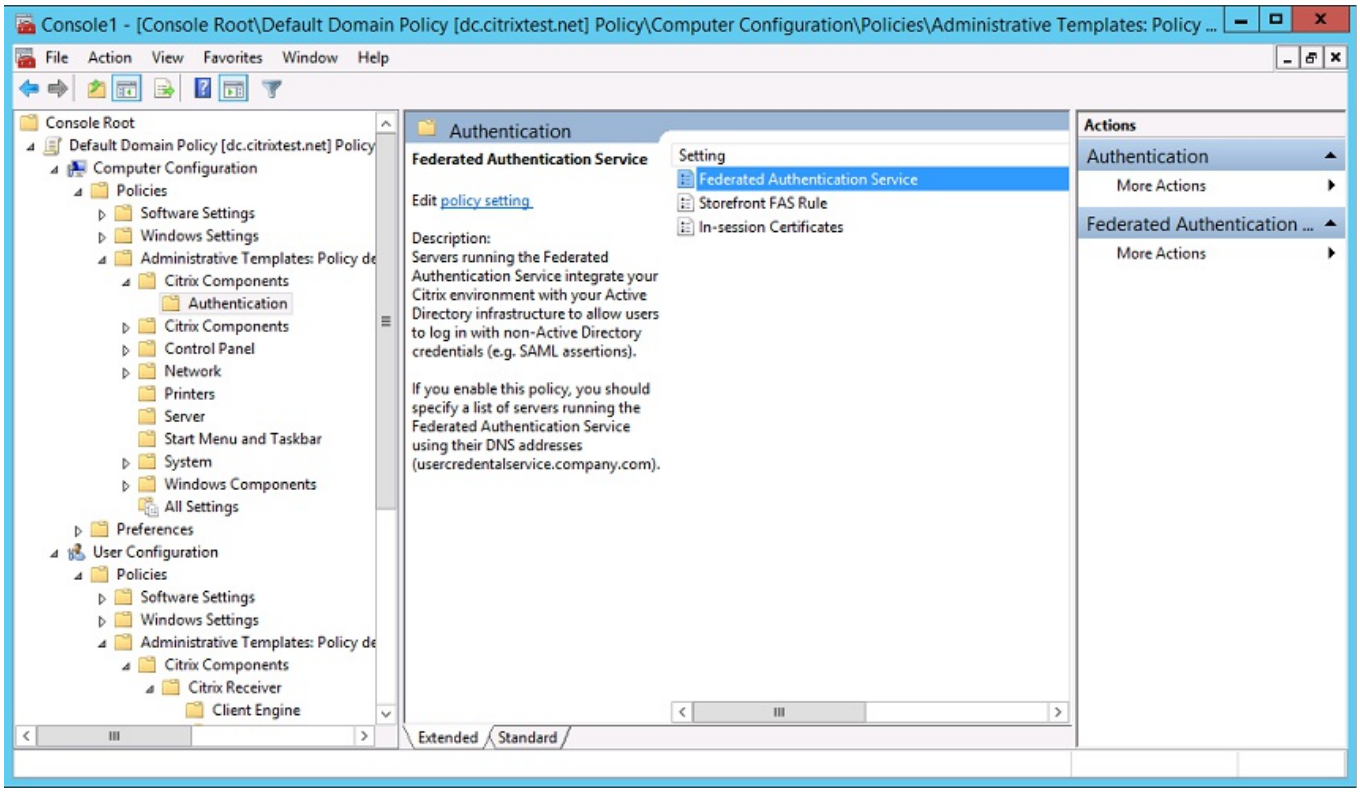
手順3：コマンドラインからMicrosoft管理コンソールを実行します（mmc.exe）。メニューバーから、**[ファイル] > [スナップインの追加と削除]**の順に選択します。**グループポリシー管理エディター**を追加します。

グループポリシーオブジェクトを入力するための画面が開いたら、**[参照]**を選択してから**[既定のドメインポリシー]**を選択します。 または、任意のツールを使用して、環境に応じたポリシーオブジェクトを作成して選択することもできます。 このポリシーは、影響を受けるCitrixソフトウェア（VDA、StoreFrontサーバー、管理ツール）を実行しているすべてのマシンに適用する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

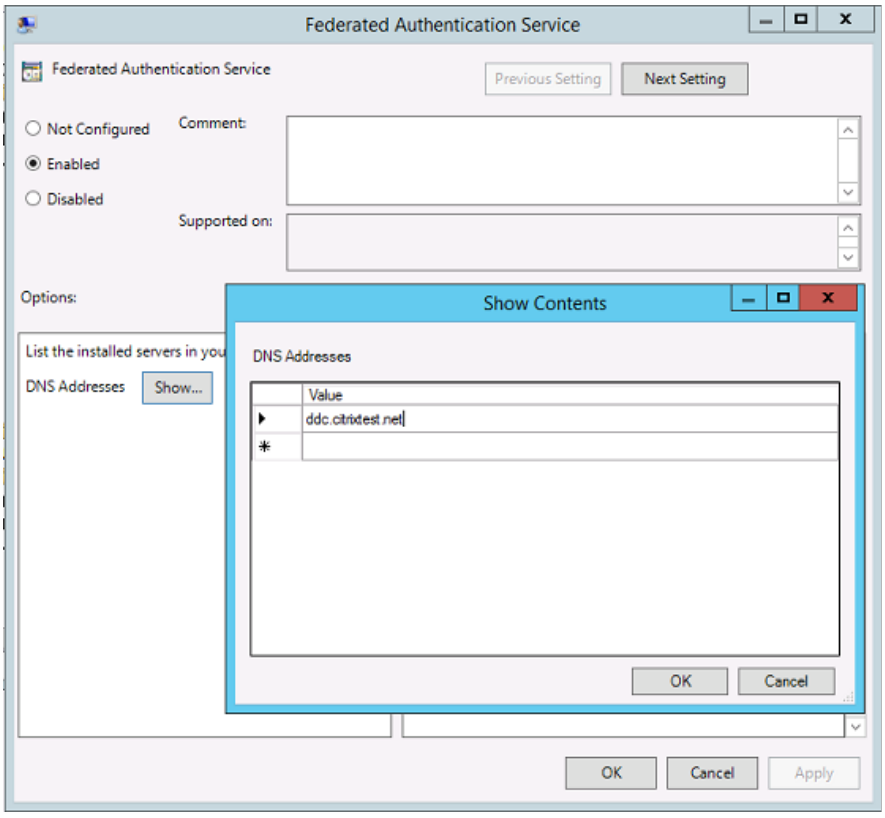


手順**4**：Computer Configuration/Policies/Administrative Templates/Citrix Components/Authenticationに配置されている Federated Authentication Serviceポリシーを参照します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順5：Federated Authentication Serviceポリシーを開き、**[有効]**を選択します。これにより、FASサーバーのDNSアドレスを構成する**[表示]**ボタンを選択できるようになります。



手順6：Federated Authentication Serviceをホストしているサーバーの DNSアドレスを入力します。

そのほかの注意事項：複数のアドレスを入力する場合は、StoreFrontサーバーとVDA間で一覧の順番が統一されている必要があります。 これには、空白や使用されないエントリも含まれます。

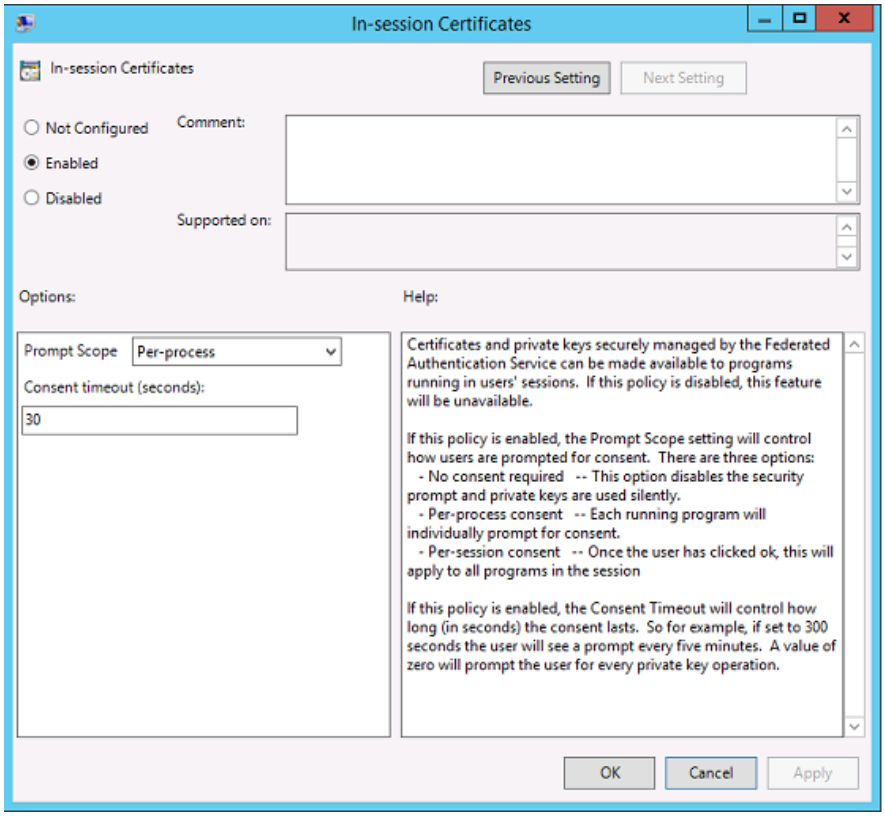
手順7：[OK]をクリックしてグループポリシーウィザードを終了し、グループポリシーの変更を適用します。 変更を反映

© 1999-2017 Citrix Systems, Inc. All rights reserved.

させるには、マシンを再起動（またはコマンドラインから**gpupdate /force**を実行）する必要がある場合があります。

セッション中の証明書サポートの有効化

グループポリシーテンプレートには、セッション中の証明書についてのシステムの構成のサポートが含まれます。これにより、ログオン後に、アプリケーションが使用できるようにユーザーの個人証明書ストアに証明書が配置されます。たとえば、VDAセッション内でWebサーバーへのTLS認証が必要な場合、証明書はInternet Explolerによって使用されます。デフォルトで、VDAはログオン後の証明書へのアクセスを許可しません。

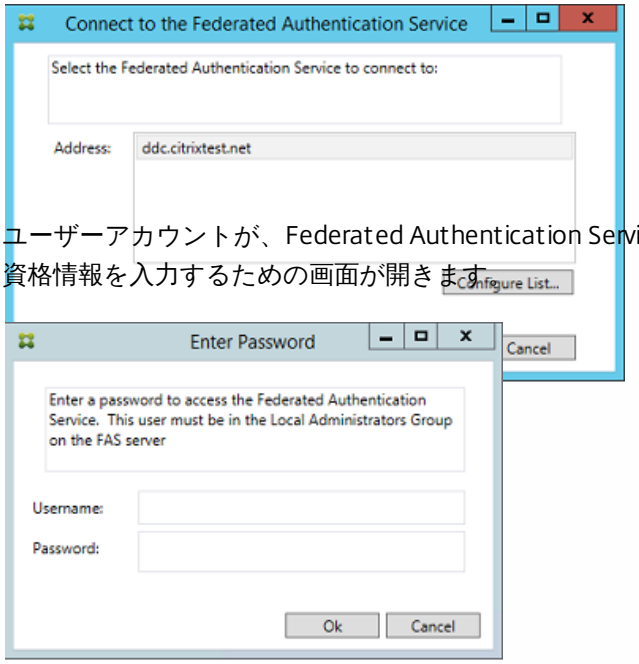


Federated Authentication Service管理コンソールの使用

Federated Authentication Service管理コンソールは、Federated Authentication Serviceの一部としてインストールされます。［スタート］メニューにアイコン（Citrix Federated Authentication Service）が配置されます。

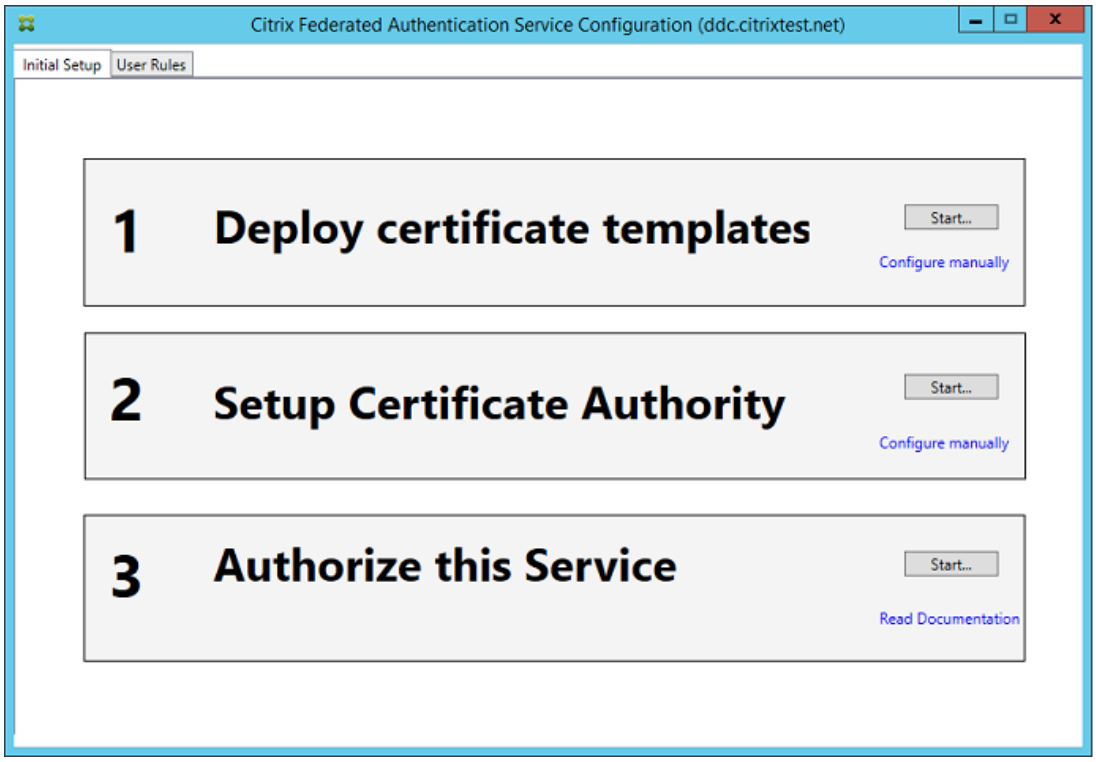
この管理コンソールは、グループポリシー構成を使用して、環境内のFASサーバーを自動的に検出します。 この検出に失敗した場合は、「グループポリシーの構成」セクションを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ユーザーアカウントが、Federated Authentication Serviceを実行しているマシンの管理者グループのメンバーでない場合は、資格情報を入力するための画面が開きます。

管理コンソールの初回使用時は、証明書テンプレートの展開、証明機関のセットアップ、およびFederated Authentication Serviceへの証明機関の使用権限の付与を行う3段階の手順が表示されます。 一部の手順は、OS構成ツールを使用して手動で完了することもできます。



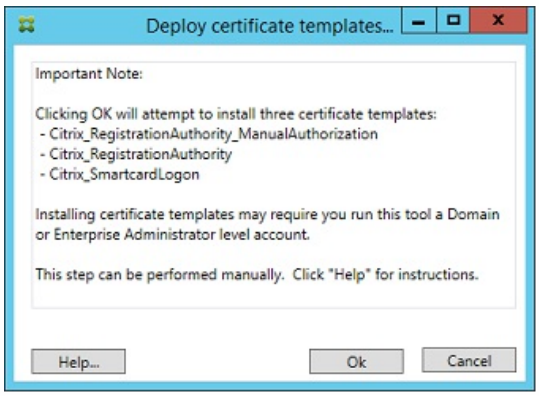
© 1999-2017 Citrix Systems, Inc. All rights reserved.

証明書テンプレートの展開

他のソフトウェアとの相互運用性の問題を避けるため、Federated Authentication Serviceでは、独自の目的で使用する3つのCitrix証明書テンプレートが用意されています。

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

これらのテンプレートは、Active Directoryで登録する必要があります。 コンソールでこれらのテンプレートが見つからない場合は、**証明書テンプレートの展開**ツールでインストールできます。 このツールは、Enterpriseフォレストの管理権限があるアカウントとして実行する必要があります。



テンプレートの構成は、以下のフォルダーにFederated Authentication Serviceと一緒にインストールされた、拡張子「.certificatetemplate」のXMLファイル内にあります。

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

これらのテンプレートファイルをインストールする権限がない場合は、テンプレートファイルをActive Directory管理者に渡してください。

以下のPowerShellコマンドを使用すると、テンプレートを手動でインストールできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-command

コピー

```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

$CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)

$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)


$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

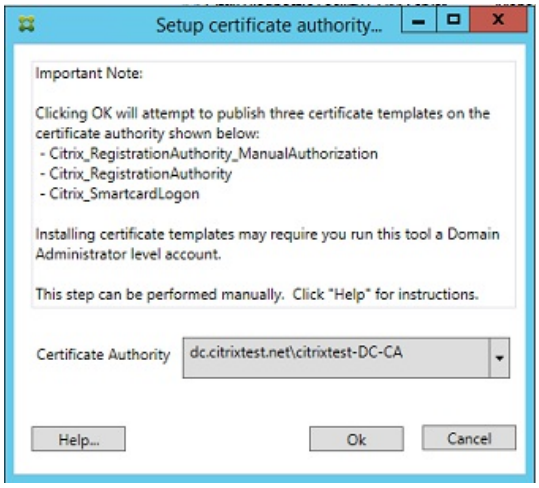
$writabletemplate.Commit(1, $NULL)
```

Active Directory証明書サービスのセットアップ

Citrix証明書テンプレートのインストール後は、これらのテンプレートを1つまたは複数のMicrosoft証明機関サーバーで公開する必要があります。Active Directory証明書サービスの展開方法について詳しくは、Microsoft社のドキュメントを参照してください。

どのサーバーでもテンプレートが公開されていない場合は、**証明書機関のセットアップ**ツールによって公開できます。このツールは、証明機関の管理権限のあるユーザーとして実行する必要があります。

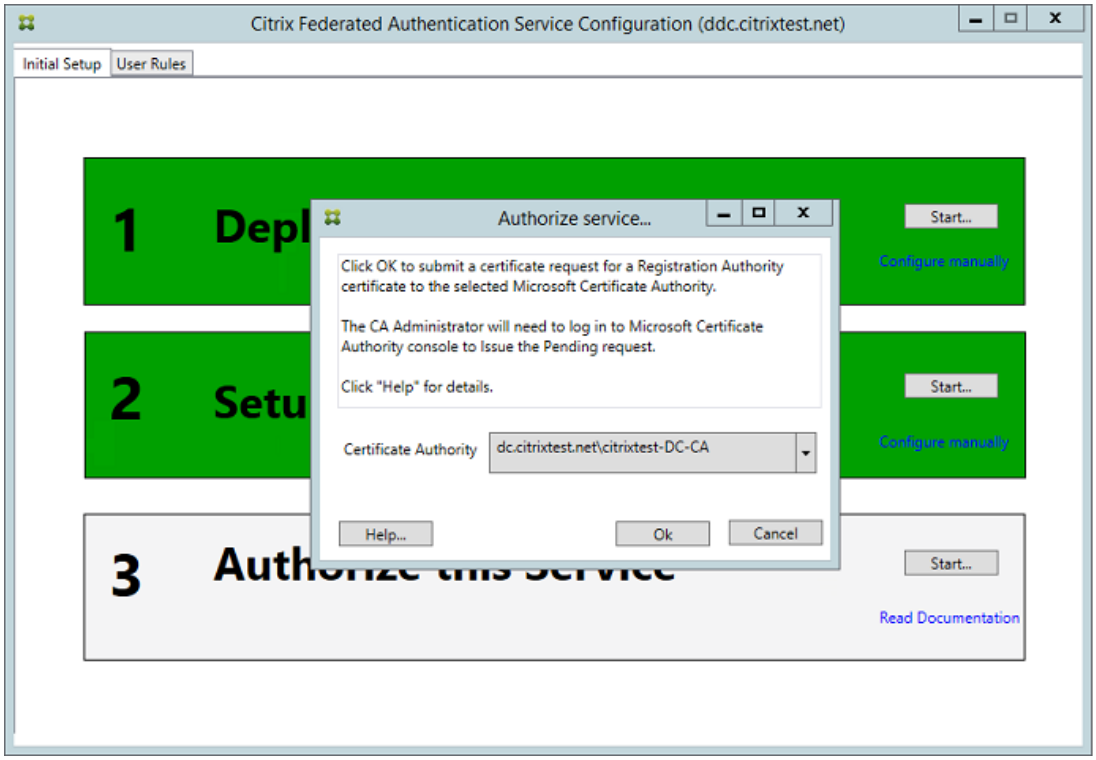
（証明書テンプレートは、Microsoft証明機関コンソールを使用して公開することもできます。）



© 1999-2017 Citrix Systems, Inc. All rights reserved.

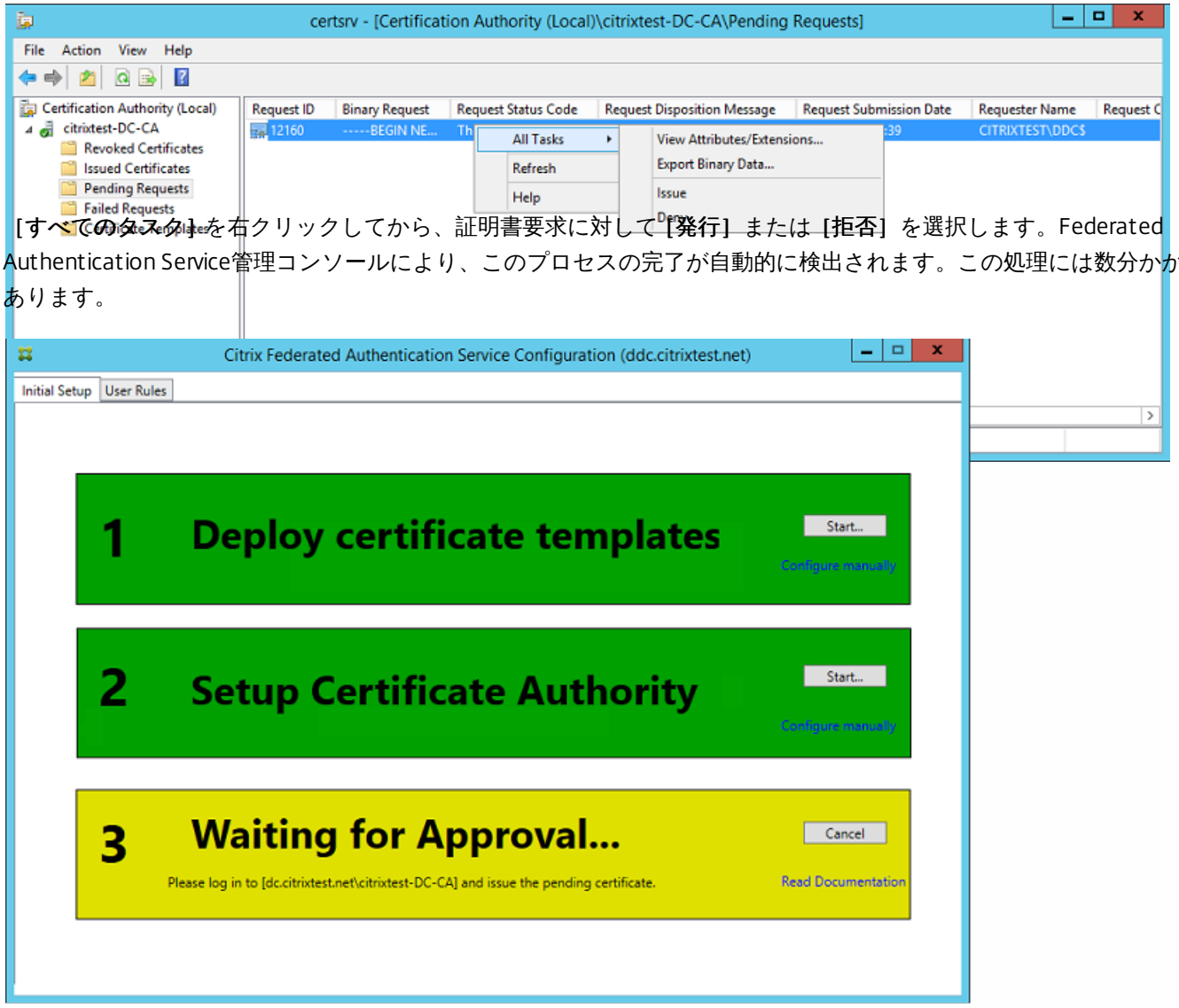
Federated Authentication Serviceへの権限付与

コンソールでの最終セットアップ手順では、Federated Authentication Serviceへの権限付与が開始されます。 管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorizationテンプレートを使用して証明書の要求生成し、この要求をテンプレートを公開する証明機関のいずれかに送信します。



要求は、送信後、Microsoft証明機関コンソールの **[保留中の要求]** リストに表示されます。Federated Authentication Serviceの構成を続行するには、証明機関の管理者が要求の **[発行]** または **[拒否]** を選択する必要があります。承認要求は、FASマシンアカウントからの **[保留中の要求]** として表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



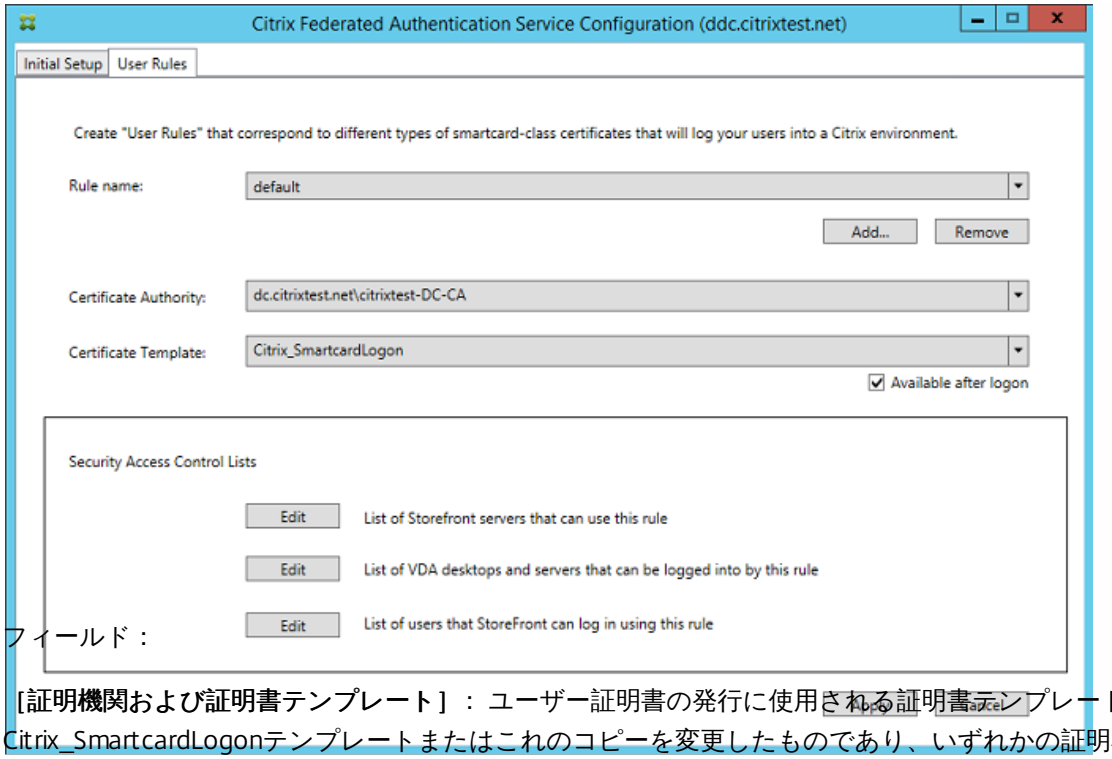
[すべてのタスク]を右クリックしてから、証明書要求に対して［発行］または［拒否］を選択します。Federated Authentication Service管理コンソールにより、このプロセスの完了が自動的に検出されます。この処理には数分かかることがあります。

ユーザールールの構成

ユーザールールにより、StoreFrontの指示に従って、VDAログオンおよびセッション中の使用に関する証明書発行の権限が付与されます。各ルールでは、証明書の要求を信頼するStoreFrontサーバー、証明書を要求できる一連のユーザー、および証明書の使用を許可する一連のVDAマシンを指定します。

Federated Authentication Serviceのセットアップを完了するには、管理者がFAS管理コンソールの［ユーザールール］タブに切り替え、Citrix_SmartcardLogonテンプレートの公開先となる証明機関を選択し、StoreFrontサーバーの一覧を編集して、デフォルトのルールを定義する必要があります。デフォルトでは、VDAの一覧には各ドメインコンピューターが含まれ、ユーザーの一覧には各ドメインユーザーが含まれます。デフォルトが適切でない場合は、これらを変更できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



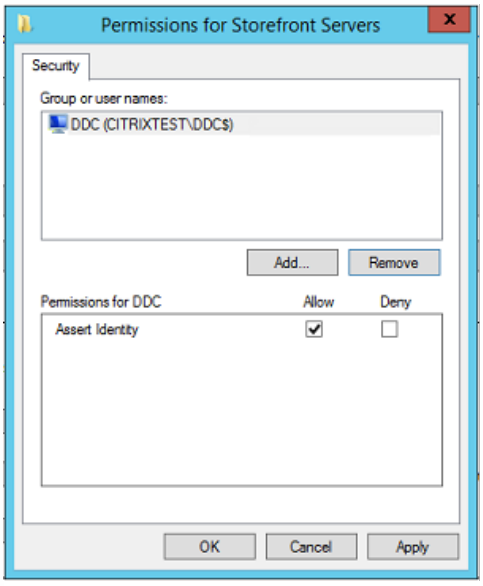
フィールド：

[証明機関および証明書テンプレート]：ユーザー証明書の発行に使用される証明書テンプレートおよび証明機関。これは、Citrix_SmartcardLogonテンプレートまたはこれのコピーを変更したものであり、いずれかの証明機関にはこのテンプレートが公開されている必要があります。

FASでは、フェールオーバーおよび負荷分散のために、PowerShellを使用して複数の証明機関の追加することができます。同様に、コマンドラインと構成ファイルを使用して、より詳細な証明書生成オプションを構成できます。詳しくは、「PowerShell」セクションおよび「ハードウェアセキュリティモジュール」セクションを参照してください。

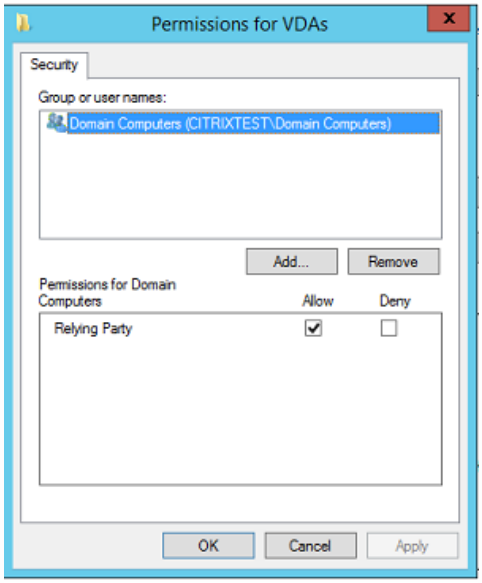
[セッション中の証明書]：**[ログオン後に使用可能]**チェックボックスで、証明書をセッション中の証明書としても使用可能かどうかを制御します。このチェックボックスがオフの場合、証明書はログオンまたは再接続にのみ使用され、ユーザーは認証後、証明書にアクセスできなくなります。

[このルールを使用できるStoreFrontサーバーの一覧]：ユーザーのログオンまたは再接続用に証明書を要求する権限が付与された、信頼済みStoreFrontサーバーの一覧。この設定はセキュリティ上非常に重要であり、慎重に管理する必要があります。

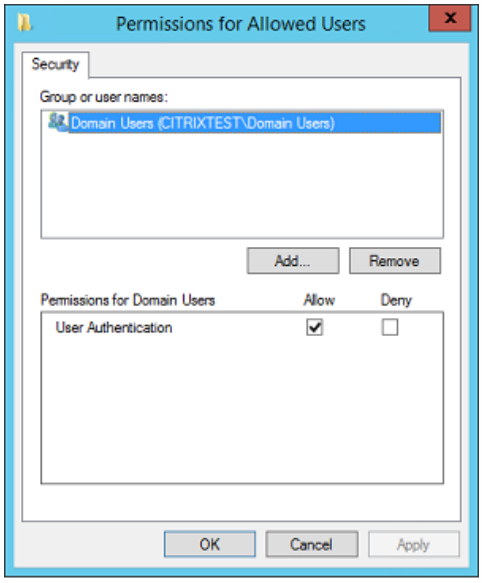


© 1999-2017 Citrix Systems, Inc. All rights reserved.

[このルールによってログインできるVDAデスクトップおよびサーバーの一覧] :Federated Authentication Serviceシステムを使用してユーザーをログオンさせることができるVDAマシンの一覧。



[このルールを使用してStoreFrontがログインさせることのできるユーザーの一覧] :Federated Authentication Serviceを通じて証明書の発行を受けられるユーザーの一覧。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

高度な使用方法

追加のルールを作成して、各種プロパティや権限が含まれるように構成されたさまざまな証明書テンプレートおよび証明機関を参照することができます。これらのルールは、名前別に新しいルールを要求するように構成する必要がある、各StoreFrontサーバーでの使用に合わせて構成できます。デフォルトでは、StoreFrontはFederated Authentication Serviceにアクセスするときに**デフォルト**を要求します。これは、グループポリシー構成オプションを使って変更できます。

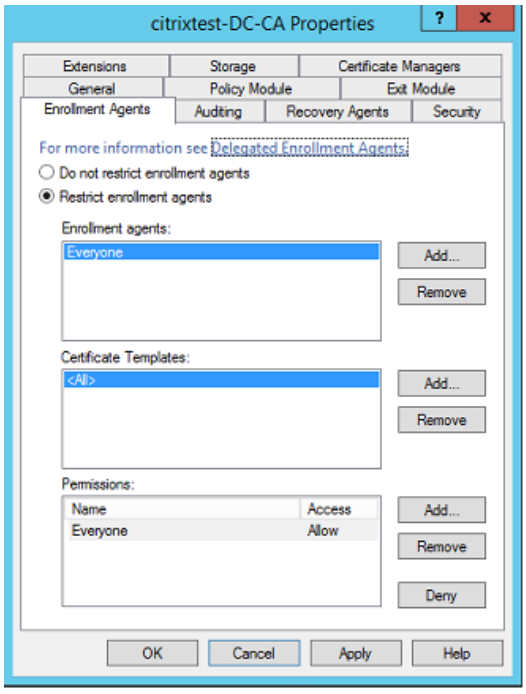
新しい証明書テンプレートを作成するには、Microsoft証明機関コンソールでCitrix_SmartcardLogonテンプレートを複製して名前を（Citrix_SmartcardLogon2などに）変更し、必要に応じて変更を加えます。 **[追加]** をクリックして新しい証明書テンプレートを参照し、新しいユーザールールを作成します。

セキュリティに関する注意事項

Federated Authentication Serviceには、Federated Authentication Serviceがドメインユーザーの代わりに自律的に証明書を発行できるようにする、登録機関の証明書があります。このため、セキュリティポリシーを作成および実装してFASサーバーを保護し、権限を制限することは重要です。

委任された登録エージェント

Microsoft証明機関では、FASサーバーが使用可能なテンプレートの管理、およびFASサーバーが証明書を発行可能な対象ユーザーの制限を行うことができます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Serviceが必要なユーザーにのみ証明書を発行できるように、これらのオプションを構成することを強くお勧めします。 たとえば、管理グループまたは保護されたユーザーのグループに属するユーザーにFederated Authentication Serviceが証明書を発行できないようにすることをお勧めします。

アクセス制御リストの構成

「ユーザーロールの構成」セクションで説明しているように、証明書が発行された場合のFederated Authentication Serviceに対するユーザーIDの承認を信頼するStoreFrontサーバーの一覧を構成する必要があります。 同様に、証明書の発行対象となるユーザー、およびユーザーが認証可能なVDAマシンを制限することができます。 この操作は、標準で構成を行うActive Directoryまたは証明機関のセキュリティ機能に追加で行います。

ファイアウォールの設定

FASサーバーへのすべての通信では、相互認証されたWindows Communication Foundation（WCF）Kerberosネットワーク接続がポート80で使用されます。

イベントログの監視

Federated Authentication ServiceおよびVDAは、Windowsイベントログに情報を書き込みます。 これは、情報の監視および監査に使用できます。 「イベントログ」セクションに、生成される可能性のあるイベントログの一覧を示します。

ハードウェアセキュリティモジュール

Federated Authentication Serviceによって発行されたユーザー証明書の秘密キーを含むすべての秘密キーは、Network Serviceアカウントによってエクスポート不可の秘密キーとして保存されます。 Federated Authentication Serviceは、セキュリティポリシーで暗号化ハードウェアセキュリティモジュールが必要とされる場合、このモジュールの使用をサポートします。

FederatedAuthenticationService.exe.configファイルでは、低レベルの暗号化構成が使用可能です。これらの設定は、秘密キーが最初に作成されたときに適用されます。 そのため、登録機関の秘密キー（4096ビット、TPM保護など）およびランタイムのユーザー証明書には異なる設定が使用されることがあります。

パラメーター	説明
ProviderLegacyCsp	trueに設定した場合、FASではMicrosoft CryptoAPI（CAPI）が使用されます。 falseに設定した場合、FASではMicrosoft Cryptography Next Generation（CNG）APIが使用されます。
ProviderName	使用するCAPIまたはCNGプロバイダーの名前。
ProviderType	Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24を参照します。CAPIでHSMを使用する場合、およびHSMベンダーで別のタイプを指定さ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	れている場合以外は、常に24である必要があります。
KeyProtection	秘密キーの「エクスポート可能」フラグを制御します。 さらに、ハードウェアでサポートされている場合は、トラステッドプラットフォームモジュール（TPM）のキーストレージの使用も許可されます。
KeyLength	RSA秘密キーのキー長。 サポートされる値は1024、2048、および4096です（デフォルトは 2048です）。

PowerShell SDK

シンプルな展開にはFederated Authentication Service管理コンソールが適していますが、PowerShellインターフェイスにはより詳細なオプションもあります。 コンソールでは使用できないオプションを使用する場合は、PowerShellのみを使用して構成を行うことをお勧めします。

次のコマンドによってPowerShellコマンドレットが追加されます。

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Get-Help <*cmdlet name*>を使用すると、コマンドレットのヘルプが表示されます。 次の表にいくつかのコマンドの一覧を示します。「*」は標準のPowerShellの動詞を表します（New、Get、Set、Removeなど）。

コマンド	概要
*-FasServer	現在の環境のFASサーバーを一覧表示および再構成します。
*-FasAuthorizationCertificate	登録機関証明書を管理します。
*-FasCertificateDefinition	FASが証明書の生成に使用するパラメーターを制御します。
*-FasRule	Federated Authentication Serviceで構成済みのユーザールールを管理します。
*-FasUserCertificate	Federated Authentication Serviceによってキャッシュされた証明書を一覧表示および管理します。

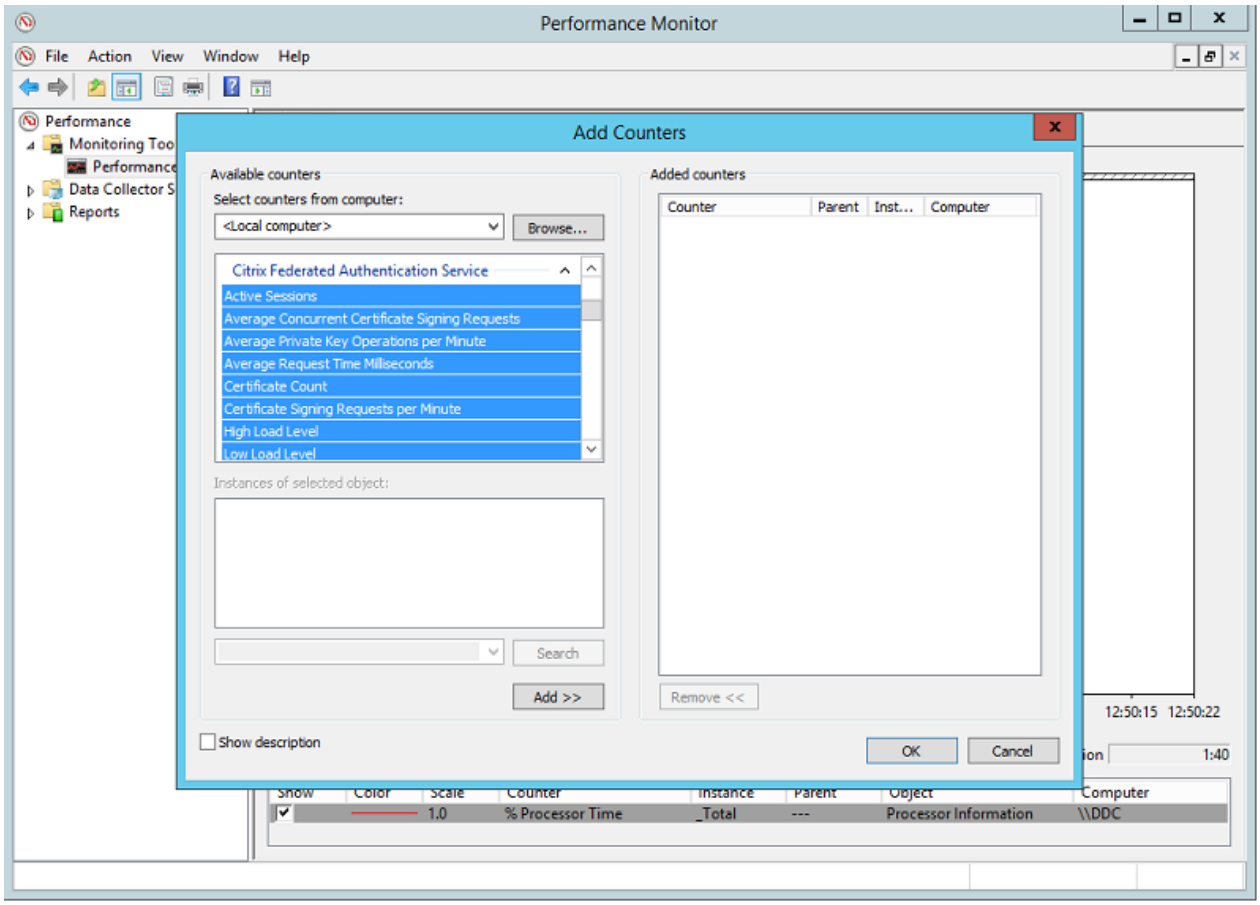
PowerShellコマンドレットは、FASサーバーのアドレスを指定することによってリモートで使用できます。

FAS PowerShellコマンドレットのすべてのヘルプファイルを含むzipファイルをダウンロードすることもできます。PowerShell SDKの記事を参照してください。

パフォーマンスカウンター

Federated Authentication Serviceには、負荷の追跡用の一連のパフォーマンスカウンターが含まれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



次の表は、使用可能なカウンターの一覧です。ほとんどのカウンターは、5分間の移動平均値です、

でのデータソース名	説明
アクティブなセッション	Federated Authentication Serviceによって追跡される接続の数。
同時実行CSR数	同時に処理される証明書要求の数。
秘密キーの処理数	1分あたりに実行される秘密キー処理の数。
要求時間	証明書の生成および署名にかかる時間の長さ。
証明書の数	Federated Authentication Serviceでキャッシュされた証明書の数。
1分あたりのCSR	1分あたりに処理されるCSRの数。
低/中/高	「1分あたりのCSR」の観点からFederated Authentication Serviceが許容できる負荷の推定値。「高負荷」しきい値を超過すると、セッションの起動に失敗することがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

イベントログ

次の表は、Federated Authentication Serviceで生成されるイベントログエントリの一覧です。

管理イベント

［イベントソース：Citrix.Authentication.FederatedAuthenticationService］

これらのイベントは、Federated Authentication Serviceサーバーでの構成変更に応じて記録されます。

ログコード
［S001］アクセス拒否：ユーザー［{0}］は管理者グループのメンバーではありません
［S002］アクセス拒否：ユーザー［{0}］はロール［{1}］の管理者ではありません
［S003］管理者［{0}］は保守モードを［{1}］に設定しています
［S004］管理者［{0}］はCA［{1}］テンプレート［{2} および {3}］で登録しています
［S005］管理者［{0}］はCA［{1}］の権限を取り消しています
［S006］管理者［{0}］は新しい証明書定義［{1}］を作成しています
［S007］管理者［{0}］は証明書定義［{1}］を更新しています
［S008］管理者［{0}］は証明書定義［{1}］を削除しています
［S009］管理者［{0}］は新しいロール［{1}］を作成しています
［S010］管理者［{0}］はロール［{1}］を更新しています
［S011］管理者［{0}］はロール［{1}］を削除しています
［S012］管理者［{0}］は証明書を作成しています［UPN：{0} SID：{1} ロール：{2}］［証明書定義：{3}］
［S013］管理者［{0}］は証明書を削除しています［UPN：{0}ロール：{1} 証明書定義：{2}］

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログコード
［S401］構成アップグレードを実行中です -- ［開始バージョン{0}］ ［終了バージョン{1}］
［S402］エラー：Citrix Federated Authentication ServiceはNetwork Serviceとして実行する必要があります ［現在は{0}として実行中］

IDアサーションの作成［Federated Authentication Service］

これらのイベントは、信頼済みのサーバーがユーザーログオンをアサートすると、ランタイム時にFederated Authentication Serviceサーバーに記録されます。

ログコード
［S101］サーバー ［{0}］にはロール ［{1}］のIDをアサートする権限がありません
［S102］サーバー ［{0}］はUPN ［{1}］のアサートに失敗しました（例外：{2}{3}）
［S103］サーバー ［{0}］はUPN ［{1}］、SID {2}を要求しましたが、検索でSID {3}が返されました
［S104］サーバー ［{0}］はUPN ［{1}］のアサートに失敗しました（UPNはロール ［{2}］によって許可されていません）
［S105］サーバー ［{0}］はIDのアサーションを発行しました ［UPN：{0}、ロール：{1}、セキュリティコンテキスト：［{2}］
［S120］ ［UPN：{0}、ロール：{1}、セキュリティコンテキスト： ［{2}］ ］に対して証明書を発行しています
［S121］ ［UPN：{0}、ロール：{1}］に対してアカウント{2}の代わりに証明書を発行しています
［S122］警告：サーバー過負荷です ［UPN：{0}、ロール：{1}］ ［1分あたりの要求{2}］。

証明書利用者としての機能［Federated Authentication Service］

これらのイベントは、VDAにユーザーがログオンすると、ランタイム時にFederated Authentication Serviceサーバーに記録されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログコード
[S201] 証明書利用者 [{0}] にはパスワードへのアクセス権がありません。
[S202] 証明書利用者 [{0}] には証明書へのアクセス権がありません。
[S203] 証明書利用者 [{0}] にはログオンCSPへのアクセス権がありません
[S204] 証明書利用者 [{0}] がログオンCSPにアクセスしています [操作 : {1}]
[S205] 呼び出しアカウント [{0}] はロール [{1}] の証明書利用者ではありません
[S206] 呼び出しアカウント [{0}] は証明書利用者ではありません
[S207] 証明書利用者 [{0}] はロール : [{2}] のIDをアサートしています [UPN : {1}]
[S208] 秘密キーの処理が失敗しました [操作 : {0}] [UPN : {1}、ロール : {2}、証明書定義{3}] [エラー {4} {5}]

セッション内証明書サーバー [Federated Authentication Service]

これらのイベントは、ユーザーはセッション内証明書を使用すると、Federated Authentication Serviceサーバーで記録されます。

ログコード
[S301] アクセス拒否 : ユーザー [{0}] には仮想スマートカードへのアクセス権がありません
[S302] ユーザー [{0}] は不明な仮想スマートカードを要求しました [拇印 : {1}]
[S303] ユーザー [{0}] が仮想スマートカードと一致しません [UPN : {1}]
[S304] コンピューター [{3}] でプログラム [{2}] を実行中のユーザー [{1}] は秘密キー処理 : [{6}] のために仮想スマートカードを使用しています [UPN : {4}、ロール : {5}]
[S305] 秘密キーの処理が失敗しました [操作 : {0}] [UPN : {1}、ロール : {2}、コンテナ名{3}] [エラー {4} {5}] 。

ログオン [VDA]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

［イベントソース：Citrix.Authentication.IdentityAssertion］

これらのイベントは、ログオン時にVDAで記録されます。

ログコード
［S101］IDアサーションログオンに失敗しました。 認識できないFederated Authentication Service［ID：{0}］
［S102］IDアサーションログオンに失敗しました。 {0}のSIDが見つかりませんでした［例外：{1}{2}］
［S103］IDアサーションログオンに失敗しました。 ユーザー{0}のSIDは{1}ですが、想定されたSIDは{2}です
［S104］IDアサーションログオンに失敗しました。 Federated Authentication Serviceへの接続に失敗しました：{0}［エラー：{1} {2}］
［S105］IDアサーションログオン。 ［ユーザー名：{0}］［ドメイン：{1}］にログインしています
［S106］IDアサーションログオン。 ［証明書：{0}］にログインしています。
［S107］IDアサーションログオンに失敗しました。 ［例外：{1} {2}］
［S108］IDアサーションサブシステム。 ACCESS_DENIED［呼び出し元：{0}］

セッション内証明書［VDA］

これらのイベントは、ユーザーがセッション内証明書を使用しようとすると、VDAに記録されます。

ログコード
［S201］仮想スマートカードが認証されました［ユーザー：{0}］［PID：{1}、名前：{2}］［証明書{3}］
［S202］仮想スマートカードサブシステム。セッション{0}で使用可能なスマートカードはありません
［S203］仮想スマートカードサブシステム。 アクセスが拒否されました［呼び出し元：{0}、セッション：{1}、予測：{2}］
［S204］仮想スマートカードサブシステム。 スマートカードのサポートが無効化されました。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

証明書要求および生成コード［Federated Authentication Service］

［イベントソース：Citrix.TrustFabric］

これらの低レベルイベントは、Federated Authentication Serviceサーバーがログレベルの暗号化操作を実行すると記録されます。

ログコード
［S0001］TrustArea::TrustArea：証明書チェーンがインストールされました
［S0002］TrustArea::Join：信頼されていない証明書がコールバックによって認証されました
［S0003］TrustArea::Join：信頼済みサーバーに参加しています
［S0004］TrustArea::Maintain：証明書が更新されました
［S0005］TrustArea::Maintain：新しい証明書チェーンが取得されました
［S0006］TrustArea::Export：秘密キーをエクスポートしています
［S0007］TrustArea::Import：信頼領域をインポートしています
［S0008］TrustArea::Leave：信頼領域を終了しています
［S0009］TrustArea::SecurityDescriptor：セキュリティ記述子を設定しています
［S0010］CertificateVerification：新しい信頼済みの証明書をインストールしています
［S0011］CertificateVerification：期限の切れた信頼済みの証明書をアンインストールしています
［S0012］TrustFabricHttpClient：{0}へのシングルサインオンを試行しています
［S0013］TrustFabricHttpClient：{0}に対して指定ユーザー資格情報が入力されました
［S0014］Pkcs10Request::Create：PKCS10要求が作成されました
［S0015］Pkcs10Request::Renew：PKCS10要求が作成されました
［S0016］PrivateKey::Create

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S0017] PrivateKey::Delete
[S0018] TrustArea::TrustArea：承認待ち
[S0019] TrustArea::Join：参加遅延
[S0020] TrustArea::Join: 参加遅延
[S0021] TrustArea::Maintain：証明書チェーンがインストールされました

ログコード
[S0101] TrustAreaServer::ルート証明書が作成されました
[S0102] TrustAreaServer::Subordinate：参加に成功しました
[S0103] TrustAreaServer::PeerJoin：参加に成功しました
[S0104] MicrosoftCertificateAuthority::GetCredentials：{0}の使用権限が付与されました
[S0104] MicrosoftCertificateAuthority::SubmitCertificateRequest エラー{0}
[S0105] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書{0}が発行されました
[S0106] MicrosoftCertificateAuthority::PublishCRL：CRLが公開されました
[S0107] MicrosoftCertificateAuthority::ReissueCertificate エラー{0}
[S0108] MicrosoftCertificateAuthority::ReissueCertificate 証明書{0}が発行されました
[S0109] MicrosoftCertificateAuthority::CompleteCertificateRequest - 承認待機継続中
[S0110] MicrosoftCertificateAuthority::CompleteCertificateRequest - 保留中の証明書が拒否されました
[S0111] MicrosoftCertificateAuthority::CompleteCertificateRequest 証明書が発行されました

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S0112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待機中
[S0120] NativeCertificateAuthority::SubmitCertificateRequest 証明書{0}が発行されました
[S0121] NativeCertificateAuthority::SubmitCertificateRequest エラー
[S0122] NativeCertificateAuthority::RootCARollover 新規ルート証明書
[S0123] NativeCertificateAuthority::ReissueCertificate 新規証明書
[S0124] NativeCertificateAuthority::RevokeCertificate
[S0125] NativeCertificateAuthority::PublishCRL

関連情報

- 一般的なFAS環境については、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」では「方法」記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Serviceのアーキテクチャの概要

Dec 05, 2017

はじめに

Federated Authentication Service（FAS）はActive Directory証明機関（CA）と統合して、Citrix環境内でのシームレスなユーザー認証を実現するCitrixコンポーネントです。 このドキュメントでは、環境に適した、さまざまな認証アーキテクチャについて説明します。

FASが有効化されると、信頼されたStoreFrontサーバーにユーザー認証の判断が委任されます。 StoreFrontは最新のWebテクノロジを中心に構築されたビルトイン認証オプションの包括的なセットを搭載しており、StoreFront SDKやサードパーティのIISプラグインを使用して容易に拡張できます。 基本的な設計目標は、Webサイトへのユーザー認証が可能なすべての認証テクノロジを、Citrix XenAppまたはXenDesktopの展開へのログインに活用することです。

このドキュメントでは、複雑さを増す上位レベルの展開アーキテクチャについて、例をいくつか説明します。

- 内部展開
- NetScaler Gatewayの展開
- ADFS SAML
- B2Bアカウントのマッピング
- Windows 10 Azure ADへの参加

FAS関連記事にリンクしています。すべてのアーキテクチャにおけるFASのセットアップについては「Federated Authentication Service」を参照してください。

仕組み

FASには、StoreFrontの認証したActive Directoryユーザーの代わりに、スマートカードクラスの証明書を自動的に発行する権限が付与されます。 これは、管理者が物理スマートカードをプロビジョニングできるツールと同様のAPIを使用します。

ユーザーがCitrix XenAppまたはXenDesktopのVirtual Delivery Agent（VDA）に仲介されると、マシンに証明書がアタッチされ、Windowsドメインはログオンを標準のスマートカード認証と見なします。

内部展開

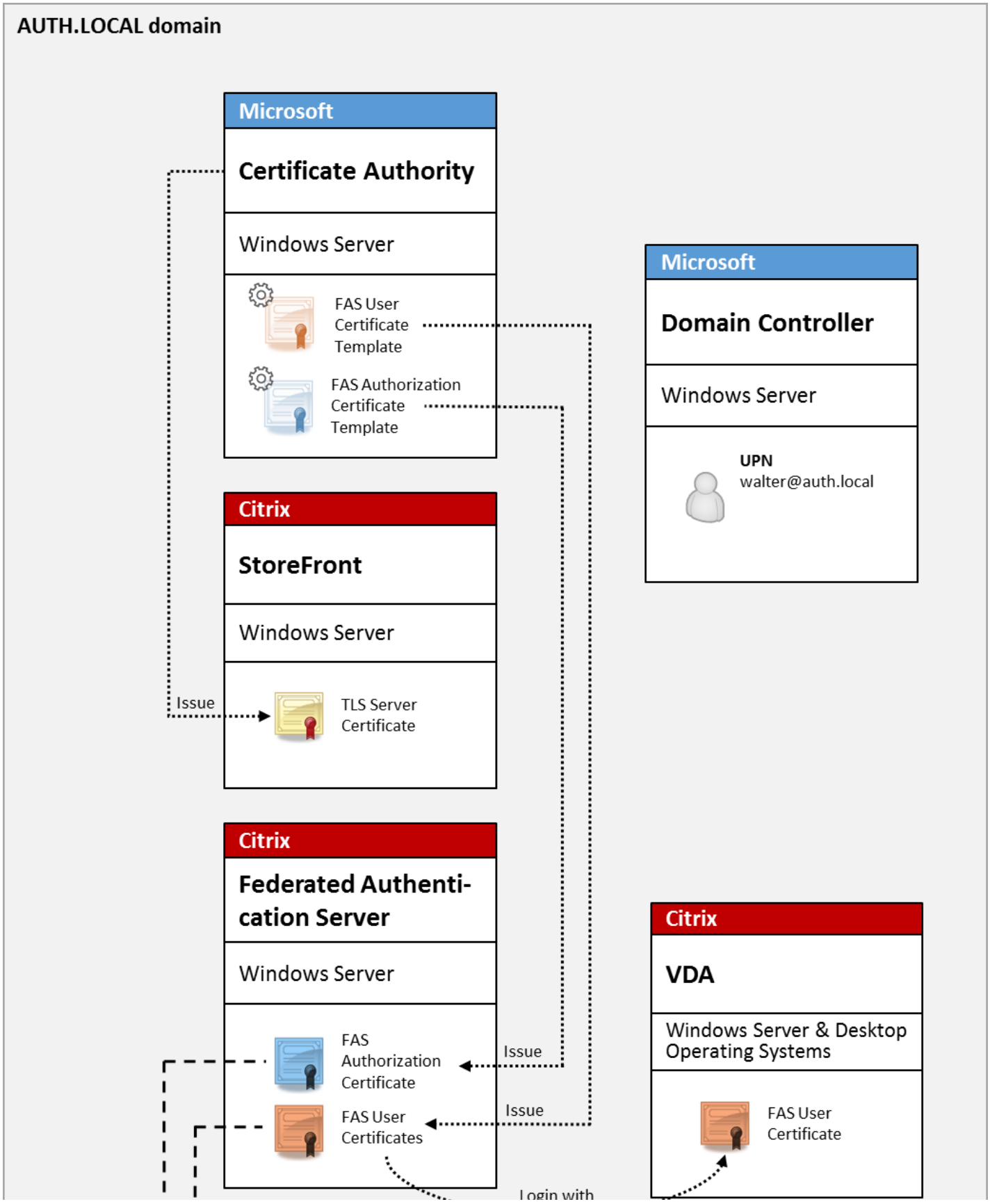
FASでは、さまざまな認証オプション（Kerberos シングルサインオンを含む）を使用したStoreFrontへの安全なユーザー認証、および十分に認証されたCitrix HDXセッションへの接続が可能です。

これにより、Windows認証にユーザーの資格情報やスマートカードのPINの入力が求められることはありません。また、シングルサインオンサービスのような「保存されたパスワードの管理」機能を使用する必要もありません。 これを使用して、XenAppの旧バージョンで利用可能なKerberos制約付き委任のログオン機能を置き換えることができます。

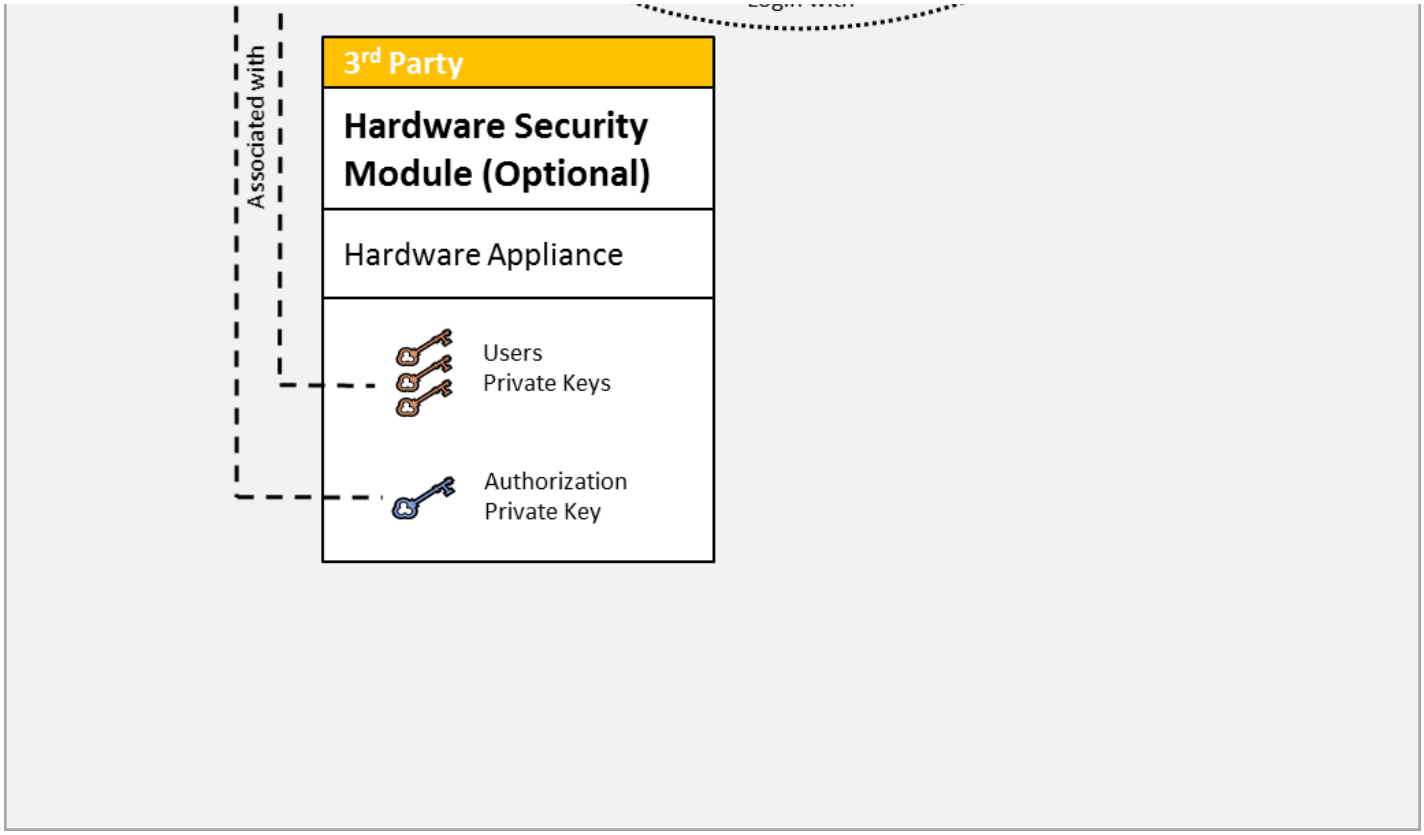
エンドポイントデバイスへのログオンにスマートカードを使用したかどうかにかかわらず、セッション内ではすべてのユーザーが、公開キー基盤（PKI）の証明書にアクセスできます。このため、スマートフォンやタブレットのように、スマートカードリーダーを搭載していないデバイスからも、2要素認証モデルへの円滑な移行が可能です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この展開では、FASを実行する新しいサーバーが追加されますが、このサーバーにはユーザーの代わりにスマートカードクラスの証明書を発行する権限が付与されます。これらの証明書は、スマートカードによるログオンの代わりとして、Citrix HDX環境でのユーザーセッションへのログオンに使用されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



XenAppまたはXenDesktop環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加するMicrosoft証明機関（CA）を利用可能にし、ドメインコントローラーにドメインコントローラー証明書を割り当てるだけで済みます。 （CTX206156の「Issuing Domain Controller Certificates」セクションを参照してください。）

関連情報

- キーは、ハードウェアセキュリティモジュール（HSM）やビルトインのトラステッドプラットフォームモジュール（TPM）に保存できます。 詳しくは、「Federated Authentication Serviceの秘密キー保護」を参照してください。
- 「Federated Authentication Service」では、FASのインストールと構成の方法について説明します。

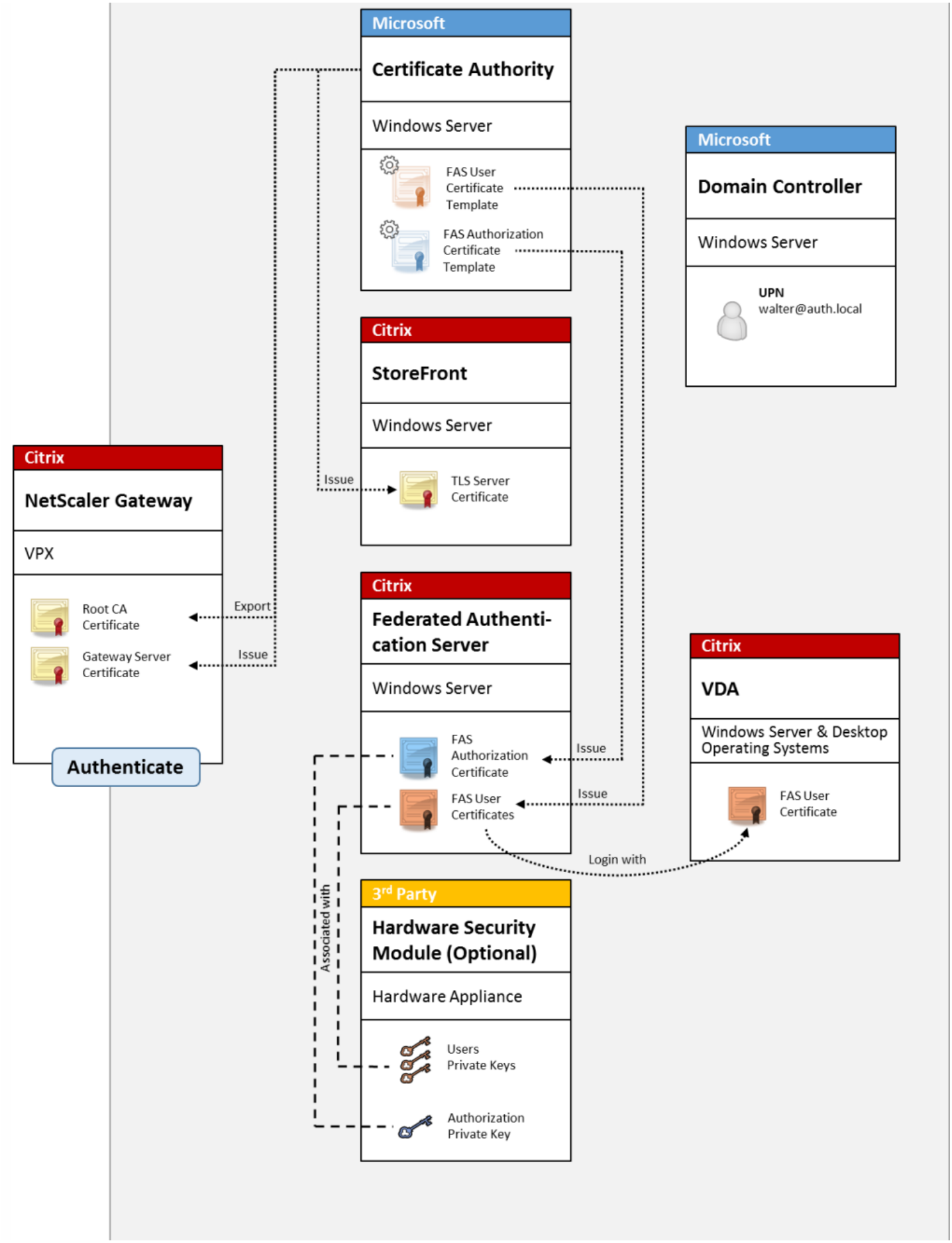
NetScaler Gatewayの展開

NetScalerの展開は内部展開と似ていますが、StoreFrontと組み合わせたCitrix NetScaler Gatewayが追加されており、認証のプライマリポイントがNetScalerそのものに移動されています。Citrix NetScalerには、企業Webサイトへのリモートアクセスの保護に使用できる、認証および承認の高度なオプションが含まれています。

この展開を利用すれば、NetScalerへの初回認証時およびユーザーセッションへのログイン時に、何度もPINの入力が求められることはありません。 また、ADパスワードやスマートカードを必要とせずに、高度なNetScaler認証テクノロジを利用することができます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

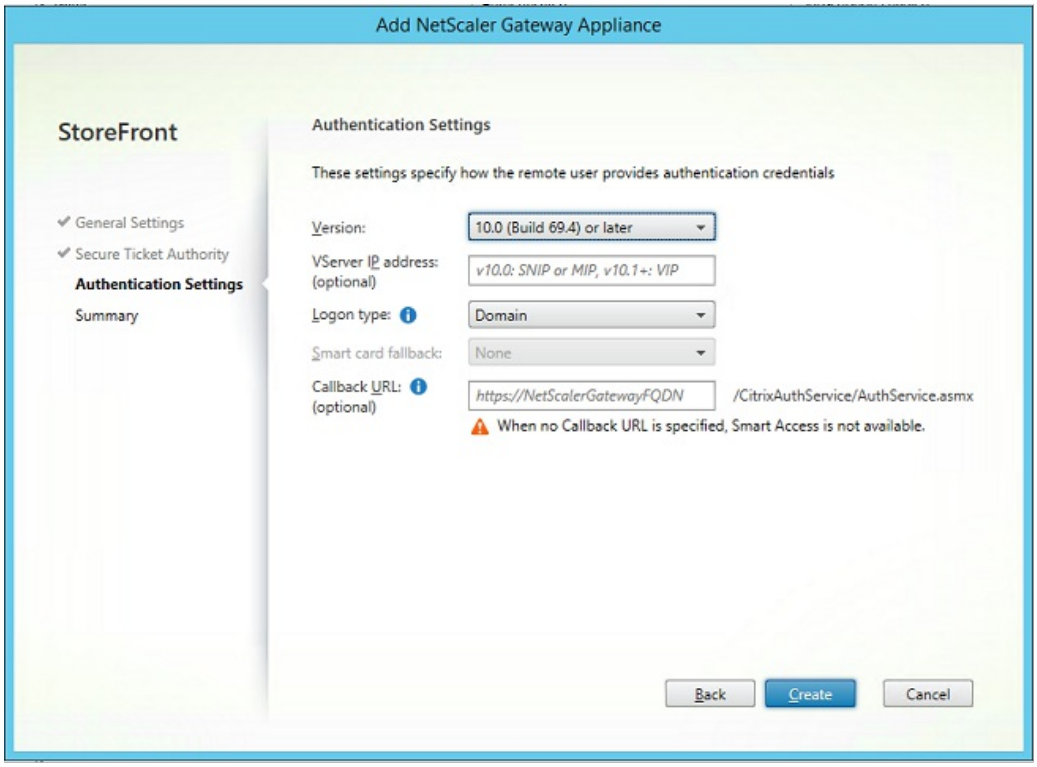


© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenAppまたはXenDesktop環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加するMicrosoft証明機関（CA）を利用可能にし、ドメインコントローラーにドメインコントローラー証明書を割り当てるだけで済みます。 （CTX206156の「Issuing Domain Controller Certificates」セクションを参照してください）。

NetScalerをプライマリ認証システムとして構成する場合は、NetScalerとStoreFront間のすべての接続をTLSで保護するようにします。特に、この展開ではNetScalerサーバーの認証にコールバックURLが使用されるため、コールバックURLがNetScalerサーバーを指すよう正しく構成する必要があります。



関連情報

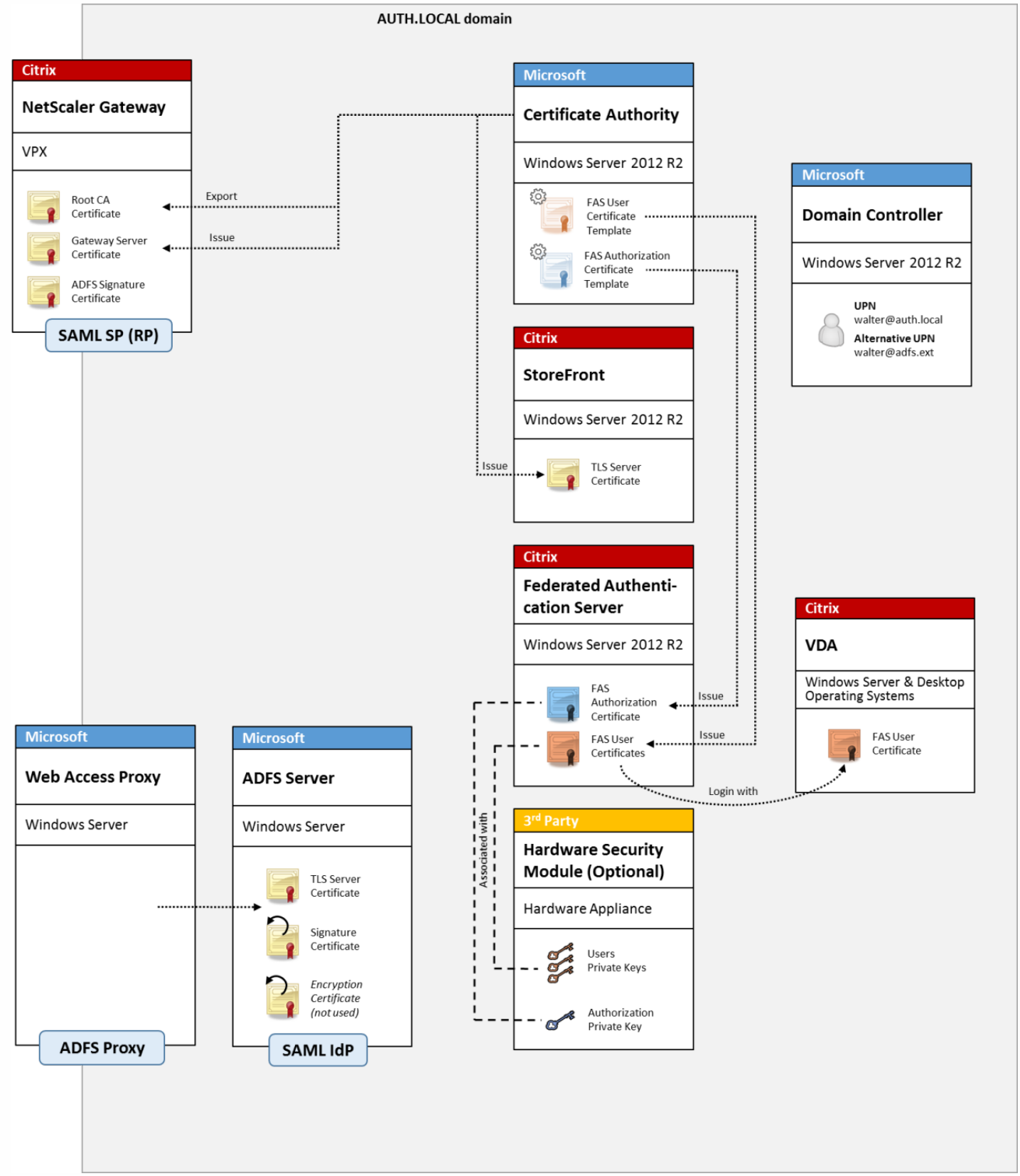
- NetScaler Gatewayを構成するには、「How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6」を参照してください。
- 「Federated Authentication Service」では、FASのインストールと構成の方法について説明します。

ADFS SAMLの展開

NetScalerの主要な認証テクノロジにより、SAML IDプロバイダー（IdP）として機能できる、Microsoft ADFSとの統合が実現します。 SAMLアサーションは暗号を使用して署名されたXMLブロックであり、コンピューターシステムへのユーザーのログオンを承認する、信頼されたIdPによって発行されます。 つまり、FASサーバーによって、Microsoft ADFSサーバー（または

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ほかのSAML対応IdP）へのユーザー認証の委任が許可されます。



ADFSは、一般的にインターネットを利用して企業リソースにリモートでユーザーを安全に認証するために使用され、たとえば、Office 365の統合に多く利用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

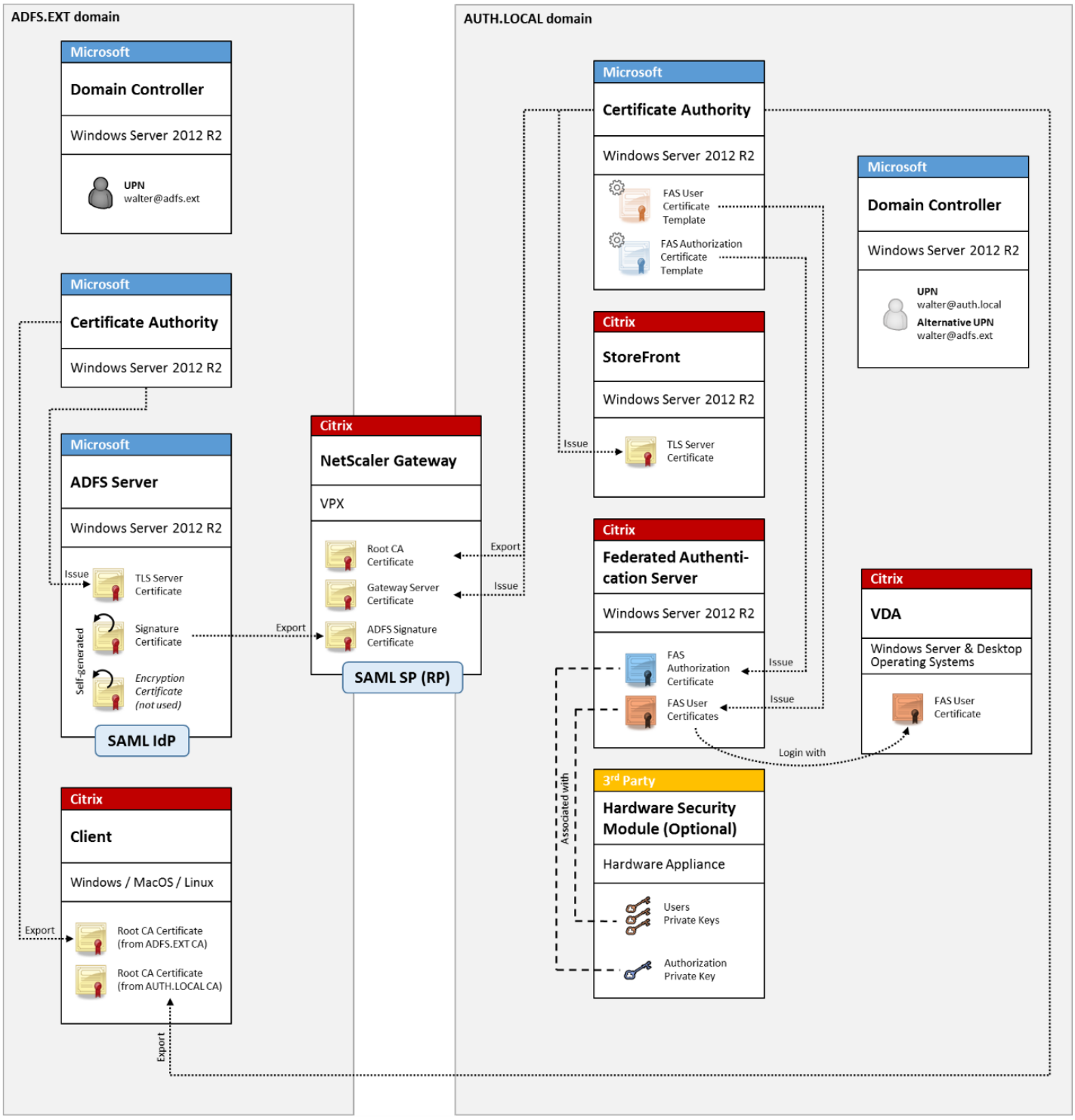
関連情報

- 詳しくは、「Federated Authentication ServiceのADFSの展開」を参照してください。
- 「Federated Authentication Service」では、FASのインストールと構成の方法について説明します。
- 構成に関する考慮事項については、この記事の「NetScaler Gatewayの展開」セクションを参照してください。

B2Bアカウントのマッピング

2つの会社が互いのコンピューターシステムを利用する場合、一般的なオプションはActive Directoryフェデレーションサービス（ADFS）サーバーを信頼関係でセットアップすることです。これにより、一方の会社のユーザーが、他方の会社のActive Directory（AD）環境にシームレスに認証されるようになります。 ログオン時に、各ユーザーは自社のログオン資格情報を使用します。ADFSはこれを相手の会社のAD環境の「シャドウアカウント」に自動的にマップします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



関連情報

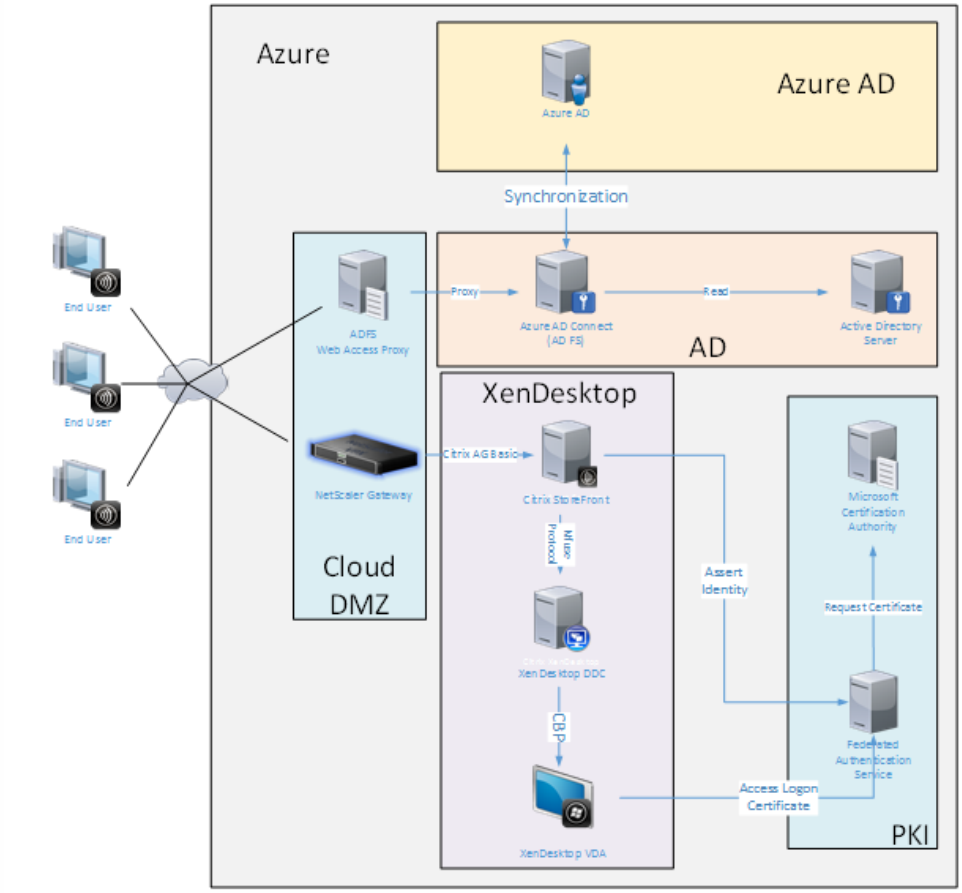
- 「Federated Authentication Service」では、FASのインストールと構成の方法について説明します。

Windows 10 Azure ADへの参加

Windows 10によって、「Azure ADへの参加」というコンセプトが導入されました。これは、従来のWindowsドメインへの参

© 1999-2017 Citrix Systems, Inc. All rights reserved.

加とコンセプトが似ていますが、「インターネット上」のシナリオに焦点を当てている点が特徴です。 これは、ラップトップおよびタブレットとうまく機能します。 従来のWindowsドメイン参加と同様に、Azure ADには企業のWebサイトやリソースで、シングルサインオンモデルを実現する機能があります。 これらはすべて「インターネットに対応」しているため、社内LANだけでなく、インターネットに接続したすべての場所から機能します。



この展開は、事実上「オフィスにいるエンドユーザー」の概念のない一例です。ラップトップコンピューターは最新のAzure AD機能を使用して完全にインターネット経由で登録および認証されています。

この展開では、IPアドレスが使用可能なすべての場所、つまりオンプレミス、ホストされたプロバイダー、Azure、あるいはそのほかのクラウドプロバイダーで、インフラストラクチャが実行できる点に注意してください。 Azure AD Connectの同期機能により、自動的にAzure ADに接続します。 例として示した図では、簡単にするためにAzure仮想マシンを使用しています。

関連情報

- 「Federated Authentication Service」では、FASのインストールと構成の方法について説明します。
- 詳しくは、「Federated Authentication ServiceのAzure ADの統合」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication ServiceのADFSの展開

Dec 05, 2017

はじめに

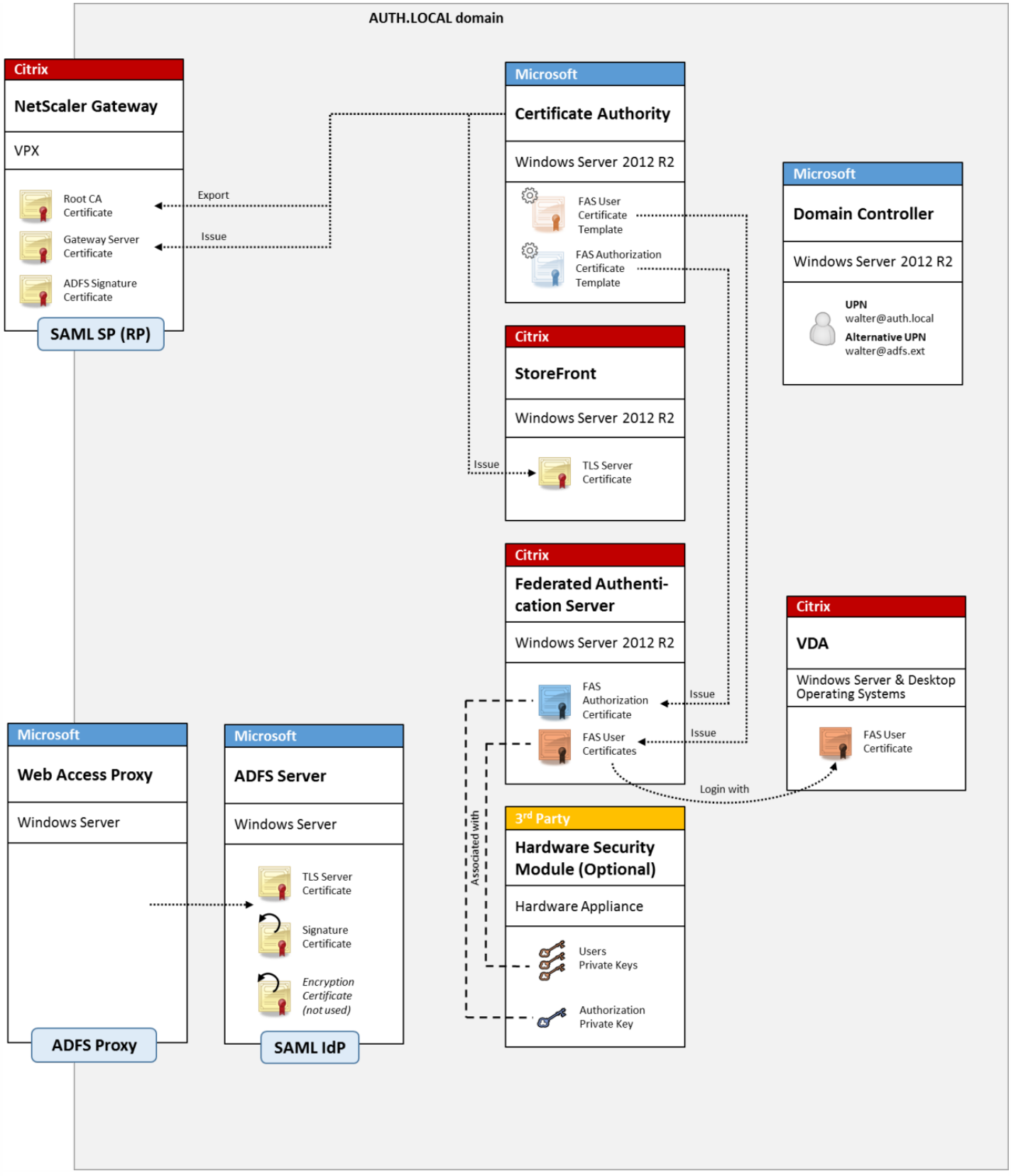
このドキュメントでは、Citrix環境をMicrosoft ADFSと統合する方法について説明します。

ADFSは、多くの組織で単一の認証ポイントが必要なWebサイトへのセキュアなユーザーアクセスを管理するために使用されます。 たとえば、従業員にとって利用可能な追加のコンテンツやダウンロードがある場合、これらの場所は、標準のWindowsログオン資格情報で保護する必要があります。

また、Federated Authentication Service（FAS）では、Citrix NetScalerおよびCitrix StoreFrontをADFSのログオンシステムに統合できるため、企業担当者が混乱する可能性を削減します。

この展開で、NetScalerはMicrosoft ADFSの証明書利用者として統合されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



SAMLの概要

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SAML（Security Assertion Markup Language）は、シンプルな「ログオンページへのリダイレクト」を実現する、Webブラウザーのログオンシステムです。 構成には次の項目が含まれます。

リダイレクトURL［シングルサインオンサービスURL］

ユーザー認証の必要があることをNetScalerが検出すると、NetScalerはユーザーが使用するWebブラウザーに、ADFSサーバー上のSAMLログオンWebページにHTTP POSTを実行するよう指示します。 これは、通常、次の形式のhttps://アドレスです。 https://adfs.mycompany.com/adfs/ls

このWebページのPOSTには、ログオン完了時にADFSがユーザーを返す「リターンアドレス」などの情報も含まれます。

識別子［発行者名/EntityID］

EntityIdは、NetScalerがADFSに送信するPOSTデータに含まれる一意の識別子です。 EntityIdはADFSに、ユーザーがどのサービスにログオンしようとしているかを知らせ、必要に応じてさまざまな認証ポリシーが適用されるようにします。 発行されると、SAML認証XMLは、EntityIdの識別したサービスへのログオンのみに使用されます。

通常、EntityIDは、NetScalerサーバーのログオンページのURLですが、一般的には、次のように、NetScalerおよびADFSが同意する限りどんなものでも可能です。https://ns.mycompany.com/application/logonpage

リターンアドレス［応答URL］

認証に成功すると、ADFSはユーザーのWebブラウザーに、EntityIDのために構成された応答URLの1つに、SAML認証XMLをPOSTし返すよう指示します。 これは、通常、元のNetScalerサーバー上では次の形式のhttps://アドレスです。 https://ns.mycompany.com/cgi/samlauth

構成された応答URLアドレスが複数ある場合、NetScalerはADFSへの元のPOST内にある1つを選択できます。

署名証明書［IDP証明書］

ADFSは秘密キーを使用して、SAML認証XML BLOBに暗号で署名します。 この署名を検証するには、NetScalerを構成し、証明書ファイルに含まれる公開キーを使用して、これらの署名を確認する必要があります。証明書ファイルは、通常、ADFSサーバーから取得されるテキストファイルです。

シングルサインアウトURL［シングルログアウトURL］

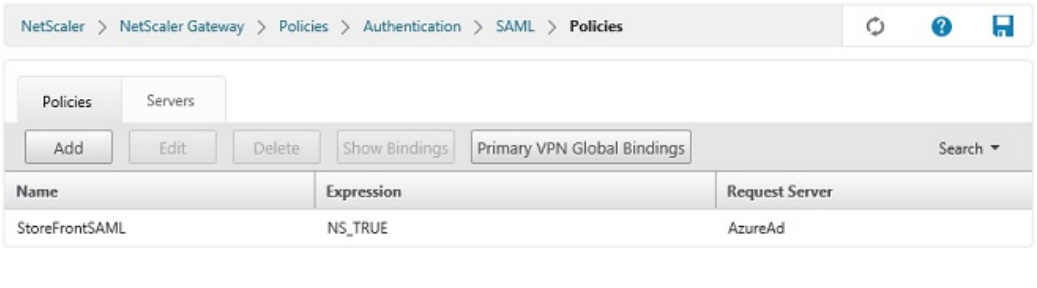
ADFSおよびNetScalerは、「中央ログアウト」システムをサポートしています。 これはNetScalerがポーリングすることがあるURLであり、SAML認証XML BLOBが現在ログオン中のセッションをまだ示していることを確認します。

これは、構成する必要がないオプション機能です。これは、通常、次の形式のhttps://アドレスです。 https://adfs.mycompany.com/adfs/logout （シングルログオンURLと同じ場合があることに注意してください。）

構成

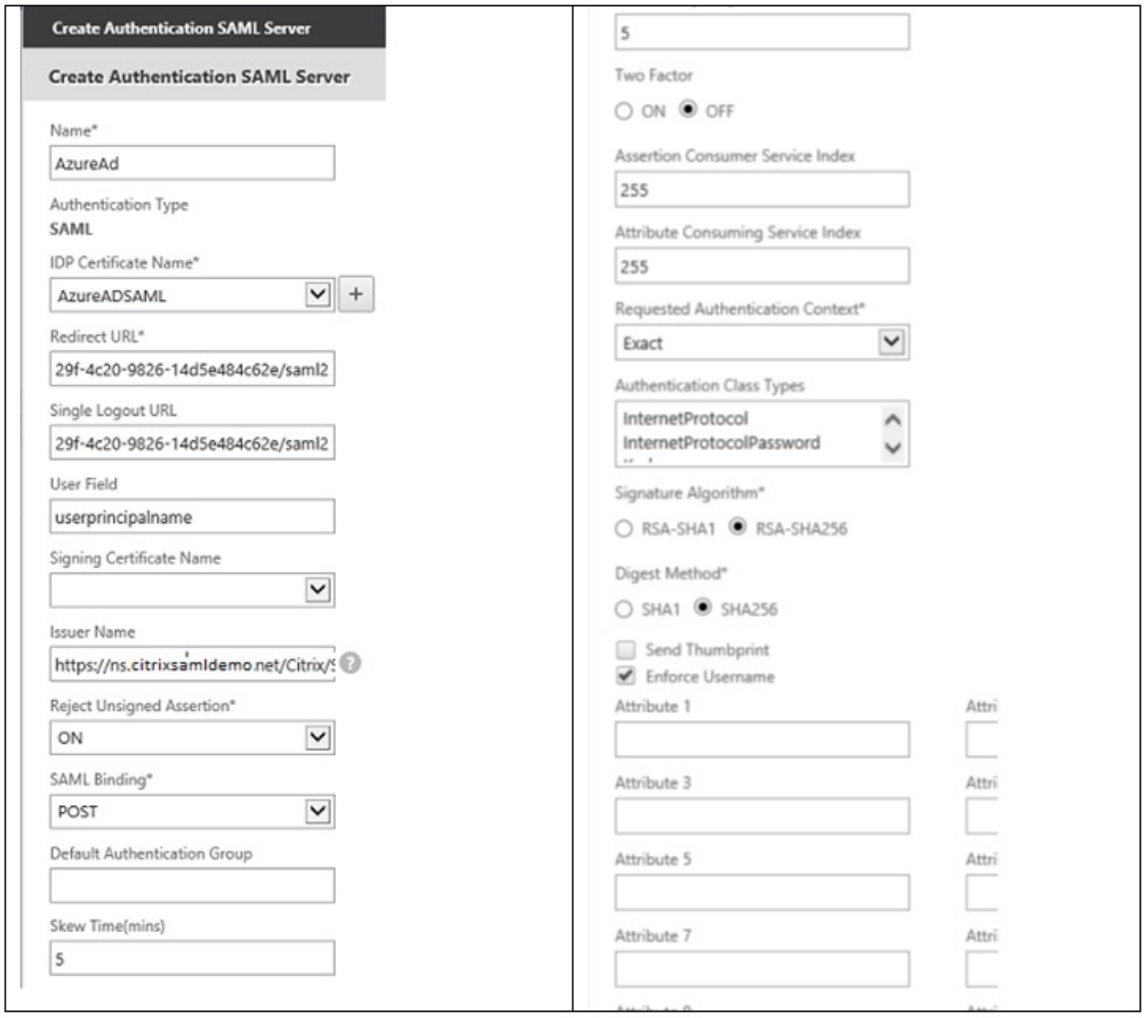
「Federated Authentication Servicesアーキテクチャ」の「NetScaler Gatewayの展開」セクションでは、XenAppおよびXenDesktopのNetScalerセットアップウィザードを使用してNetScaler Gatewayをセットアップし、標準的なLDAP認証オプションを処理する方法について説明します。これが正常に完了すると、SAML認証を許可するNetScalerで、新しい認証ポリシーを作成することができます。 その後、NetScalerセットアップウィザードで使用されたデフォルトのLDAPポリシーを置き換えることができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



SAMLポリシーの記入

ADFS管理コンソールから前に取得した情報を使用して、新しいSAML IdPサーバーを構成します。このポリシーが適用されると、NetScalerはログオンのためにユーザーをADFS-signedにリダイレクトし、ADFSの署名したSAML認証トークンを代わりに受け取ります。



関連情報

- FASのインストールと構成については、「Federated Authentication Service」を参照してください。
- 一般的なFAS環境については、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」では「方法」記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication ServiceのAzure ADの統合

Dec 05, 2017

ここでは次のことについて説明します。

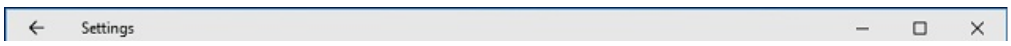
- はじめに
- アーキテクチャ
- DNSゾーンの作成
- クラウドサービスの作成
- Windows仮想マシンの作成
- 内部DNSの構成
- 外部DNSアドレスの構成
- セキュリティグループの構成
- ADFS証明書の作成
- Azure ADのセットアップ
- Azure ADへの参加の有効化
- XenAppまたはXenDesktopのインストール
- 新しいAzure ADアプリケーションをStoreFrontへのシングルサインオンに構成
- NetScaler Gatewayのインストールと構成
- StoreFrontアドレスの構成
- NetScaler SAML認証サポートの有効化
- エンドツーエンドシステムの検証
- 付録

はじめに

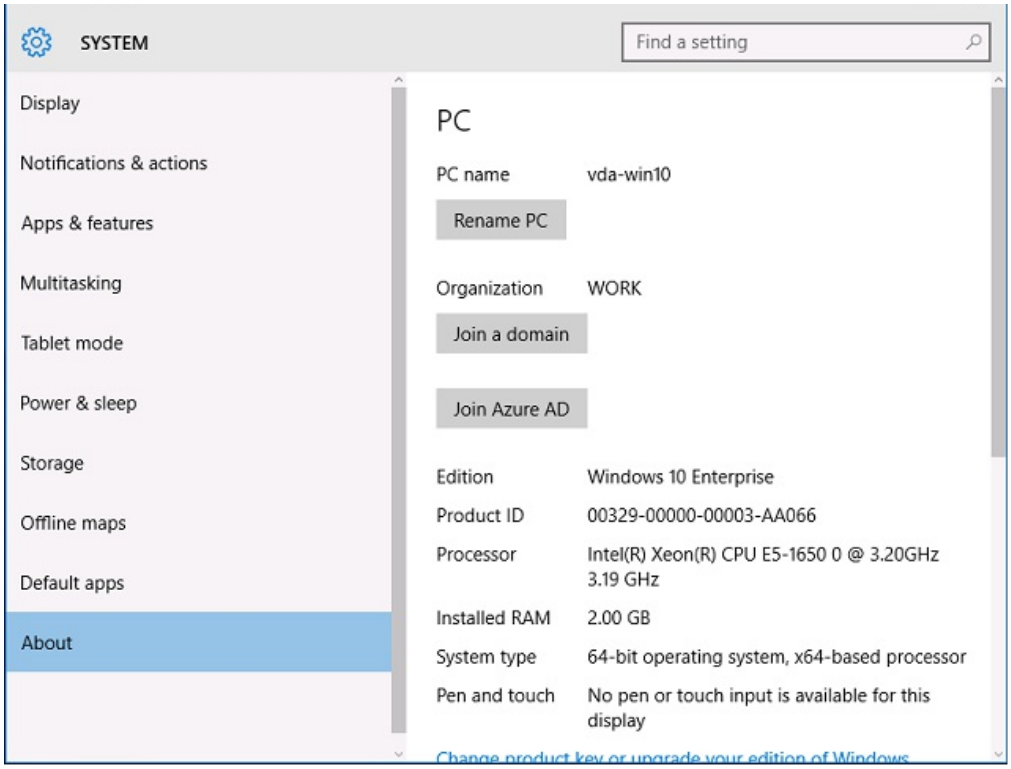
このドキュメントでは、Citrix環境をWindows 10 Azure AD機能と統合する方法について説明します。

Windows 10が導入したAzure ADは、ドメイン参加の新しいモデルです。これを利用すれば、管理とシングルサインオンの目的で、ローミングラップトップを、インターネット上で企業ドメインに参加させることができます。

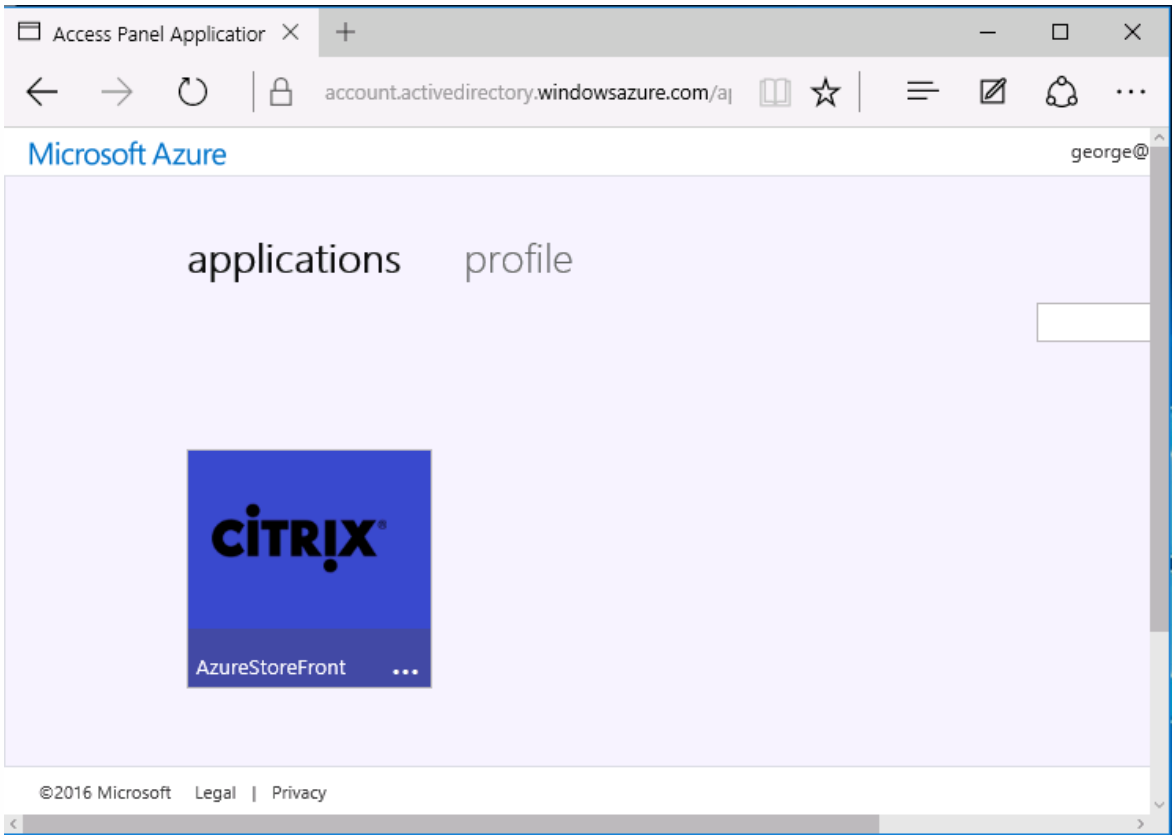
このドキュメントで例として示した展開では、新規ユーザーのWindows 10ラップトップに会社のメールアドレスと登録コードが提供されるシステムを説明しています。 ユーザーは **[設定]** パネルの［システム］>［バージョン情報］>［Azure ADに参加］から、このコードにアクセスします。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



ラップトップが登録されると、Microsoft EdgeのWebブラウザーは、Azure SaaSアプリケーションの Webページから、会社の WebサイトやCitrixの公開アプリケーション、およびOffice 365などのAzureアプリケーションに自動的にサインオンします。



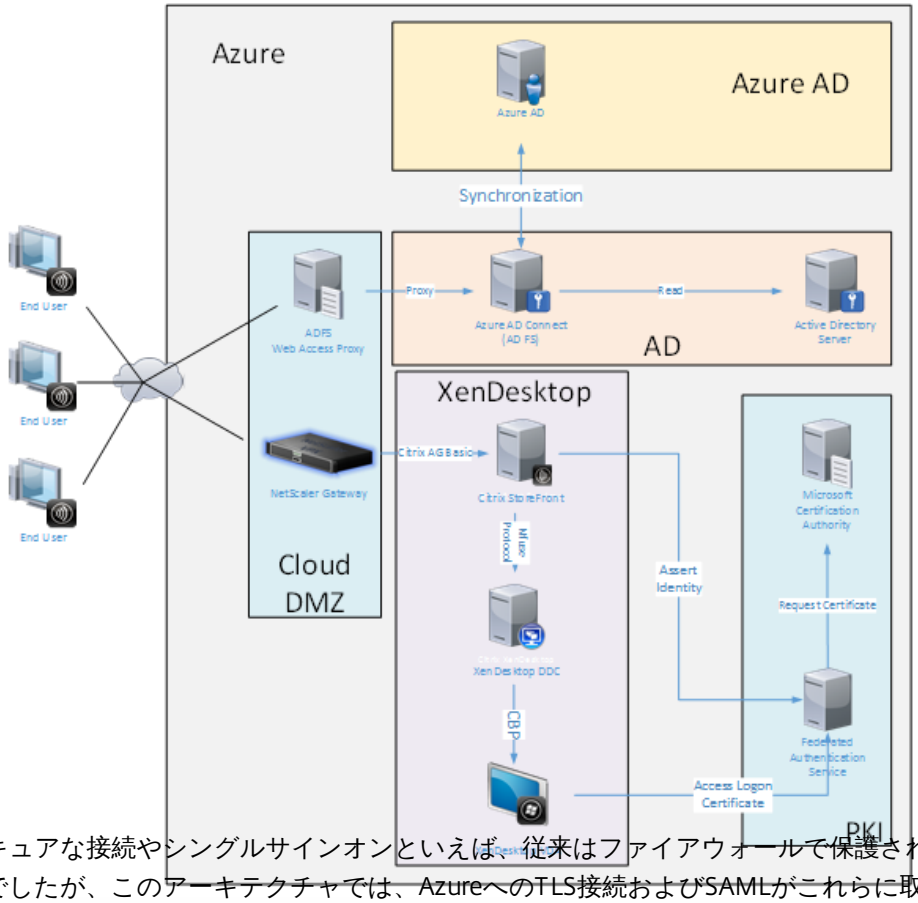
© 1999-2017 Citrix Systems, Inc. All rights reserved.

アーキテクチャ

このアーキテクチャでは、Azure ADやOffice 365などの最新クラウドテクノロジとの統合により、従来の企業ネットワークがAzure内に完全に複製されます。 すべてのエンドユーザーがリモートワーカーと見なされ、社内イントラネット上にはエントユーザーが存在しないというコンセプトです。

Azure AD Connectの同期サービスが、インターネット上でAzureへの橋渡しとして機能するため、既存のオンプレミスシステムを持つ企業はこのモデルを適用することができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



セキュアな接続やシングルサインオンといえば、従来はファイアウォールで保護されたLANや、Kerberos認証およびNTLM認証でしたが、このアーキテクチャでは、AzureへのTLS接続およびSAMLがこれらに取って代わります。 Azureアプリケーションのの参加により、新しいサービスが生み出されています。Active Directoryを必要とする既存のアプリケーション（SQL Serverデータベースなど）は、AzureクラウドサービスのIaaS部分にある、標準的なActive Directoryサーバーの仮想マシンを使用して実行できます。

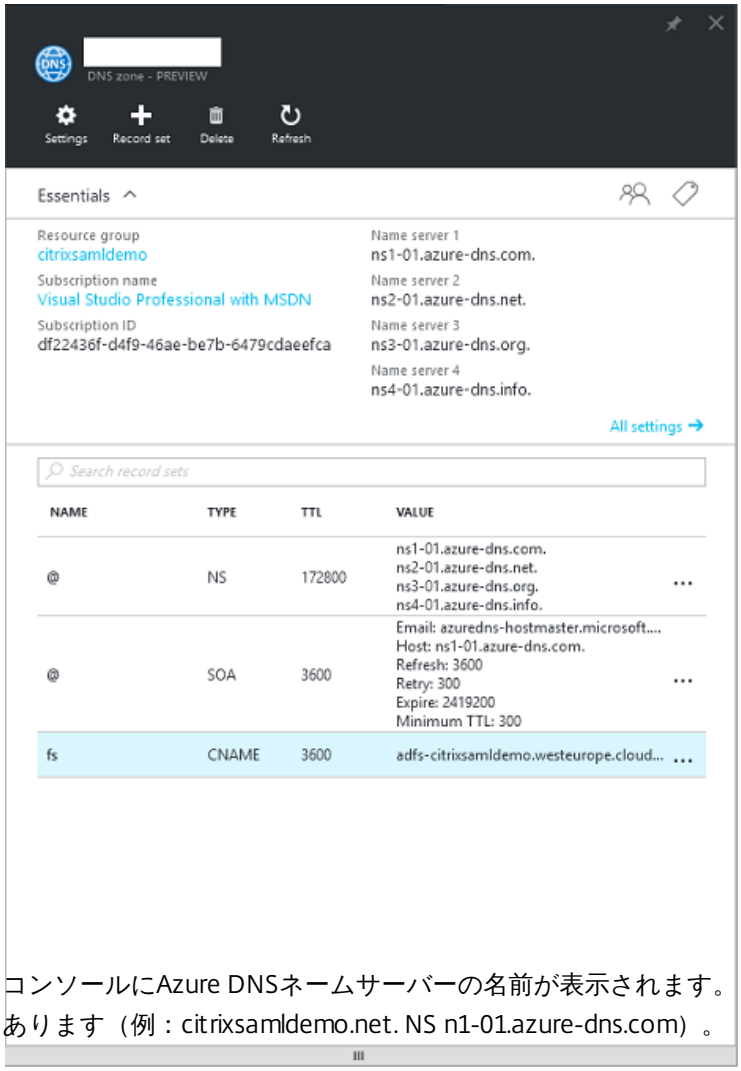
ユーザーが従来のアプリケーションを起動すると、XenAppおよびXenDesktopの公開アプリケーションを使用してアクセスします。 Microsoft Edgeのシングルサインオン機能を使用して、ユーザーの **[Azureアプリケーション]** ページからさまざまな種類のアプリケーションが照合されます。 また、Microsoftは、Azureアプリケーションの一覧表示と起動ができるAndroidおよびiOSアプリを提供しています。

DNSゾーンの作成

Azure ADでは、管理者がパブリックDNSアドレスを登録し、ドメイン名サフィックスの委任ゾーンを管理する必要があります。 これを実行するために、管理者はAzure DNSゾーン機能を使用できます。

この例では、DNSゾーン名「citrixsamldemo.net」を使用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



コンソールにAzure DNSネームサーバーの名前が表示されます。 これらはゾーンのDNS登録のNSエントリで参照する必要があります（例：citrixsamldemo.net. NS n1-01.azure-dns.com）。

Azureで実行される仮想マシンへの参照を追加する場合は、CNAMEポインターを、Azureが管理する仮想マシンのDNSレコードに使用するのが最も簡単です。 仮想マシンのIPアドレスが変更されている場合は、DNSゾーンファイルを手動で更新する必要はありません。

内部および外部のDNSアドレスサフィックスは、この展開に一致します。 ドメインはcitrixsamldemo.netで、スプリットDNS（内部で10.0.0.*）を使用します。

Webアプリケーションプロキシサーバーを参照する、「fs.citrixsamldemo.net」エントリを追加します。 これがこのゾーンのフェデレーションサービスです。

クラウドサービスの作成

この例では、Azureで実行されるADFSサーバーが設置されたAD環境を含む、Citrix環境を構成します。 クラウドサービスを作成し、「citrixsamldemo」と名づけます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

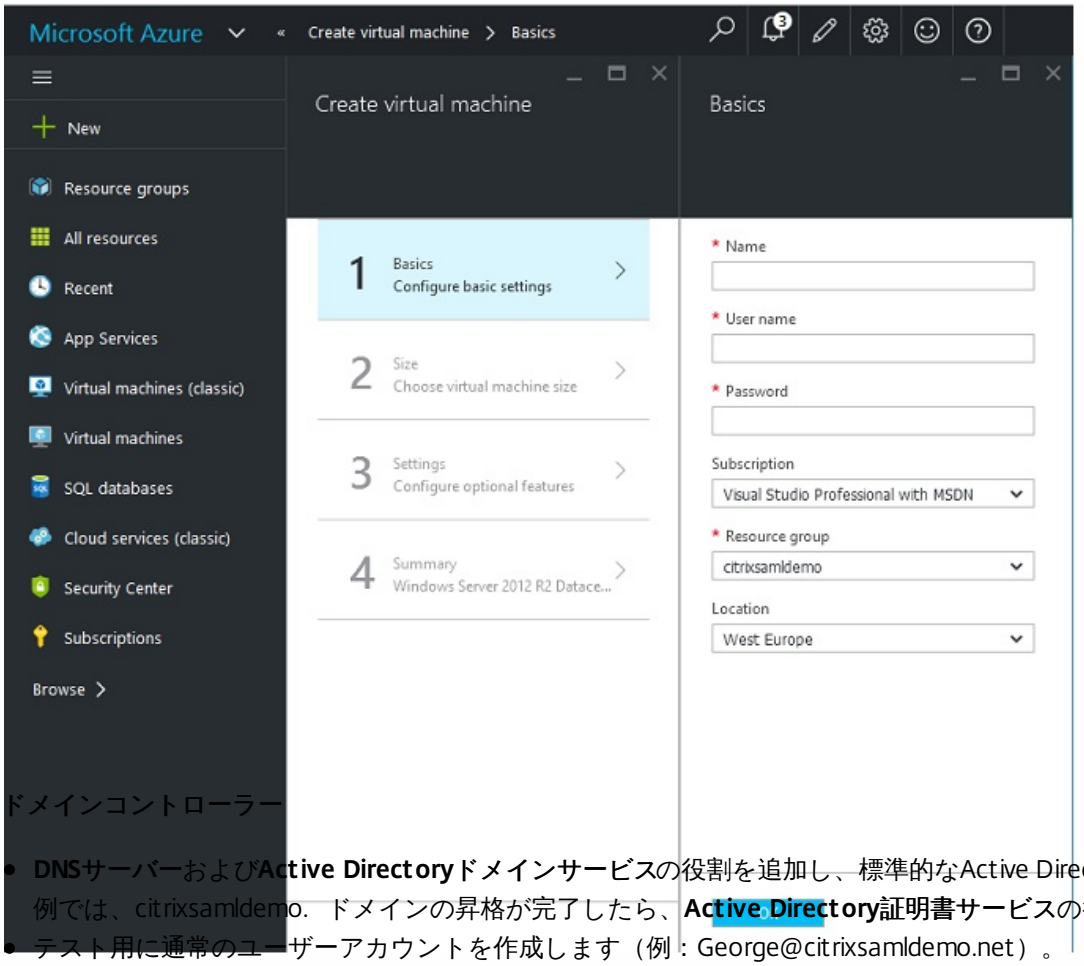


Windows仮想マシンの作成

クラウドサービスで実行されるWindows仮想マシンを5台作成します。

- ドメインコントローラー（domaincontrol）
- Azure Connect ADFSサーバー（adfs）
- ADFS Webアクセスプロキシ（ドメインに参加していないWebアプリケーションプロキシ）
- Citrix XenDesktop Delivery Controller（ddc）
- Citrix XenDesktop Virtual Delivery Agent（vda）

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ドメインコントローラー

- **DNSサーバー**および**Active Directoryドメインサービス**の役割を追加し、標準的なActive Directory展開を作成します（この例では、citrixsamldemo. ドメインの昇格が完了したら、**Active Directory証明書サービス**の役割を追加します。
- テスト用に通常のユーザーアカウントを作成します（例：George@citrixsamldemo.net）。
- このサーバーでは内部DNSが実行されるため、すべてのサーバーはDNS解決にこのサーバーを参照する必要があります。**［Azure DNS設定］**ページで行います。（詳しくは、このドキュメントの付録を参照してください。）

ADFSコントローラーとWebアプリケーションプロキシサーバー

- ADFSサーバーをcitrixsamldemoドメインに参加させます。 Webアプリケーションプロキシサーバーは、分離されたワークグループにとどまる必要があるため、AD DNSでDNSアドレスを手動で登録します。
- これらのサーバーで**Enable-PSRemoting –Force**コマンドレットを実行して、Azure AD Connectツールからファイアウォール経由のPSリモーティングを有効にします。

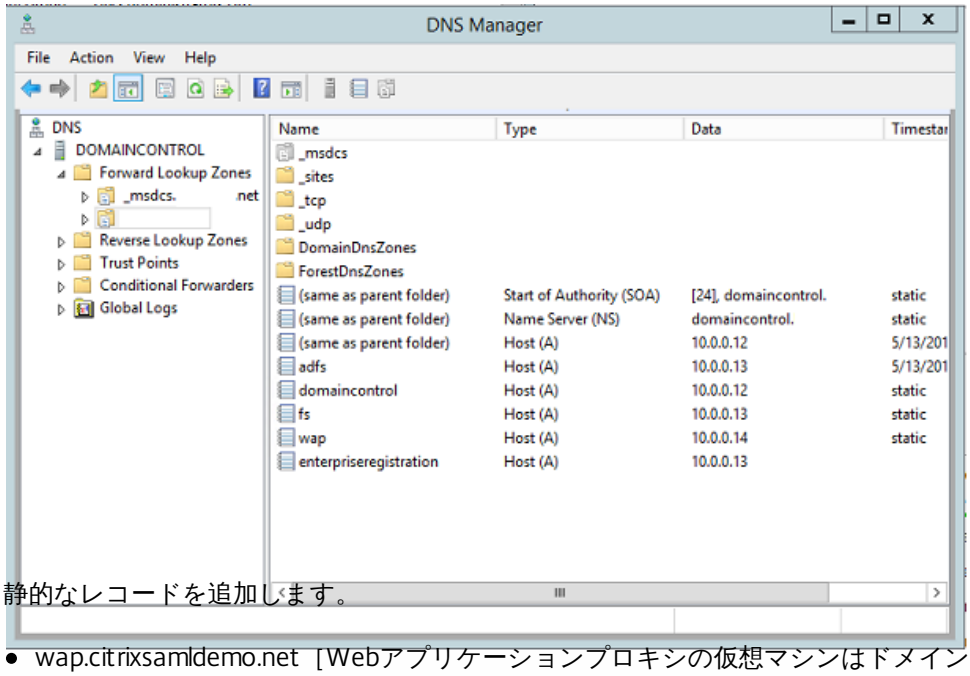
XenDesktop Delivery ControllerとVDA

- XenAppまたはXenDesktop Delivery Controller、およびVDAを、citrixsamldemoに参加した残り2台のWindowsサーバーにインストールします。

内部DNSの構成

ドメインコントローラーのインストール後にDNSサーバーを構成し、citrixsamldemo.netの内部ビューを処理し、外部DNSサーバーに対してフォワーダーとして機能するように設定します（例：8.8.8.8）。

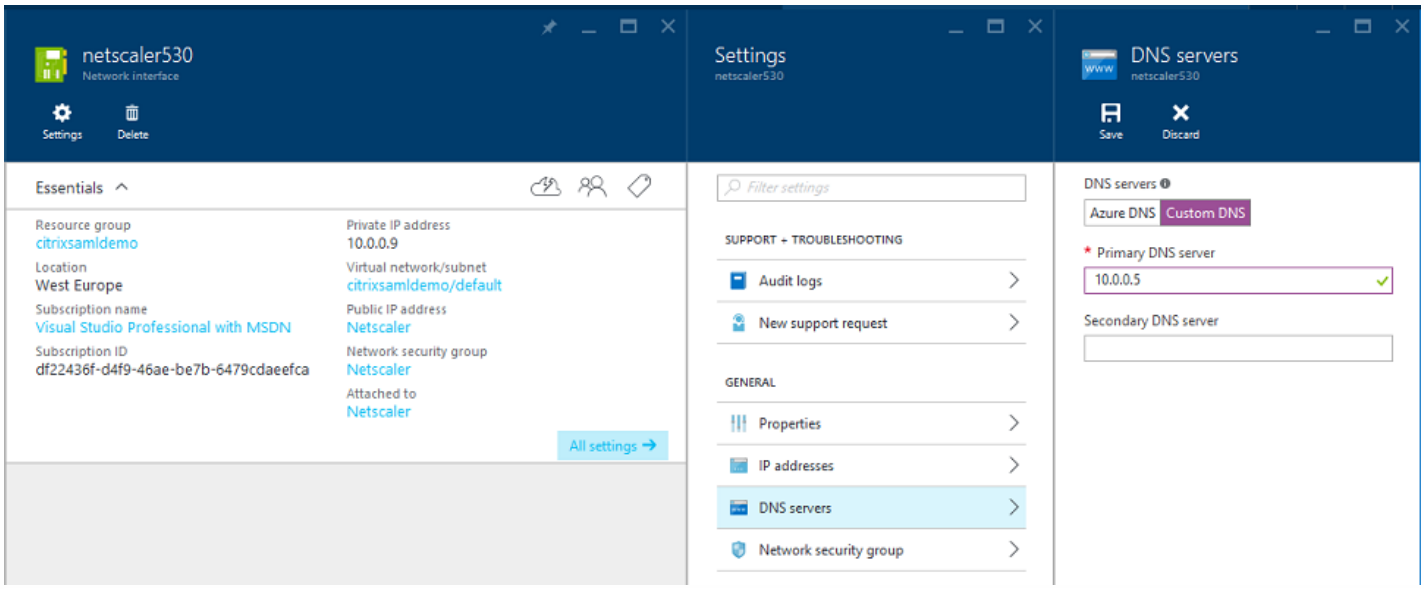
© 1999-2017 Citrix Systems, Inc. All rights reserved.



静的なレコードを追加します。

- wap.citrixsamldemo.net［Webアプリケーションプロキシの仮想マシンはドメインに参加しません］
- fs.citrixsamldemo.net［内部フェデレーションサーバーのアドレス］
- enterpriseregistration.citrixsaml.net［fs.citrixsamldemo.netと同じ］

Azureで実行されるすべての仮想マシンは、このDNSサーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェイスGUIから実行できます。



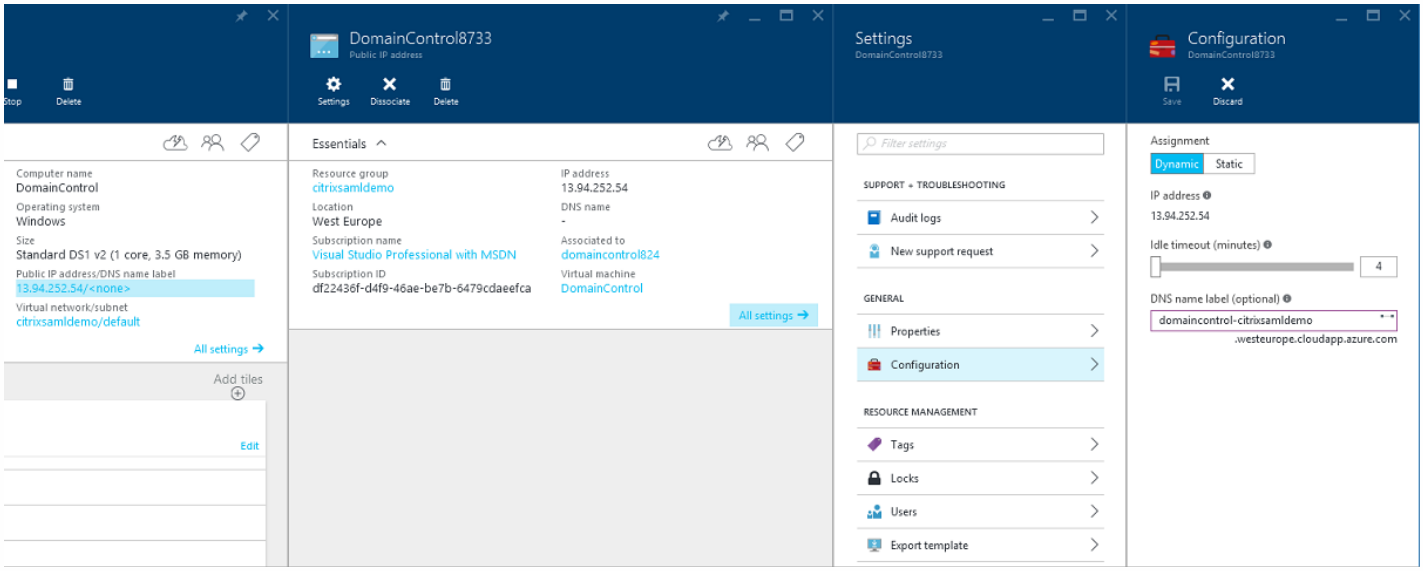
デフォルトでは、内部IP（10.0.0.9）アドレスは動的に割り当てられます。 IPアドレスの設定を使用して、IPアドレスを永続的に割り当てることができます。これは、Webアプリケーションプロキシサーバーとドメインコントローラーで実行する必要があります。

外部DNSアドレスの構成

仮想マシン実行時に、Azureは、仮想マシンに割り当てられた現在のパブリックIPアドレスを指す自身のDNSゾーンサーバー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

を維持します。 Azureはデフォルトで各仮想マシンの起動時にIPアドレスを割り当てるため、この便利な機能を有効にします。

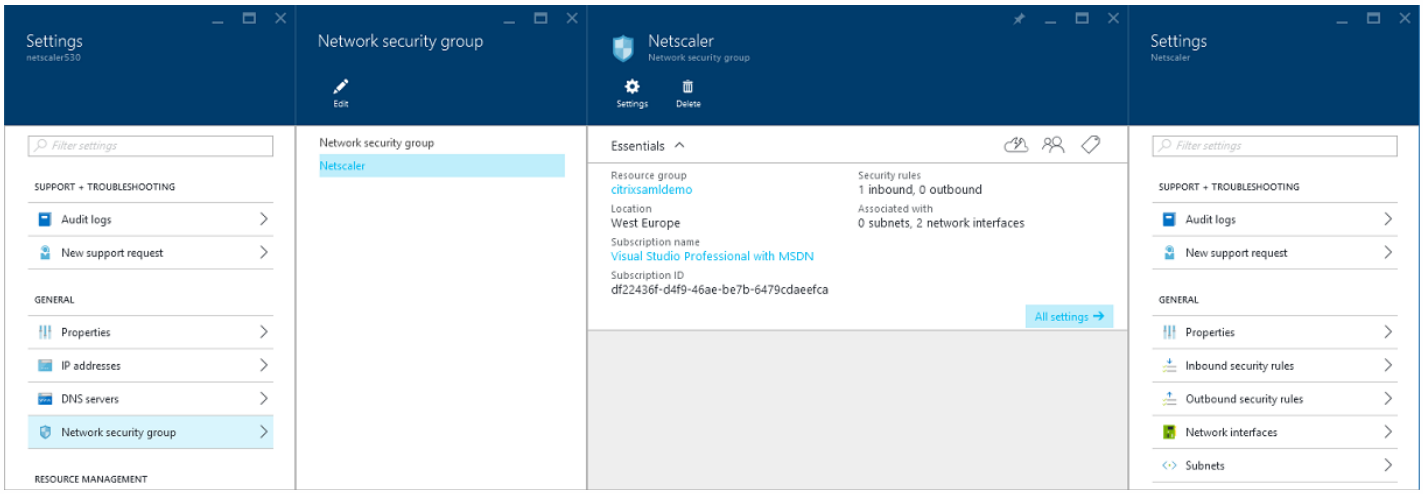


この例では、DNSアドレスdomaincontrol-citrixsamldemo.westeurope.cloudapp.azure.comを、ドメインコントローラーに割り当てています。

リモート構成の完了時にパブリックIPアドレスを有効にする必要があるのは、WebアプリケーションプロキシとNetScaler仮想マシンだけである点に注意してください。（構成では、環境へのRDPアクセスにパブリックIPアドレスが使用されます）。

セキュリティグループの構成

Azureクラウドは、セキュリティグループを使用して、インターネットから仮想マシンへのTCPおよびUDPアクセスのファイアウォールルールを管理します。 デフォルトでは、すべての仮想マシンでRDPアクセスが許可されます。 また、NetScalerおよびWebアプリケーションプロキシサーバーでは、ポート443でTLSを許可する必要があります。



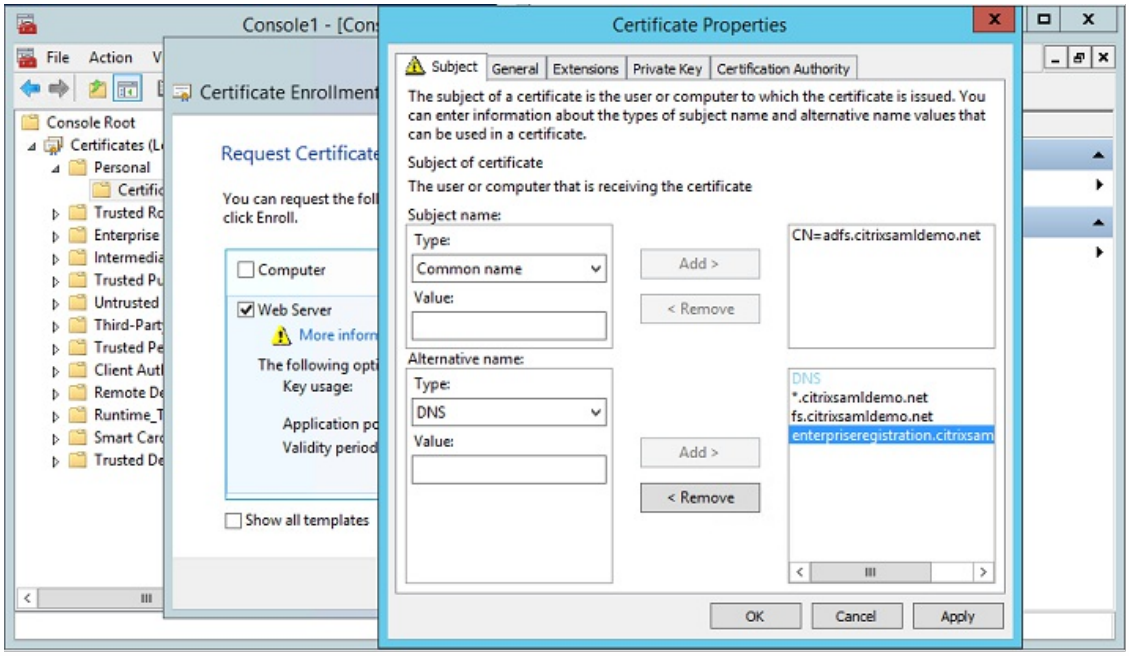
ADFS証明書の作成

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft証明機関（CA）で**Webサーバー**証明書テンプレートを有効にします。 これにより、PFXファイルにエクスポート（秘密キーも含む）できる、カスタムDNSアドレスを持つ証明書を作成できます。 PFXファイルを優先オプションにするには、この証明書をADFSとWebアプリケーションプロキシサーバーの両方にインストールする必要があります。

次のサブジェクト名を使用して、Webサーバー証明書を発行します。

- Commonname:
  - Adfs.citrixsamldemo.net［コンピューター名］
- SubjectAltname:
  - *.Citrixsamldemo.net ［ゾーン名］
  - fs.citrixsamldemo. net ［DNSのエントリ］
  - enterpriseregistration.citrixsamldemo.net



パスワードで保護された秘密キーを含め、証明書をPFXファイルにエクスポートします。

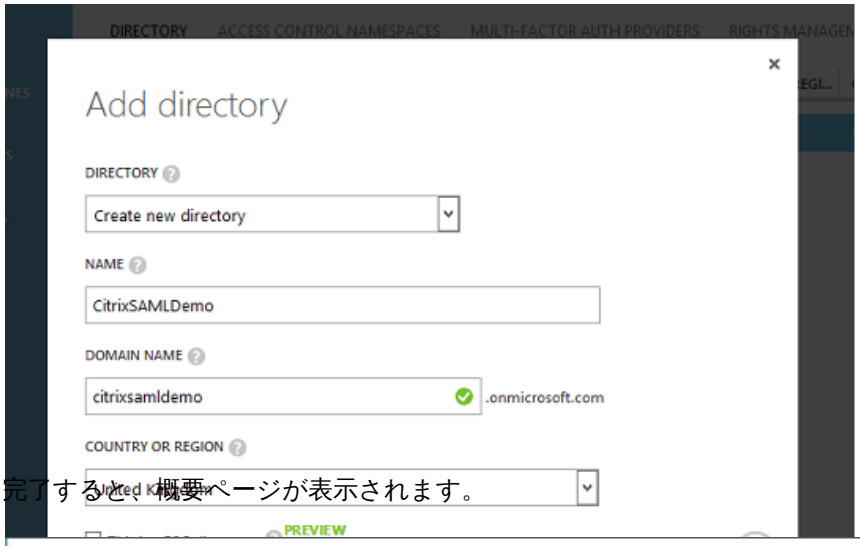
Azure ADのセットアップ

このセクションでは、新しいAzure ADインスタンスをセットアップして、Windows 10をAzure ADに参加させるために使用できるユーザーIDを作成する方法について説明します。

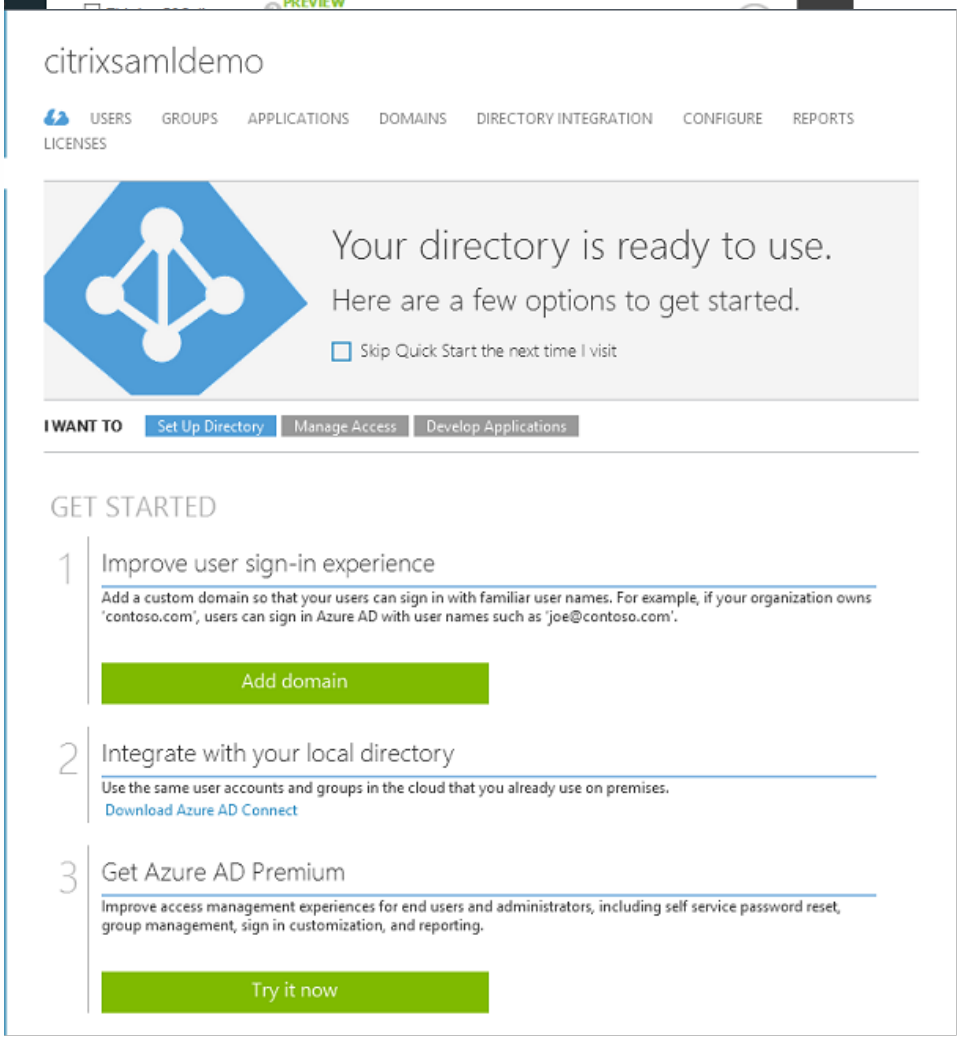
新しいディレクトリの作成

Azureクラシックポータルにログオンして、新しいディレクトリを作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



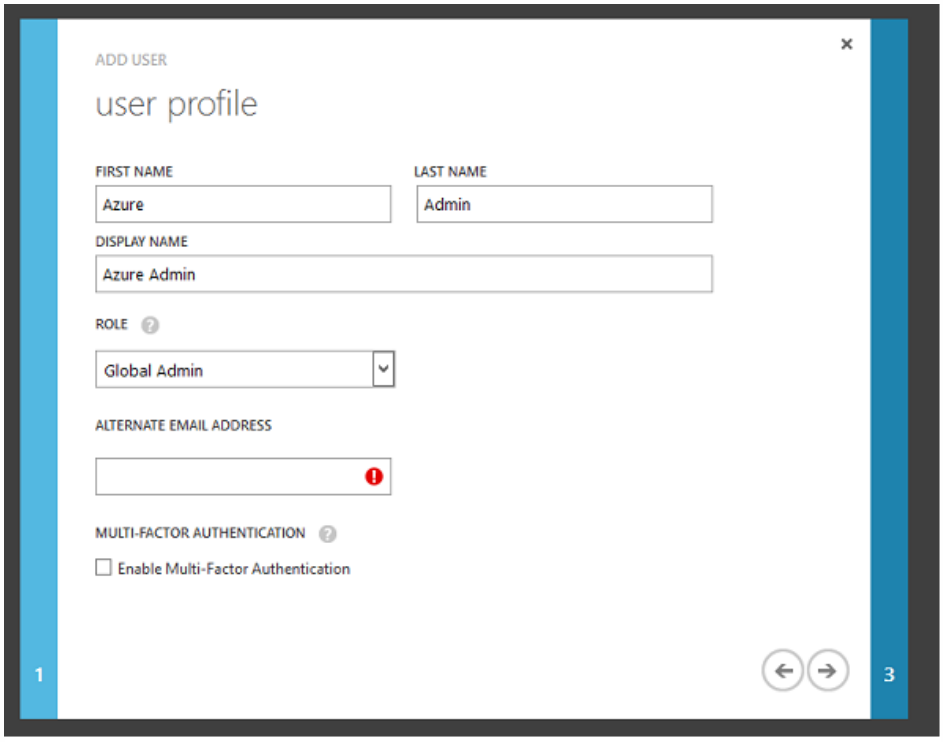
完了すると、概要ページが表示されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

グローバル管理者ユーザー（AzureAdmin）の作成

Azureのグローバル管理者を作成し（この例ではAzureAdmin@citrixsamldemo.onmicrosoft.com）、新しいアカウントでログオンしてパスワードをセットアップします。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

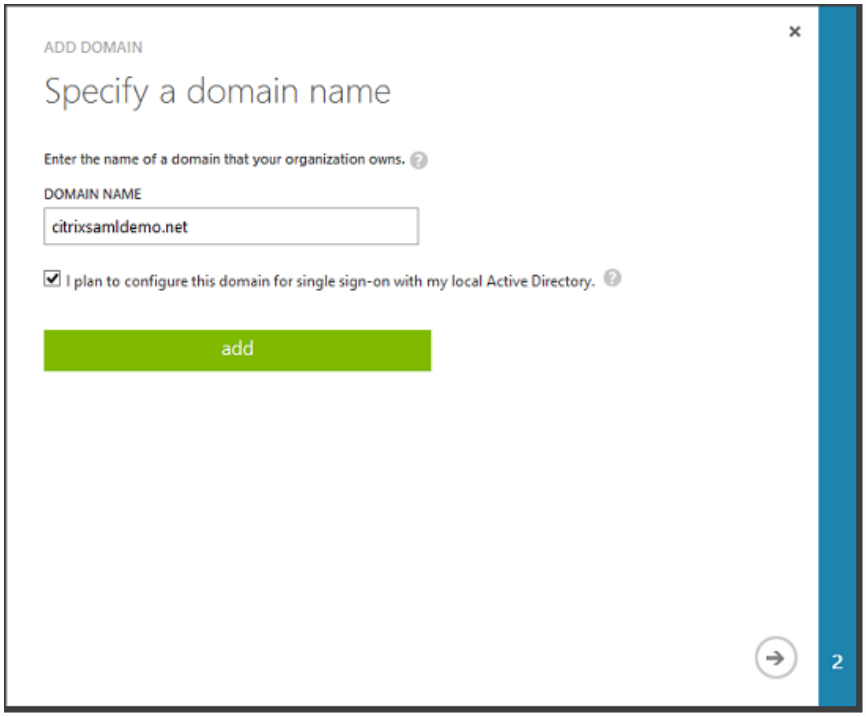
Azure ADを使用したドメインの登録

デフォルトでは、ユーザーは次の形式のメールアドレスで識別されます。 *<user.name>@<company>.onmicrosoft.com*.

これは追加の構成なしで機能しますが、エンドユーザーのメールアカウントと一致する、次の標準形式のメールアドレスをお勧めします。@.com

[ドメインの追加] で、ユーザーの会社のドメインからのリダイレクトを構成します。 この例ではcitrixsamldemo.netを使用します。

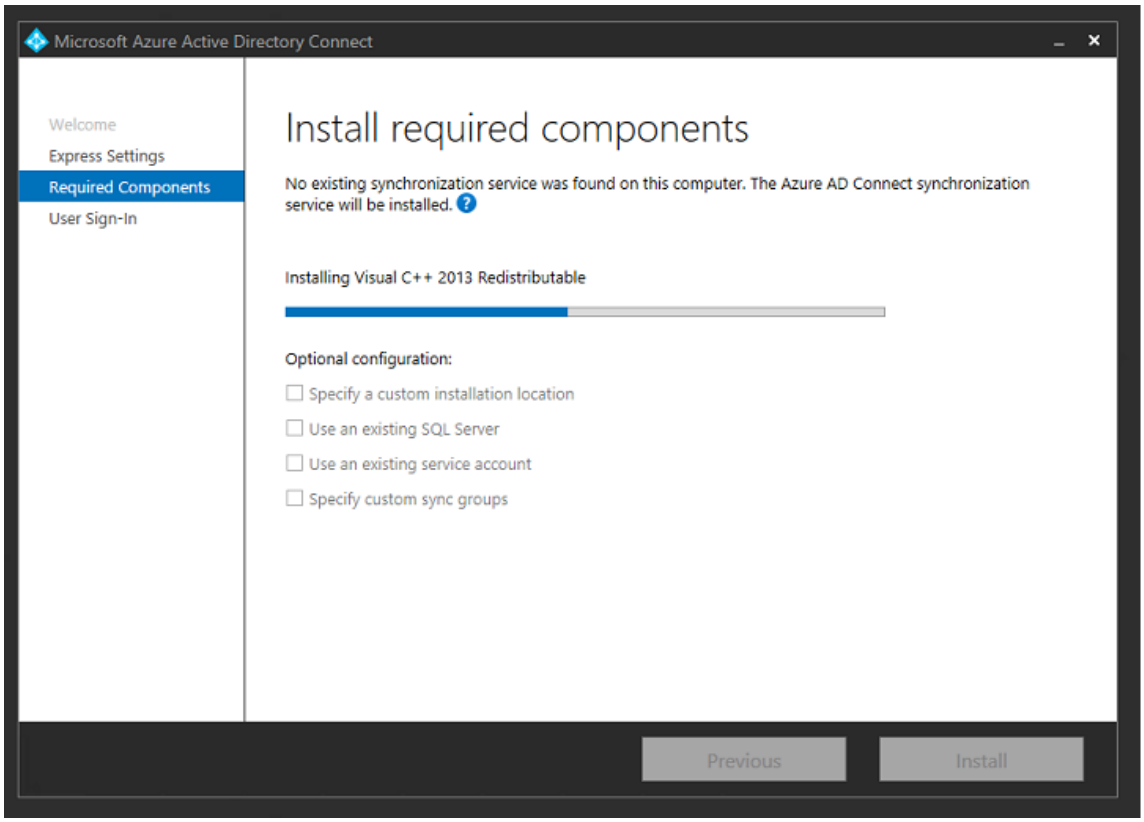
ADFSをシングルサインオンにセットアップしている場合は、チェックボックスにチェックマークを入れます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

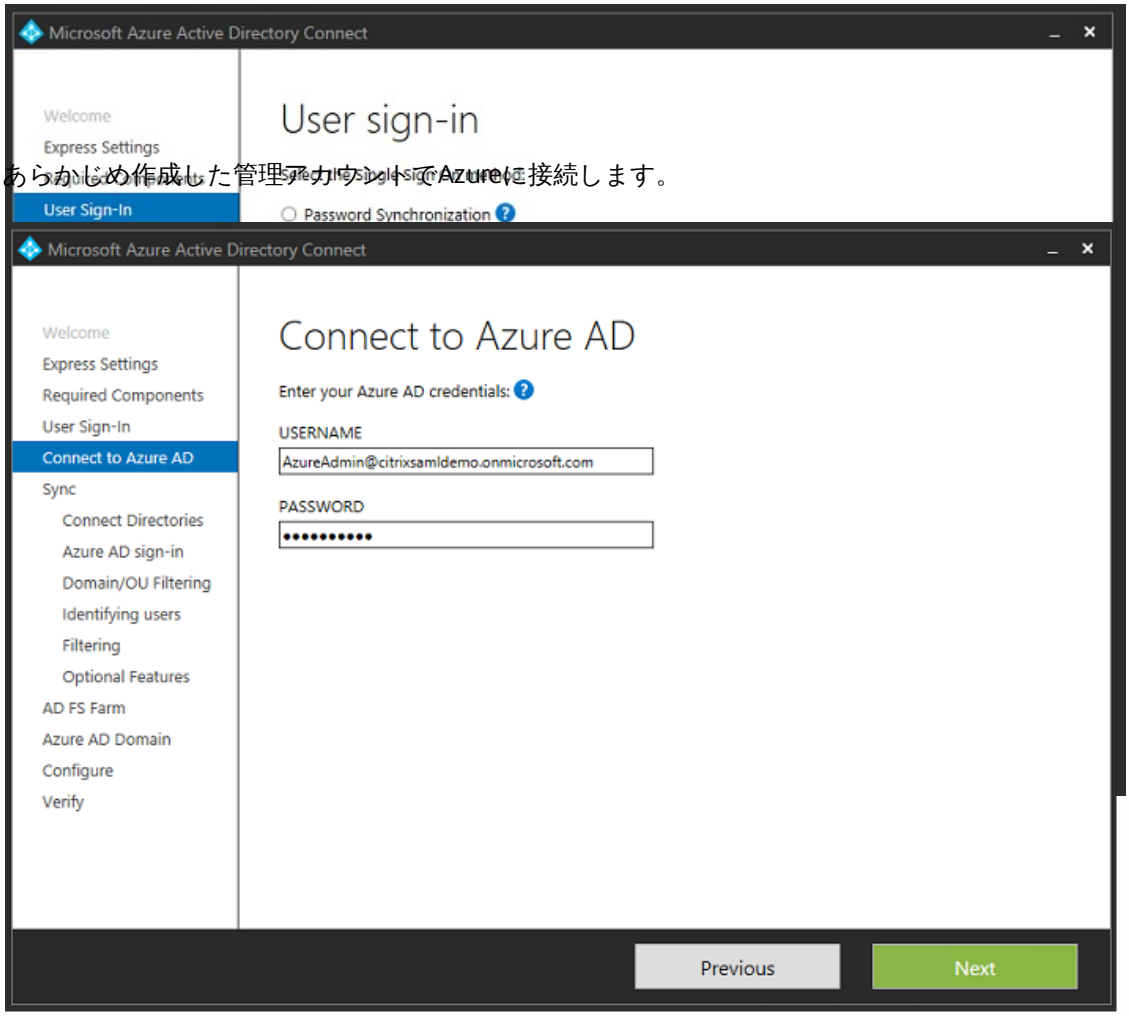
Azure AD Connectのインストール

Azure AD構成GUIの手順2により、Azure AD ConnectのMicrosoftダウンロードページにリダイレクトされます。 これをADFS仮想マシンにインストールします。 **[簡単設定]** ではなく **[カスタムインストール]** を使用し、ADFSのオプションが利用できるようにします。



[AD FSとのフェデレーション] シングルサインオンオプションを選択します。

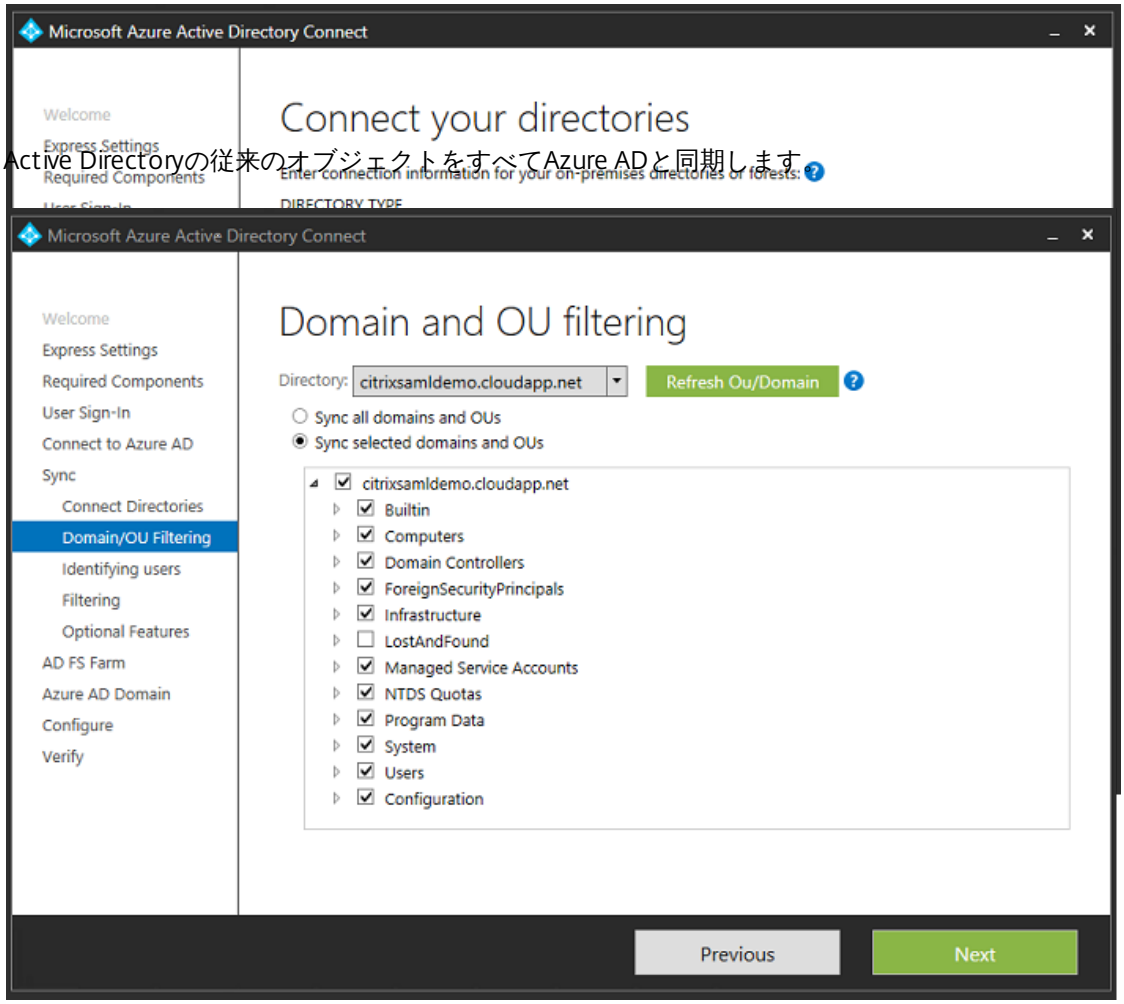
© 1999-2017 Citrix Systems, Inc. All rights reserved.



あらかじめ作成した管理アカウントでAzureに接続します。

内部ADフォレストを選択します。

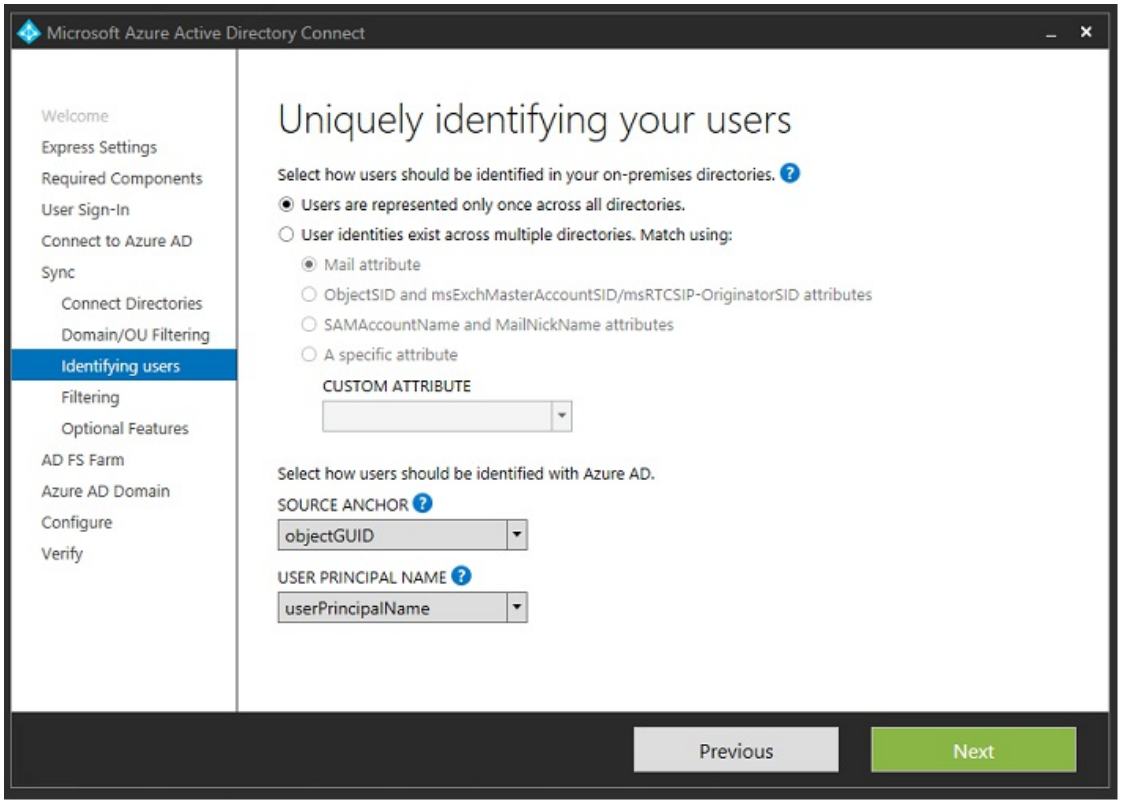
© 1999-2017 Citrix Systems, Inc. All rights reserved.



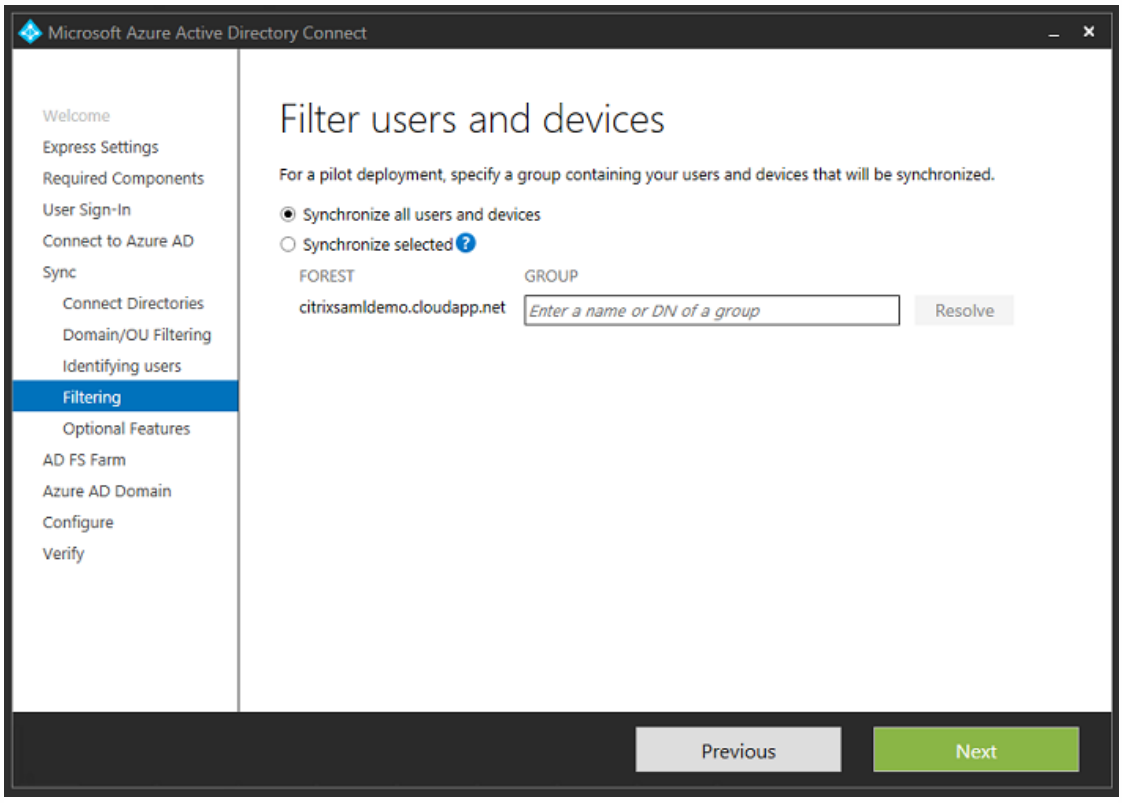
Active Directoryの従来のオブジェクトをすべてAzure ADと同期します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ディレクトリ構造がシンプルな場合は、ユーザー名の一意性に依存して、ログオンするユーザーを識別することができます。

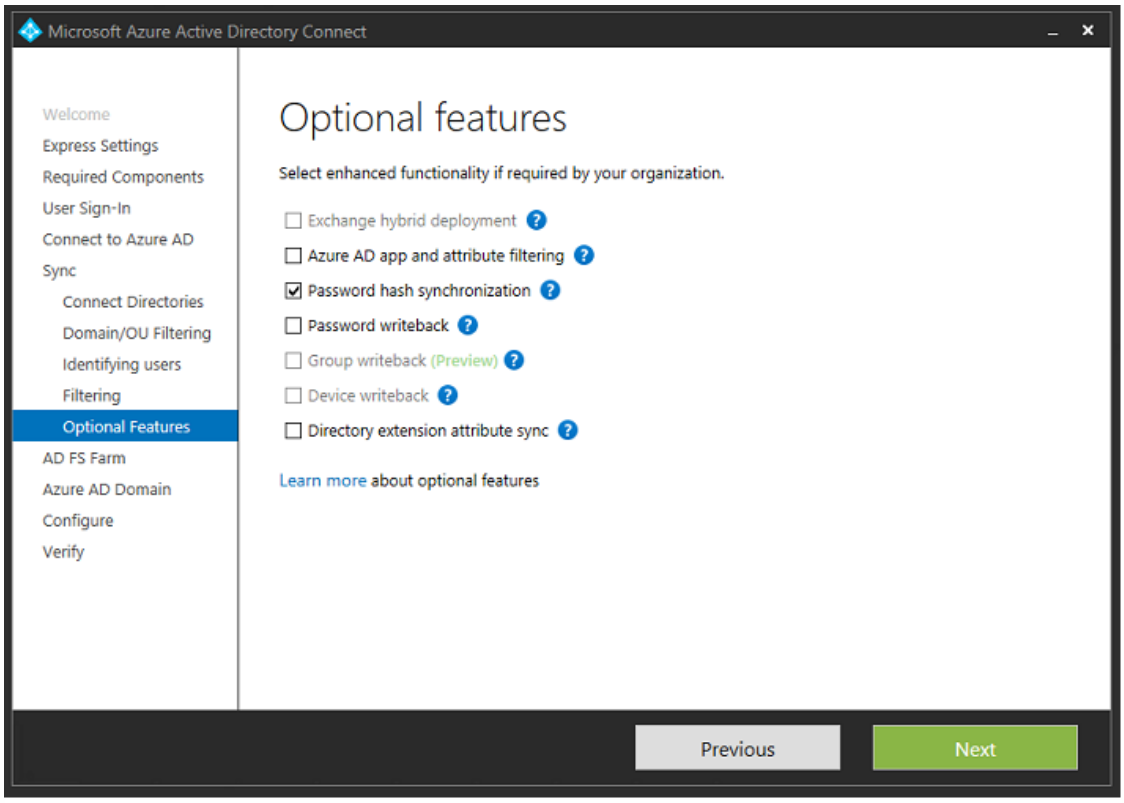


デフォルトのフィルタリングオプションを使用するか、あるいはユーザーとデバイスを特定のグループセットに制限します。



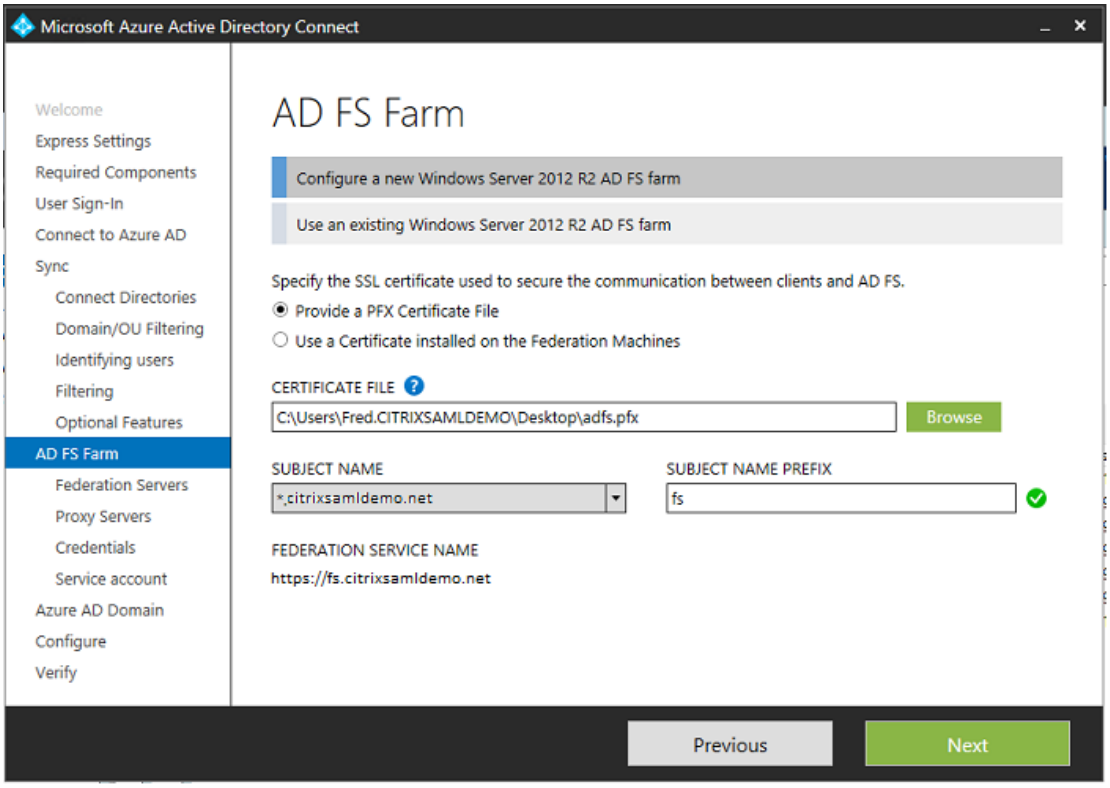
© 1999-2017 Citrix Systems, Inc. All rights reserved.

必要に応じて、Azure ADパスワードをActive Directoryと同期することができます。これは、通常、ADFSベースの認証では必要ありません。

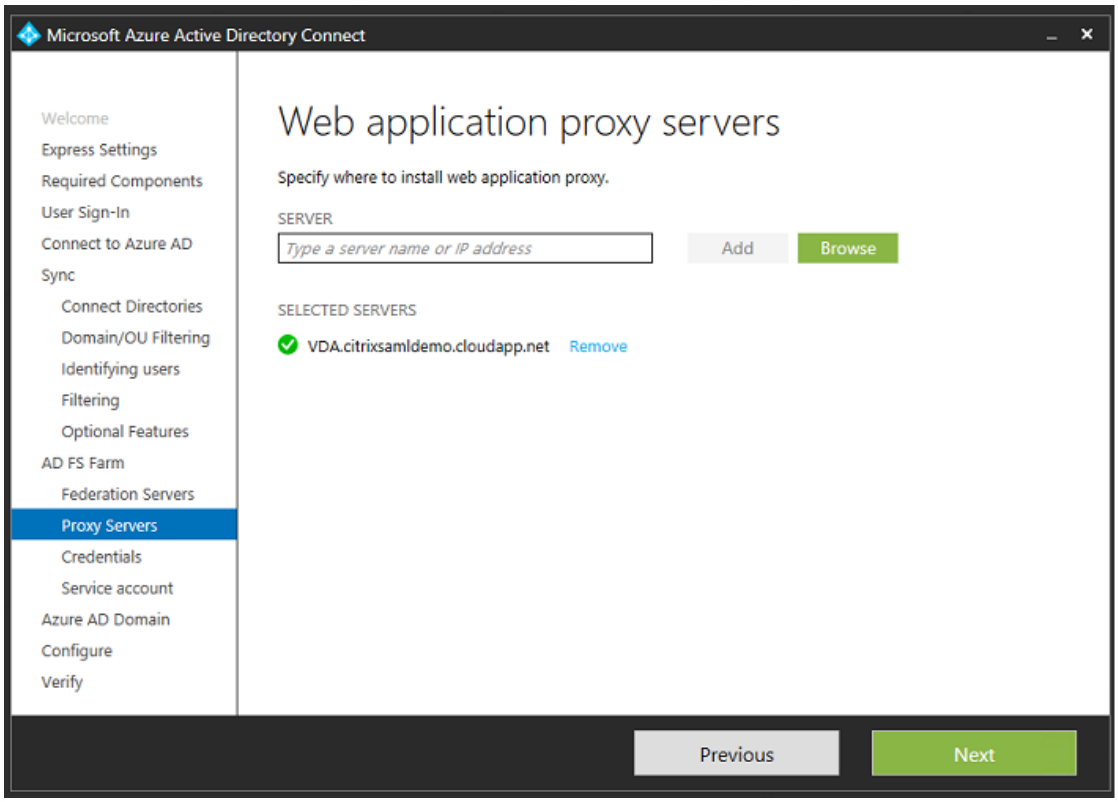


証明書のPFXファイルをAD FSで使用するように選択します。DNS名としてfs.citrixsamldemo.netを指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



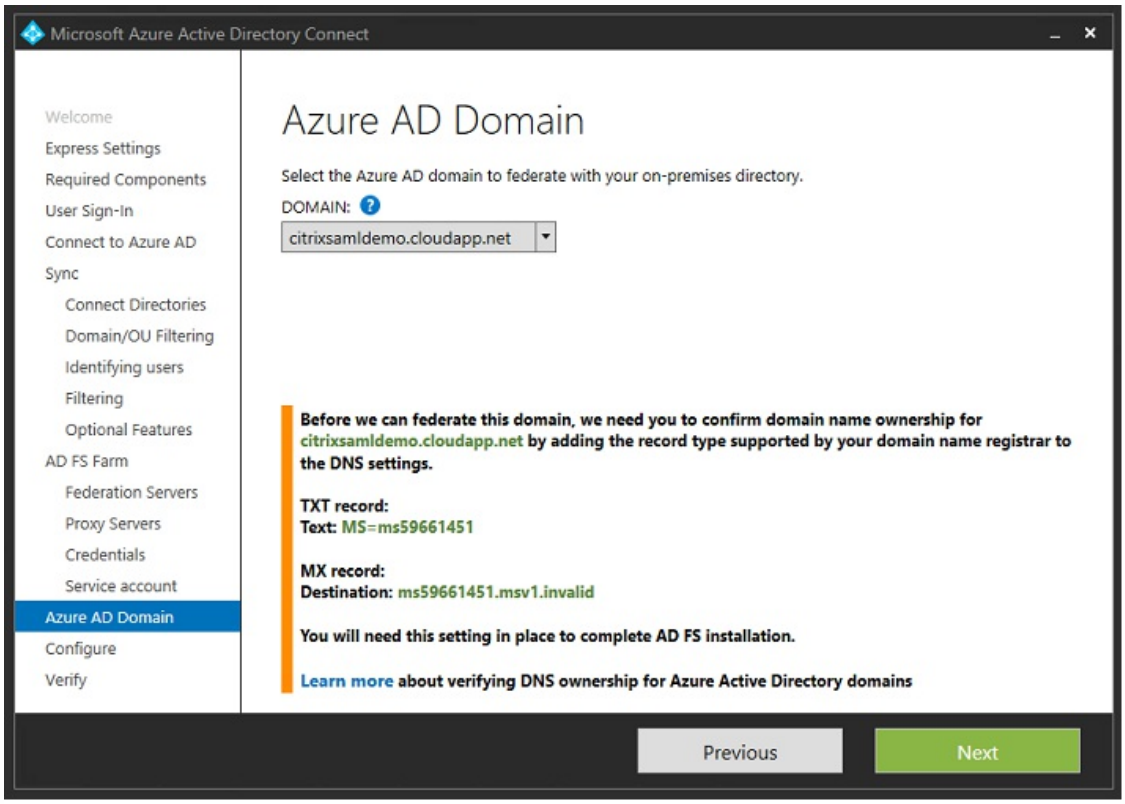
プロキシサーバーの選択を求める画面が表示されたら、wap.citrixsamldemo.netサーバーのアドレスを入力します。 Azure AD Connectが構成できるよう、Webアプリケーションプロキシサーバーの管理者として**Enable-PSRemoting –Force**コマンドレットを実行する必要がある場合があります。



注： Remote PowerShellの信頼性の問題でこの手順に失敗した場合は、Webアプリケーションプロキシサーバーをドメインに参加させてみてください。

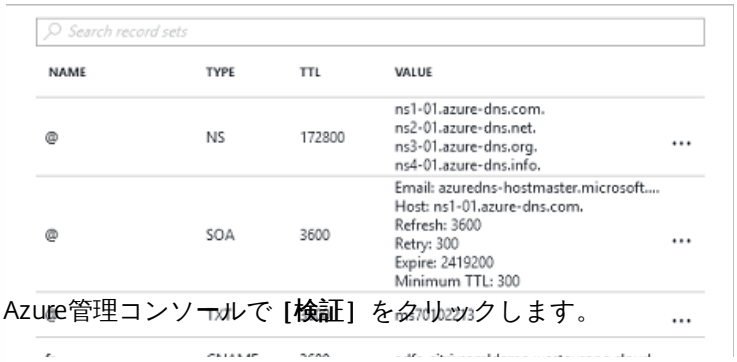
© 1999-2017 Citrix Systems, Inc. All rights reserved.

ウィザードの残りの手順については、標準の管理者パスワードを使用して、ADFSのサービスアカウントを作成します。Azure AD Connectにより、DNSゾーンの所有権の検証が求められます。

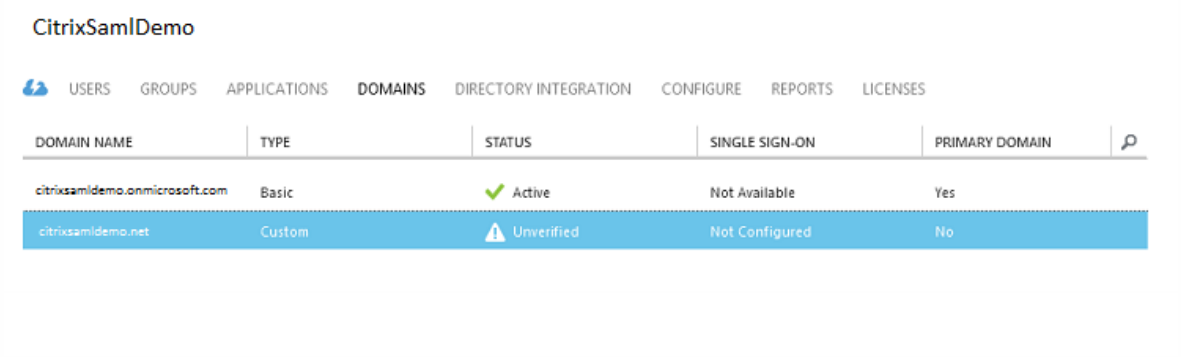


TXTレコードとMXレコードをAzureのDNSアドレスレコードに追加します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

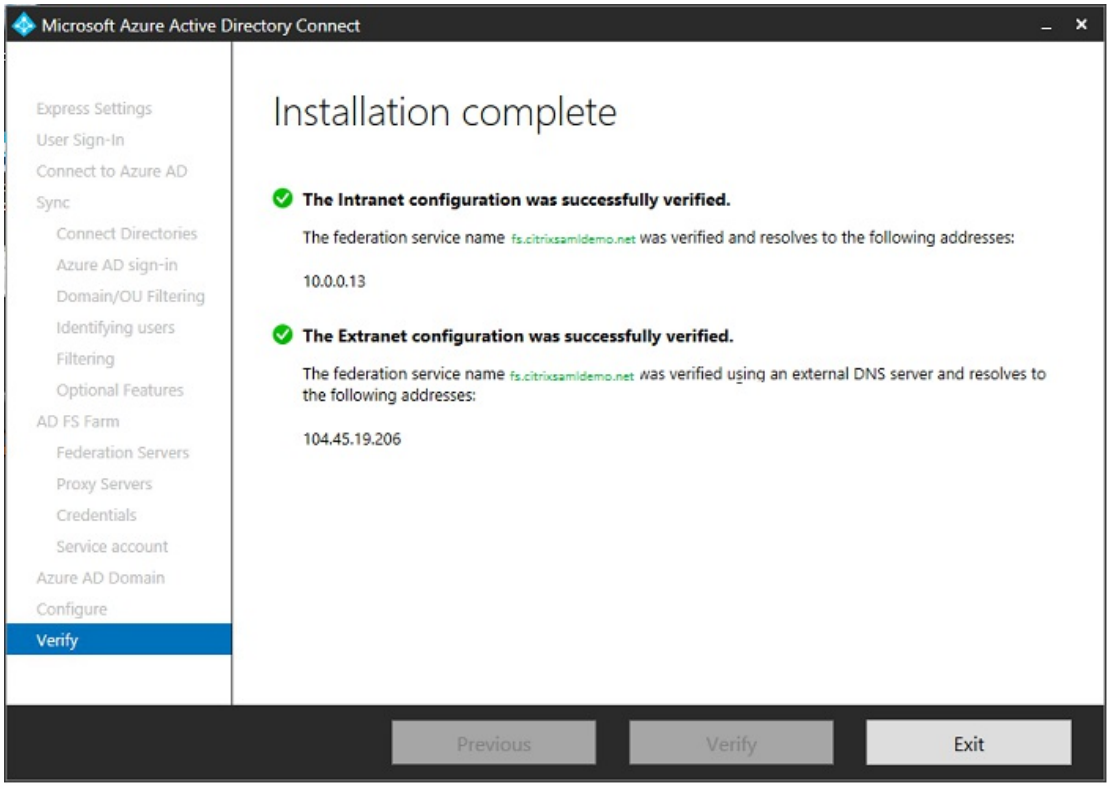


Azure管理コンソールで［検証］をクリックします。



注： この手順に失敗した場合は、Azure AD Connectを実行する前にドメインを検証します。

完了すると、外部アドレスfs.citrixsamldemo.netがポート443で接続されます。



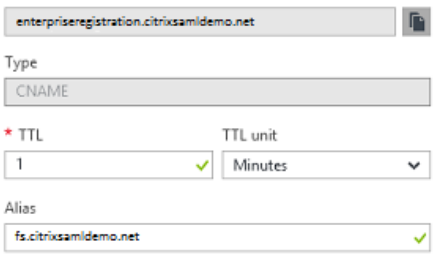
Azure ADへの参加の有効化

Windows 10がAzure ADへの参加を実行するよう、メールアドレスを入力すると、ADFSを指す必要があるCNAME DNSレコー

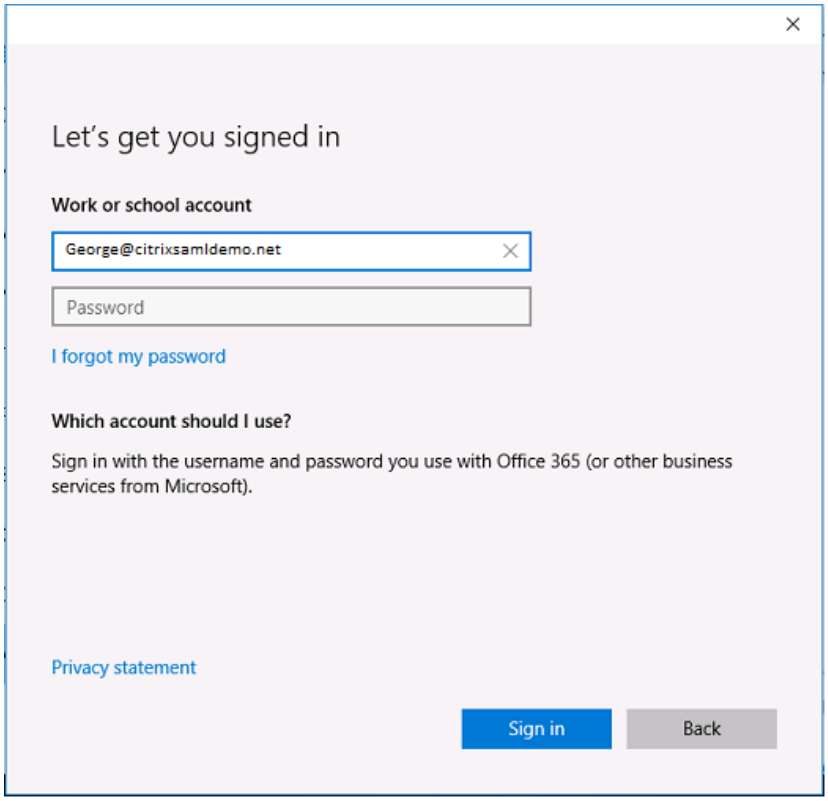
© 1999-2017 Citrix Systems, Inc. All rights reserved.

ドの作成にDNSサフィックスが使用されます（enterpriseregistration.）。

この例ではfs.citrixsamldemo.netです。

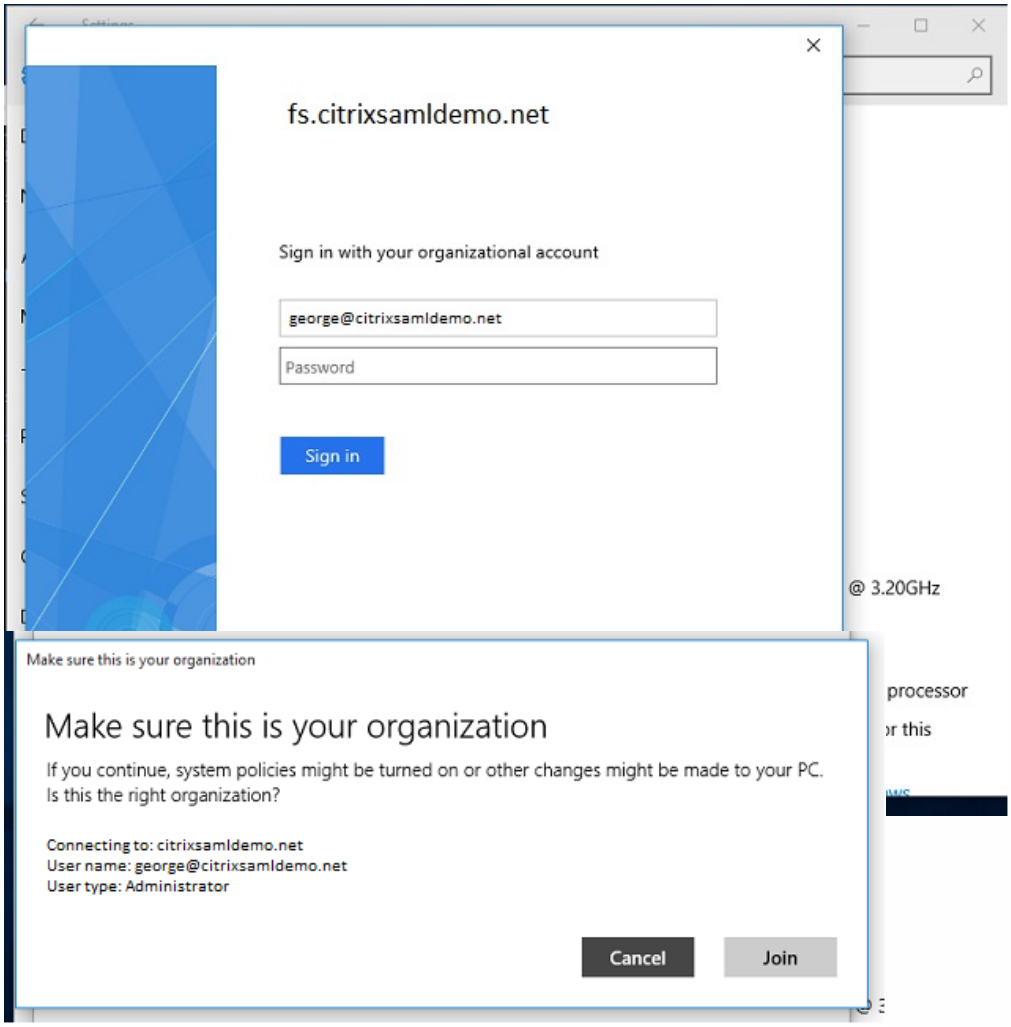


パブリックCAを使用していない場合は、WindowsがADFSサーバーを信頼するよう、ADFSのルート証明書をWindows 10コンピューターにインストールします。 あらかじめ生成された標準のユーザーアカウントを使用して、Azure ADドメインに参加します。



UPNは、ADFSドメインコントローラーで認識されるUPNと一致する必要があることに注意してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

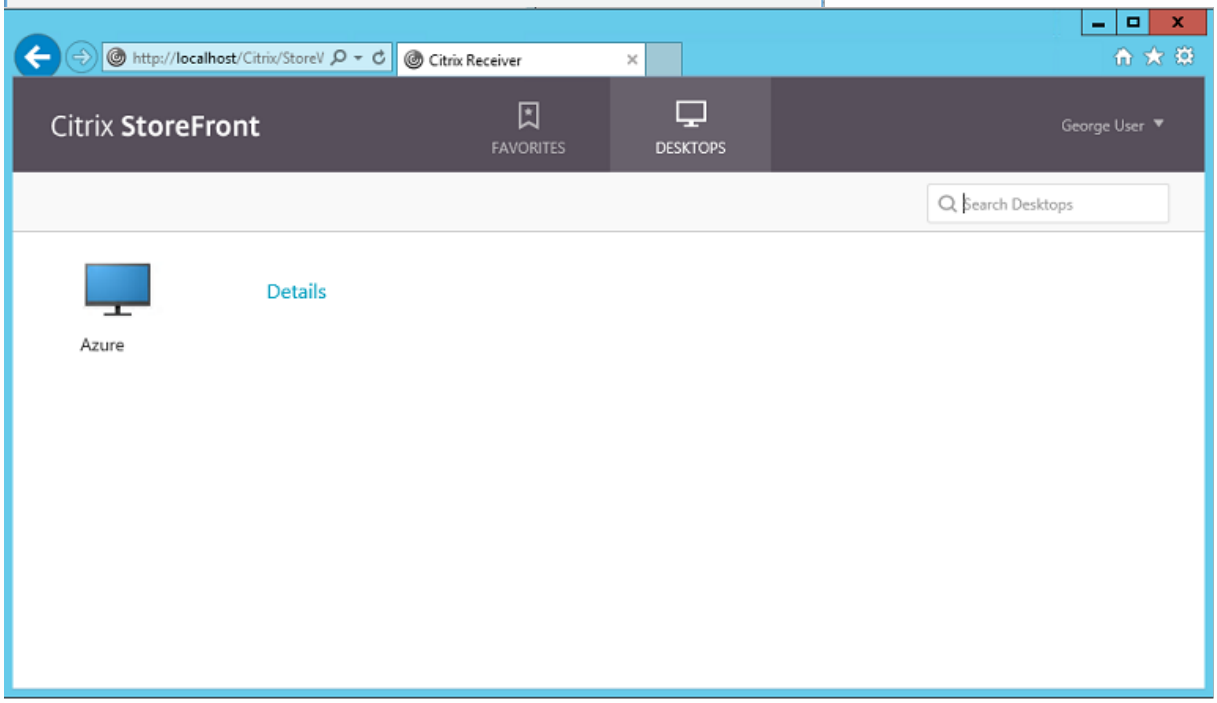


メールアドレスを使用してマシンの再起動とログオンを行い、Azure ADへの参加が正常に行われたことを検証します。 ログオンするとMicrosoft Edgeが起動してhttp://myapps.microsoft.comに接続します。このWebサイトでは、シングルサインオンが自動的に使用されます。

XenAppまたはXenDesktopのインストール

通常の方法で、XenAppまたはXenDesktop ISOから、Delivery ControllerおよびVDA仮想マシンをAzureに直接インストールすることができます。

この例では、StoreFrontはDelivery Controllerと同じサーバーにインストールされています。 VDAはスタンドアロンのWindows 2012 R2用RDSワーカーとしてインストールされ、Machine Creation Servicesとは統合していません（ただしオプションで構成することができます）。 作業を続行する前に、ユーザーGeorge@citrixsamldemo.netがパスワードで認証できることを確認します。

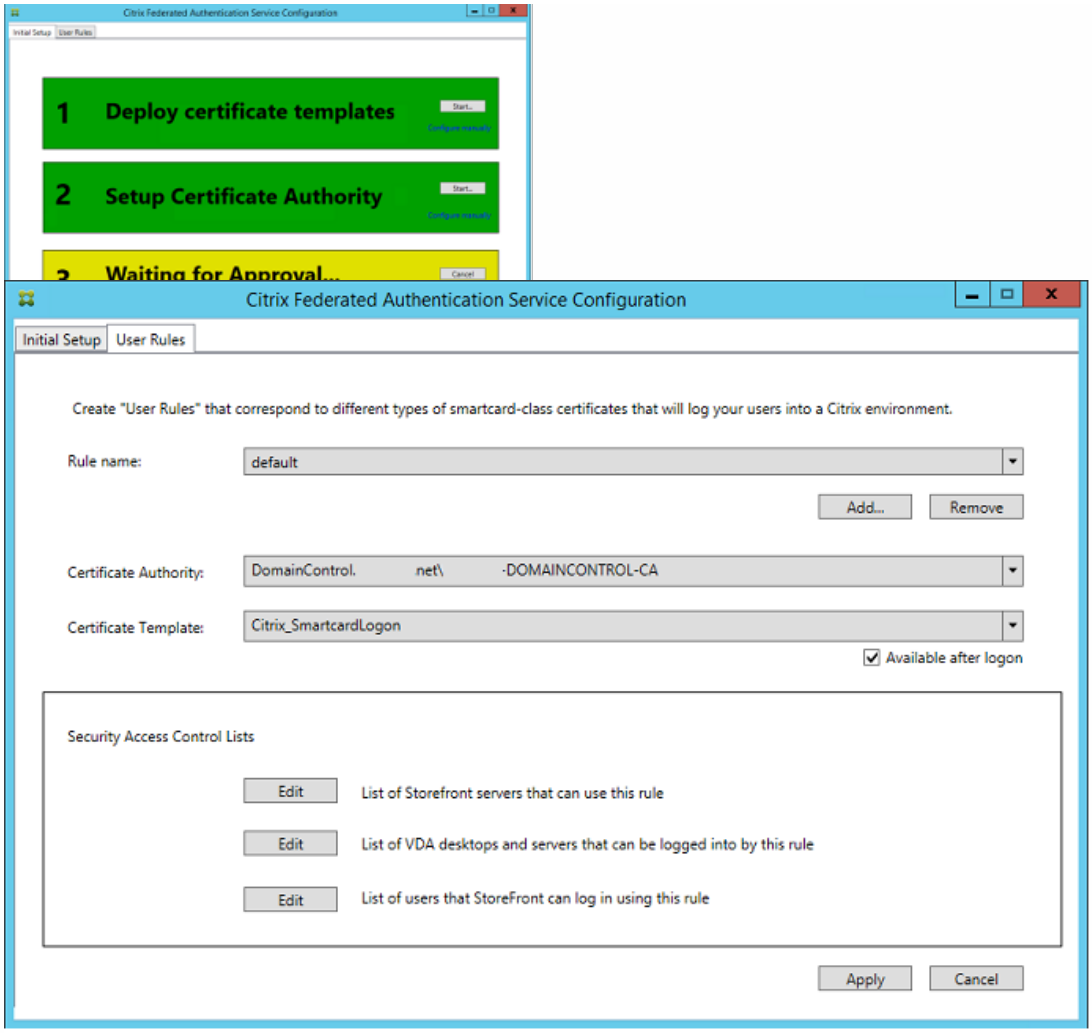


StoreFrontがユーザー資格情報なしに認証できるよう、**Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShellコマンドレットをControllerで実行します。

Federated Authentication Serviceのインストール

Federated Authentication Service（FAS）コンポーネントをADFSサーバーにインストールしてControllerのルールを構成し、信頼されたStoreFrontとして機能するように設定します。

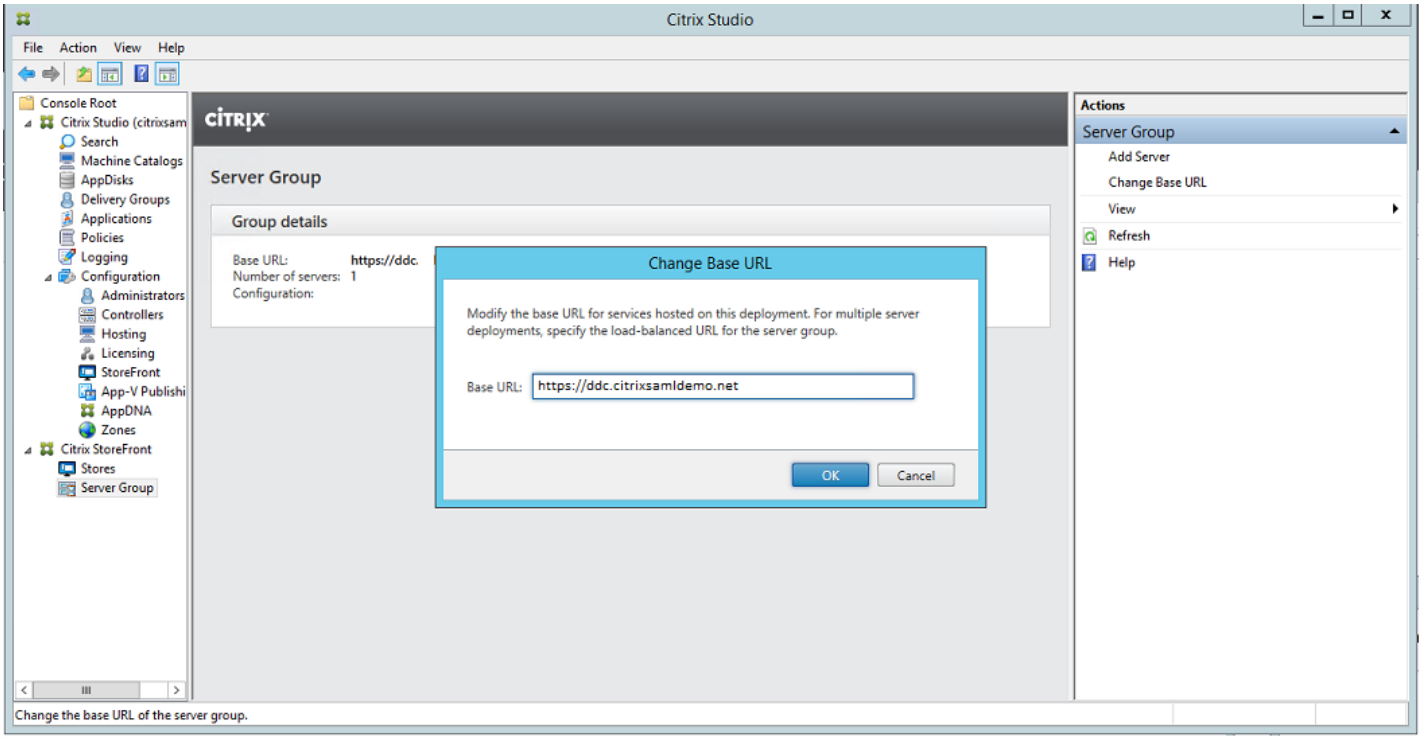
© 1999-2017 Citrix Systems, Inc. All rights reserved.



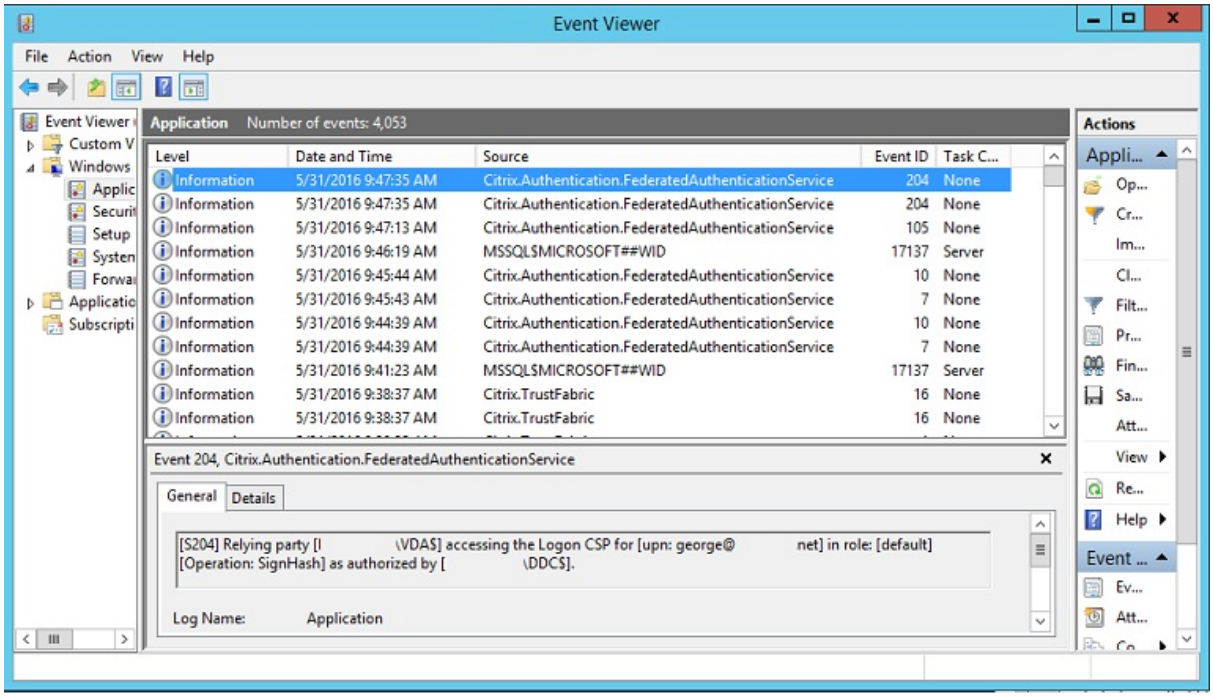
StoreFrontの構成

Delivery Controllerのコンピューター証明書を要求します。また、ポート443にIISバインドを設定し、StoreFrontのベースアドレスをhttps:に変更して、IISおよびStoreFrontでHTTPSが使用されるように構成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



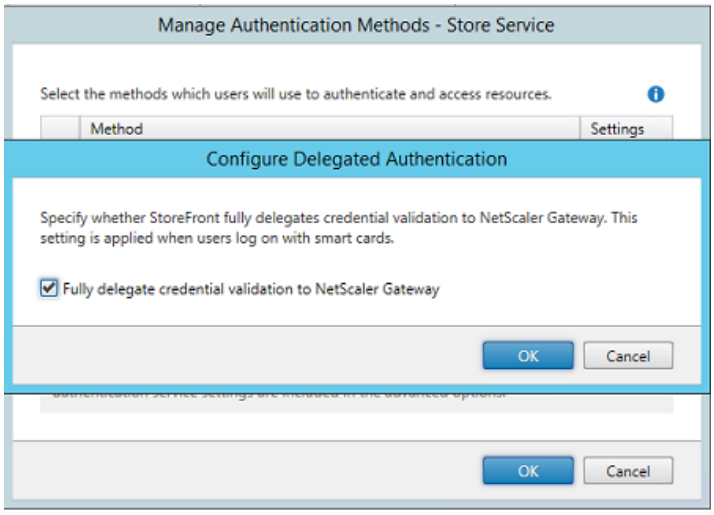
StoreFrontでFASサーバーが使用されるように構成し（「Federated Authentication Service」のPowerShellスクリプトを使用します）、Azure内で内部テストを行います。FASサーバーのイベントビューアーをチェックして、ログオンにFASが使用されることを確認します。



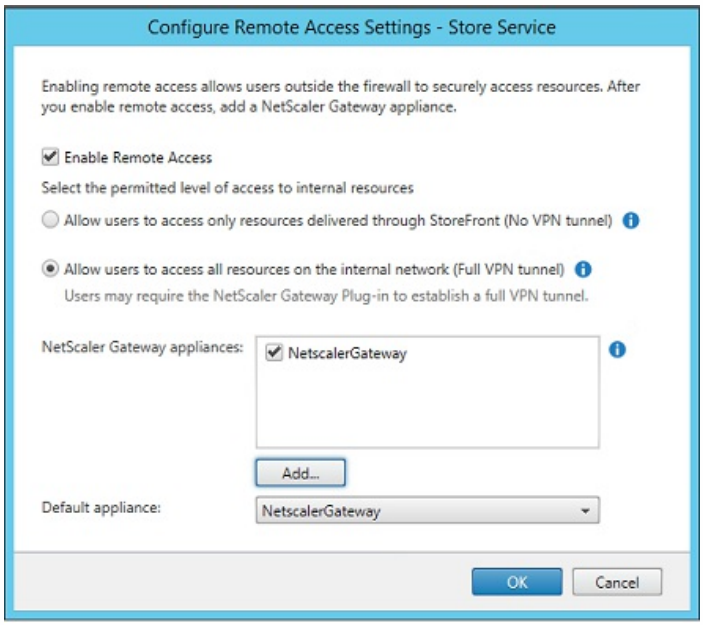
StoreFrontがNetScalerを使用するように構成

StoreFront管理コンソールの**[認証方法の管理]** GUIを使用して、StoreFrontが認証にNetScalerを使用するよう構成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



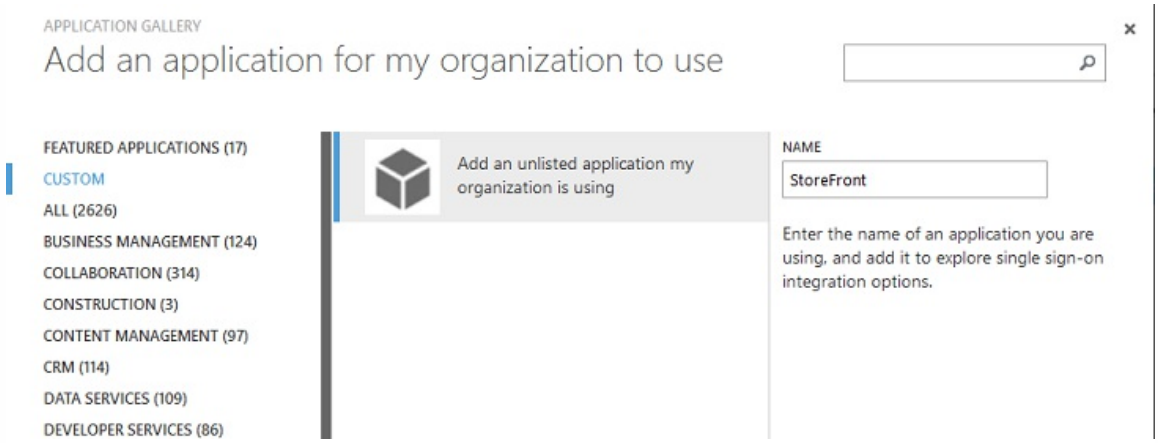
NetScaler認証オプションを統合するには、Secure Ticket Authority（STA）の構成およびNetScaler Gatewayアドレスの構成を行います。



新しいAzure ADアプリケーションをStoreFrontへのシングルサインオンに構成

このセクションでは、Azure AD SAML 2.0シングルサインオン機能を使用します。現在は、Azure Active Directoryプレミアムサブスクリプションが必要です。 Azure AD管理ツールで **[新しいアプリケーション]** を選択し、 **[ギャラリーからアプリケーションを追加します]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



［カスタム］カテゴリの［私の組織で使用している、一覧にないアプリケーションを追加］を選択して、ユーザーが使用する新しいカスタムアプリケーションを作成します。

アイコンの構成

縦横215ピクセルの画像を作成して［構成］ページにアップロードし、アプリケーションのアイコンとして使用します。

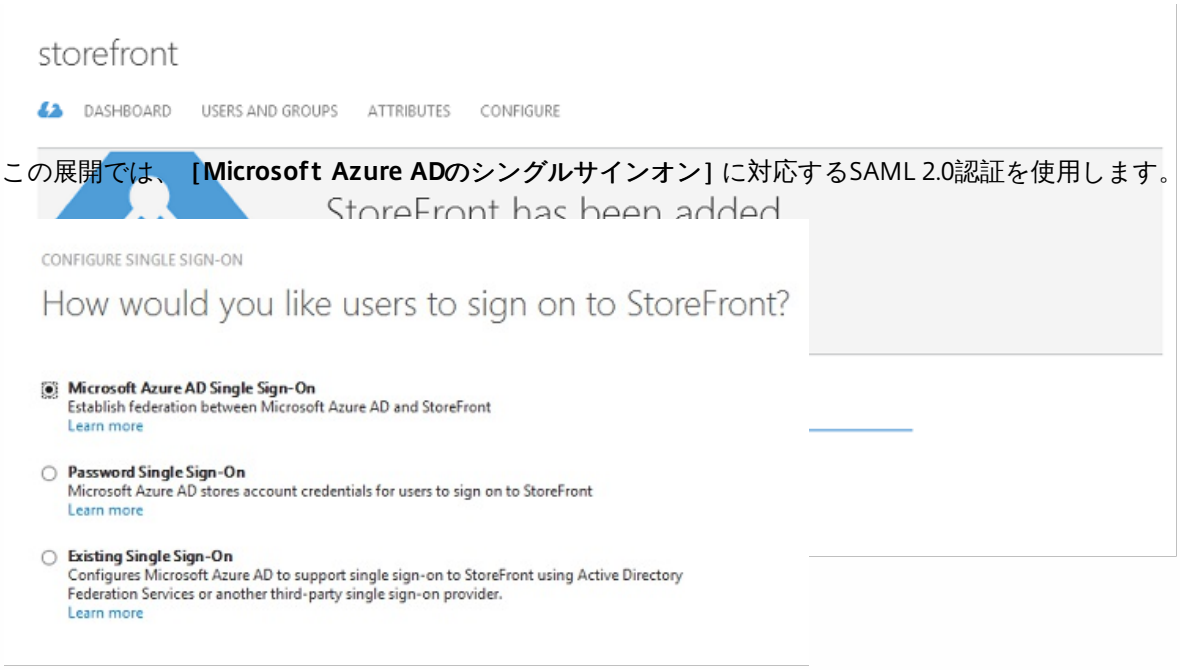


SAML認証の構成

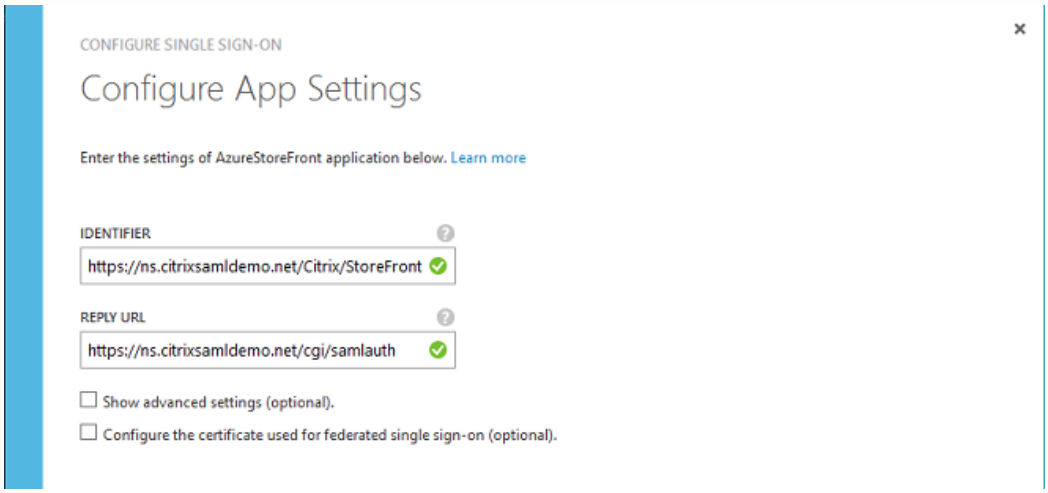
アプリケーションダッシュボードの概要ページに戻り、**[シングルサインオンの構成]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この展開では、**[Microsoft Azure ADのシングルサインオン]** に対応するSAML 2.0認証を使用します。

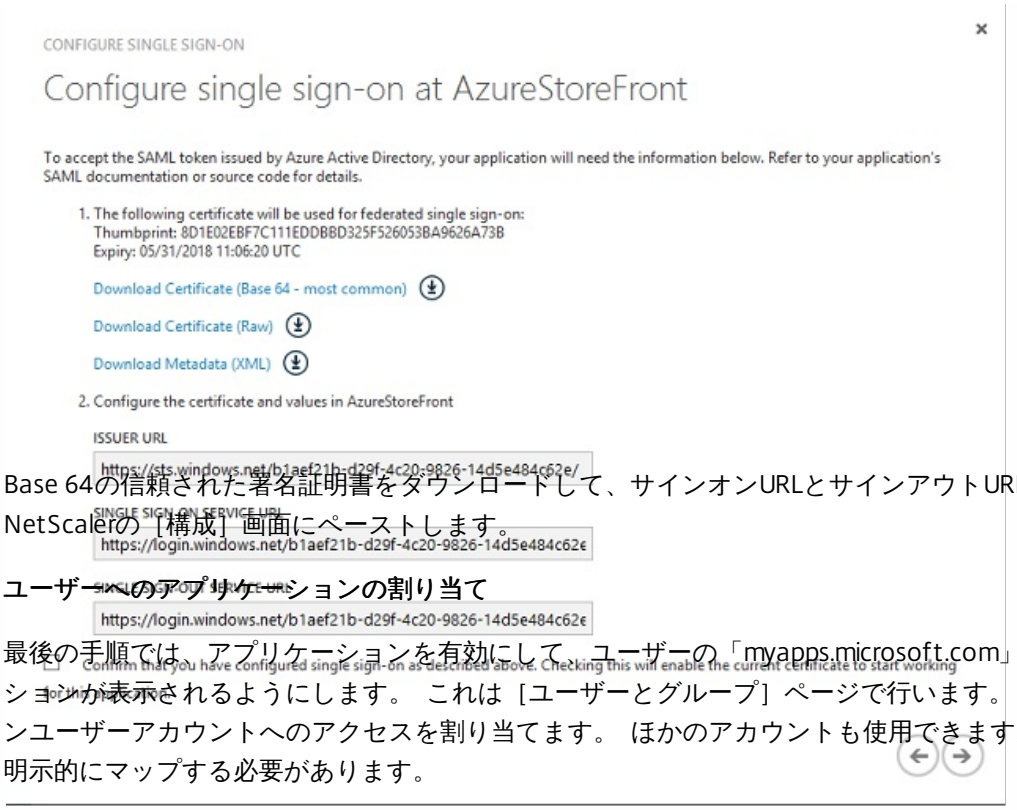


[識別子] は任意の文字列です（NetScalerに提供された構成と一致する必要があります）。この例では、**[応答URL]** がNetScalerサーバーの/cgi/samlauthになっています。



次のページには、NetScalerをAzure ADの証明書利用者として構成するために使用される情報が含まれています。

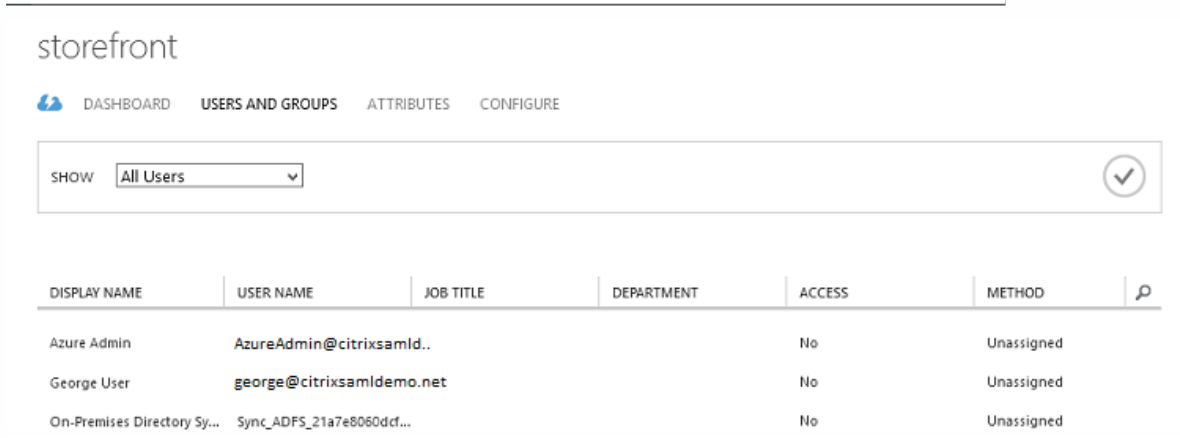
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Base 64の信頼された署名証明書をダウンロードして、サインオンURLとサインアウトURLをコピーします。 これらをNetScalerの［構成］画面にペーストします。

ユーザーへのアプリケーションの割り当て

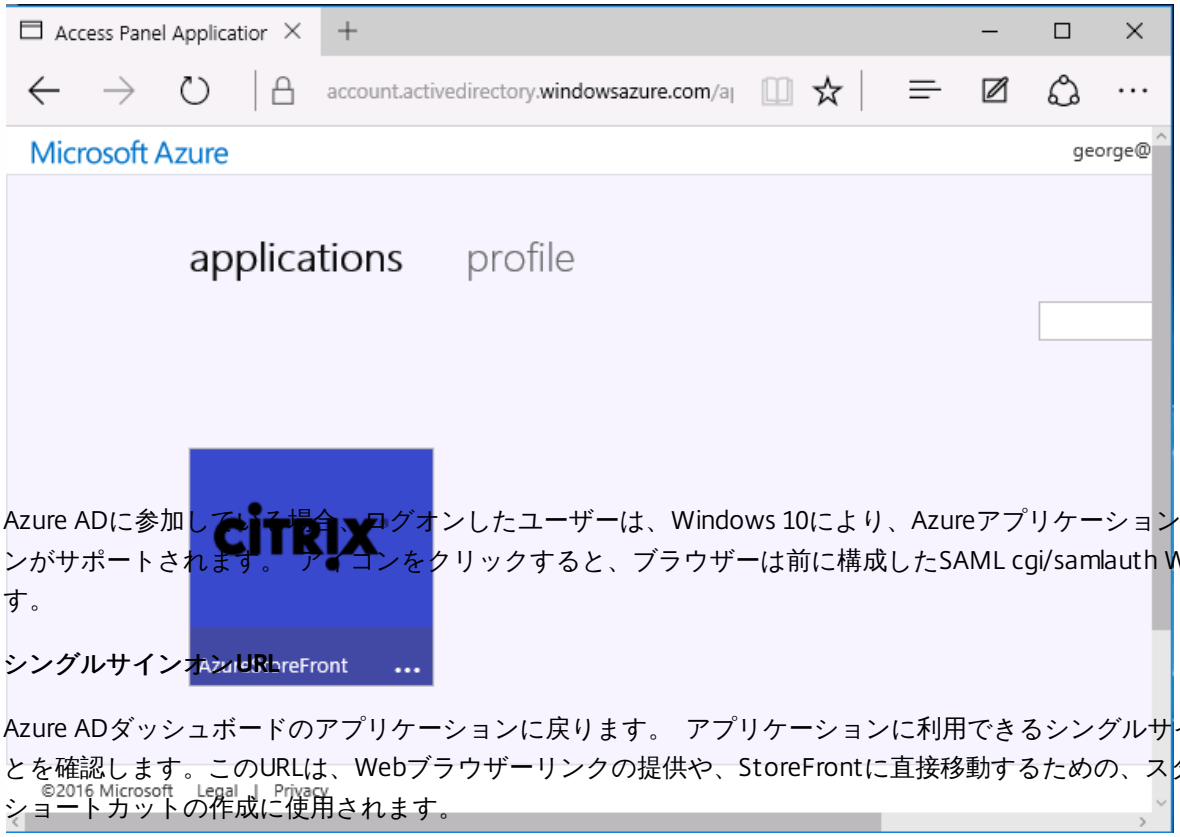
最後の手順では、アプリケーションを有効にして、ユーザーの「myapps.microsoft.com」コントロールページにアプリケーションが表示されるようにします。 これは［ユーザーとグループ］ページで行います。 Azure AD Connectが同期したドメインユーザーアカウントへのアクセスを割り当てます。 ほかのアカウントも使用できますが、@パターンに従っていないため明示的にマップする必要があります。



MyAppsページ

アプリケーションが構成されると、https://myapps.microsoft.comで、Azureアプリケーションのユーザー一覧に表示されます。

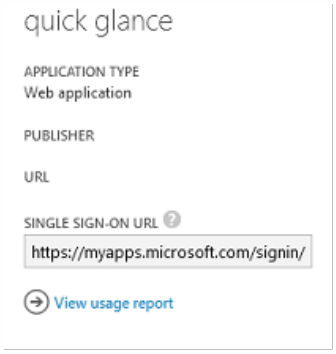
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Azure ADに参加している場合、ログオンしたユーザーは、Windows 10により、Azureアプリケーションへのシングルサインオンがサポートされます。 アイコンをクリックすると、ブラウザーは前に構成したSAML cgi/samlauth Webページに移動します。

シングルサインオンURL

Azure ADダッシュボードのアプリケーションに戻ります。 アプリケーションに利用できるシングルサインオンURLがあることを確認します。このURLは、Webブラウザーリンクの提供や、StoreFrontに直接移動するための、スタートメニューのショートカットの作成に使用されます。

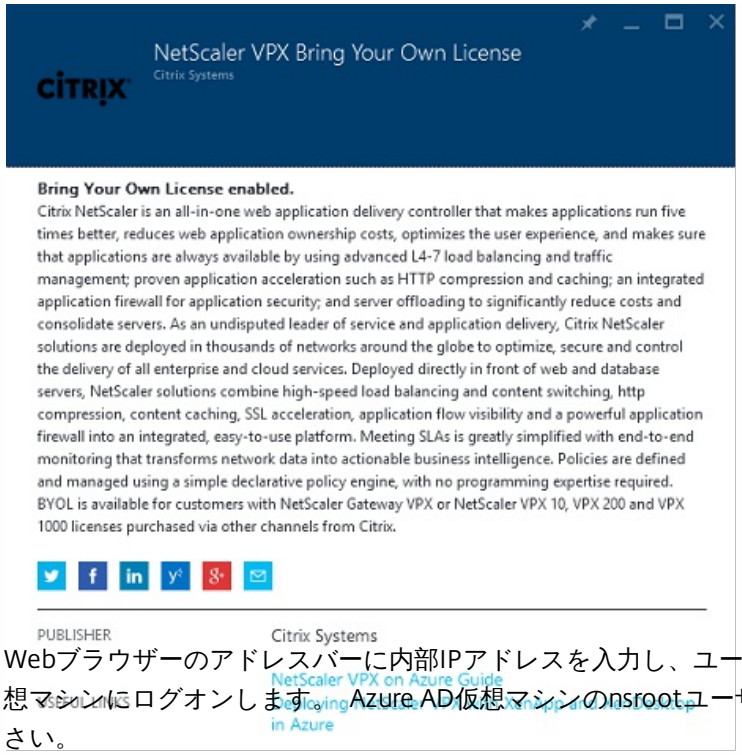


このURLをWebブラウザーにペーストして、前に構成したNetScaler cgi/samlauth Webページに、Azure ADがリダイレクトするようにします。 これが機能するのは、割り当てられたユーザーだけです。また、シングルサインオンが利用できるのは、Windows 10のAzure ADに参加しているログオンセッションだけです。（そのほかのユーザーには、Azure ADの資格情報の入力が求められます。）

NetScaler Gatewayのインストールと構成

この例では、展開へのリモートアクセスに、NetScalerを実行する独立した仮想マシンを使用します。 仮想マシンはAzureストアで購入できます。 この例では、NetScaler 11.0の「Bring your own License」バージョンを使用しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

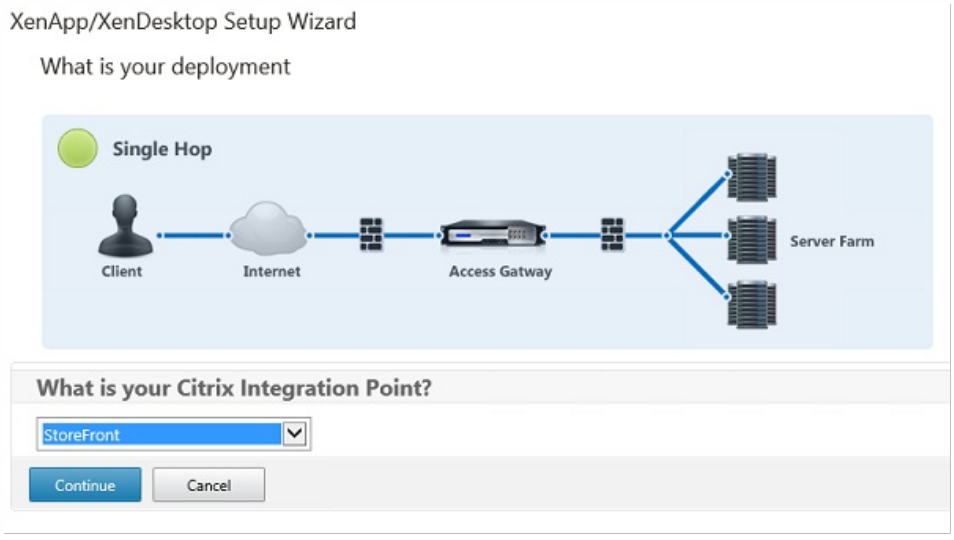


Webブラウザーのアドレスバーに内部IPアドレスを入力し、ユーザー認証の際に指定された資格情報を使用して、NetScaler仮想マシンにログオンします。Azure AD仮想マシンのnsrootユーザーのパスワードを変更する必要があることに注意してください。

ライセンスを追加し、各ライセンスファイルが追加されたら **[再起動]** を選択して、DNSリゾルバーがMicrosoftドメインコントローラーをポイントするようにします。

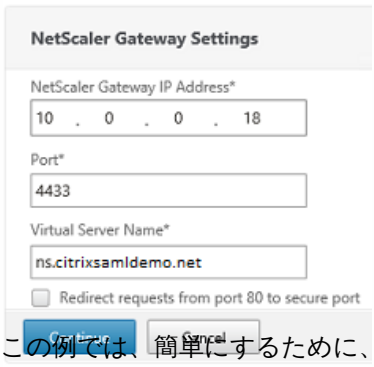
XenAppおよびXenDesktopセットアップウィザードの実行

この例では、SAMLを使用しない、シンプルなStoreFront統合を構成することから始めます。この展開が機能するようになってから、SAMLのログオンポリシーが追加されます。

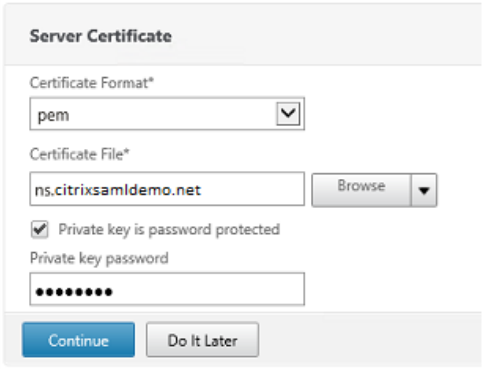


NetScalerおよびStoreFrontの標準設定を選択します。Microsoft Azureでの使用のため、この例ではポート443ではなく、ポート4433を構成します。 あるいは、ポート転送したり、NetScaler管理Webサイトを再マップしたりすることもできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



この例では、簡単にするために、ファイルに保存された既存のサーバー証明書と秘密キーをアップロードします。



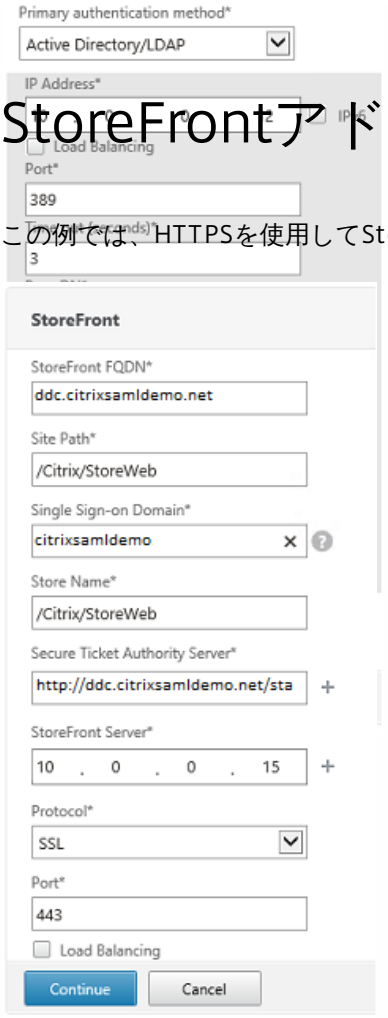
ADアカウント管理のためのドメインコントローラーの構成

ドメインコントローラーはアカウント解決に使用されるため、そのIPアドレスをプライマリ認証方法に追加します。 ダイアグボックスの各フィールドで求められる形式に注意してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFrontアドレスの構成

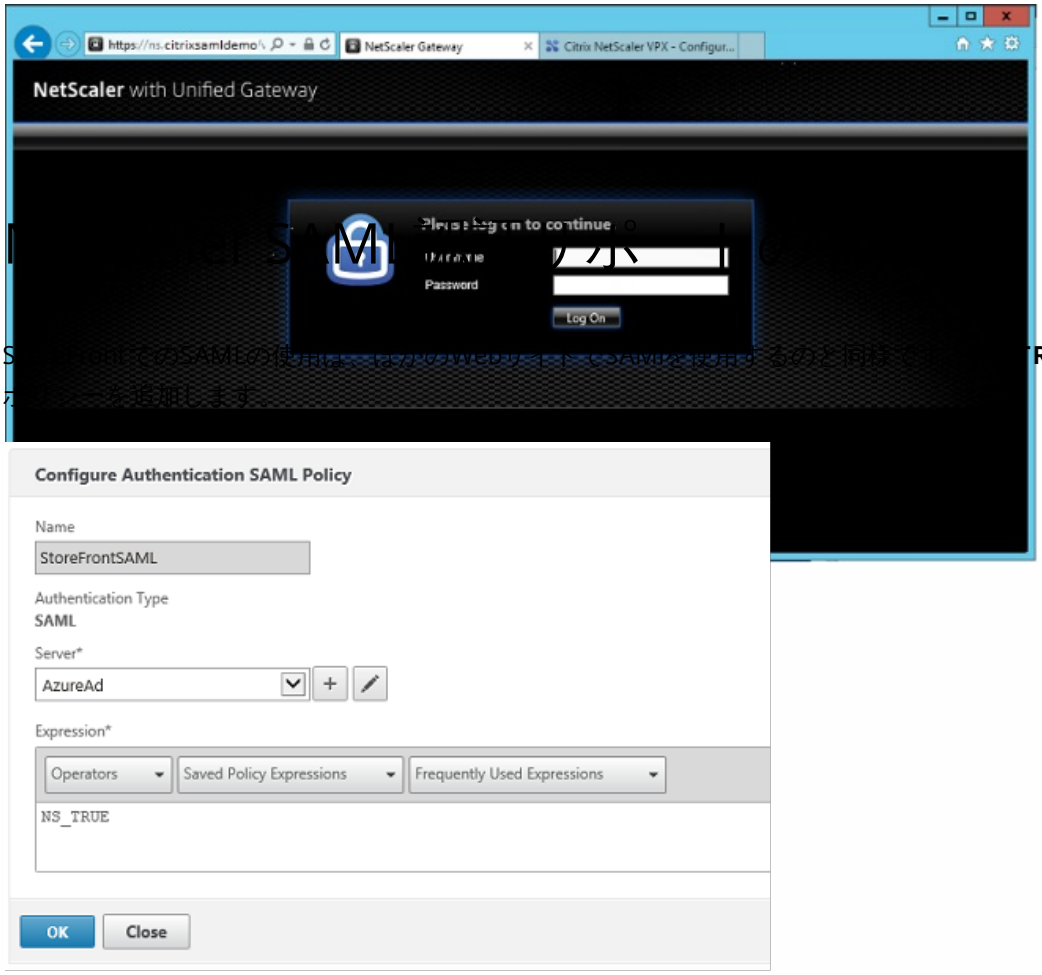
この例では、HTTPSを使用してStoreFrontが構成されているため、SSLプロトコルのオプションを選択します。



NetScalerの展開を検証

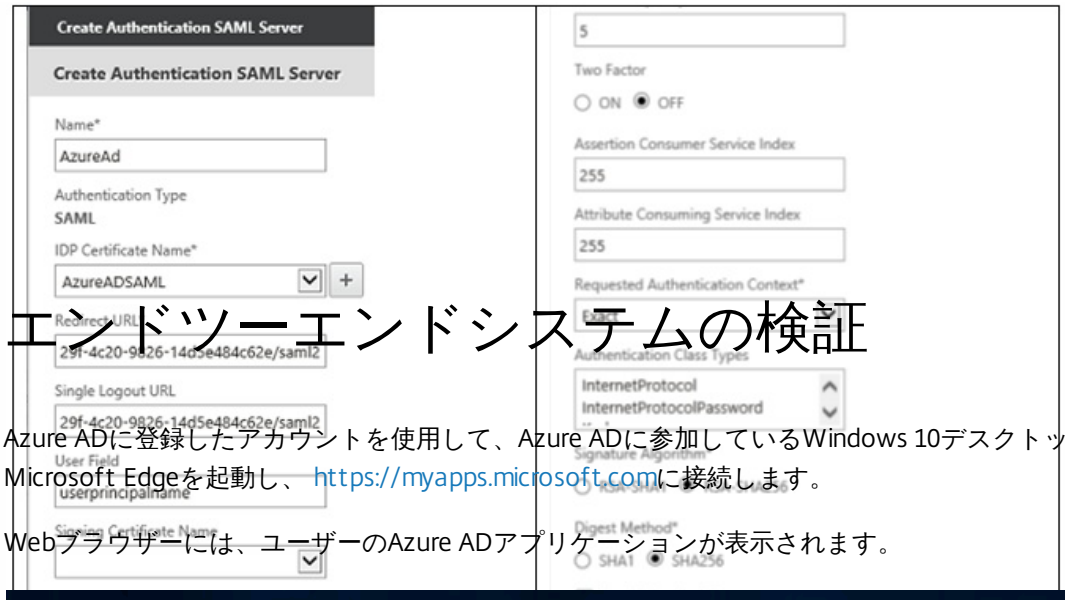
NetScalerに接続し、ユーザー名とパスワードを使用して、認証と起動が正常に行われることを確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Azure ADから前に取得した情報を使用して、新しいSAML IdPサーバーを構成します。

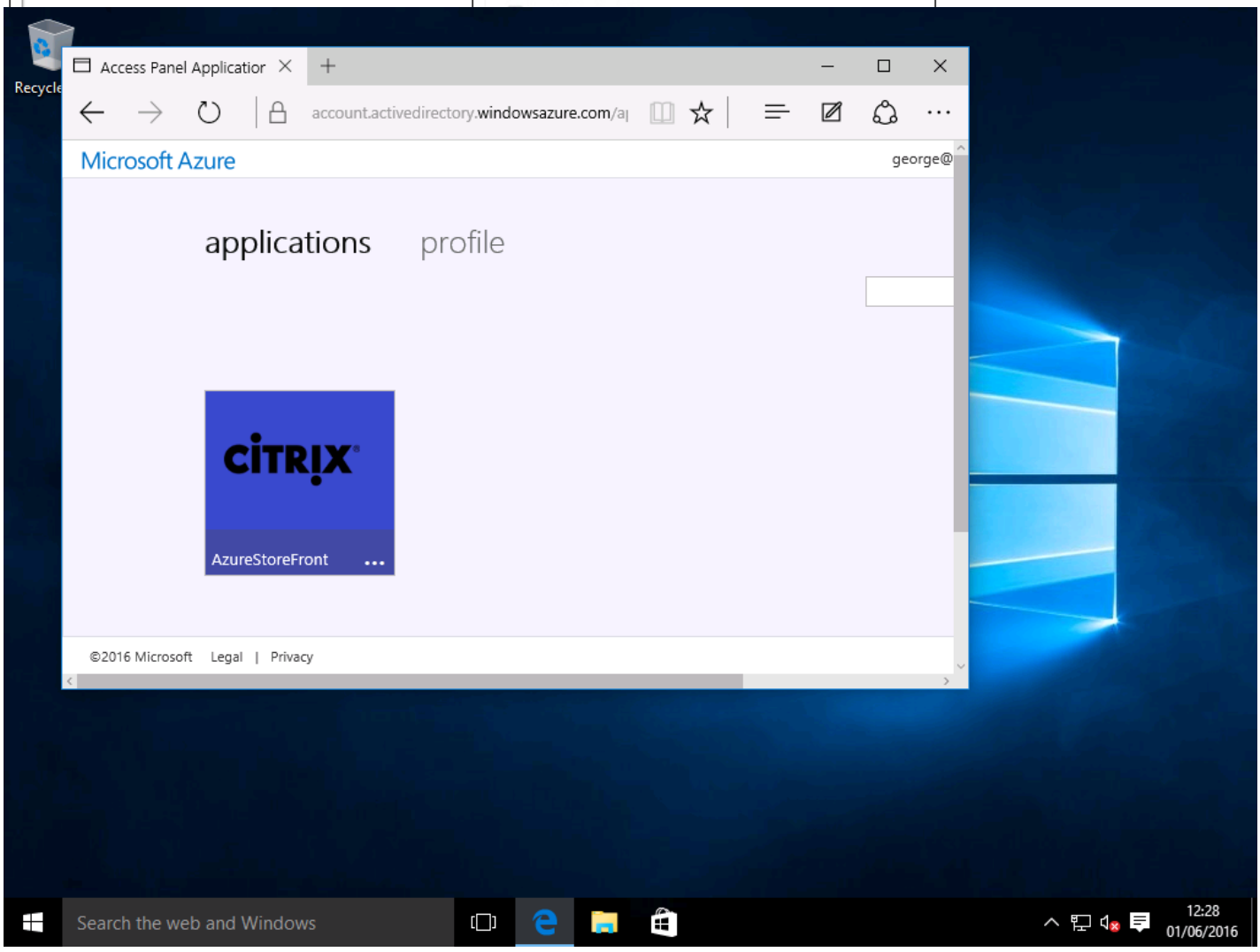
© 1999-2017 Citrix Systems, Inc. All rights reserved.



エンドツーエンドシステムの検証

Azure ADに登録したアカウントを使用して、Azure ADに参加しているWindows 10デスクトップにログオンします。
Microsoft Edgeを起動し、 https://myapps.microsoft.comに接続します。

Webブラウザーには、ユーザーのAzure ADアプリケーションが表示されます。



アイコンをクリックすると認証されたStoreFrontサーバーにリダイレクトされることを確認します。

同様に、シングルサインオンURLを使用した直接接続、およびNetScalerのサイトへの直接接続により、Microsoft Azureとの間でリダイレクトされることを確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

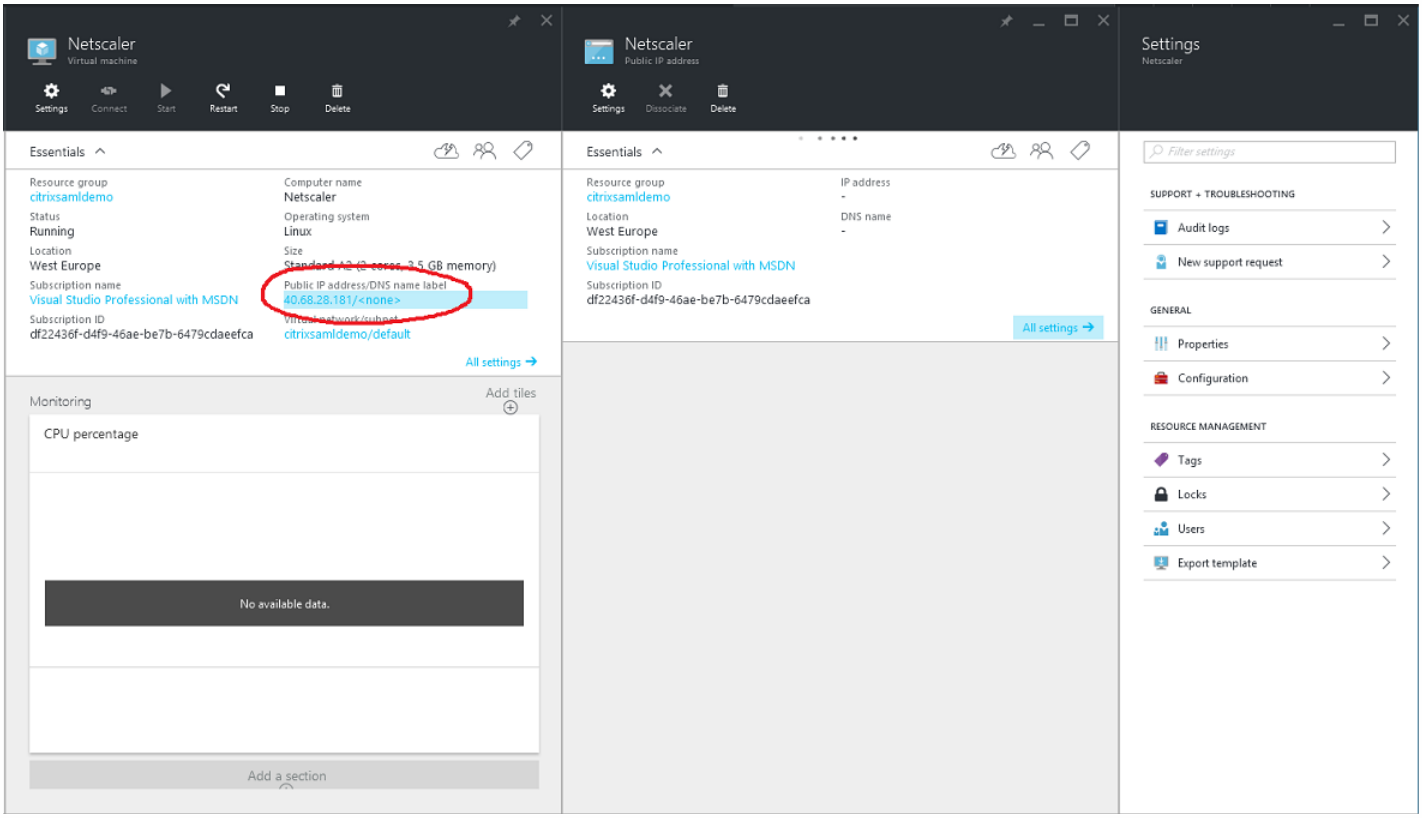
最後に、Azure ADに参加していないマシンも同じURLで動作することを確認します（ただし、最初の接続時に、Azure ADへの明示的なサインオンが1回行われます）。

付録

Azureで仮想マシンをセットアップする場合は、構成に必要な標準オプションがいくつかあります。

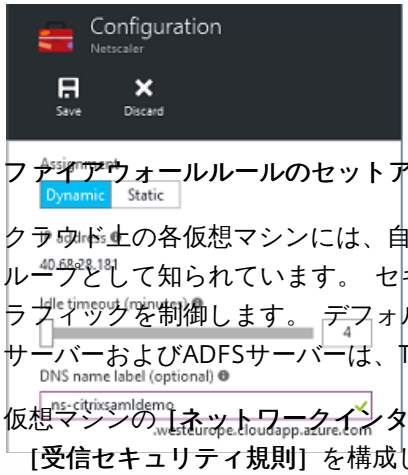
パブリックIPアドレスとDNSアドレスの入力

Azureは内部サブネット上で、すべての仮想マシンにIPアドレスを提供します（この例では10.*.*.*）。 デフォルトでは、動的に更新されたDNSラベルで参照できる、パブリックIPアドレスも提供されます。



[パブリックIPアドレス/DNS名]ラベルの**[構成]**を選択します。 仮想マシンのパブリックDNSアドレスを選択します。 これは、ほかのDNSゾーンファイルでのCNAME参照に使用でき、IPアドレスが再割り当てされた場合も、すべてのDNSレコードが正しく仮想マシンをポイントするようにします。

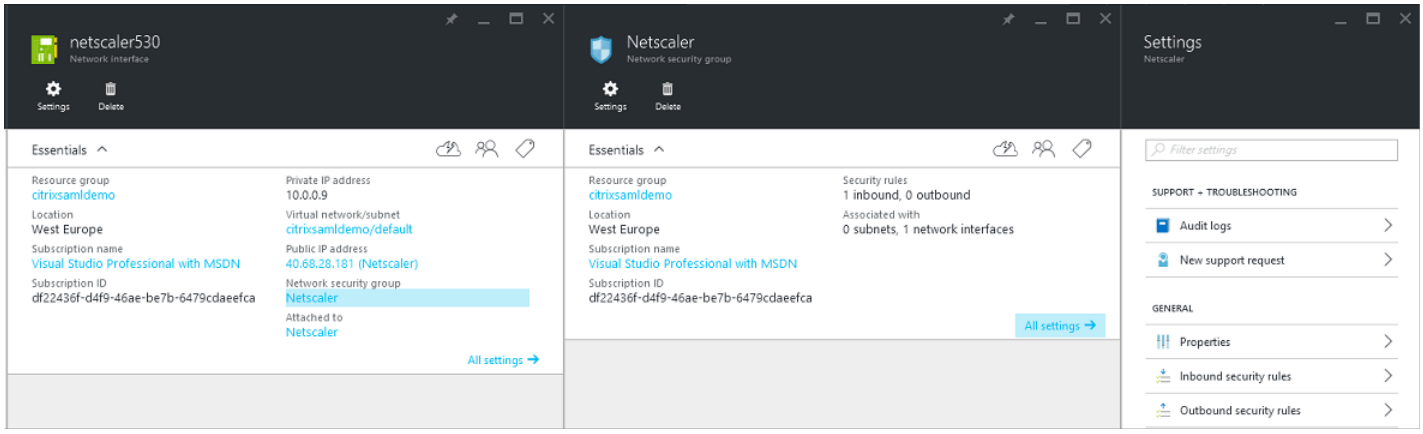
© 1999-2017 Citrix Systems, Inc. All rights reserved.



ファイアウォールルールのセットアップ（セキュリティグループ）

クラウド上の各仮想マシンには、自動的に適用されたファイアウォールルールのセットがあり、このセットはセキュリティグループとして知られています。 セキュリティグループはパブリックIPアドレスからプライベートIPアドレスに転送されるトラフィックを制御します。 デフォルトでは、Azureはすべての仮想マシンへのRDPの転送を許可します。 また、NetScalerサーバーおよびADFSサーバーは、TLSトラフィック（443）を転送する必要があります。

仮想マシンの **[ネットワークインターフェイス]** を開いて **[ネットワークセキュリティグループ]** ラベルをクリックします。 **[受信セキュリティ規則]** を構成し、適切なネットワークトラフィックを許可します。



関連情報

- FASのインストールと構成については、「Federated Authentication Service」を参照してください。
- 一般的なFAS環境については、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」では「方法」記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Systemの方法：構成と管理

Dec 05, 2017

次の「方法」記事では、Federated Authentication System（FAS）の高度な構成および管理について説明します。

- 秘密キー保護
- 証明機関の設定
- セキュリティとネットワークの管理
- Windowsログオンの問題のトラブルシューティング
- PowerShell SDKコマンドレットのヘルプファイル

関連情報

- FASのインストールと初期セットアップについては、「Federated Authentication Service」を参照してください。
- 「Federated Authentication Serviceのアーキテクチャの概要」では、FASの主要アーキテクチャの概要を説明し、より複雑なアーキテクチャに関するそのほかの記事へのリンクを掲載しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Serviceの証明機関の設定

Dec 05, 2017

この記事では、Citrix Federated Authentication Service（FAS）をFAS管理コンソールでサポートされていない証明機関（CA）サーバーと統合するための詳細設定について説明します。この説明では、FASが提供するPowerShell APIを使用します。この記事に記載されている説明を実行する前に、PowerShellの基礎知識を確認してください。

FASで使用するための複数CAサーバーのセットアップ

このセクションでは、複数のCAサーバーを使用して証明書を発行するための単一FASのセットアップ方法について説明します。 これにより、CAサーバーの負荷分散とフェールオーバーが可能になります。

手順1：FASが検出できるCAサーバーの数の確認

Get-FASMsCertificateAuthorityコマンドレットを使用して、FASが接続できるCAサーバーを特定します。次の例は、FASが3つのCAサーバーに接続できることを示しています。

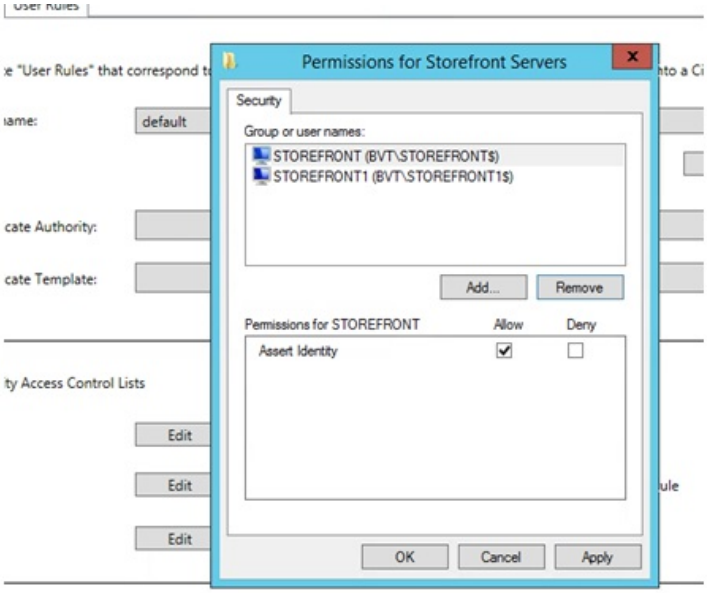
```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                          IsDefault PublishedTemplates
-------                          --------- ------------------
DC1.bvt.local\bvt-DC1-CA             False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
```

手順2：既存の証明書定義の変更

ロールの作成には、PowerShellではなくFAS管理コンソールを使用することをお勧めします。これにより、後から手動でSDLを追加する手間が省けます。次の例では、アクセスの規則が構成された「default」という名前の役割が作成されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

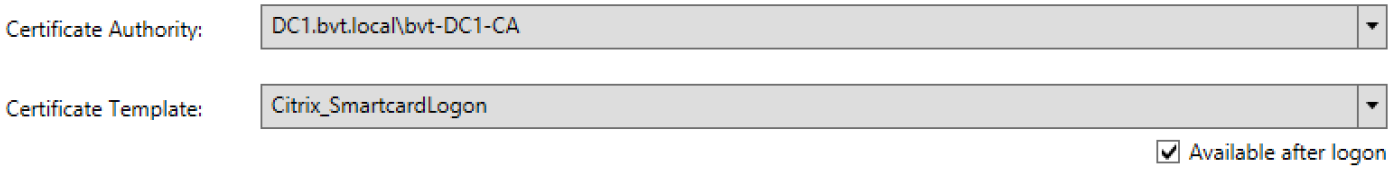


証明機関フィールドに複数のCAを追加（このリリースでは管理コンソールからの操作はサポートされていません）するには、証明書定義を構成する必要があります。最初に、証明書定義の名前が必要です。この名前を管理コンソールから特定できない場合は、Get-FASCertificateDefinitionコマンドレットを使用してください。

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

UIと同等のもの



証明書定義の名前が特定できたら、証明書定義を変更してCertificateAuthoritiesが1つではなく一覧で含まれるようにします。

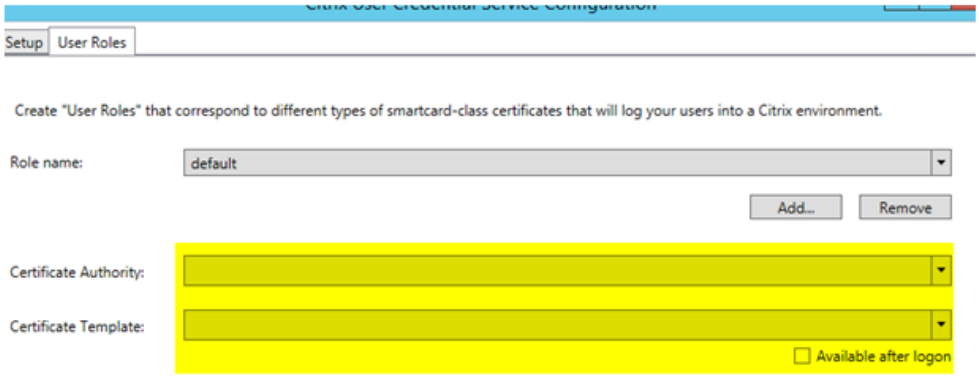
```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

Get-FASCertificateDefinitionコマンドレットによって以下が返されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

注： これを行った後、FAS管理コンソールは機能しなくなります。ロード時に「Certificate Authority」および「Certificate Template」の両方で空白のフィールドが表示されます。



機能としては、FASに問題はありません。管理コンソールを使用してアクセス規則を変更する場合は、手順2を繰り返してすべての証明機関を表示します。

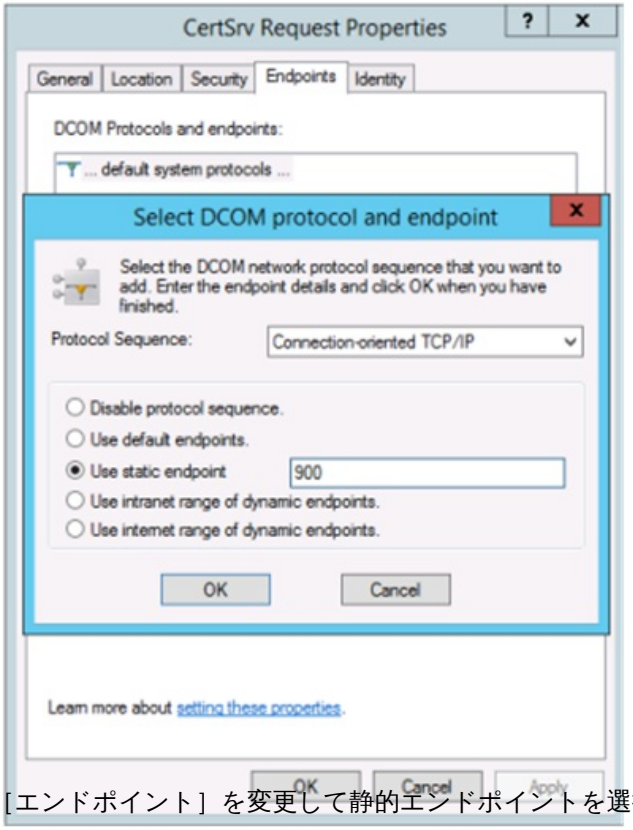
想定される動作の変更

FASサーバーを複数のCAサーバーで構成した後は、ユーザー証明書の生成は構成済みのすべてのCAサーバー間で配信されます。さらに、構成済みのCAサーバーのうちいずれかでエラーが発生すると、FASサーバーは別の使用可能なCAサーバーに切り替えます。

Microsoft CAをTCPアクセス用に構成する

デフォルトでは、Microsoft CAはアクセスにDCOMを使用します。この場合、ファイアウォールの実装が複雑になるため、静的TCPポートに切り替えることができます。Microsoft CAでDCOM構成パネルを開き、「CertSrv要求」DCOMアプリケーションのプロパティを編集します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[エンドポイント]を変更して静的エンドポイントを選択し、TCPポート番号を指定します（上の図では900です）。

Microsoft CAを再起動して、証明書要求を送信します。「netstat –a –n –b」を実行する場合は、certsvrがポート900をリスンしていることを確認する必要があります。

```
  TCP    0.0.0.0:636            dc:0                   LISTENING
[lsass.exe]
  TCP    0.0.0.0:900            dc:0                   LISTENING
[certsrv.exe]
  TCP    0.0.0.0:3268           dc:0                   LISTENING
[lsass.exe]
  TCP    0.0.0.0:3269           dc:0                   LISTENING
```

DCOMにはRPCポートを使用するネゴシエーションステージがあるため、FASサーバー（またはCAを使用するその他のマシン）を構成する必要はありません。 クライアントがDCOMを使用する必要がある場合、クライアントは証明書サーバーのDCOM RPC Serviceに接続して特定のDCOMサーバーへのアクセスを要求します。 これによってポート900が開かれ、DCOMサーバーはFASサーバーに接続方法を指示します。

ユーザー証明書の事前生成

ユーザー証明書がFASサーバー内で事前生成されると、ユーザーのログオンにかかる時間が大幅に短縮されます。次のセクションでは、単一または複数のFASサーバーでユーザー証明書を事前生成する方法について説明します。

Active Directoryユーザーの一覧を取得します。

AD に対してクエリを実行し、ユーザーの一覧を次の例のようにファイル（.csvファイルなど）に保存することにより、証明書の生成を改善することができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Import-Module ActiveDirectory

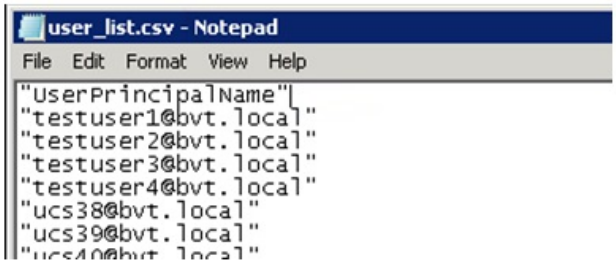
$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

if ($searchbase –ne “”) {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter ","
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

Get-ADUserは、ユーザーの一覧を要求するための標準コマンドレットです。上述の例にはUserPrincipalNameでステータスが「有効」のユーザーのみを一覧表示するためのフィルター引数が含まれています。

SearchBase引数によって、ADのユーザー検索が制限されます。すべてのユーザーをADに含めたい場合、これを省略できます。注：このクエリによって、多数のユーザーが返される可能性があります。

CSVの外観は、次のようになります。



FASサーバー

以下のPowerShellスクリプトでは、以前生成されたユーザーの一覧を使用してユーザー証明書の一覧が作成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

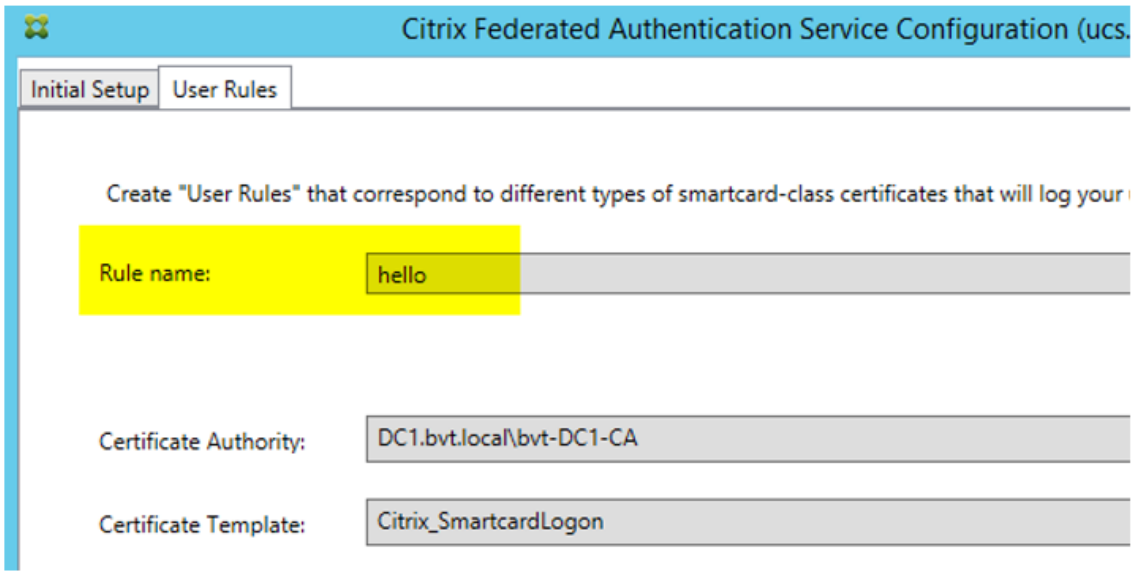
```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ) {
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ) {
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

複数のFASサーバーが存在する場合は、特定のユーザーの証明書がメインサーバーで1回、フェールオーバーサーバーで1回の合計2回生成されます。

上述の例は「default」という名前の規則の場合です。規則名が異なる場合（「hello」など）は、スクリプトの$rule変数を変更してください。



登録機関証明書を更新します。

複数のFASサーバーを使用中の場合は、ログオン中のユーザーに影響することなくFAS認証証明書を更新できます。 注： GUIを使用してFASの権限を取り消したり再び付与したりすることもできますが、これによってFASの構成オプションがリセットされます。

以下の手順を実行します。

1. 新しい認証証明書を作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

New-FasAuthorizationCertificate

2. 次のコマンドによって返される新しい認証証明書のGUIDをメモします。

Get-FasAuthorizationCertificate

3. FASサーバーをメンテナンスモードにします。

Set-FasServer –Address -MaintenanceMode $true

4. 新しい認証証明書を置換します。

Set-FasCertificateDefinition –AuthorizationCertificate

5. FASサーバーのメンテナンスモードを解除します。

Set-FasServer –Address -MaintenanceMode $false

6. 古い認証証明書を削除します。

Remove-FasAuthorizationCertificate

関連情報

- FASのインストールと構成については、「Federated Authentication Service」を参照してください。
- 一般的なFAS環境については、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」ではそのほかの「方法」に関する記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Serviceの秘密キー保護

Dec 05, 2017

はじめに

秘密キーはNetwork Serviceアカウントを使用して保存され、デフォルトでエクスポート不可としてマークされます。

秘密キーには2つの種類があります。

- 登録機関（RA）証明書に関連付けられている、Citrix_RegistrationAuthority証明書テンプレートからの秘密キー
- ユーザー証明書に関連付けられている、Citrix_SmartcardLogon証明書テンプレートからの秘密キー

RA証明書にはCitrix_RegistrationAuthority_ManualAuthorization（デフォルトで24時間有効）およびCitrix_RegistrationAuthority（デフォルトで2年間有効）の2つの種類があります。

> FAS管理コンソールの初回セットアップの手順3で、管理者が［許可する］をクリックすると、FASサーバーによってキーペアが生成され、証明書署名要求（CSR）がCitrix_RegistrationAuthority_ManualAuthorization 証明書の証明機関（CA）に送信されます。これは一時的な証明書であり、デフォルトで24時間有効です。CAは自動的に証明書を発行しません。証明書を発行するには、管理者によるCAでの手動の権限許可が必要です。証明書がFASサーバーに発行されると、FASはCitrix_RegistrationAuthority_ManualAuthorization証明書を使用してCitrix_RegistrationAuthority 証明書（デフォルトで2年間有効）を自動的に取得します。FASサーバーは、Citrix_RegistrationAuthority証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorizationの証明書とキーを削除します。

RA証明書ポリシーは秘密キーを所有するものすべてに対して、テンプレートで構成されたユーザーセットに対する証明書要求の発行を許可するため、RA証明書に関連付けられた秘密キーは特に機密です。結果として、このキーを管理するものはだれでも、セット内のユーザーと同様、環境に接続できます。

次のいずれかを使用して、組織のセキュリティ要件に準拠して秘密キーが保護されるようにFASサーバーを構成できます。

- Microsoft Enhanced RSA、AES Cryptographic Provider、またはMicrosoftソフトウェアキー記憶域プロバイダー（RA証明書およびユーザー証明書両方の秘密キー用）。
- トラステッドプラットフォームモジュール（TPM）チップを使用したMicrosoftプラットフォームキー記憶域プロバイダー（RA証明書の秘密キー用）、およびMicrosoft Enhanced RSA、AES Cryptographic Provider、またはMicrosoftソフトウェアキー記憶域プロバイダー（ユーザー証明書の秘密キー用）。
- ハードウェアセキュリティモジュール（HSM）ベンダーのHSMデバイスを使用した暗号サービスまたはキー記憶域プロバイダー（RA証明書およびユーザー証明書両方の秘密キー用）。

秘密キーの構成設定

3つのオプションのうちいずれかを使用してFASを構成します。テキストエディターを使用して、Citrix.Authentication.FederatedAuthenticationService.exe.configファイルを編集します。ファイルのデフォルトの場所はFASサーバーのProgram Files\Citrix\Federated Authentication Serviceフォルダーです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

FASは、サービスの起動時にのみ構成ファイルを読み込みます。いずれかの値が変更された場合、新しい設定を反映させるためにFASを再起動する必要があります。

Citrix.Authentication.FederatedAuthenticationService.exe.configファイルの関連する値を次のとおり設定します：

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**（CAPIとCNG APIの切り替え）

値	コメント
真	CAPI APIを使用
false（デフォルト）	CNG APIを使用

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName**（使用するプロバイダーの名前）

値	コメント
Microsoft Enhanced RSAおよびAES Cryptographic Provider	デフォルトはCAPIプロバイダーです
Microsoftソフトウェアキー記憶域プロバイダー	デフォルトはCNGプロバイダーです
Microsoftプラットフォームキー記憶域プロバイダー	デフォルトはTPMプロバイダーです。TPMはユーザーキーにはお勧めしません。TPMはRAキーにのみお使いください。FASサーバーを仮想化環境で実行する予定の場合は、TPMおよびハイパーバイザーのベンダーに仮想化がサポートされているかどうかを確認してください。
HSM_Vendor CSP/Key 記憶域プロバイダー	HSMベンダーによって提供されます。値はベンダーによって異なります。FASサーバーを仮想化環境で実行する

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	予定の場合は、HSMベンダーに仮想化がサポートされているかどうかを確認してください。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType**（CAPI APIの場合のみ必要）

値	コメント
24	Default。Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24を参照します。CAPIでHSMを使用する場合、およびHSMベンダーで別のタイプを指定されている場合以外は、常に24である必要があります。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**（FASが秘密キー操作を実行する必要がある場合は、ここで使用されている値を使用します）。秘密キーの「エクスポート可能」フラグを制御します。 ハードウェアでサポートされている場合は、TPMキーストレージの使用が許可されます。

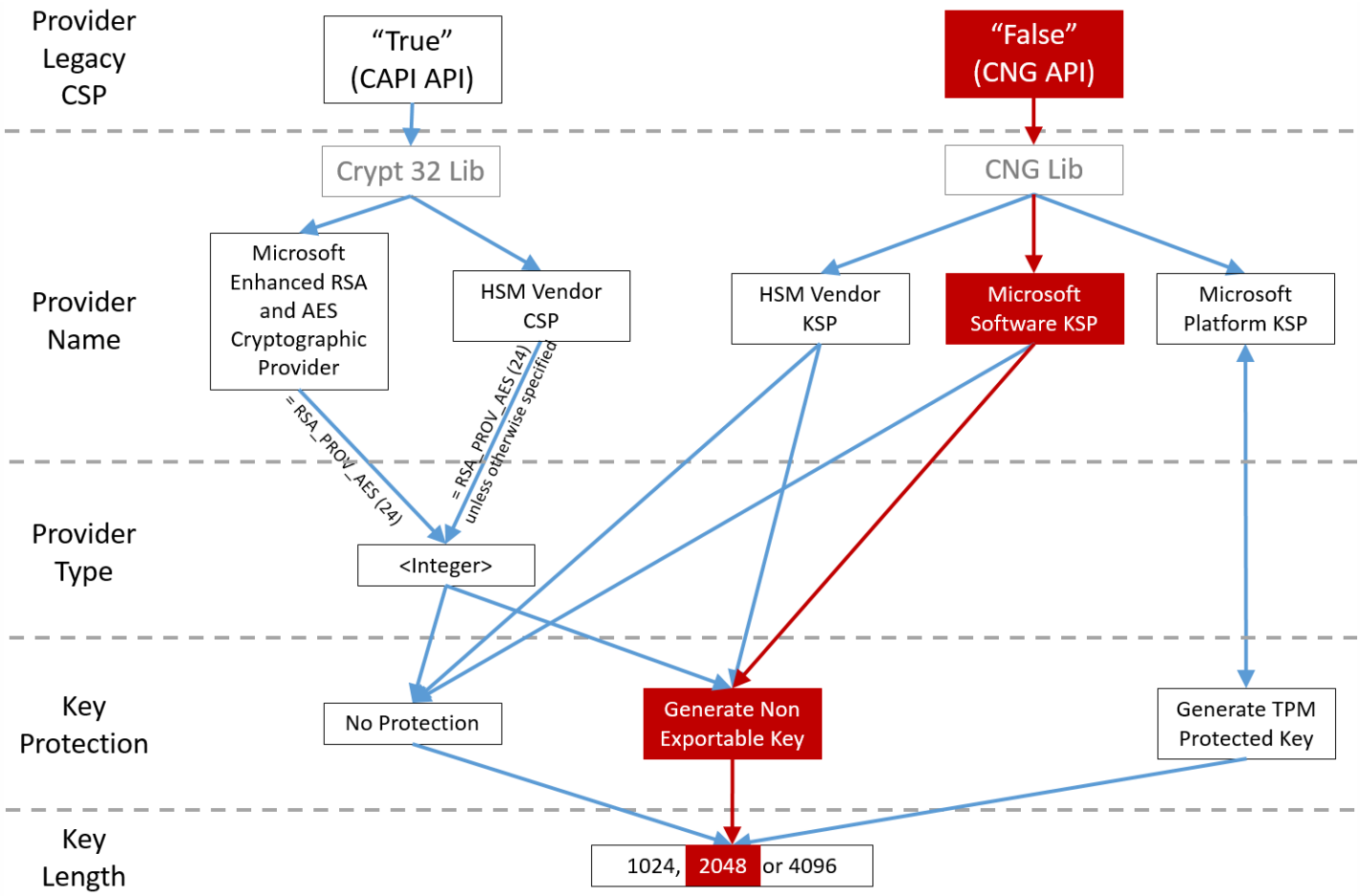
値	コメント
NoProtection	秘密キーをエクスポートできます。
GenerateNonExportableKey	Default。秘密キーをエクスポートできません。
GenerateTPMProtectedKey	秘密キーはTPMを使用して管理されます。秘密キーはProviderNameで指定したProviderName（例：Microsoftプラットフォームキー記憶域プロバイダー）を介して格納されます

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength**（秘密キーのサイズをビットで指定）

値	コメント
2048	デフォルト値です。 1024または4096を使用することもできます。

構成ファイルの設定を以下に図解します（インストール時のデフォルト設定は赤で示しています）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



構成シナリオの例

例1

この例では、Microsoftソフトウェアキー記憶域プロバイダーを使用して格納されているRA証明書の秘密キーおよびユーザー証明書の秘密キーについて説明します。

これはデフォルトのインストール後の構成です。追加の秘密キー構成は不要です。

例2

この例は、Microsoftプラットフォームキー記憶域プロバイダーを使用してFASサーバーのマザーボードのハードウェアTPMに格納されているRA証明書秘密キー、およびMicrosoftソフトウェアキー記憶域プロバイダーを使用して格納されているユーザー証明書秘密キーを示しています。

このシナリオでは、FASサーバーのマザーボード上のTPMはTPMの製造元のドキュメントに基づいてBIOSで有効化され、その後Windowsで初期化されているものとみなしています。詳しくは、https://technet.microsoft.com/ja-jp/library/cc749022(v=ws.10).aspxを参照してください。

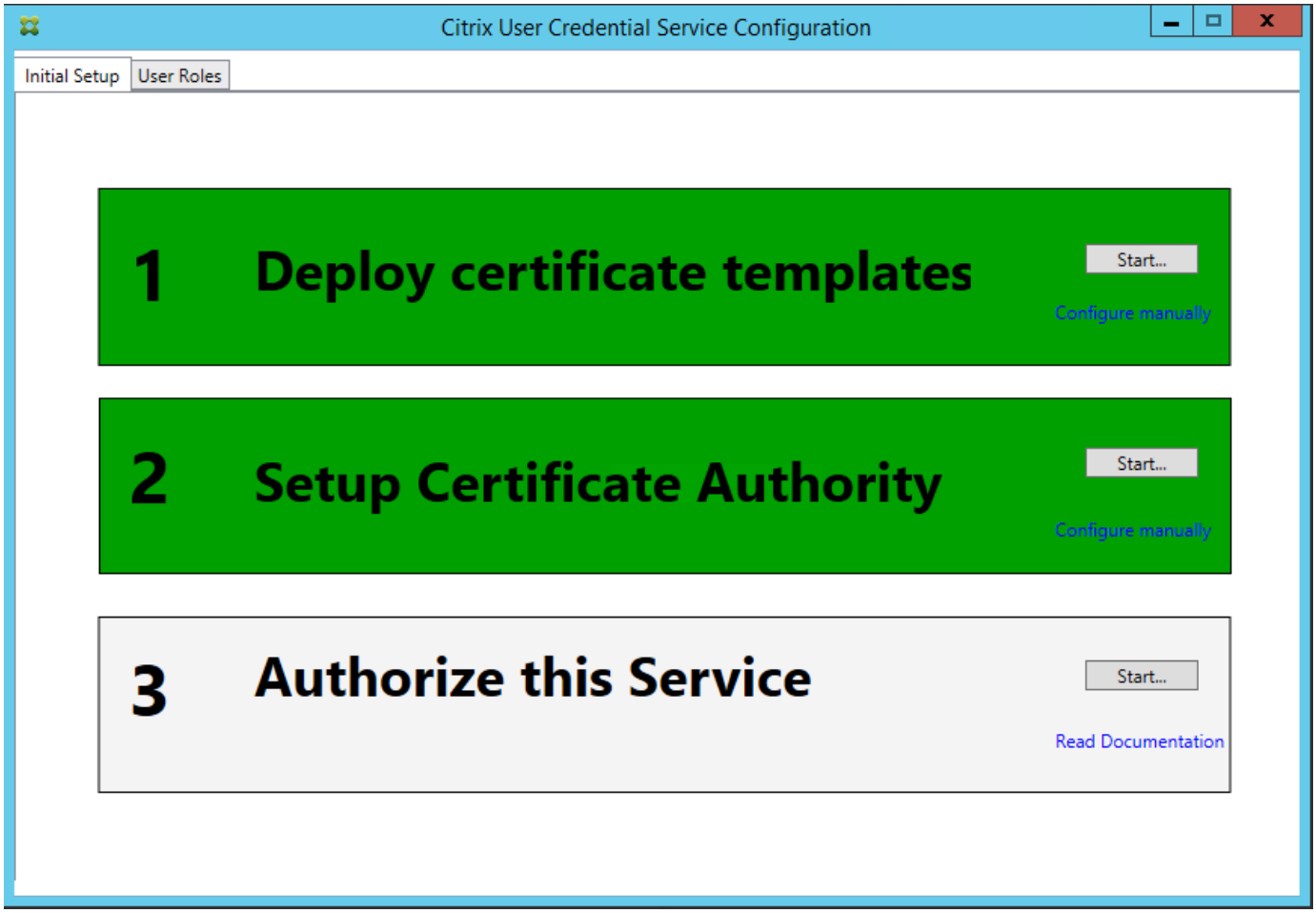
PowerShellの使用（推奨）

PowerShellを使用して、RA証明書をオフラインで要求できます。これは、CAがオンラインのCSRでRA証明書を発行しないよ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

うにする組織にお勧めです。FAS管理コンソールを使用してオフラインのRA CSRを行うことはできません。

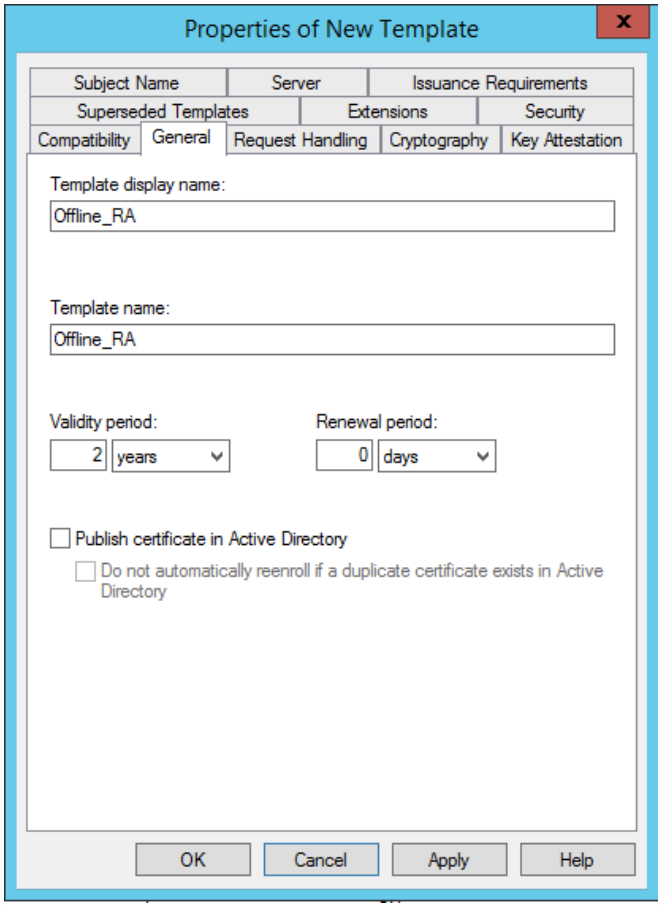
手順1： 管理コンソールを使用したFAS構成の初回セットアップ時には、 最初の「証明書テンプレートの展開」および「証明機関のセットアップ」の2つの手順だけを完了します。



手順2： CAサーバーで、証明書テンプレートMMCスナップインを追加します。**Citrix_RegistrationAuthority_ManualAuthorization**テンプレートを右クリックし、**[テンプレートの複製]**を選択します。

[一般]タブを選択します。テンプレート名と有効期間を変更します。この例では、テンプレート名はOffline_RA、有効期間は2年間です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



手順3：CAサーバーで、CA MMCスナップインを追加します。**[証明書テンプレート]**を右クリックします。**[新規作成]**を選択し、**[発行する証明書テンプレート]**をクリックします。作成したばかりのテンプレートを選択します。

手順4：FASサーバーで次のPowerShellコマンドレットを読み込みます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

手順5：RSAキーペアをFASサーバーのTPM内で生成し、FASサーバーで次のPowerShellコマンドレットを入力してCSRを作成します。**注**：一部のTPMではキーの長さが制限されます。デフォルトでは、証明書のキーの長さは2048ビットに制限されています。ハードウェアでサポートされているキーの長さを指定してください。

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address
```

次に例を示します。

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

以下が表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

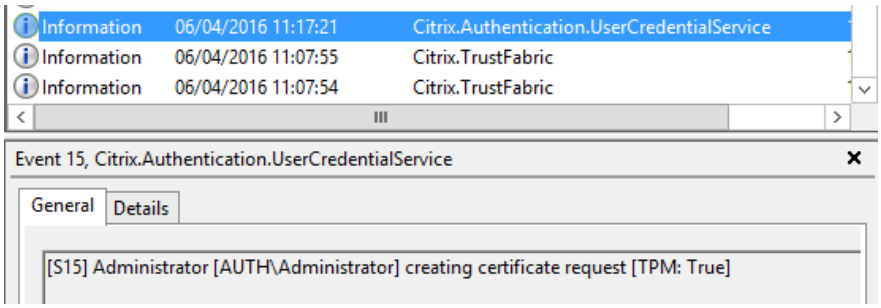
Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRyd%NORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCL%JuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2Bw%6JNZrLi9hAf1bInFPgrz+
                      vbG3YjKuKtK35JpGqWWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIb%D9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9%BwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5N%%%ATJ+xxYEPLp9JuJaElW%rTJG+%P3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9%WHlvztpjxPeJzAVDsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4%Qvr1F+TO15PM5Fxjj6PEKWopWTYZ%GzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3%G/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

注：

- Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は後続の手順で必要です。
- このPowerShellコマンドレットは、RA証明書の秘密キーの生成に使用される一時的な「上書き」と認識してください。
- このコマンドレットを実行する場合、FASサービスが開始されるときに構成ファイルから読み込まれる値がチェックされ、使用するキーの長さが決定されます（デフォルトは2048です）。
- この手動のPowerShellによって開始されるRA証明書秘密キー操作で-UseTPMが$trueに設定されているため、ファイルからの値でTPMの使用に必要な設定に一致しないものは無視されます。
- このコマンドレットの実行によって、構成ファイルの設定が変更されることはありません。
- FASで開始される後続のユーザー証明書秘密キー自動操作の実行中は、FASサービスが開始したときにファイルから読み込まれた値が使用されます。
- FASサーバーがユーザー証明書を発行するときに構成ファイルでKeyProtection値をGenerateTPMProtectedKeyに設定して、TPMで保護されるユーザー証明書秘密キーを生成することもできます。

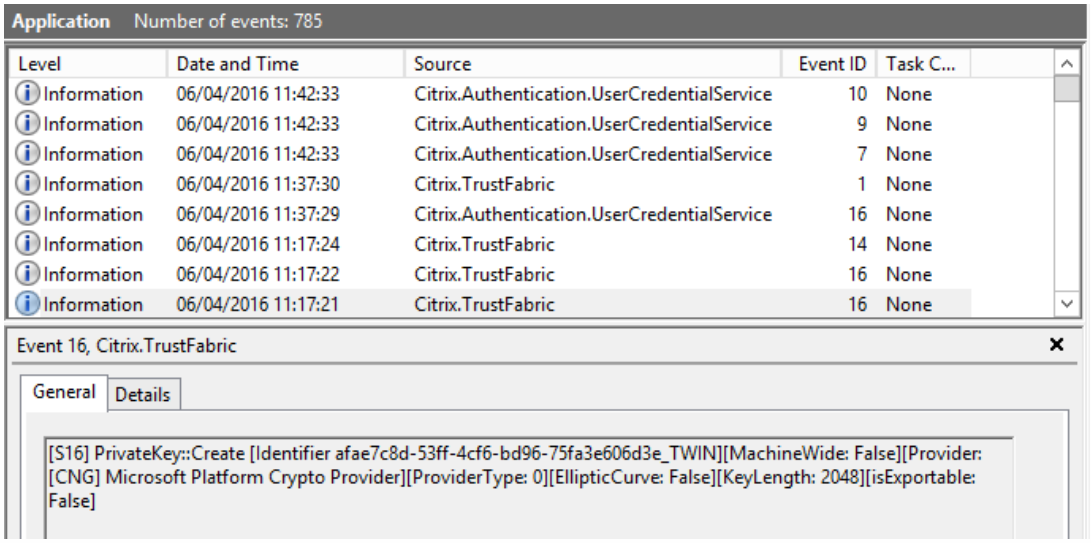
TPMがキーペアの生成に使用されたことを確認するには、FASサーバー上でキーペアが生成された時間のWindowsイベントビューアーのアプリケーションログをチェックします。



「[TPM: True]」であることを確認します。

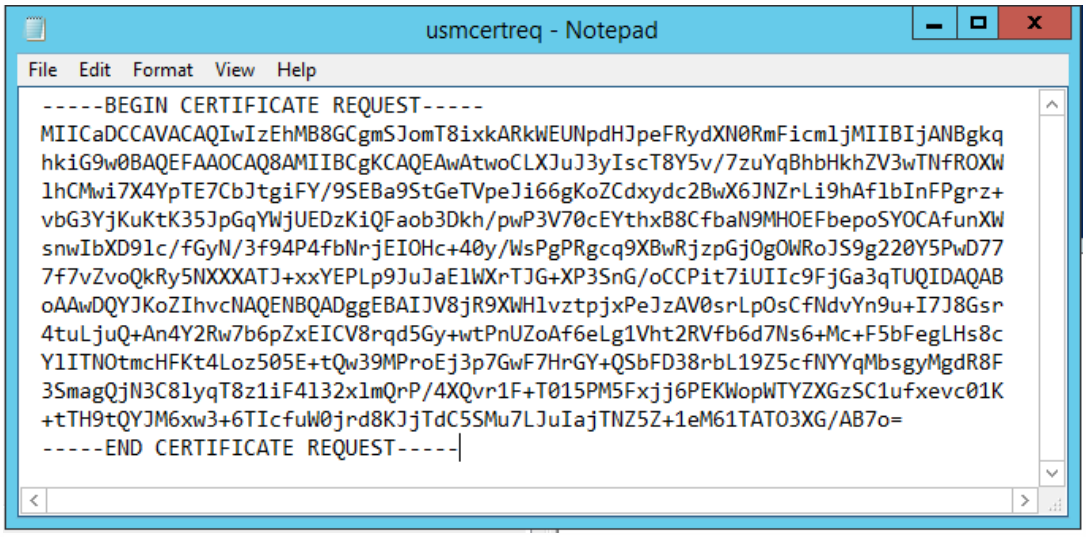
ログは以下のように続きます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



「Provider: [CNG] Microsoft Platform Crypto Provider」を確認します。

手順6： 証明書要求セクションをテキストエディターにコピーし、テキストファイルとしてディスクに保存します。



手順7： 以下のコマンドをFASサーバーのPowerShellに入力して、CSRをCAに送信します。

certreq -submit -attrib "certificatetemplate:<手順2の証明書テンプレート>" <手順6の証明書要求ファイル>

次に例を示します。

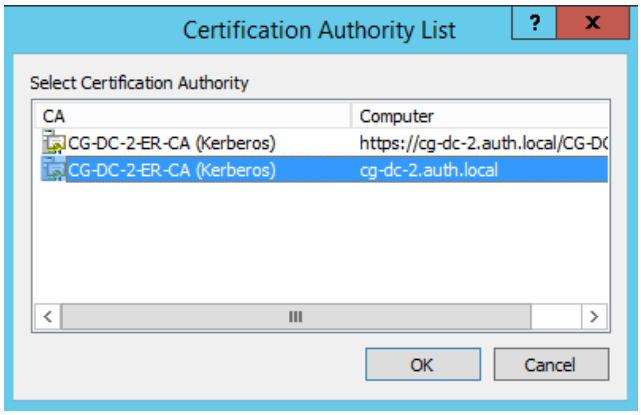
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

以下が表示されます。



この時点で、「証明機関の一覧」ウィンドウが表示される可能性があります。この例のCAではhttp（上部）およびDCOM（下部）登録の両方が有効です。 使用できる場合はDCOMオプションを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



CAが指定されると、PowerShellによってRequestIDが表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH> _
```

手順8： CAサーバーのCA MMCスナップインで、**[保留中の要求]** をクリックします。要求ID を記録します。要求を右クリックし、**[発行]** を選択します。

手順9： **[発行した証明書]** ノードを選択します。発行したばかりの証明書（要求IDが一致する証明書）を見つけます。証明書をダブルクリックして開きます。**[詳細]** タブをクリックします。**[ファイルへコピー]** をクリックします。証明書のエクスポートウィザードが開きます。**[次へ] をクリックします。**次のファイル形式のオプションを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



形式は「**Cryptographic Message Syntax Standard- PKCS #7証明書(.P7B)**」を選択し、「**証明のパスにある証明書を可能であればすべて含む**」をチェックする必要があります。

手順10： エクスポートした証明書をFASサーバーにコピーします。

手順11： FASサーバー上で次のPowerShellコマンドレットを入力して、RA証明書をFASサーバーレジストリにインポートします。

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

次に例を示します。

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

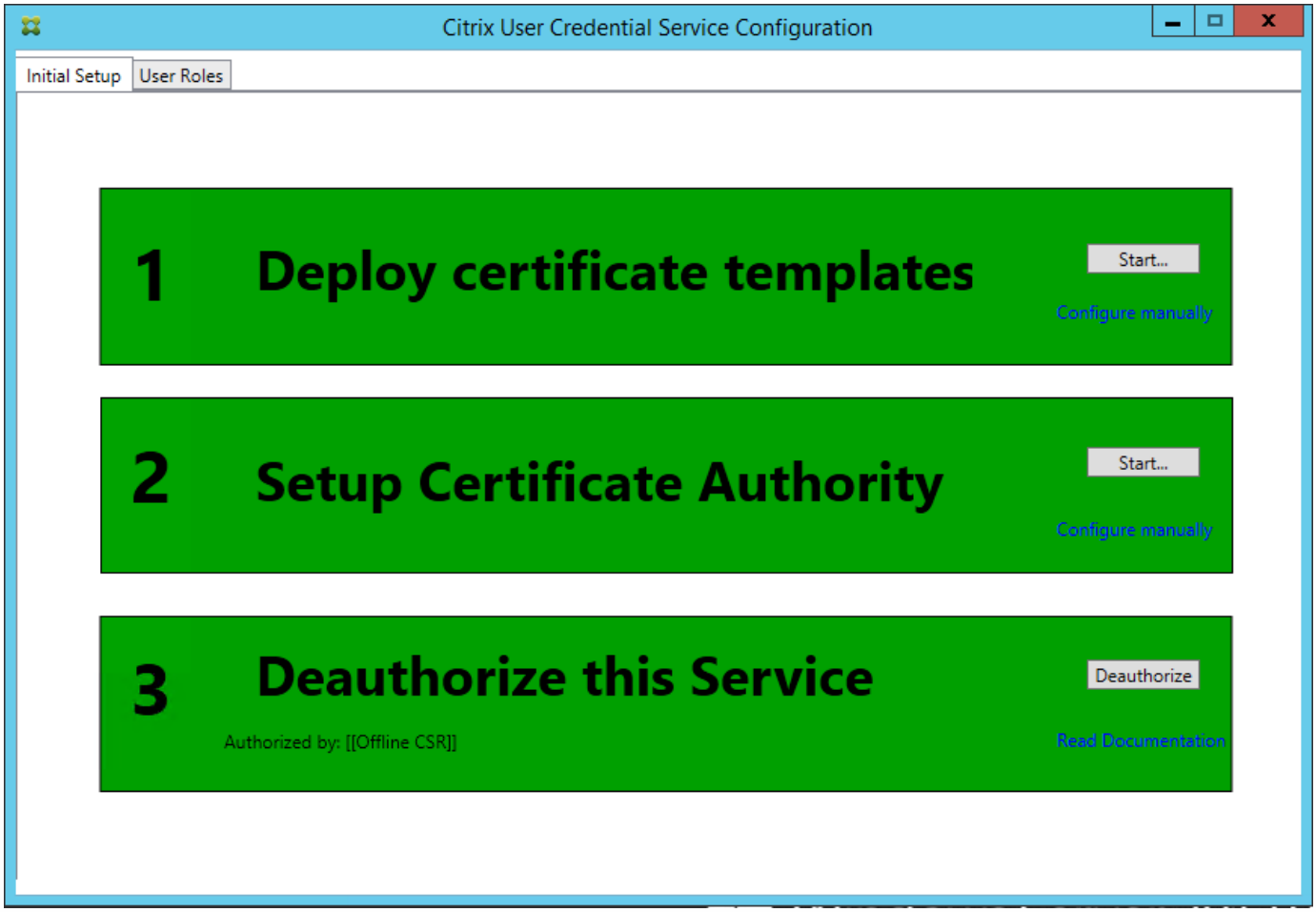
以下が表示されます。

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec311020fc
CertificateRequest :
Status              : Ok
```

手順12： FAS管理コンソールを終了して再起動します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



手順「このサービスを許可する」が緑色になり、表示が「このサービスの許可を取り消す」に変更されます。下部のエントリには、「認証元： オフラインCSR」と表示されます。

手順13： FAS管理コンソールで **[ユーザーロール]** タブを選択し、メインのFAS記事の記述に従って設定を編集します。

注：管理コンソールからFASの権限を取り消すと、ユーザー規則が削除されます。

FAS管理コンソールの使用

FAS管理コンソールではオフラインCSRを行うことができないため、組織でRA証明書のオンラインCSRが許可されない限り、FAS管理コンソールの使用はお勧めしません。

FASの初回のセットアップ手順の実行中、証明書テンプレートを展開してCAをセットアップした後、サービスを許可（構成順序の手順3）する前に次を行います。

手順1： 以下の行を次のとおり変更して、構成ファイルを編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

ファイルは以下のように表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

一部のTPMではキーの長さが制限されています。デフォルトのキーの長さは、2048ビットです。ハードウェアでサポートされているキーの長さを指定してください。

手順2： サービスを許可します。

手順3： CAサーバーから、保留中の証明書要求を手動で発行します。RA証明書が取得されたら、管理コンソールのセットアップ順序の手順3が緑色に変わります。この時点で、RA証明書の秘密キーはTPMで生成されています。証明書はデフォルトで2年間有効です。

手順4： 次のように構成ファイルを編集し直します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

注：FASはTPMで保護されたキーでユーザー証明書を生成できますが、TPMは大規模の展開には速度が遅すぎる可能性があります。

手順5： Citrix Federated Authentication Serviceを再起動します。これにより、サービスによる構成ファイルの再読み込みが強制され、変更された値が反映されます。後続の自動秘密キー操作はユーザー証明書キーに影響します。これらの操作ではTPMに秘密キーが保存されませんが、Microsoftソフトウェアキー記憶域プロバイダーが使用されます。

手順6： FAS管理コンソールで［ユーザーロール］タブを選択し、メインのFAS記事の記述に従って設定を編集します。

注：管理コンソールからFASの権限を取り消すと、ユーザー規則が削除されます。

例3

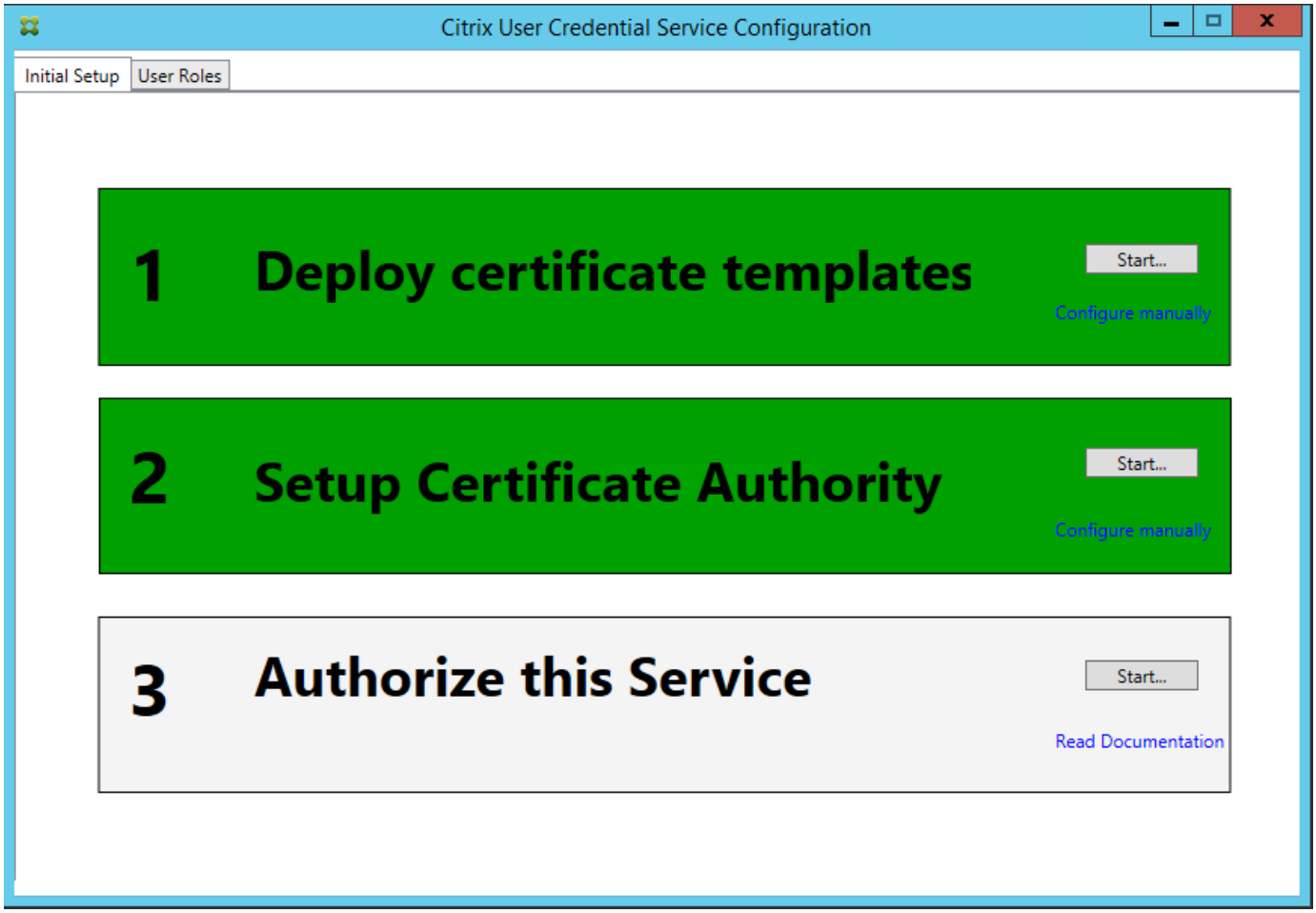
この例では、HSMに格納されているRA証明書の秘密キーおよびユーザー証明書の秘密キーについて説明します。この例では、構成済みのHSMを想定しています。HSMにはプロバイダー名（「HSM_Vendor's Key Storage Provider」など）が含まれます。

FASサーバーを仮想化環境で実行する予定の場合は、HSMベンダーにハイパーバイザーがサポートされているかどうかを確認

© 1999-2017 Citrix Systems, Inc. All rights reserved.

してください。

手順1： 管理コンソールを使用したFAS構成の初回セットアップ時には、 最初の「証明書テンプレートの展開」および「証明機関のセットアップ」の2つの手順だけを完了します。



手順2： HSMベンダーのドキュメントで、HSMのProviderNameの値を確認します。HSMがCAPIを使用している場合、プロバイダーはドキュメントで暗号化サービスプロバイダー（CSP）と記述されている可能性があります。HSMがCNGを使用している場合、プロバイダーはキー記憶域プロバイダー（KSP）と記述されている可能性があります。

手順3： 構成ファイルを次のように編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

ファイルは以下のように表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

このシナリオでは、HSMがCNGを使用していると想定しているため、ProviderLegacyCspの値はfalseに設定されています。HSMがCAPIを使用している場合は、ProviderLegacyCspの値はtrueに設定されます。HSMベンダーのドキュメントで、HSMがCAPICNとCNGのどちらを使用しているかを確認してください。また、非対称RSAキー生成でサポートされているキーの長さについても、HSMベンダーのドキュメントで確認してください。この例では、キーの長さはデフォルトの2048ビットに設定されています。指定したキーの長さがお使いのハードウェアでサポートされていることを確認してください。

手順4： Citrix Federated Authentication Serviceを再起動して、構成ファイルからの値を読み込みます。

手順5： HSM内でRSAキーペアを生成し、FAS管理コンソールの初回セットアップタブで **[許可する]** をクリックしてCSRを作成します。

手順6： Windowsイベントログのアプリケーションエントリをチェックして、キーペアがHSM内で生成されていることを確認します。

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

[Provider: [CNG] HSM_Vendor's Key Storage Provider]を確認します。

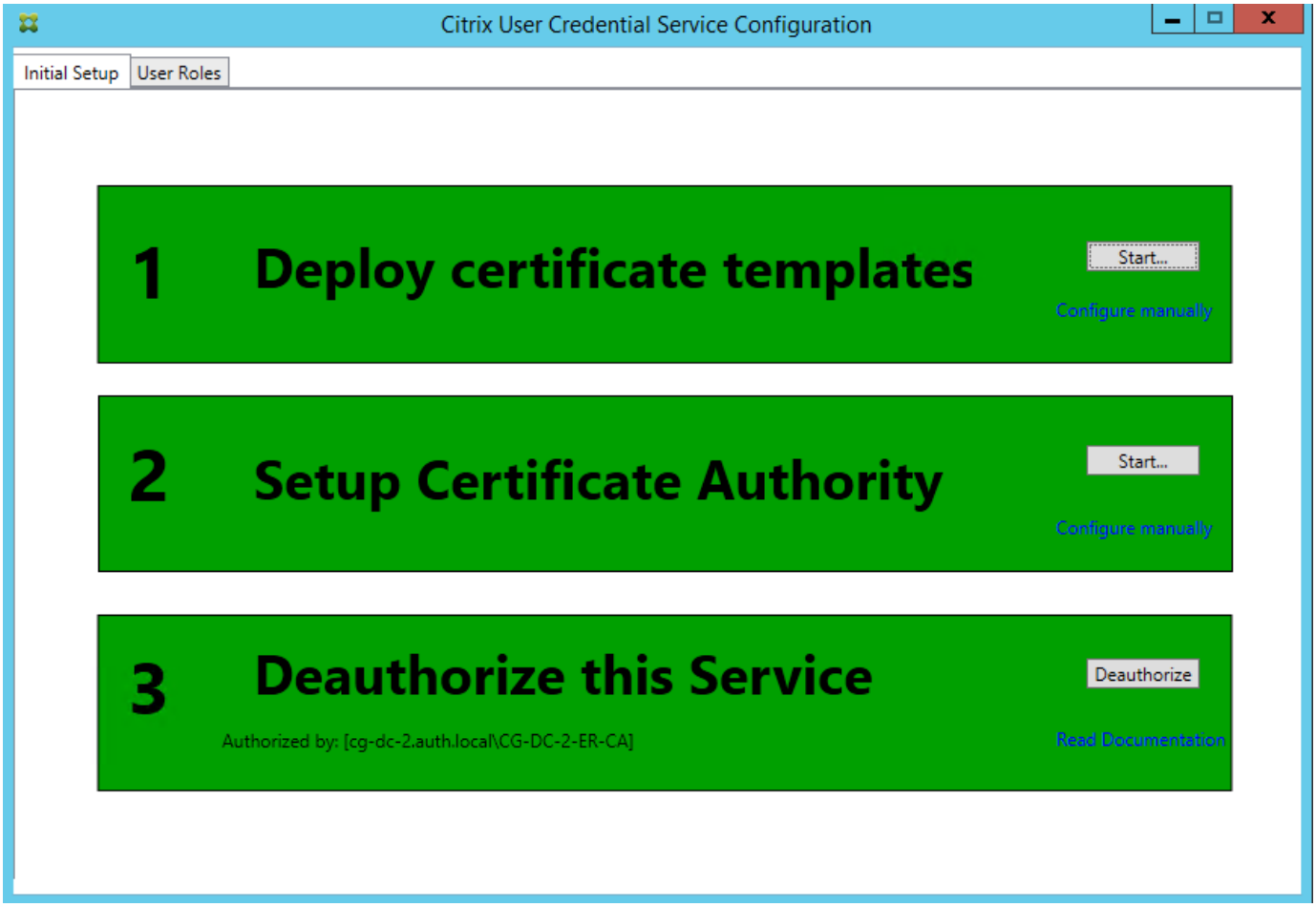
手順7： CAサーバーのCA MMCで、 **[保留中の要求]** ノードを選択します。

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

要求を右クリックし、 **[発行]** を選択します。

手順「このサービスを許可する」が緑色になり、表示が「このサービスの許可を取り消す」に変更されます。下部のエントリには、「認証元： []」と表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



手順8： FAS管理コンソールで **[ユーザーロール]** タブを選択し、メインのFAS記事の記述に従って設定を編集します。

注：管理コンソールからFASの権限を取り消すと、ユーザー規則が削除されます。

FAS証明書ストレージ

FASでは、証明書の保存にFASサーバー上のMicrosoft証明書ストアを使用しません。FASではレジストリを使用します。

注：HSMを使用して秘密キーを保存する場合、HSMコンテナーはGUIDで識別されます。HSMにある秘密キーのGUIDは、レジストリにある同等の証明書のGUIDに一致します。

RA証明書のGUIDを特定するには、FASサーバーで次のPowerShellコマンドレットを入力します。

```
Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address
```

次に例を示します。

```
Get-FasAuthorizationCertificate –address cg-fas-2.auth.net
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                     MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEg0xlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

ユーザー証明書の一覧を取得するには、以下を入力します。

Get-FasUserCertificate –address

次に例を示します。

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

関連情報

- FASのインストールと構成については、「Federated Authentication Service」を参照してください。
- 一般的なFAS環境については、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」ではそのほかの「方法」に関する記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication Serviceのセキュリティとネットワークの構成

Dec 05, 2017

CitrixのFederated Authentication Service（FAS）は、Microsoft Active DirectoryおよびMicrosoft証明機関（CA）と密接に統合しています。 ドメインコントローラーやそのほかの重要なインフラストラクチャと同様に、セキュリティポリシーを展開することによって、システムの適切な管理と保護を行うことが重要です。

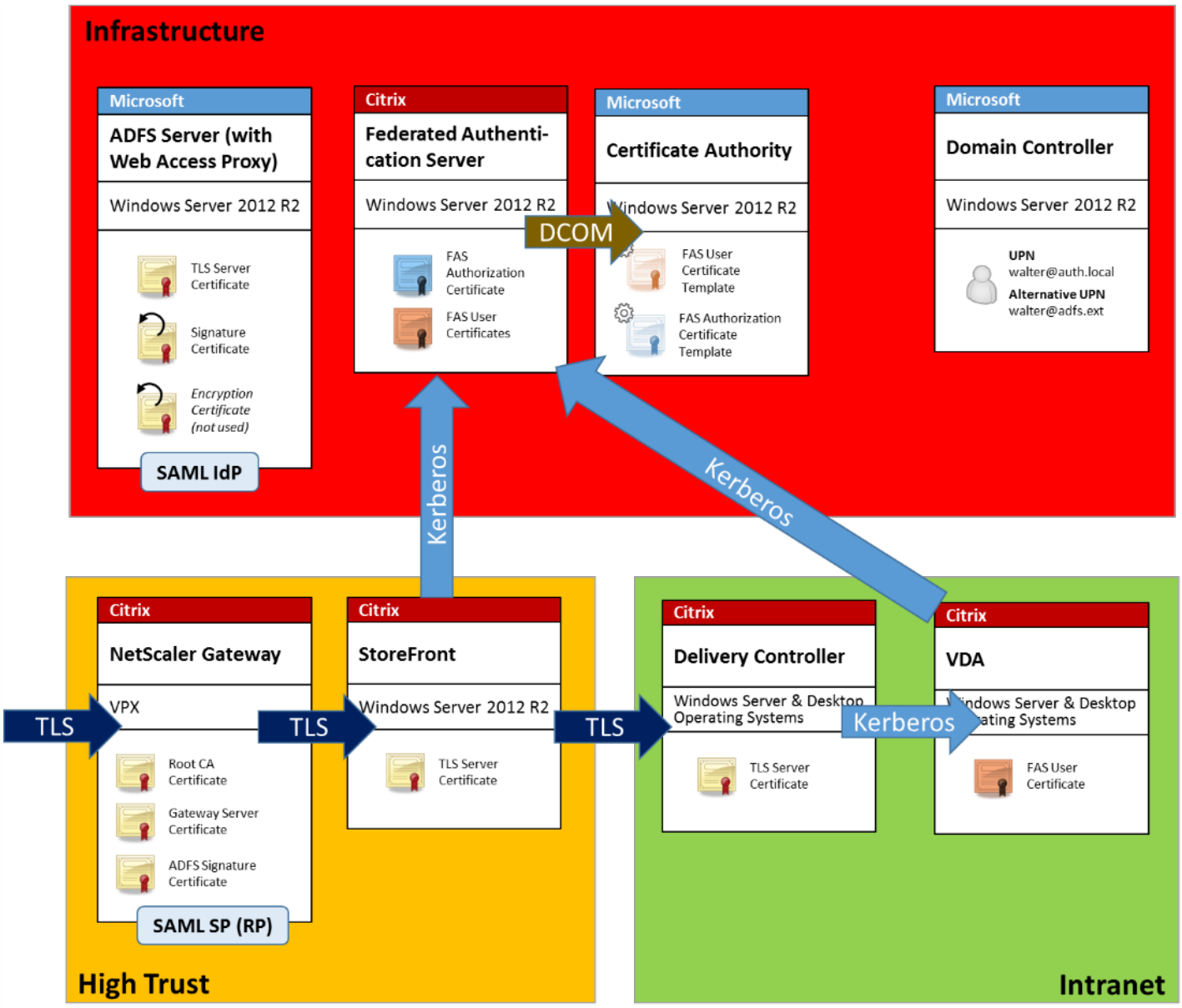
このドキュメントでは、FASを展開する場合に考慮する、セキュリティ問題の概要について説明します。 また、インフラストラクチャのセキュリティ保護に役立つ利用可能な機能の概要についても説明します。

ネットワークアーキテクチャ

次の図は、FAS展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FASサーバーは、CAやドメインコントローラーと共に、セキュリティ上重要なインフラストラクチャの一部として扱われる必要があります。 フェデレーション環境では、Citrix NetScalerおよびCitrix Storefrontはユーザー認証を行うことが信頼されたコンポーネントです。そのほかのXenAppおよびXenDesktopコンポーネントは、FAS導入の影響を受けません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ファイアウォールとネットワークセキュリティ

NetScaler、StoreFront、およびDelivery Controllerコンポーネント間の通信は、ポート443上でTLSによって保護される必要があります。 StoreFrontサーバーは発信接続のみを行い、NetScaler Gatewayは、HTTPSのポート443を使用したインターネット上の接続のみを受け入れるようにする必要があります。

StoreFrontサーバーは相互認証されたKerberosを使用して、ポート80でFASサーバーと通信します。 認証には、FASサーバーのKerberos HOST/fqdn ID、およびStoreFrontサーバーのKerberosマシンアカウントIDが使用されます。 これにより、CitrixのVirtual Delivery Agent（VDA）がユーザーにログオンするのに必要な、1回限り有効の「資格情報ハンドル」が生成されます。

HDXセッションがVDAに接続されると、VDAもポート80でFASサーバーと通信します。 認証には、FASサーバーのKerberos HOST/fqdn ID、およびVDAのKerberosマシンIDが使用されます。 また、VDAは、証明書と秘密キーへのアクセスに「資格情報ハンドル」を提供する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft CAは、固定TCPポートの使用を構成できる、Kerberos認証のDCOMを使用して、接続を受け入れます。 また、CAは、FASサーバーに信頼された登録エージェント証明書による署名済みのCMCパケットを提供するよう要求します。

サーバー	ファイアウォールポート
Federated 認証サービス	[in] StoreFrontおよびVDAからのHTTP上のKerberos [out] DCOMからMicrosoft CAへ
NetScaler	[in] クライアントマシンからのHTTPS [in/out] StoreFrontサーバーを出入りするHTTPS [out] HDXからVDAへ
StoreFront	[in] NetScalerからのHTTPS [out] Delivery ControllerへのHTTPS [out] FASへのKerberos HTTP
Delivery Controller	[in] StoreFrontサーバーからのHTTPS [in/out] VDAからのHTTP上のKerberos
VDA	[in/out] Delivery ControllerからのHTTP上のKerberos [in] NetScaler GatewayからのHDX [out] FASへのKerberos HTTP
Microsoft CA	[in] DCOMと、FASからの署名

管理の責任

環境の管理は、次のグループに分かれます。

でのデータソース名	責任
エンタープライズ管理者	フォレスト内の証明書テンプレートのインストールおよび保護
ドメイン管理者	グループポリシー設定の構成

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CA管理者	証明機関の設定
FAS管理者	FASサーバーのインストールと構成
StoreFrontおよびNetscaler管理者	ユーザー認証の構成
XenDesktop管理者	VDAおよびコントローラーの構成

各管理者は、セキュリティモデル全体のさまざまな面を制御し、システムのセキュリティ保護のための、徹底した防御対策のアプローチを実現します。

グループポリシー設定

信頼されたFASマシンは、グループポリシーで構成された「index number -> FQDN」のルックアップテーブルで識別されます。 FASサーバーに接続する場合、クライアントはFASサーバーのHOST\ Kerberos IDを検証します。 FASサーバーにアクセスするすべてのサーバーは、同じインデックスに同一のFQDNを持つ必要があります。そうでない場合は、StoreFrontおよびVDAが別のFASサーバーに接続することがあります。

構成ミスを防ぐために、環境内のすべてのマシンに、単一のポリシーを適用することをお勧めします。 FASサーバーの一覧に変更を加える場合、特にエントリの削除や順序の変更は、注意して行ってください。

このGPOの管理は、FASサーバーのインストールおよび運用停止を担当するFAS管理者（またはドメイン管理者）に限定する必要があります。 FASサーバーの運用停止直後に、そのFQDNを再度使用しないように注意してください。

証明書テンプレート

FASから提供されるCitrix_SmartcardLogon証明書テンプレートを使用しない場合、証明書のコピーを変更できます。以下の変更がサポートされています。

証明書テンプレートの名前の変更

Citrix_SmartcardLogonの名前を変更する場合、所属組織のテンプレート命名標準に従って、以下を行う必要があります。

- 証明書テンプレートのコピーを作成し、所属組織のテンプレート命名標準に従ってその名前を変更します。
- 管理ユーザーインターフェイスではなく、管理FASへのFAS PowerShellコマンドを使用します。（管理ユーザーインターフェイスは、Citrixのデフォルトのテンプレート名での使用のみを対象としています。）
  - Microsoft MMC証明書テンプレートスナップインかPublish-FasMsTemplateコマンドを使用して、自身のテンプレートを公開し、
  - New-FasCertificateDefinition コマンドにより、自身のテンプレートの名前を使用してFASを構成します。

全般プロパティの変更

証明書テンプレートの有効期間を変更できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更新期間は変更しないでください。FASは証明書テンプレートのこの設定を無視します。FASは有効期間の半ばで証明書を自動的に更新します。

要求処理プロパティの変更

これらのプロパティは変更しないでください。FASは証明書テンプレートのこれらの設定を無視します。FASでは常に、**[秘密キーのエクスポートを許可する]** と **[同一キーで更新する]** はオフにされています。

暗号プロパティの変更

これらのプロパティは変更しないでください。FASは証明書テンプレートのこれらの設定を無視します。

FASで提供される該当の設定については、「Federated Authentication Serviceの秘密キー保護」を参照してください。

キーの構成証明プロパティの変更

これらのプロパティは変更しないでください。FASではキーの構成証明はサポートされません。

優先テンプレートプロパティの変更

これらのプロパティは変更しないでください。FASでは優先テンプレートはサポートされません。

拡張プロパティの変更

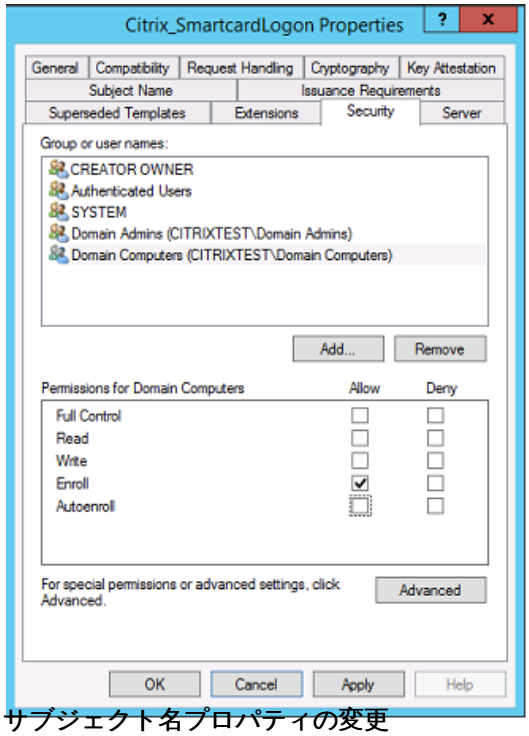
所属組織のポリシーに合わせてこれらの設定を変更できます。

注：不適切な拡張設定を行うと、セキュリティの問題が発生したり、証明書が使用できなくなる場合があります。

セキュリティプロパティの変更

FASサーバーのマシンアカウントにのみ**登録**権限が許可されるようにこれらの設定を変更することをお勧めします。その他のサービスに関しては、システムへの **フルコントロール**権限も許可します。それ以外の権限は必要ありません。ただし、それ以外の権限を許可することもできます。たとえば、トラブルシューティングの目的で、FAS管理者が変更されたテンプレートを表示できるようにするなどです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



サブジェクト名プロパティの変更

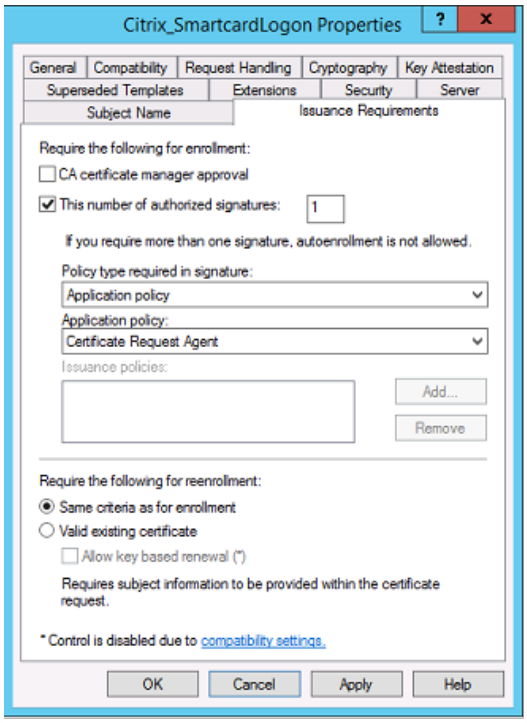
必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

サーバープロパティの変更

推奨はされませんが、必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

発行要件プロパティの変更

これらの設定は変更しないでください。これらは以下のように設定する必要があります。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

互換性プロパティの変更

これらの設定は変更できます。この設定は、**Windows Server 2003 CA**（スキーマバージョン2）以上とする必要があります。ただし、FASがサポートするのはWindows Server 2008以降のCAのみです。上記の説明のとおり、**Windows Server 2008 CA**（スキーマバージョン3）または**Windows Server 2012 CA**（スキーマバージョン4）を選択することにより使用可能となる追加設定は、FASでは無視されます。

証明機関の管理

CA管理者の任務は、CAサーバーの構成、およびCAサーバーが使用する証明書用秘密キーの発行です。

テンプレートの公開

エンタープライズ管理者の提供するテンプレートに基づいた証明書を証明機関が発行するには、CA管理者がテンプレートの公開を選択する必要があります。

シンプルなセキュリティ対策としては、FASサーバーのインストール時にのみRA証明書テンプレートを公開するか、またはオフラインの証明書発行手続きを選択することです。 いずれの場合も、CA管理者はRA証明書の要求の承認において全面的なコントロールを維持し、FASサーバーの承認に関するポリシーを持つ必要があります。

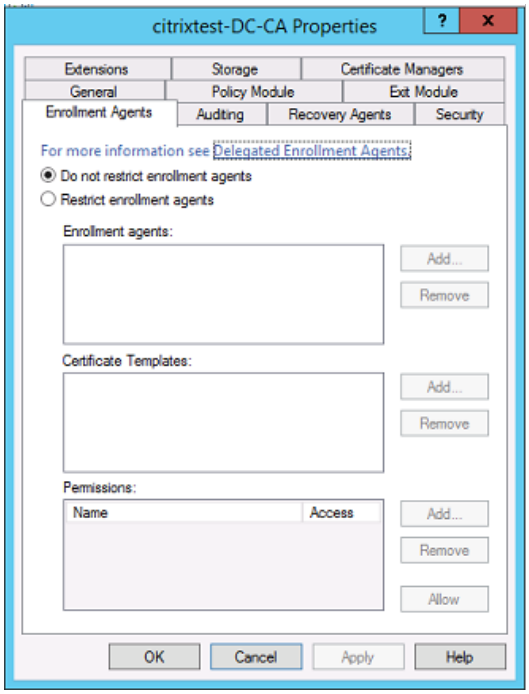
ファイアウォールの設定

一般的に、CA管理者は、CAのネットワークファイアウォール設定も管理して、受信接続の制御を行います。 CA管理者は、DCOM TCPおよびファイアウォールルールを構成し、FASサーバーだけが証明書を要求できるようにすることができます。

登録の制限

デフォルトでは、RA証明書のすべての保持者が、アクセス可能な証明書テンプレートを使用して、ユーザーに証明書を発行することができます。 これを、CAプロパティの「登録エージェントの制限」で、特権のないユーザーグループに制限する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ポリシーモジュールと監査

高度な展開には、カスタムセキュリティモジュールを使用して、証明書の発行の追跡と拒否を行うことができます。

FASの管理

FASにはいくつかのセキュリティ機能があります。

アクセス制御リスト（ACL）によるStoreFront、ユーザー、およびVDAの制限

FASセキュリティモデルの中心となるのが、機能にアクセスできるKerberosアカウントの管理です。

アクセスベクトル	説明
StoreFront［IdP］	これらのKerberosアカウントは、ユーザーが正しく認証されたと宣言することを信頼されています。 Kerberosアカウントのいずれかが危害を受けた場合には、証明書が作成され、FASの構成で許可されたユーザーに証明書が使用されます。
VDA［証明書利用者］	これらは、証明書および秘密キーへのアクセスが許可されたマシンです。 このグループ内の危害を受けたVDAアカウントによるシステム攻撃の範囲が制限されるよう、IdPが取得した資格情報ハンドルも必要です。
ユーザー	IdPがどのユーザーをアサートするかを管理します。 CAの「制限付き登録エージェント」構成オプションと重複していることに注意してください。 一般的に、アクセス制御リストには、特権のないアカウントのみを加えることをお勧めします。これにより、危害を受けたStoreFrontアカウントが、権限をより高い管理者レベルに高めることを防ぎます。 特に、ドメイン管理者のアカウントは、このアクセス制御リ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	ストで許可されるべきではありません。

ルールの構成

独立した複数のXenAppまたはXenDesktopの展開で同じFASサーバーインフラストラクチャが使用されている場合には、ルールが役立ちます。 各ルールにはそれぞれの構成オプションセットがあり、特にアクセス制御リストは、個別に構成することができます。

CAおよびテンプレートの構成

証明書テンプレートおよびCAは、それぞれ異なるアクセス権のために構成することができます。 高度な構成は、環境に応じて、権限の度合いが異なる証明書を使用するよう選択する場合があります。 たとえば、「外部」と識別されたユーザーには、「内部」ユーザーよりも権限が弱い証明書が発行されることがあります。

セッション中および認証の証明書

FAS管理者は、認証に使用された証明書を、ユーザーのセッションで使用するかどうか管理します。 たとえば、より権限のある「ログオン」証明書はログオン時にのみ使用するように、セッションでは「署名」証明書のみ使用可能にすることができます。

秘密キー保護およびキー長

FAS管理者は、FASが秘密キーをハードウェアセキュリティモジュール（HSM）、またはトラステッドプラットフォームモジュール（TPM）に保存するよう構成できます。 少なくともRA証明書の秘密キーは、TPMに保存して保護することをお勧めします。このオプションは、「オフライン」証明書要求手続きの中で提供されます。

同様に、ユーザー証明書の秘密キーもTPMまたはHSMに保存できます。 すべてのキーは「エクスポート不可能」として生成し、キー長は2048ビット以上でなければなりません。

イベントログ

FASサーバーによって、詳細な構成およびランタイムイベントのログが提供されるため、監査と侵入検出に役立てることができます。

管理アクセスと管理ツール

FASには、リモート管理の機能（相互認証のKerberos）およびツールが含まれています。 「ローカル管理者グループ」のメンバーが、FASの構成を全面的に管理します。この一覧は、注意して維持する必要があります。

XenApp、XenDesktop、およびVDAの管理者

「Active Directoryパスワード」はFASの「資格情報ハンドル」にそのまま置き換えられるため、一般的には、FASの利用によってDelivery ControllerやVDA管理者のセキュリティモデルが変更されることはありません。ControllerおよびVDAの管理グループのメンバーは、信頼されたユーザーに限定する必要があります。 監査とイベントログを維持する必要があります。

一般的なWindowsサーバーセキュリティ

すべてのサーバーにパッチを完全に適用し、標準のファイアウォールとアンチウィルスソフトウェアを使用する必要があり

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ます。 セキュリティ上重要なインフラストラクチャのサーバーは、物理的に安全な場所に設置し、ディスクの暗号化や仮想マシンのメンテナンスオプションにも十分配慮する必要があります。

監査データとイベントログは、リモートマシンに安全に保存する必要があります。

RDPアクセスは、承認された管理者のみに制限する必要があります。可能な場合は、ユーザーアカウント、特にCAおよびドメイン管理者のアカウントでは、スマートカードを使用したログオンが要求されるようにする必要があります。

関連情報

- FASのインストールと構成については、「Federated Authentication Service」を参照してください。
- FASアーキテクチャについては、「Federated Authentication Serviceのアーキテクチャの概要」を参照してください。
- 「Federated Authentication Serviceの構成と管理」ではそのほかの「方法」に関する記事を紹介しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication ServiceによるWindowsログオンの問題のトラブルシューティング

Dec 05, 2017

ここでは次のことについて説明します。

- 証明書と公開キー基盤
- UPN名と証明書マッピング
- ログオンドメインコントローラーの選択制御
- アカウント監査イベントの有効化
- 証明書検証ログ
- Kerberosログ
- イベントログメッセージ
- エンドユーザーエラーメッセージ
- 関連情報

ここでは、ユーザーが証明書やスマートカードを使用してログオンするときに、Windowsが提供するログおよびエラーメッセージについて説明します。 これらのログには、認証の失敗をトラブルシューティングするために使用できる情報が含まれています。

証明書と公開キー基盤

Windows Active Directoryは、ユーザーのログオン用証明書を管理するいくつかの証明書ストアを保守しています。

- **NTAuth証明書ストア**： Windowsでの認証のため、ユーザー証明書をすぐに発行するCA（つまりチェーンはサポートされません）をNTAuthストアに配置する必要があります。 これらの証明書を表示するには、certutilプログラムから次のように入力します。certutil –viewstore –enterprise NTAuth
- **ルートおよび中間証明書ストア**：通常、証明書ログオンシステムは単一の証明書のみを提供できるため、チェーンが使用中の場合、すべてのマシン上の中間証明書ストアがこれらの証明書を含んでいる必要があります。 ルート証明書は信頼されたルートストアに、最後から2番目の証明書はNTAuthストアにある必要があります。
- **ログオン証明書拡張とグループポリシー**：EKUや他の証明書ポリシーを強制的に検証するようにWindowsを構成できます。詳しくは、Microsoftのドキュメントを参照してください。 https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にスマートカードログオン拡張キー使用法（Extended Key Usage：EKU）が含まれる必要があります。
AllowSignatureOnlyKeys	デフォルトで、Windowsは、RSA復号化を許可しない証明書秘密キーを拒否します。 このオプションは、そのフィルターを上書きします。
AllowTimeInvalidCertificates	デフォルトで、Windowsは期限切れの証明書を拒否します。 こ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	のオプションは、そのフィルターを上書きします。
EnumerateECCCerts	楕円曲線認証を有効化します。
X509HintsNeeded	証明書に一意のユーザープリンシパル名（UPN）が含まれないか、複数の解釈が可能な場合、このオプションを使用すると、ユーザーが手動でWindowsログオンアカウントを指定できます。
UseCachedCRLOnlyAnd IgnoreRevocationUnknownErrors	失効チェックを無効にします（通常ドメインコントローラー上で設定）。

- **ドメインコントローラー証明書**: Kerberos接続を認証するには、すべてのサーバーが適切な「ドメインコントローラー」証明書を持っている必要があります。 これらは、［Local Computer Certificate Personal Store］MMCスナップインメニューを使用して要求できます。

UPN名と証明書マッピング

ユーザー証明書は、一意のユーザープリンシパル名（UPN）をサブジェクトの別名拡張機能に含めることをお勧めします。

Active DirectoryでのUPN名

デフォルトで、Active Directoryのすべてのユーザーは、パターン@および@に基づく暗黙的UPNを持っています。 利用できるドメインおよびFQDNは、フォレストに対応するRootDSEエントリに含まれています。 RootDSEで、単一のドメインに対して複数のFQDNアドレスが登録されていることがあることに注意してください。

また、Active Directoryのすべてのユーザーは明示的なUPNとaltUserPrincipalNamesを持っています。 これらはユーザーのUPNを指定するLDAPエントリです。

UPNでユーザーを検索する場合、Windowsは、まず（UPNを参照するプロセスのIDに基づいて）現在のドメインで明示的なUPNを、続けて代替UPNを探します。 一致するものがない場合、暗黙的UPNを探しますが、これはフォレストの異なるドメインで解決されることがあります。

証明書マッピングサービス

証明書に明示的なUPNが含まれない場合、Active Directoryは各使用に対して正確な公開証明書を「x509certificate」属性に保管するオプションを持っています。 そのような証明書をユーザーに解決するために、コンピューターは直接この属性を問い合わせることができます（デフォルトでは単一のドメインで）。

用意されているオプションを使用すると、ユーザーがユーザーアカウントを指定してこの検索の速度を上げたり、この機能がクロスドメイン環境で使用されるようにしたりできます。

フォレストに複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active DirectoryのrootDSEが証明書マッピングサービスの場所を指定します。 これは通常グローバルカタログマシンに置かれ、フォレスト内のすべてのx509certificate属性のキャッシュビューを持っています。 このコンピューターは、証明書だけに基づいて任意のドメインで

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーアカウントを効率的に検出するために使用できます。

ログオンドメインコントローラーの選択制御

ある環境に複数のドメインコントローラーが含まれる場合、認証にどのドメインコントローラーが使用されているかを把握して制限すると、ログを有効化して取得するのに便利です。

ドメインコントローラーの選択制御

Windowsに対して、ログオンで特定のWindowsドメインコントローラーを強制的に使用させるために、lmhostsファイル（\Windows\System32\drivers\etc\lmhosts）を構成することで、Windowsマシンが使用するドメインコントローラーのリストを明示的に設定することができます。

通常その場所には「lmhosts.sam」という名のサンプルファイルがあります。単に次の1行を追加します。

1.2.3.4　dcnetbiosname #PRE #DOM:mydomai

ここで、「1.2.3.4」は、「mydomain」ドメインで「dcnetbiosname」という名前が付けられているドメインコントローラーのIPアドレスです。

再起動後に、Windowsマシンはその情報を使用してmydomainにログオンします。 デバッギングが完了したら、この構成を取り消す必要があることに注意してください。

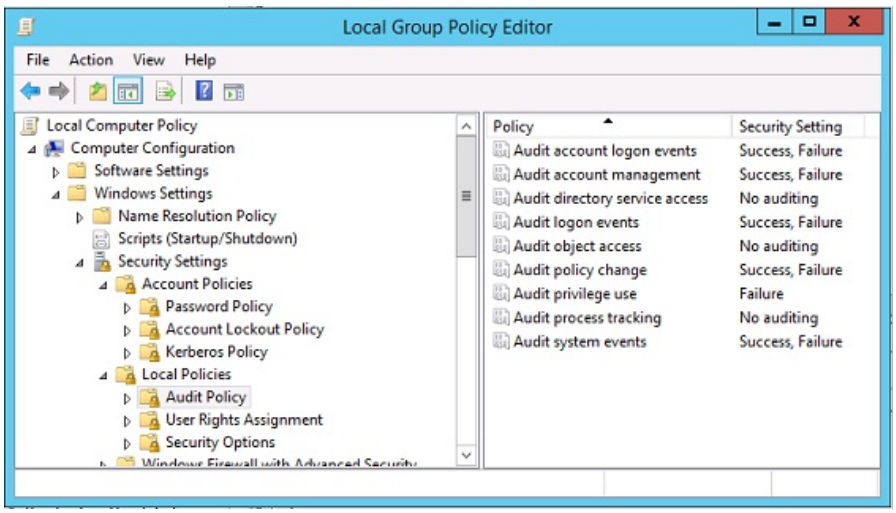
使用中のドメインコントローラーの識別

Windowsはログオン時に、ユーザーをログオンさせたドメインコントローラーをMSDOS環境変数に設定します。 これを参照するには、次のコマンドでコマンドプロンプトを起動します。 **echo %LOGONSERVER%**

認証に関するログは、このコマンドで返されたコンピューターに保存されます。

アカウント監査イベントの有効化

デフォルトで、Windowsドメインコントローラーは完全なアカウント監査ログを有効化していません。 これは、グループポリシーエディターで、セキュリティ設定の監査ポリシーを介して制御できます。有効化すると、ドメインコントローラーはセキュリティログファイル内に追加のイベントログ情報を作成します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

証明書検証ログ

証明書の有効性チェック

スマートカード証明書がDER証明書（秘密キー不要）としてエクスポートされた場合、次のコマンドで検証できます。certut –verify user.cer

CAPIログの有効化

ドメインコントローラーとユーザーマシンでは、イベントビューアーを開いて、Microsoft/Windows/CAPI2/Operational Logsのロギングを有効化します。

CAPIログは、次のレジストリキーで制御できます。CurrentControlSet\Services\crypt32

値	説明
DiagLevel（DWORD）	詳細度レベル（0～5）
DiagMatchAnyMask（QUADWORD）	イベントフィルター（すべてに0xffffffを使用）
DiagProcessName（MULTI_SZ）	プロセス名（たとえば、LSASS.exe）によるフィルター

CAPIのログ

メッセージ	説明
チェーンの構築	LSAがCertGetCertificateChainをコールしました（結果含む）
失効確認	LSAがCertVerifyRevocationをコールしました（結果含む）
X509オブジェクト	詳細モードでは、証明書と証明書失効リスト（CRL）がAppData\LocalLow\Microsoft\X509Objectsにダンプされます

© 1999-2017 Citrix Systems, Inc. All rights reserved.

チェーンポリシーの検証	LSAがCertVerifyChainPolicyをコールしました（パラメーター含む）

エラーメッセージの意味

エラーコード	説明
信頼されていない証明書	スマートカード証明書を、証明書を使用してコンピューターの中間証明書ストアおよび信頼できるルート証明書ストアに作成できませんでした。
証明書失効のチェックエラー	証明書CRL配布ポイントによって指定されたアドレスからスマートカードのCRLをダウンロードできませんでした。失効チェックが必須の場合、これが原因となってログオンが失敗します。「証明書と公開キー基盤」を参照してください。
証明書使用状況エラー	証明書がログオンに適していません。たとえば、サーバー証明書または署名証明書の可能性があります。

Kerberosログ

Kerberosログを有効化するには、ドメインコントローラーおよびエンドユーザーマシン上で次のレジストリ値を作成します。

ハイブ	値の名前	値［DWORD］
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberosログはシステムイベントログに出力されます。

- 「信頼できない証明書」などのメッセージは診断が簡単です。
- 次の2つのエラーコードは情報提供目的のもので、無視しても問題ありません。
  - KDC_ERR_PREAUTH_REQUIRED（以前のドメインコントローラーとの後方互換性のために使用）
  - 不明なエラー0x4b

© 1999-2017 Citrix Systems, Inc. All rights reserved.

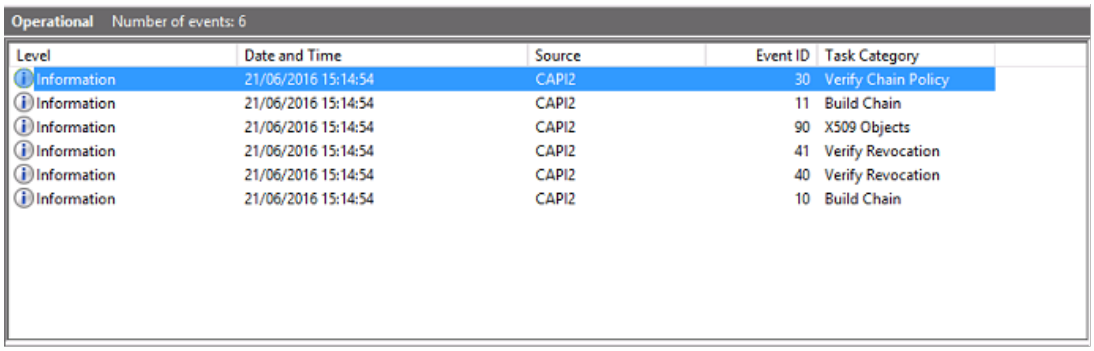
イベントログメッセージ

ここでは、ユーザーが証明書を使用してログオンした場合にドメインコントローラーおよびワークステーションに出力されるログエントリの例について説明します。

- ドメインコントローラーCAPI2ログ
- ドメインコントローラーセキュリティログ
- VDAセキュリティログ
- VDA CAPIログ
- VDAシステムログ

ドメインコントローラーCAPI2ログ

ログオン時にドメインコントローラーは発信者の証明書を検証し、一連のログエントリを次の形式で作成します。



最終イベントログメッセージは、VDAによって提供される証明書に基づいてチェーンを作成するドメインコントローラー上にlsass.exeを表示し、その妥当性（失効など）を検証します。結果は「ERROR_SUCCESS」として戻されます。

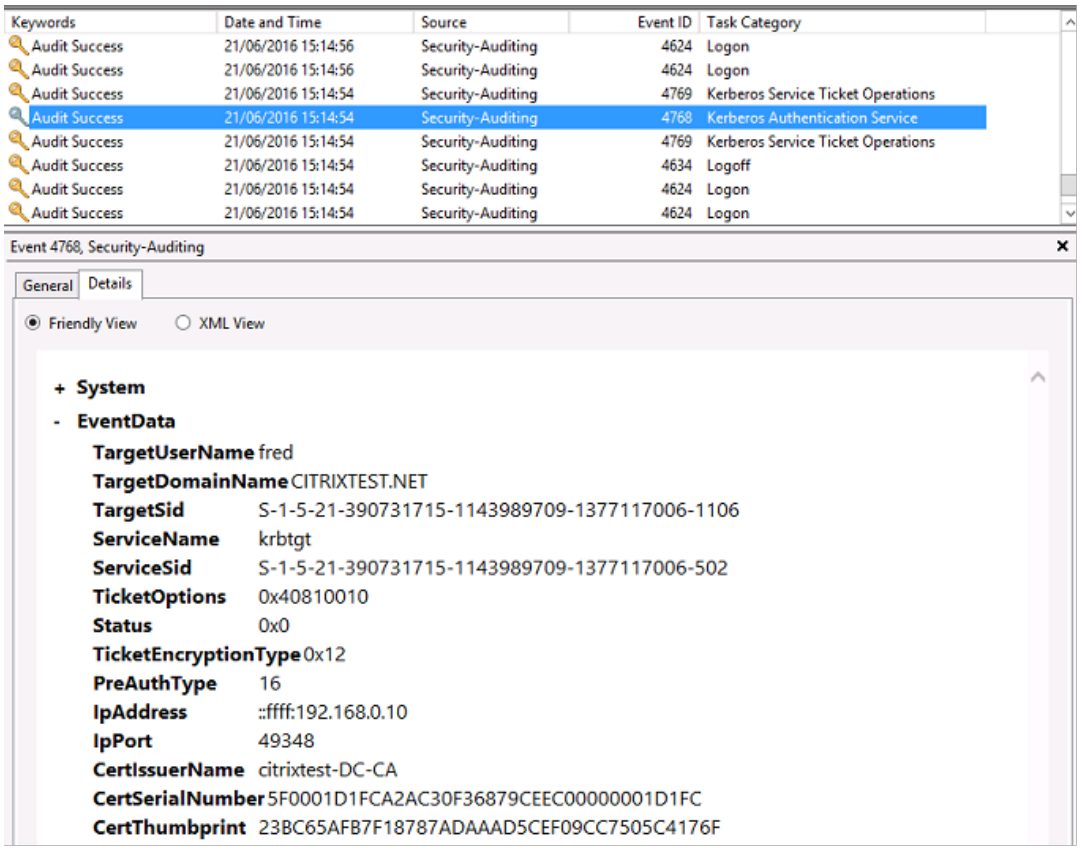
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ドメインコントローラーセキュリティログ

ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは4768で、証明書を使用してKerberos Ticket Granting Ticket（krbtgt）を発行します。

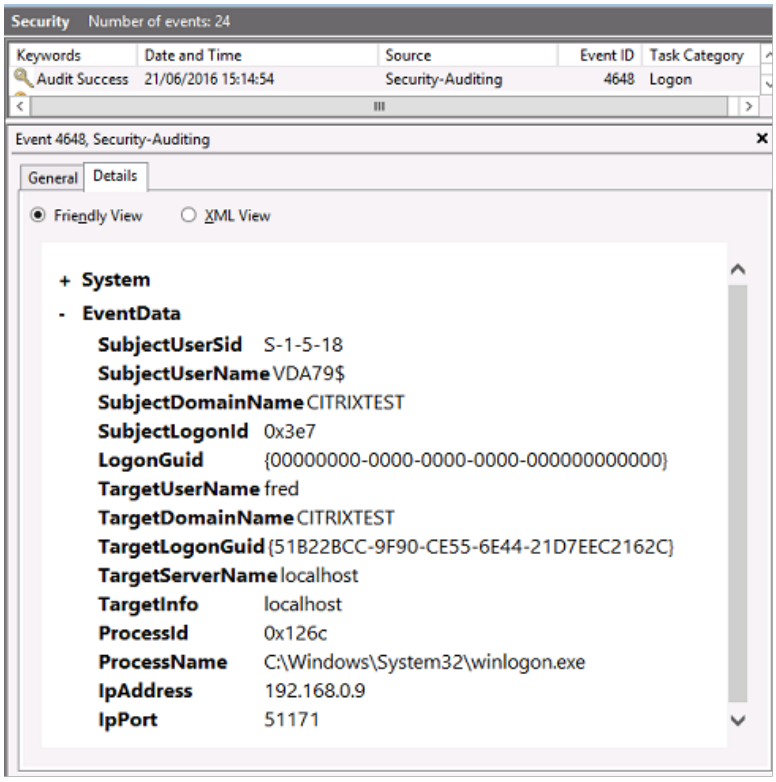
これより前のメッセージは、ドメインコントローラーに対して認証するサーバーのマシンアカウントを表示します。 これより後のメッセージは、ドメインコントローラーに対して認証するために使用される新しいkrbtgtに属するユーザーアカウントを表示します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAセキュリティログ

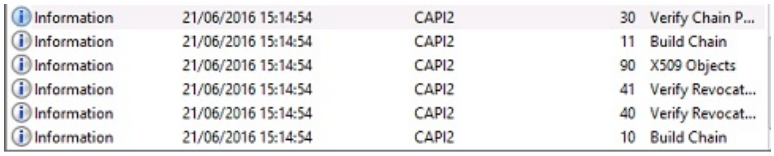
ログオンイベントに対応するVDAセキュリティ監査ログはイベントIDが4648のエントリで、winlogon.exeにより記録されます。



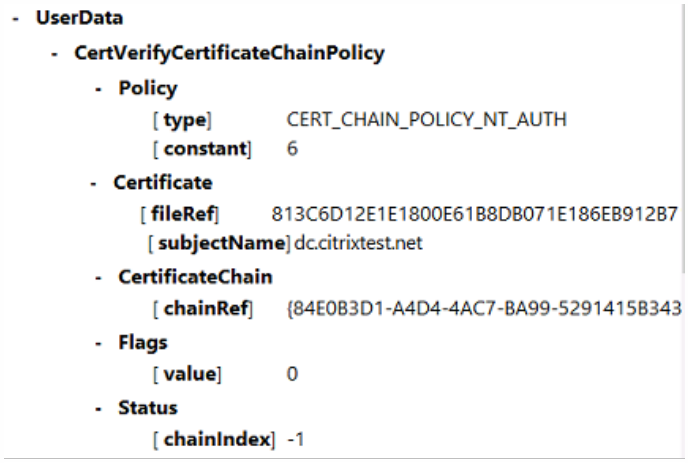
© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA CAPIログ

このサンプルのVDA CAPIログは、lsass.exeから単一のチェーンビルドおよび検証シーケンスを示しており、ドメインコントローラー証明書（dc.citrixtest.net）を検証しています。



Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain P...
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

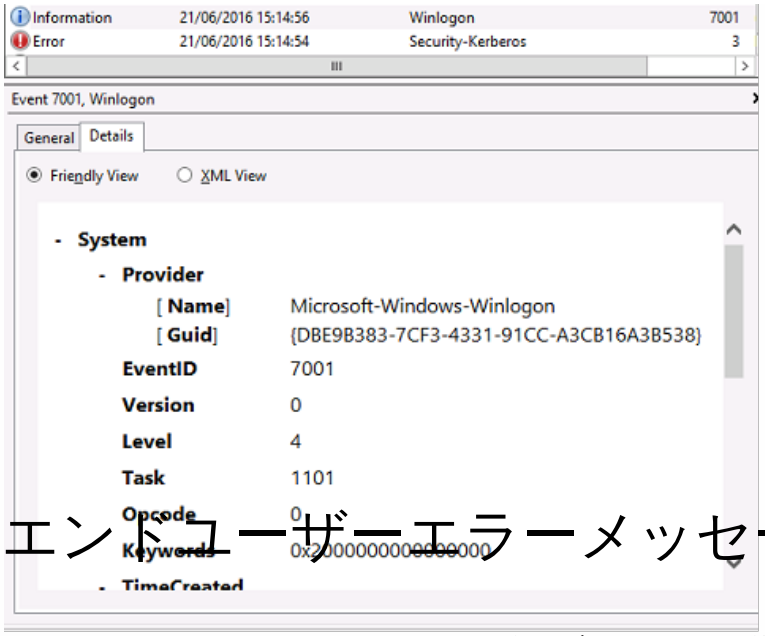


- **UserData**
  - **CertVerifyCertificateChainPolicy**
    - **Policy**
      - [**type**] CERT_CHAIN_POLICY_NT_AUTH
      - [**constant**] 6
    - **Certificate**
      - [**fileRef**] 813C6D12E1E1800E61B8DB071E186EB912B7
      - [**subjectName**] dc.citrixtest.net
    - **CertificateChain**
      - [**chainRef**] {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - **Flags**
      - [**value**] 0
    - **Status**
      - [**chainIndex**] -1

VDAシステムログ

Kerberosログが有効化されている場合、システムログは、エラーKDC_ERR_PREAUTH_REQUIRED（無視してかまいません）と、Kerberosログオンが成功したことを示すWinlogonからのエントリを表示します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



エンドユーザーエラーメッセージ

ここでは、Windowsログオンページでユーザーに表示される一般的なエラーメッセージの一覧を示します。

表示されるエラーメッセージ	説明および参照先
無効なユーザー名またはパスワードです。	コンピューターはユーザーが有効な証明書および秘密キーを持っていると判断していますが、Kerberosドメインコントローラーが接続を拒否しました。この記事の「Kerberosログ」を参照してください。
システムにログオンできませんでした。資格情報を確認できませんでした。 要求がサポートされていません	ドメインコントローラーに通信できないか、ドメインコントローラーに適切な証明書がインストールされていません。 CTX206156の記述に従って、「ドメインコントローラー」および「ドメインコントローラーの認証」証明書をドメインコントローラーに再登録します。 これは通常試す価値があります。既存の証明書が有効に見える場合でも同様です。
システムにログオンできませんでした。認証のために使用されたスマートカード証明書が信頼できませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。ドメイン不参加のコンピューターへのスマートカード証明書のインストール手順は、CTX206156を参照してください。この記事の証明書と公開キー基盤も参照してください。
アカウントでスマートカードログオンがサポートされていないためログオンできません。	ワークグループユーザーアカウントが、スマートカードログオンに対して完全には構成されていません。
要求されたキーが存在しません	証明書が秘密キーを参照しており、アクセスできません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	PIVカードが完全に構成されていないか、CHUIDまたはCCCファイルがない場合に発生することがあります。
スマートカードの使用を試行中にエラーが発生しました	スマートカードミドルウェアが正しくインストールされていません。 スマートカードのインストール手順はCTX206156を参照してください。
スマートカードを挿入してください	スマートカードまたはリーダーが検出されませんでした。スマートカードが挿入されている場合、このメッセージはハードウェアまたはミドルウェアに問題があることを示します。スマートカードのインストール手順はCTX206156を参照してください。
PINが不正確です	ユーザーが入力したPINをスマートカードが拒否しました。
有効なスマートカード証明書が見つかりませんでした。	T証明書の拡張子が正しく設定されていないか、RSAキーが短すぎます（2048ビット未満）。 有効なスマートカード証明書の生成について詳しくは、CTX206901を参照してください。
スマートカードがブロックされています	スマートカードがロックされています（たとえば、ユーザーが不正確なPINを複数回入力しました）。 管理者は、スマートカードベンダー提供のツールを使用してカードのPINロック解除コード（puk）を取得し、ユーザーPINをリセットできる場合があります。 pukコードが利用できないかロックアウトされている場合、カードを工場出荷時の設定にリセットする必要があります。
不正な要求	スマートカード秘密キーが、ドメインコントローラーが必要とする暗号化をサポートしていません。たとえば、ドメインコントローラーが「秘密キー復号化」を要求したのに、スマートカードが署名しかサポートしていないことがあります。 これは通常、証明書の拡張子が正しく設定されていないか、RSAキーが短すぎることを示します（2048ビット未満）。 有効なスマートカード証明書の生成について詳しくは、CTX206901を参照してください。

関連情報

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- スマートカードログオン用のドメインの構成：http://support.citrix.com/article/CTX206156
- スマートカードログオンポリシー：https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- CAPIログの有効化： http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Kerberosログの有効化： https://support.microsoft.com/en-us/kb/262177
- サードパーティの証明機関を使用してスマートカードログオンを有効化するためのガイドライン： https://support.microsoft.com/en-us/kb/281245

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Federated Authentication ServiceのPowerShellコマンドレット

Dec 05, 2017

シンプルな展開ではFederated Authentication Service管理コンソールも使用できますが、PowerShellインターフェイスにはより詳細なオプションがあります。 コンソールでは使用できないオプションを使用する場合は、PowerShellのみを使用して構成を行うことをお勧めします。

次のコマンドによってFAS PowerShellコマンドレットが追加されます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

PowerShellウィンドウでは、Get-Help <*cmdlet name*>を使用して、コマンドレットのヘルプを表示できます。

次のリンク先にあるzipファイルには、すべてのFAS PowerShell SDKコマンドレットのヘルプファイルが含まれています。このファイルを使用するにはリンクをクリックします。zipファイルがダウンロードされます。続いて、ローカルフォルダーに内容を展開します。index.htmlファイルには、すべてのコマンドレットの一覧が、各コマンドレットヘルプファイルへのリンクとともに記載されています。

ZIP Federated Authentication ServiceのPowerShellコマンドレットのヘルプファイル

© 1999-2017 Citrix Systems, Inc. All rights reserved.

グラフィック

Dec 05, 2017

Citrix HDXグラフィックは広範囲な一連のグラフィックアクセラレーションと、XenAppおよびXenDesktopからのリッチグラフィックアプリケーションの配信を最適化するエンコード技術を備えています。このグラフィック技術は、グラフィックを多用する仮想アプリケーションをリモートで使用する際に、物理デスクトップを使う場合と同じ操作性を提供します。

グラフィックにはハードウェアまたはソフトウェアレンダリングが使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティのライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックのためのWARPラスタライザーが含まれています。他のソフトウェアレンダラーを使うことも可能です（OpenGL Software Acceleratorなど）。ハードウェアレンダリング（ハードウェアアクセラレーション）にはグラフィックプロセッサー（GPU）が必要です。

HDXグラフィックは、一般的なユースケースのほとんどの場合に最適化された、デフォルトのエンコーディング構成を備えています。Citrixポリシーを使用すると、IT管理者は異なる要件を満たすさまざまなグラフィック関連の設定を構成し、望ましいユーザーエクスペリエンスを実現することもできます。

Thinwire

Thinwireとは、XenAppおよびXenDesktopで使用される、Citrixのデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。グラフィックは、ユーザー入力（たとえば、キー入力やマウス操作）の結果として生成されます。

HDX 3D Pro

XenAppおよびXenDesktopのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィック処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGLやDirectXを使用する3Dプロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準VDAでは、DirectXのGPUアクセラレーションのみがサポートされます。

WindowsデスクトップOSのためのGPUアクセラレーション

HDX 3D Proを使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりデスクトップOSマシンのアプリケーションとして配信したりできます。HDX 3D Proは、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、およびHyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化技術をサポートします。

GPUパススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数のGPUを装着して、各仮想マシンにGPUを1つずつ割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンで単一の物理GPUによるグラフィック処理能力に直接アクセスできるようになります。

WindowsサーバーOSのためのGPUアクセラレーション

HDX 3D Pro機能により、WindowsサーバーOSのセッションで実行しているグラフィック処理アプリケーションで、サーバー上のGPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）の処理をサーバーのGPUに移すことで、グラフィック処理によりサーバーのCPU

© 1999-2017 Citrix Systems, Inc. All rights reserved.

速度が低下することを回避できます。また、ワークロードがCPUとGPUで分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Framehawk

Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawkはスペクトル干渉や 多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供しています。

OpenGLソフトウェアアクセラレータ

OpenGLソフトウェアアクセラレータは、ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、コンピューター支援設計、およびコンピューター支援製造などのOpenGLアプリケーションで使用するソフトウェアラスタライザーです。OpenGLソフトウェアアクセラレータを使用すると、グラフィックカードを装着しなくてもユーザーに良好なユーザーエクスペリエンスを提供できる場合があります。

関連情報

- Thinwire
- HDX 3D Pro
- GPU acceleration for Windows Desktop OS
- GPU acceleration for Windows Server OS
- Framehawk
- OpenGL Software Accelerator

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Framehawk

Dec 05, 2017

Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawkはスペクトル干渉や 多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供しています。Framehawkは、少量のパケット損失がユーザーエクスペリエンスを低下させる可能性がある、長距離（低速）ブロードバンドネットワーク接続を利用しているユーザーに適している場合があります。このユースケースではアダプティブトランスポートを使用することをお勧めします。詳細については、「アダプティブトランスポート」を参照してください。

Citrixポリシーテンプレートを使用し、組織に適した方法で、一連のユーザーとアクセスシナリオ用にFramehawkを実装します。Framehawkは、ラップトップやタブレットなど、単一画面でのモバイルユースケースをターゲットにしています。リアルタイムの対話的なパフォーマンスによってサーバーリソースの追加コストやブロードバンド接続の要件の正当性が証明される場合にFramehawkを使用します。

Framehawkはどのようにして円滑なユーザーエクスペリエンスを維持するか

Framehawkは人間の目をソフトウェアとして実装したもので、フレームバッファーの中に何があるかを確認したり、画面上のさまざまなコンテンツの種類を識別したりするものと考えてください。ユーザーにとって重要なものはなんでしょうか。画面エリアが動画や動くグラフィックのように急速に変化している場合は、多少のピクセルが失われていても、新しいデータですぐに上書きされますから、人間の目にとっては大したことではありません。

しかし、通知エリアやツールバーのアイコン、読み始めたいところまでユーザーがスクロールした後のテキストのように画面で変化しない領域は、人間の目が細部にまでこだわるところです。ユーザーは、このようなエリアではピクセルが完璧であることを期待します。**0**と**1**の観点から技術的に正確であることを目的としたプロトコルと異なり、Framehawkの目的は、このテクノロジーを使用する人間にとって適切なものであることです。

Framehawkは、次世代QoS信号増幅器に加え、ワークロードをきめ細かく、より効率的に識別するための時間をベースにしたヒートマップを搭載しています。Framehawkはデータ圧縮に加えて、自動自己回復変換を使用します。また、データの再送信を回避し、クリック応答、線形性、一貫したリズムを維持します。損失の多いネットワーク接続では、Framehawkは補間を使って損失を隠すため、ユーザーは良好なイメージ品質を感じながら、流れるようなエクスペリエンスを楽しむことができます。さらに、Framehawkのアルゴリズムはさまざまな種類のパケット損失をインテリジェントに区別します。たとえば、ランダム損失（補正のためにさらにデータを送信）と輻輳損失（チャンネルはすでに渋滞しているので追加のデータは送信しない）などです。

Citrix ReceiverのFramehawk Intent Engineは、上スクロールと下スクロール、ズーム、左または右方向への移動、読み込み、入力などの一般的な操作を区別します。エンジンはまた、共有ディクショナリを使用して、Virtual Delivery Agent（VDA）への通信を管理します。ユーザーが読もうとしているテキストは、高い品質で表示されなければなりません。スクロールはすばやく、スムーズであることが必要です。また、一時停止もできなければなりません。これにより、ユーザーはアプリケーションやデスクトップとのやりとりを常に制御できる立場でいられます。

ネットワーク接続のリズムを測定すること（自転車のチェーンの張力にたとえて「**ギアリング**」）により、Framehawkロジックはよりすばやく反応し、遅延の大きな接続でも優れたエクスペリエンスを提供します。特許を取得したこの独特なギアリングシステムから、ネットワーク接続について、継続的に最新のフィードバックが得られるため、Framehawkは帯域幅や遅延性、損失率の変化に即対応できます。

ThinwireとFramehawkを使用する場合の設計について考慮すべきこと

Thinwireは帯域幅効率において業界をリードし、さまざまなアクセス条件やネットワーク状態に適合していますが、信頼でき

© 1999-2017 Citrix Systems, Inc. All rights reserved.

るデータ通信を実現するためにTCPを使用しています。そのため、損失率の高いネットワークや過負荷状態のネットワークでは、パケットを再送信しなければならず、これがユーザーエクスペリエンスの低下につながります。Enlightened Data Transport（EDT）レイヤー上でThinwireを使用可能にすることによって、高遅延ネットワーク接続上でのTCP制限に対処しています。

Framehawkは、UDP（ユーザーデータグラムプロトコル）上に作成されたデータ転送レイヤーを使用します。Framehawkとその他のUDPベースのプロトコルのパフォーマンスを比較すればわかるとおり、UDPは、Framehawkで損失性を打開する方法のほんの一部に過ぎません。UDPは、Framehawkを際立たせる、人間を主体にした技術の重要な基礎を提供します。

Framehawkで必要な帯域幅

ブロードバンドワイヤレスの意味は、接続を共有するユーザーの人数、接続の品質、使用しているアプリなどいくつかの要素によって変わります。最適なパフォーマンスを上げるには、基本の4Mbpsまたは5Mbpsに、同時に使用しているユーザー1人につき約150Kbpsを加えることをお勧めします。

Thinwireの帯域幅の推奨は、通常、基本の1.5Mbpsに、ユーザー1人につき150Kbpsを追加します。詳しくは、XenApp およびXenDesktop帯域幅ブログを参照してください。Thinwire over TCPでは3%のパケットが失われるため、有益なユーザーエクスペリエンスを保証するには、Framehawkよりもかなり大きな帯域幅が必要であることがわかります。

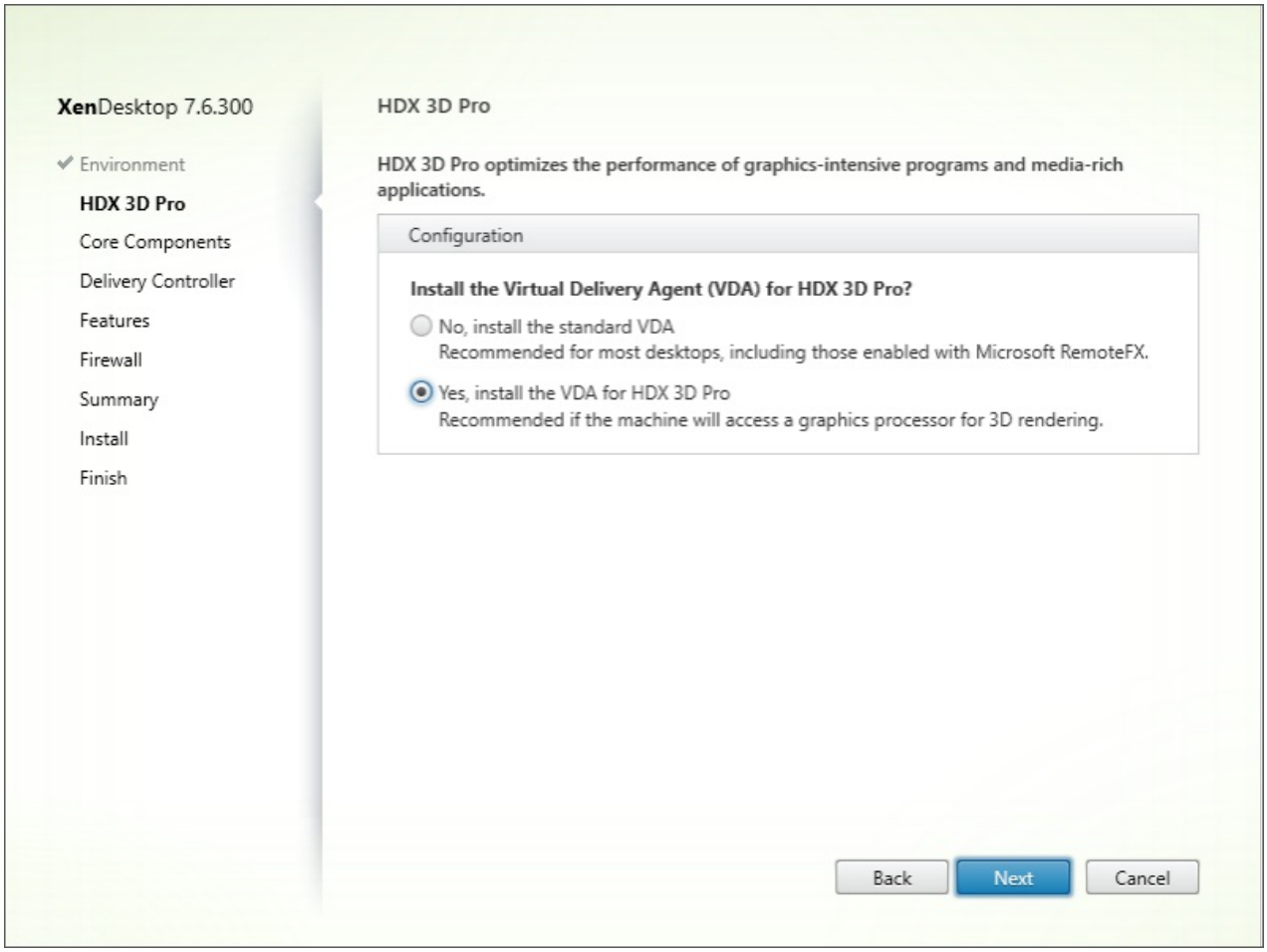
Thinwireは、ICAプロトコルのディスプレイリモート処理では、プライマリチャネルのままです。Framehawkは、デフォルトで無効になっています。Citrixは必要に応じて有効、無効を切り替えることで、組織のブロードバンドワイヤレスアクセスシナリオに対応することを推奨します。Framehawkは、Thinwireよりかなり多くのサーバーリソース（CPUとメモリ）を必要とすることに注意してください。

FramehawkおよびHDX 3D Pro

Framehawkでは、XenApp（サーバーOS）およびXenDesktop（デスクトップOS）アプリケーションの両方で、すべてのHDX 3D Proのユースケースがサポートされます。遅延が400～500ミリ秒、パケット損失が1～2%の顧客環境で検証されました。そのため、AutoCADやSiemens NXなどの一般的な3Dモデリングアプリケーションで素晴らしい対話操作性が得られます。これにより、移動中や、国外または劣悪なネットワーク環境で作業を行う場合も、より大規模なCADモデルを表示させて操作できるようになりました。（長距離ネットワーク接続上で3Dアプリケーションを提供する必要がある組織は、アダプティブトランスポートを使用することをお勧めします。詳細については、「アダプティブトランスポート」を参照してください。）

この機能を有効にするために、追加の構成作業を行う必要はありません。VDAをインストールするとき、最初に3DProオプションを選択してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



このように選択すると、HDXはCitrixビデオドライバーでなくGPUベンダーのビデオドライバーを使用します。通常のデフォルトであるSelective H.264エンコーディングを使用するアダプティブ表示でなく、Thinwire上の全画面H.264エンコーディングをデフォルトとします。

要件および考慮事項

Framehawkでは、少なくとも、VDA 7.6.300およびグループポリシー管理7.6.300が必要です。

エンドポイントには、少なくとも、Citrix Receiver for Windows 4.3.100、またはCitrix Receiver for iOS 6.0.1が必要です。

デフォルトではFramehawkは、双方向のユーザーデータグラムプロトコル（UDP）ポート範囲（3224～3324）を使用して、Framehawkディスプレイチャネルデータ がCitrix Receiverと交換されます。この範囲は、**Framehawkディスプレイチャネルのポート範囲**と呼ばれるポリシー設定でカスタマイズできます。クライアントと仮想デスクトップの間の同時接続1つにつき、固有のポートが1つ必要になります。XenAppサーバーなど、マルチユーザーOS環境では、同時ユーザーセッションを上限までサポートするために、十分な数のポートを定義してください。VDIデスクトップのようなシングルユーザーOSでは、UDPポートを1つ定義すれば十分です。Framehawkは最初に定義されたポートを使用しようとし、範囲内で指定された最後のポートまで進みます。これは、NetScaler Gatewayを通過する場合と、StoreFrontサーバーへの直接内部接続の両方に当てはまります。

リモートアクセスの場合は、NetScaler Gatewayを必ず展開してください。デフォルトでは、NetScalerは、クライアントCitrix ReceiverとGatewayの間での暗号化通信のためにUDPポート443を使用します。双方向通信を確実に行うためには、外側のファイアウォールすべてで、このポートを開いておく必要があります。この機能はDatagram Transport Layer Security（DTLS）と呼ばれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注： Framehawk/DTLS接続は、FIPSアプライアンスではサポートされません。

暗号化されたFramehawk接続は、NetScaler Gateway Version 11.0.62およびNetScaler Unified Gateway Version 11.0.64.34からサポートされています。

NetScaler High Availability（HA）は、XenAppおよびXenDesktop 7.12以降でサポートされています。

Framehawkを実装する前に、以下のベストプラクティスを検討してください。

- セキュリティ管理者に問い合わせ、Framehawk用に定義されたUDPポートがファイアウォールで開かれていることを確認してください。インストール中にファイアウォールが自動的に構成されることはありません。
- 多くの場合、NetScaler GatewayはDMZにインストールされ、外側だけでなく内側もファイアウォールで守られます。外側のファイアウォールでUDPポート443が開いていることを確認してください。デフォルトのポート範囲を使用している環境では、内側のファイアウォールでUDPポート3224～3324が開いていることを確認してください。

構成

注意： Citrixは、大きなパケット損失が発生していると思われるユーザーについてのみ、Framehawkを有効化することを推奨します。また、Framehawkを、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。

Framehawkは、デフォルトで無効になっています。この機能を有効にすると、ユーザーのグラフィックスおよび入力に対して、サーバーでFramehawkの使用が試みられます。何らかの理由で前提条件が満たされていない場合、接続はデフォルトモード（Thinwire）で確立されます。

Framehawkに影響を与えるポリシー設定は以下のとおりです。

- Framehawkディスプレイチャネル：機能を有効または無効にします。
- Framehawkディスプレイチャネルのポート範囲：ユーザーデバイスとFramehawkディスプレイチャネルデータの交換にVDAで使用するUDPポート番号の範囲（最小ポート番号から最大ポート番号まで）を指定します。VDAは、各ポートの使用を試行します。まず、最小のポート番号から始めて、2回目以降の試行では1つずつ番号を増やしていきます。ポートは、受信トラフィックと送信トラフィックに使用されます。

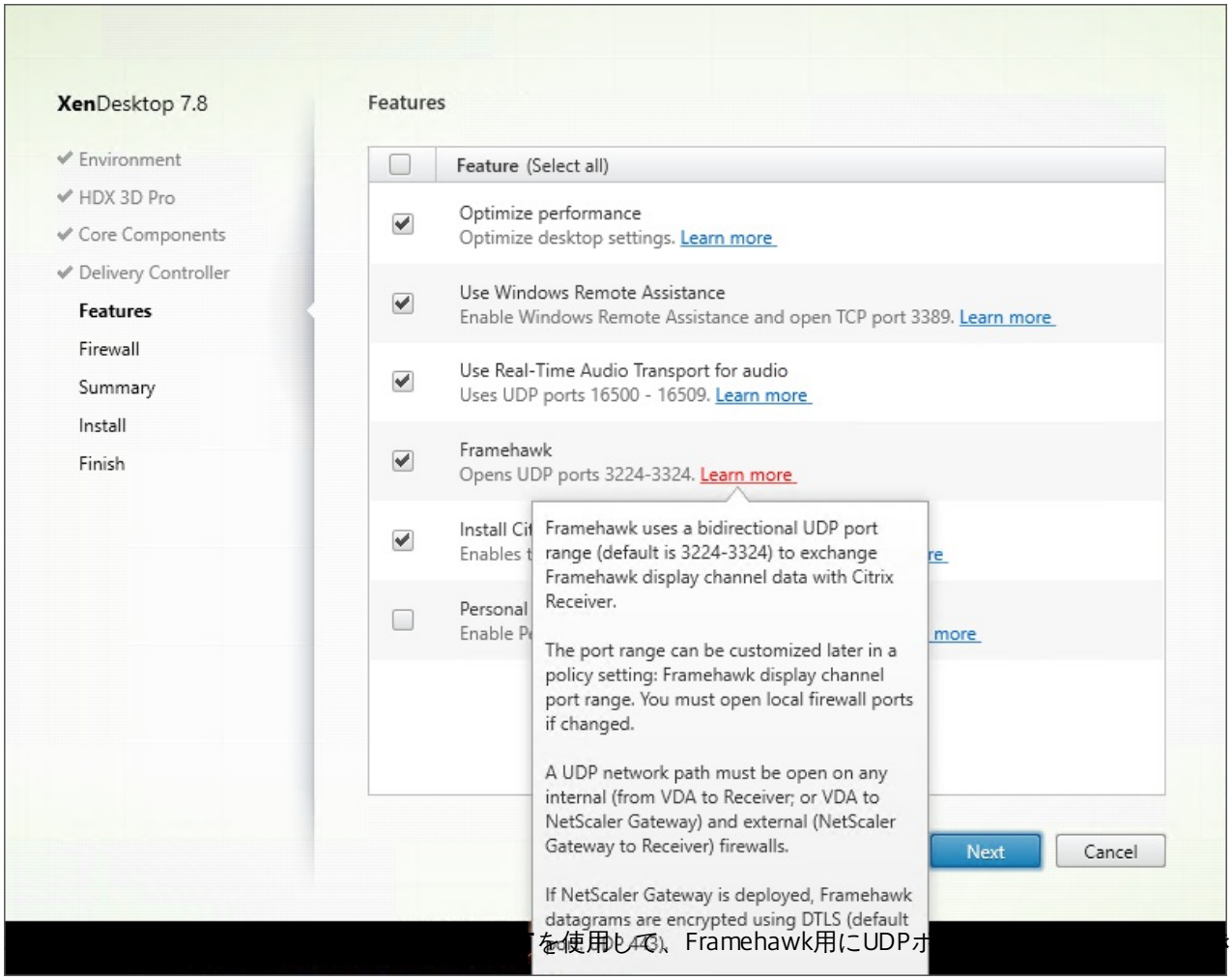
Framehawkディスプレイチャネル用のポートの開放

XenAppおよびXenDesktop 7.8以降では、VDAインストーラーの **[機能]** 手順でファイアウォールを再構成する新たなオプションが使用できるようになりました。このチェックボックスをオンにすると、WindowsのファイアウォールでUDPポート3224～3324が開放されます。以下の場合は、手動でファイアウォールを構成する必要があります。

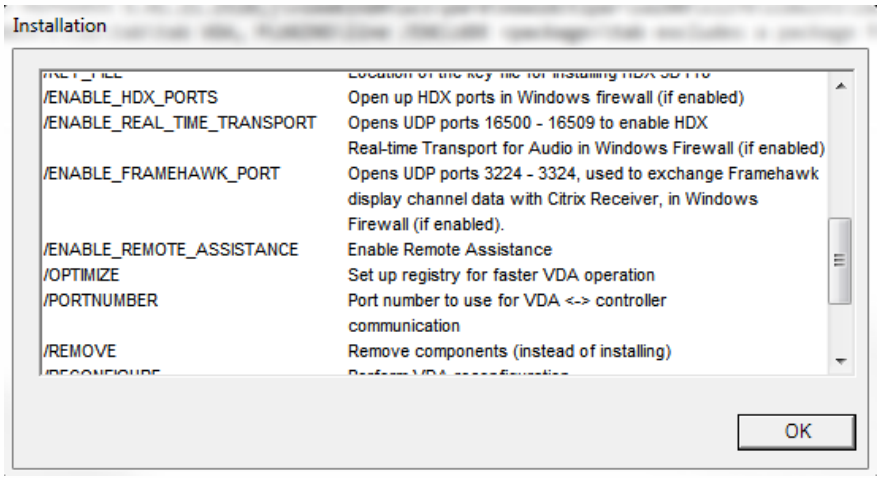
- ネットワークファイアウォールの場合。
  または
- デフォルトのポート範囲がカスタマイズされている場合。

これらのUDPポートを開放するには、 **[Framehawk]** チェックボックスをオンにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



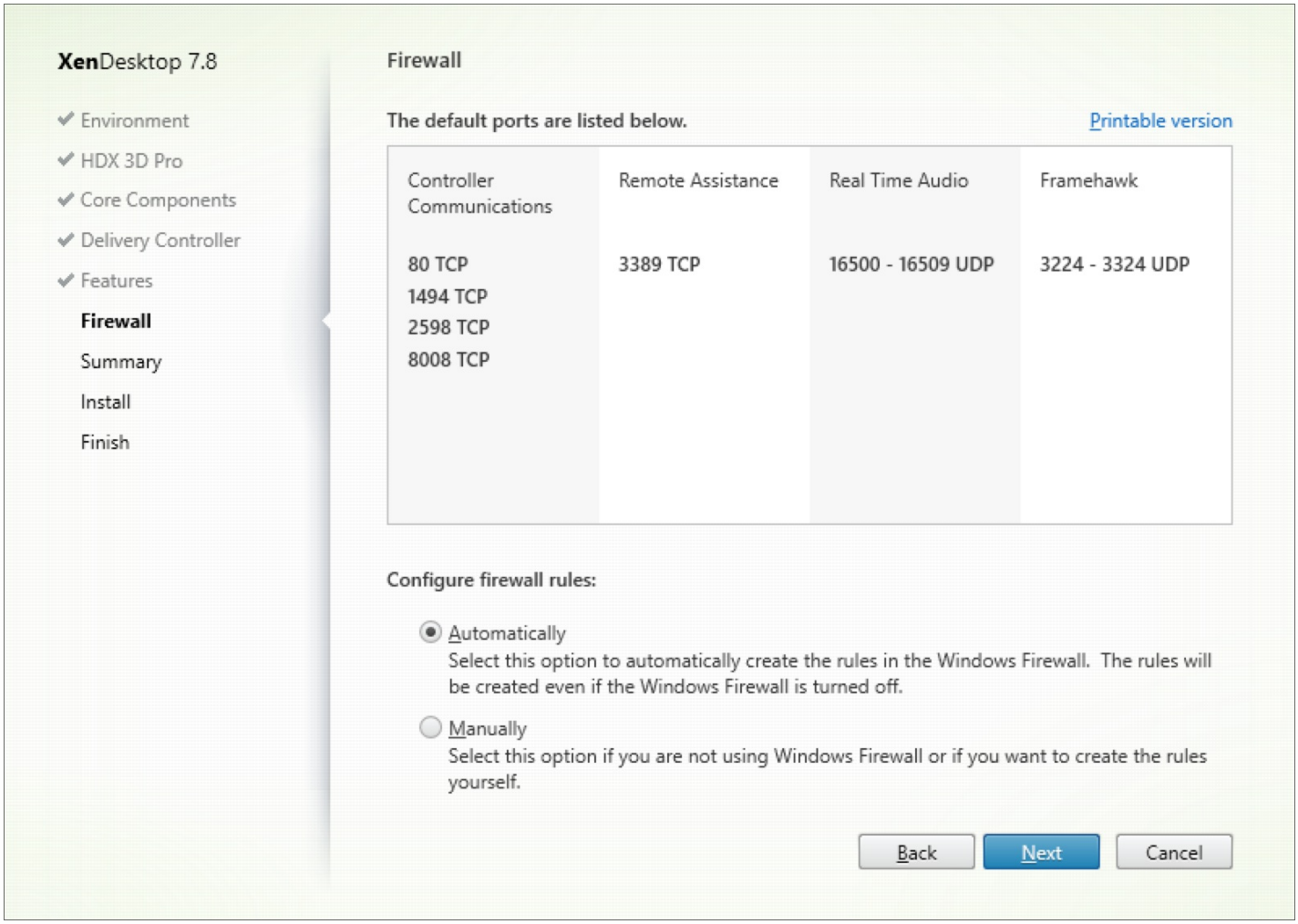
を使用して、Framehawk用にUDPポ ます。



FramehawkのUDPポートの割り当ての確認

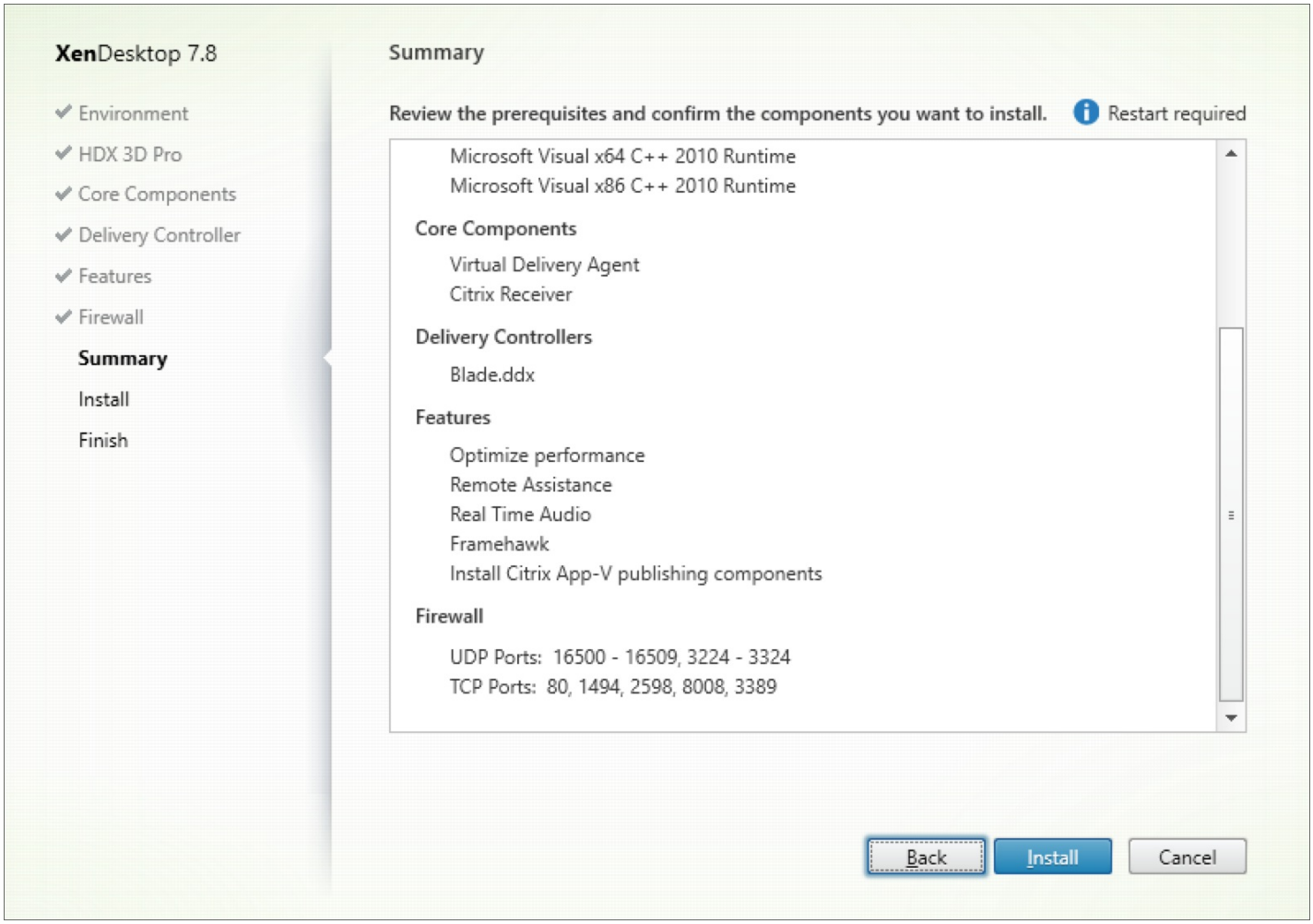
インストール中に、Framehawkに割り当てられたUDPポートを、以下のように**[ファイアウォール]** 画面で確認できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[概要] 画面には、Framehawk機能が有効になっているかどうかが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



FramehawkでのNetScaler Gatewayのサポート

暗号化されたFramehawkトラフィックは、NetScaler Gateway 11.0.62.10以降、およびNetScaler Unified Gateway 11.0.64.34以降でサポートされています。

- NetScaler Gatewayは、エンドユーザーのデバイスから直接、Gateway VPN vServerにアクセスできる展開アーキテクチャを参照します。つまり、VPN vServerには、パブリックIPアドレスが割り当てられていて、ユーザーはこのIPアドレスに直接接続します。
- Unified Gatewayを伴うNetScalerとは、Gateway VPN vServerがターゲットとしてContent Switching vServer（CS）にバインドされた展開を言います。この展開では、CS vServerはパブリックIPアドレスを持ち、Gateway VPN vServerはダミーのIPアドレスを持ちます。

NetScaler GatewayでFramehawkのサポートを可能にするには、Gateway VPN vServerレベルでDTLSパラメーターを有効化する必要があります。このパラメーターを有効化し、XenAppまたはXenDesktopでコンポーネントが正常に更新されると、Gateway VPN vServerとユーザーデバイスの間で、Framehawkのオーディオ、ビデオ、およびインタラクティブなトラフィックが暗号化されるようになります。

Framehawkでサポートされるのは、NetScaler Gateway、およびNetScaler Gatewayとグローバルサーバー負荷分散の組み合わせです。

Framehawkでは、次のシナリオはサポートされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- HDX Insight
- IPv6モードのNetScaler Gateway
- NetScaler Gatewayのダブルホップ
- クラスターセットアップ付きNetScaler Gateway

シナリオ	Framehawkのサポート
NetScaler Gateway	はい
NetScaler + グローバルサーバー負荷分散	はい
Unified Gatewayを伴うNetScaler	はい 注：バージョン11.0.64.34以降のUnified Gatewayがサポートされます。
HDX Insight	なし
IPv6モードのNetScaler Gateway	なし
NetScaler Gatewayのダブルホップ	なし
NetScaler Gateway上の複数のSecure Ticket Authority（STA）	はい
高可用性（HA）機能付きNetScaler Gateway	はい
クラスターセットアップ付きNetScaler Gateway	なし

FramehawkをサポートするようにNetScalerを構成する

NetScaler GatewayでFramehawkのサポートを可能にするには、Gateway VPN *vServer*レベルでDTLSパラメーターを有効化してください。このパラメーターを有効化し、XenAppまたはXenDesktopでコンポーネントが正常に更新されると、Gateway VPN vServerとユーザーデバイスの間で、Framehawkのオーディオ、ビデオ、およびインタラクティブなトラフィックが暗号化されるようになります。

リモートアクセスのために、NetScaler GatewayでUDP暗号化を実現するには、この構成が必須です。

FramehawkをサポートするようにNetScalerを構成する場合は

- 外側のファイアウォールすべてでUDPポート443が開いていることを確認します
- 外側のファイアウォールすべてでCGPポート（デフォルトは2598）が開いていることを確認します
- VPN仮想サーバーの設定でDTLSを有効化します
- SSL証明書とキーのペアのバインドをいったん解除してから、再びバインドしますNetScalerバージョン11.0.64.34以降をお使いの場合、この手順を行う必要はありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

FramehawkをサポートするようにNetScaler Gatewayを構成するには、以下の手順を実行します。

1. StoreFrontと通信し、XenAppおよびXenDesktopのユーザーを認証するように、NetScaler Gatewayを展開し、構成します。
2. NetScalerの［構成］タブで、［NetScaler Gateway］を展開し、**［仮想サーバー］**を選択します。
3. **［編集］**をクリックして、VPN仮想サーバーの［基本設定］を表示し、DTLS設定の状態を確認します。
4. その他の構成オプションを表示するには、**［詳細］**をクリックします。
5. Framehawkなどのデータグラムプロトコルを通信セキュリティで保護するには、**［DTLS］**を選択します。**［OK］**をクリックします。VPN仮想サーバーの［基本設定］領域には、DTLSフラグが［真］に設定されています。
6. サーバー証明書の［バインド］画面を再度開き、証明書キーペアをバインドするために、**［+］**をクリックします。
7. 前述の証明書キーペアを選択し、**［選択］**をクリックします。
8. サーバー証明書のバインドに変更を保存します。
9. 保存後、この証明書のキーペアが表示されます。**［バインド］**をクリックします。
10. 「**No usable ciphers configured on the SSL vserver/service**」という警告メッセージが表示されたら、無視してください。

旧バージョンのNetScaler Gatewayにおける手順

11.0.64.34より古いバージョンのNetScaler Gatewayを使用している場合は、以下の手順に従います。

1. サーバー証明書の［バインド］画面を再度開き、証明書キーペアをバインドするために、［+］をクリックします。
2. 前述の証明書キーペアを選択し、**［選択］**をクリックします。
3. サーバー証明書のバインドに変更を保存します。
4. 保存後、この証明書のキーペアが表示されます。**［バインド］**をクリックします。
5. 「**No usable ciphers configured on the SSL vserver/service**」という警告メッセージが表示されたら、無視してください。

FramehawkをサポートするようにUnified Gateway設定を構成するには：

1. Unified Gatewayがインストールされ、適切に構成されていることを確認します。詳しくは、製品ドキュメントサイトでUnified Gatewayの情報を参照してください。
2. ターゲット*vServer*としてCS *vServer*にバインドされているVPN*vServer*上で、DTLSパラメーターを有効にします。

制限事項

クライアントデバイス上に古いNetScaler Gateway仮想サーバーのDNSエントリがある場合、アダプティブトランスポートとFramehawkはUDPトランスポートではなくTCPトランスポートへフォールバックすることがあります。TCPトランスポートへのフォールバックが発生する場合は、クライアントのDNSキャッシュをクリアし、UDPトランスポートを使用して再接続しセッションを確立させます。

ほかのVPN製品のサポート

NetScaler Gatewayは、Framehawkで必要なUDP暗号化をサポートする唯一のSSL VPN製品です。ほかのSSL VPNや誤ったバージョンのNetScaler Gatewayが使用された場合、Framehawkポリシーの適用に失敗する可能性があります。従来型のIPSec VPN製品では、変更を加えなくともFramehawkがサポートされます。

FramehawkをサポートするようにCitrix Receiver for iOSを構成する

以前のバージョンのCitrix Receiver for iOSをFramehawkをサポートするように構成するには、default.icaを手作業で編集する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. StoreFrontサーバーで、c:\inetpub\wwwroot\にある自分のストアのApp_Dataディレクトリにアクセスします。
2. default.icaファイルを開き、[WFClient]セクションに「Framehawk=On」という行を追加します。
3. 変更を保存します。

この手順により、iOSデバイス上の互換性のあるCitrix ReceiverからFramehawkセッションを確立できるようになります。Receiver for Windowsを使用している場合、この手順は必要ありません。

> **注意**
>
> iOSバージョン7.0以降のReceiverを使用している場合、default.icaファイルにパラメータ**Framehawk=On**を明示的に追加する必要はありません。

データベースのモニター

Citrix DirectorからFramehawkの利用状況とパフォーマンスをモニターすることができます。HDX仮想チャネル詳細ビューには、あらゆるセッションで、Framehawkのトラブルシューティングやモニターに役立つ情報が表示されます。Framehawk関連のメトリックスを確認するには、**[グラフィック - Framehawk]**を選択します。

Framehawk接続が確立されていれば、詳細ページに**Provider = VD3D**と**Connected = True**が表示されます。仮想チャネルの状況がアイドルであるのは正常です。これは、モニターの対象がシグナリングチャネルで、これは最初のハンドシェイク中にしか使用されないからです。このページには、接続に関するその他の有益な統計も表示されます。

問題が発生した場合は、Framehawkのトラブルシューティングブログを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro

Dec 05, 2017

XenAppとXenDesktopのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGLやDirectXを使用する3Dプロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準VDAでは、DirectXのGPUアクセラレーションのみがサポートされます。標準またはHDX 3D Pro VDAの選択について詳しくは、「手順5：HDX 3D Proモードを有効にするかどうかを選択する」を「VDAのインストール」の記事内で参照してください。

サポートされているすべてのCitrix Receiverは、3Dグラフィックとともに使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、最新バージョンのCitrix Receiver for WindowsおよびCitrix Receiver for Linuxをお勧めします。サポートされているCitrix Receiverのバージョンについて詳しくは、「Lifecycle Milestones for Citrix Receiver」を参照してください。

これらの3Dグラフィック処理アプリケーションとして次のものがあります。

- コンピューター支援設計（CAD）、コンピューター支援製造（CAM）、およびコンピューター支援エンジニアリング（CAE）アプリケーション
- 地理情報システム（GIS）ソフトウェア
- 医療画像処理のための画像保存通信システム（PACS）
- 最新バージョンのOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLを使用するアプリケーション
- 並列計算にNVIDIA Compute Unified Device Architecture（CUDA）GPUを使用する計算集約型の非グラフィックアプリケーション

HDX 3D Proでは、さまざまな帯域幅において最適なユーザーエクスペリエンスが提供されます。

- WAN接続の場合：帯域幅が1.5MbpsのWAN接続でもインタラクティブなユーザーエクスペリエンスが提供されます。
- LAN接続の場合：LAN接続ではローカルデスクトップに匹敵するユーザーエクスペリエンスが提供されます。
  ユーザーが使用する複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えて、グラフィック処理をユーザー側から中央管理が可能なデータセンター内に移管できます。

HDX 3D Proにより、WindowsデスクトップOSマシンとWindowsサーバーOSマシンでのGPUアクセラレーションが提供されます。詳しくは、「WindowsデスクトップOSのためのGPUアクセラレーション」および「WindowsサーバーOSのためのGPUアクセラレーション」を参照してください。

HDX 3D Proは、次のハイパーバイザーが提供するGPUパススルーやGPU仮想化、およびベアメタルと互換性があります。

- Citrix XenServer
  - NVIDIA GRIDおよびIntel GVT-dによるGPUパススルー
  - NVIDIA GRIDおよびIntel GVT-gによるGPU仮想化
- Microsoft Hyper V
  - NVIDIA GRIDおよびAMDによるGPUパススルー（Discrete Device Assignment）
- VMware vSphere
  - NVIDIA GRID、Intel、およびAMD IOMMUによるGPUパススルー（vDGA）
  - NVIDIA GRIDおよびAMD MxGPUによるGPU仮想化

サポートされているXenServerバージョンについては、Citrix XenServerのハードウェア互換性リストを参照してください。

HDX Monitorを使用すると、HDX仮想テクノロジの操作と構成を検証して、HDXの問題を診断して解決できます。このツールの詳細およびダウンロードについては、https://taas.citrix.com/hdx/download/を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

WindowsデスクトップOSのためのGPUアクセラレーション

Dec 05, 2017

するX 3D Proを使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりデスクトップOSマシン上のアプリケーションとして配信したりできます。HDX 3D Proは、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、およびHyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化技術をサポートします。

GPUパススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数のGPUを装着して、各仮想マシンにGPUを1つずつ割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンで単一の物理GPUによるグラフィック処理能力に直接アクセスできるようになります。このハードウェアGPU共有により、より専門的で複雑な設計作業を行うユーザーに適したデスクトップが提供されます。NVIDIA GRIDカード（「NVIDIA GRID」参照）のGPU仮想化では、非仮想化オペレーティングシステムで動作するものと同じNVIDIAグラフィックドライバーが使用されます。GPU仮想化ではさらに、Intel GVT-g搭載のIntel Iris Graphicsを採用した第5世代および第6世代のIntel CPUもサポートされます。これらのIntelプロセッサーのファミリについて詳しくは、「第5世代Intel Coreプロセッサー」および「第6世代Intel Core i5プロセッサー」を参照してください。GPU仮想化は、AMD FirePro Sシリーズのサーバーカードでもサポートされています。AMD Professional Graphicsの仮想化ソリューションを参照してください。

HDX 3D Proの機能は以下のとおりです。

- WANおよびワイヤレス接続でのパフォーマンスを最適化するAdaptive H.264ベースの深圧縮。HDX 3D Proのデフォルトては、CPUベースの全画面H.264圧縮が使用されます。ハードウェアエンコーディングは、NVENCをサポートするNVIDIAカードで使用されます。
- 特殊なアプリケーションのための無損失圧縮オプション。HDX 3D ProではCPUベースの無損失コーデックも提供され、医療用画像処理などピクセル単位での精密なグラフィックが求められるアプリケーションがサポートされます。真の無損失圧縮はネットワークおよび処理リソースに対する負荷が非常に高いため、特殊なアプリケーションでのみ使用することをお勧めします。
  無損失圧縮を使用すると、以下のように動作します。
  - 表示しているフレームに非可逆圧縮が適用されているのか無損失圧縮が適用されているのかを示すインジケーターがユーザーの通知領域に表示されます。このインジケーターは、ポリシーの［表示品質］設定で［操作時は低品質］が選択されている場合に便利です。送信されたフレームが無損失の場合、このインジケーターが緑色になります。
  - ユーザーは、無損失スイッチを使ってセッション内でいつでも［常に無損失］モードを有効にできます。セッション中に無損失圧縮の有効/無効を切り替えるには、通知領域のインジケーターを右クリックするか、Alt+Shift+1キーを押します。
    無損失圧縮の場合：ポリシーで指定されているコーデックに関係なく、無損失コーデックが使用されます。

    非可逆圧縮の場合：デフォルトのコーデックまたはポリシーで指定されているコーデックが使用されます。

    無損失スイッチの設定は保持されず、次回のセッションではリセットされます。すべての接続で無損失コーデックが使用されるようにするには、ポリシーの［表示品質］設定で［常に無損失］を選択します。

- デフォルトのショートカットであるALT+SHIFT+1を無効にし、セッション内で無損失を選択または選択解除できます。HKLM\SOFTWARE\Citrix\HDX3D\LLIndicatorで新しいレジストリ設定を構成します。
  - 名前：HKLM_HotKey、種類：String

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ショートカットの組み合わせを構成する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=valです。キーはコンマ「,」で区切る必要があります。キーの順番は関係ありません。
- A、C、S、W、およびKはキーです。ここで、C=Control、A=ALT、S=SHIFT、W=Win、およびK=aが有効なキーです。Kに対して使用できる値は、0～9、a～z、およびすべての仮想キーコードです。仮想キーコードについて詳しくは、MSDNのVirtual-Key Codesを参照してください。
- 次に例を示します。
  - F10に、K=0x79を設定
  - Ctrl + F10に、C=1, K=0x79を設定
  - Alt + Aに、A=1, K=aまたはA=1, K=AまたはK=A, A=1を設定
  - Ctrl + Alt + 5に、C=1, A=1, K=5またはA=1, K=5, C=1を設定
  - Ctrl + Shift + F5、A=1, S=1, K=0x74を設定

注意： レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- 複数および高解像度モニターのサポート。デスクトップOSマシンでは、最大で4つのモニターが構成されたユーザーデバイスがサポートされます。ユーザーはそれらのモニターを自由に配置でき、解像度や向きが異なるモニターを組み合わせて使用できます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および使用できる帯域幅による制限を受けます。HDX 3D Proでは、ホストコンピューター上のGPUでサポートされるすべてのモニター解像度がサポートされます。
  また、Windows XPデスクトップでは、デュアルモニター構成が限定的にサポートされます。これについて詳しくは、「Windows XPまたはWindows Vista上のVDA」を参照してください。

- 動的解像度仮想デスクトップまたはアプリケーションのウィンドウのサイズを任意に変更できます。**注：** 解像度は、VDAのセッションウィンドウのサイズを変更することでのみ変更できます。VDAセッション内での解像度の変更（［コントロールパネル］>［デスクトップのカスタマイズ］>［ディスプレイ］>［画面の解像度］で変更）はサポートされていません。

- NVIDIA GRIDアーキテクチャのサポート。HDX 3D ProのGPUパススルーおよびGPU共有では、NVIDIA GRIDカードがサポートされます（「NVIDIA GRID」参照）。NVIDIA GRID vGPUを使用すると、複数の仮想マシンで単一の物理GPUに同時に直接アクセスできます。このとき、仮想化されていないオペレーティングシステムで動作するものと同じNVIDIAグラフィックドライバーが使用されます。
- Virtual Direct Graphics Acceleration（vDGA）を使ったVMware vSphereおよびVMware ESXのサポート - RDSおよびVDIの両方のワークロードで、vDGAがサポートされます。
- NVIDIA GRID vGPUおよびAMD MxGPUを使用するVMware vSphere/ESXのサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3ファミリによるデータセンターグラフィックのサポート。HDX 3D Proでは、サポートされるIntelプロセッサファミリで、マルチモニター（最大3つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。詳しくは、http://www.citrix.com/intelおよびhttp://www.intel.com/content/www/us/en/servers/data-center-graphics.htmlを参照してください。
- AMD FirePro Sシリーズのサーバーカードでの AMD RapidFireのサポート。HDX 3D Proでは、マルチモニター（最大6つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。注： HDX 3D ProによるAMD MxGPU（GPU仮想化）のサポートで対応しているのは、VMWare vSphereのvGPUのみです。GPUパススルーに対応しているのは、XenServerとHyper-Vです。詳しくは、「AMD Virtualization Solution」を参照してください。

- NVIDIA GPUの高パフォーマンスビデオエンコーダーとIntel Iris Proグラフィックプロセッサへのアクセス。この機能は、ポリシー設定（デフォルトで有効）によって制御され、H.264エンコーディングのハードウェアエンコーディングが許可さ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

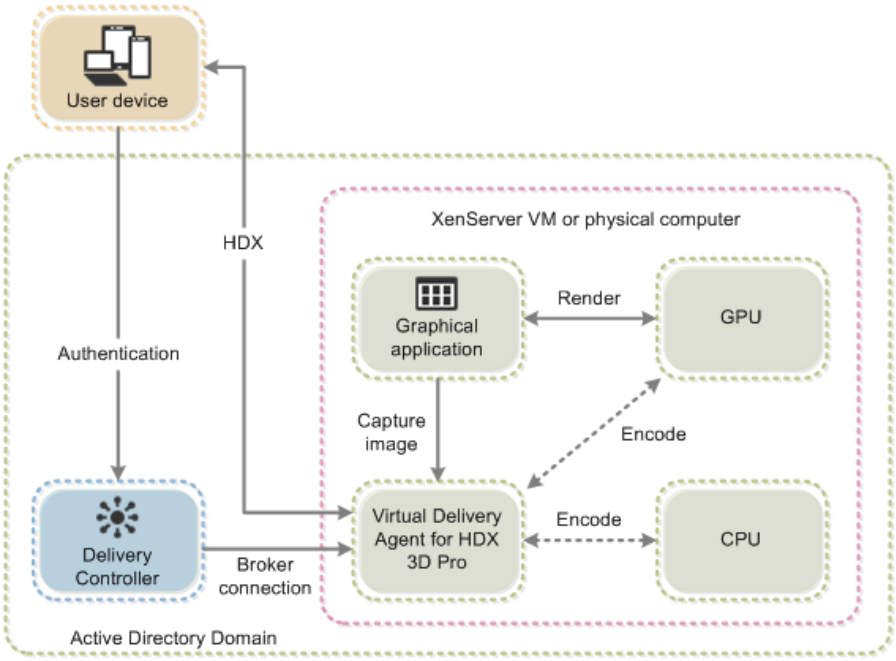
れます（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDAはソフトウェアビデオコーデックを使用してCPUベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

以下の図を参照してください。

- ユーザーがCitrix Receiverにログオンして仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証してVDA for HDX 3D Proと通信し、グラフィックアプリケーションをホストしているコンピューターへの接続を仲介します。

  VDA for HDX 3D Proはホスト上の適切なハードウェアを使って、デスクトップ全体またはグラフィックアプリケーションだけのビューを圧縮します。

- デスクトップまたはアプリケーションのビューおよびそれに対するユーザーの応答は、Citrix ReceiverとVDA for HDX 3D Pro間の直接HDX接続を介して、ホストコンピューターとユーザーデバイス間で転送されます。



VDA for HDX 3D Proのインストール

VDA for Windows Desktop OSをインストーラーのグラフィカルインターフェイスでインストールする場合は、［HDX 3D Pro］ページで［はい］をクリックします。コマンドラインでインストールする場合は、XenDesktop VdaSetup.exeコマンドに/enable_hdx_3d_proオプションを指定します。

HDX 3D Proをアップグレードするには、既存のHDX 3D for Professional GraphicsコンポーネントとVDAの両方をアンインストールしてからVDAをHDX 3D Proモードでインストールしてください。同様に、Windows Desktop OSで標準のVDAモードを3D Proモードに切り替える場合も、標準のVDAをアンインストールしてからVDAをHDX 3D Proモードでインストールしてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

標準モード	HDX 3D Proモード
一般的に、グラフィックのハードウェアアクセラレーションおよびリモートPCアクセスに最適です。	5つ以上のモニターが必要でない限り、一般的にグラフィックハードウェアアクセラレーションのあるデータセンターデスクトップに最適です。
リモートPCアクセスには、あらゆるGPUを使用できます（アプリケーション互換性の制限あり）。 • Windows 7、8、および8.1では、DirectX用GPUアクセラレーションの機能レベルは最大9.3です。一部のDirectX 10、11、12アプリケーションは、DirectX 9へのフォールバックをしない場合、実行されないことがあります。 • Windows 10の場合、GPUアクセラレーションはウィンドウ表示のDirectX 10、11、および12アプリに提供されます。DX 9アプリはWARPによってレンダリングされます。DXアプリを全画面モードで使用できません。 • GPUベンダーによってサポートされている場合はリモートセッションでのOpenGLアプリケーションアクセラレーション（現時点ではNVIDIAのみ）。	任意のGPUによるGPUアクセラレーションをサポートしますが、コンソールのブランキング、非標準画面解像度、およびTrue Multi MonitorサポートにはNVIDIA GRID、Intel Iris ProまたはAMD RapidFireグラフィックスが必要です。 広範なアプリケーション互換性のためにグラフィックベンダーのドライバーを活用します。 • GPUがサポートするすべての3D API（DirectXまたはOpenGL）。 • Intel Iris Pro（Win10のみ）、NVIDIA GRIDおよびAMD RapidFireでの全画面3Dアプリケーションサポート。 • カスタムドライバー拡張およびAPIのサポート（CUDAやOpenCLなど）。
任意のモニター解像度（上限はWindows OSおよびパフォーマンスによって決まります）および最大8つのモニター。	最大で4つのモニターをサポートします。
Intel Iris Proグラフィックプロセッサで利用可能なH.264ハードウェアエンコーディング。	Intel Iris ProグラフィックプロセッサおよびNVIDIAカードで利用可能なH.264ハードウェアエンコーディング。

NVIDIAドライバーのインストールとアップグレード

NVIDIA GRID APIでは、GPUのフレームバッファーに対する直接アクセスが提供され、スムーズでインタラクティブなユーザーエクスペリエンスのための最速のフレームレートが提供されます。NVIDIAドライバーをインストールしてからVDA for HDX 3D Proをインストールすると、NVIDIA GRIDがデフォルトで有効になります。

仮想マシン上でNVIDIA GRIDを有効にするには、デバイスマネージャーでMicrosoft基本ディスプレイアダプターを無効にします。次のコマンドを実行してからVDAを再起動します。 **NVFBCEnable.exe -enable -noreset**

VDA for HDX 3D ProをインストールしてからNVIDIAドライバーをインストールすると、NVIDIA GRIDが無効になります。この場合は、NVIDIA社から提供されるNVFBCEnableツールを使ってNVIDIA GRIDを有効にします。

NVIDIA GRIDを無効にするには、次のコマンドを実行してからVDAを再起動します。**NVFBCEnable.exe -disable -noreset**

Intelグラフィックドライバーのインストール

VDAをインストールする前にIntelグラフィックドライバーをインストールできます。次の手順は、VDA for HDX 3D Proをインストールした後、またはIntelドライバーが更新された後にのみ必要です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マルチモニターサポートに必要なIntelドライバーを有効にするには、GfxDisplayTool.exeを使用して次のコマンドを実行し、VDAを再起動します。 **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exeはVDAインストーラーに含まれています。GfxDisplayTool.exeはC:\Program Files\Citrix\ICAServicesにあります。

> **注意**
>
> ICAセッション内でのNVIDIAドライバーおよびIntelドライバーのアンインストールはサポートされていません。

HDX 3D Proのユーザーエクスペリエンスの最適化

マルチモニター環境でHDX 3D Proを使用するには、ユーザーデバイスに接続されているモニター数以上のモニターがホストコンピューター側に構成されている必要があります。ホストコンピューター側で構成されているモニターは、物理モニターまたは仮想モニターのどちらでも構いません。

ユーザーがグラフィックアプリケーションの仮想デスクトップまたはアプリケーションに接続している間は、ホストコンピューターにモニター（物理または仮想のいずれも）を接続しないでください。これを行うと、ユーザーのセッションが不安定になることがあります。

グラフィックアプリケーションセッションを実行しているときにデスクトップの解像度を変更しないようにユーザーに通知してください。アプリケーションセッションを閉じた後、［Citrix Receiver - Desktop Viewer基本設定］ダイアログボックスでDesktop Viewerウィンドウの解像度を変更できます。

支店など、帯域幅が制限された接続を複数のユーザーで共有している場合、ポリシーの[セッション全体の最大帯域幅］設定を使用して、各ユーザーが使用できる帯域幅を制限することをお勧めします。これにより、ユーザーがログオンしたりログオフしたりするときに、使用可能な帯域幅が大きく変動しなくなります。HDX 3D Proでは使用可能なすべての帯域幅が使用されるため、ユーザーのセッション中に使用可能な帯域幅が大きく増減するとパフォーマンスが低下します。

たとえば、60Mbpsの接続を20人のユーザーで共有する場合、各ユーザーが使用できる帯域幅は、同時接続ユーザーの数に応じて3Mbps～60Mbpsの間で変動します。この場合におけるユーザーエクスペリエンスを最適化するには、各ユーザーがピーク時に必要とする帯域幅を調べて、常時この値でユーザーを制限します。

ユーザーが3Dマウスを使用する場合は、汎用USBリダイレクト仮想チャネルの優先度を0にすることをお勧めします。仮想チャネルの優先度を変更する方法については、CTX128190を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

WindowsサーバーOSのためのGPUアクセラレーション

Dec 05, 2017

HDX 3D Pro機能により、WindowsサーバーOSのセッションで実行しているグラフィック処理アプリケーションで、サーバー上のGPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）の処理をサーバーのGPUに移すことで、グラフィック処理によりサーバーのCPU速度が低下することを回避できます。また、ワークロードがCPUとGPUで分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Windows Serverはマルチユーザーオペレーティングシステムなので、XenAppによってアクセスされるGPUは複数のユーザーによって共有でき、GPU仮想化（vGPU）の必要はありません。

このトピックの説明にはレジストリの編集が含まれています。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

GPU共有

GPU共有により、リモートデスクトップセッションで動作するOpenGLアプリケーションおよびDirectXアプリケーションでGPUハードウェアによるレンダリング処理が可能になります。これにより、以下の効果があります。

- ベアメタルまたは仮想マシン上で使用でき、アプリケーションのスケーラビリティとパフォーマンスが向上します。
- 複数の同時接続セッションでGPUリソースを共有できます（ほとんどのユーザーは専用GPUのレンダリングパフォーマンスを必要としません）。
- 特別な設定は必要ありません。

複数のGPUを持つグラフィックカードを装着したり、複数のグラフィックカードを装着したりして、ハイパーバイザー上に複数のGPUをインストールして各GPUを特定の仮想マシンに（1対1で）割り当てることができます。ただし、サーバー上で異なるグラフィックカードを混在させることは推奨されません。

仮想マシンでは、GPUへの直接パススルーアクセスが必要です。この機能は、Citrix XenServer、VMware vSphere vDGA、およびIntel GVT-dで提供されます。HDX 3D ProとGPUパススルーを併用すると、サーバー上の各GPUで単一のマルチユーザー仮想マシンをサポートできます。

GPU共有は、特定のグラフィックカードに依存するものではありません。

- ハイパーバイザー上では、そのハイパーバイザーのGPUパススルー機能でサポートされるハードウェアプラットフォームとグラフィックカードを選択してください。XenServerのGPUパススルー機能でテストされたハードウェアの一覧については、「GPU Pass-through Devices」を参照してください。
- ベアメタルを実行するときは、オペレーティングシステムで単一のディスプレイアダプターを有効にすることをお勧めします。複数のGPUがハードウェアに取り付けられている場合は、デバイスマネージャーを使用して1つだけ残して無効にします。

GPU共有でのスケーラビリティは、以下の要素により異なります。

- 実行するアプリケーション
- 消費されるビデオRAMの量
- グラフィックカードの処理能力

一部のアプリケーションでは、ビデオRAMの不足をより効果的に処理できます。ハードウェアの負荷が過剰になると、グラフィックカードドライバーが不安定になったり異常停止したりすることがあります。このような問題を避けるには、同時接続

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーの数を制限してください。

GPUアクセラレーションが正しく動作しているかどうかを確認するには、GPU-Zなどのサードパーティ製ツールを使用できます。このツールは、http://www.techpowerup.com/gpuz/で提供されています。

DirectX、Direct3D、およびWPFレンダリング

DirectX、Direct3D、およびWPFレンダリングは、DDI（Display Driver Interface）Version 9ex、10、または11をサポートするGPUが搭載されたサーバーでのみ使用可能です。

- Windows Server 2008 R2では、DirectXおよびDirect3Dで単一GPUを使用するために特別な設定は不要です。
- Windows Server 2016およびWindows Server 2012のRD Session Hostサーバー上のリモートデスクトップサービス（RDS）セッションでは、デフォルトのアダプターとしてMicrosoft基本レンダリングドライバーが使用されます。Windows Serve 2012上のRDSセッションでGPUを使用するには、グループポリシーの［ローカルコンピューターポリシー］>［コンピューターの構成］>［管理用テンプレート］>［Windowsコンポーネント］>［リモートデスクトップサービス］>［リモートデスクトップセッションホスト］>［リモートセッション環境］で［Use the hardware default graphics adapter for all Remote Desktop Services sessions］を有効にします。
- WPFアプリケーションでのレンダリングにサーバーのGPUが使用されるようにするには、WindowsサーバーOSセッションを実行するサーバー上で以下のレジストリキーを設定します。
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

CUDAまたはOpenCLアプリケーション用のGPUアクセラレーション機能

ユーザーセッションで実行中のCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効です。

CUDAアクセラレーションPOC機能を有効にするには、以下のレジストリを設定します。

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

OpenCLアクセラレーションPOC機能を有効にするには、以下のレジストリを設定します。

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

© 1999-2017 Citrix Systems, Inc. All rights reserved.

OpenGLソフトウェアアクセラレータ

Dec 05, 2017

OpenGLソフトウェアアクセラレータは、ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、およびCAD/CAMアプリケーションなどのOpenGLアプリケーションで使用するソフトウェアラスタライザーです。OpenGLソフトウェアアクセラレータを使用すると、グラフィックカードを装着しなくてもユーザーに良好なユーザーエクスペリエンスを提供できる場合があります。

> ## Important
>
> OpenGLソフトウェアアクセラレータは*現状有姿のまま*提供されます。このため、一部のアプリケーションがサポートされない場合があるため、すべてのアプリケーションで動作確認を行ってください。この機能は、Windows OpenGLラスタライザーで十分なパフォーマンスが得られない場合の解決策として使用してください。OpenGLソフトウェアアクセラレータがアプリケーションをサポートする場合は、GPUハードウェアのコストを削減する手段として使用できます。

OpenGLソフトウェアアクセラレータはインストールメディアのサポートフォルダーに収録されており、すべてのVDAプラットフォームをサポートしています。

OpenGLソフトウェアアクセラレータは、以下の場合に使用します。

- グラフィック処理ハードウェアのないサーバーで、XenServerやほかのハイパーバイザーの仮想マシン上で動作するOpenGLアプリケーションで十分なパフォーマンスが得られない。一部のアプリケーションでは、Windowsに付属のMicrosoft OpenGLソフトウェアラスタライザーよりも高いパフォーマンスが得られる場合があります。これは、OpenGLアクセラレータでSSE4.1およびAVXが使用されるためです。OpenGLアクセラレータは、Version 2.1までのOpenGLを使用するアプリケーションをサポートします。
- ワークステーション上で動作するアプリケーションでは、まずそのワークステーションのグラフィックアダプターで提供されるデフォルトのOpenGLサポート機能を使用してテストを行います。一般的に、最新バージョンのグラフィックカードを使用すると最高のパフォーマンスが得られます。グラフィックカードのバージョンが低い場合、または十分なパフォーマンスが得られない場合は、OpenGLソフトウェアアクセラレータを使用してテストを行います。
- 3D OpenGLアプリケーションがCPUベースのソフトウェアラスタライザーで適切に配信されていない場合は、OpenGLのGPUハードウェアアクセラレーションを使用することでパフォーマンスが向上することがあります。この機能は、ベアメタルまたは仮想マシン上で使用できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Thinwire

Dec 05, 2017

はじめに

Thinwireとは、XenAppおよびXenDesktopで使用される、Citrixのデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。

正常なディスプレイリモートソリューションでは、ローカルPCと同様の、高度にインタラクティブなユーザーエクスペリエンスが提供されます。Thinwireでは、幅広く複合的、効果的な画像解析および圧縮技術の使用により、これを実現しています。Thinwireではサーバーのスケーラビリティが最大化され、消費する帯域幅は他のディスプレイリモートテクノロジより少なくできます。

このバランスのためにThinwireは大部分の一般的なビジネスユースケースに合致しており、XenAppおよびXenDesktopのデフォルトのディスプレイリモートテクノロジとして使用されています。

ThinwireまたはFramehawk

Thinwireは、デスクトップの一般的なワークロード、たとえば、デスクトップ、オフィスの生産性、またはブラウザベースのアプリケーションを提供するために使用してください。Thinwireは、マルチモニター、高解像度、または高DPIのシナリオや、ビデオとビデオ以外の混在コンテンツを持つワークロードにも推奨されます。

Framehawkは、パケット損失が断続的に高くなることがあるブロードバンドワイヤレス接続を使用するモバイルワーカーに使用してください。

HDX 3D Pro

デフォルトの構成では、Thinwireは3Dや高度にインタラクティブなグラフィックを提供できますが、VDA for Desktop OSのインストール時にHDX 3D Proモードを有効化することが、そのようなシナリオに適切な選択です。Thinwireの3D Proモードは、全画面のH.264エンコードでのグラフィック送信のための構成です。これにより、3D Proグラフィックは、より滑らかなエクスペリエンスを実現できます。詳しくは、「HDX 3D Pro」および「WindowsデスクトップOSのためのGPUアクセラレーション」を参照してください。

要件および考慮事項

- Thinwireは、Windows Server 2012 R2、Windows Server 2016、Windows 7、およびWindows 10など、最新のオペレーティングシステムに最適化されています。Windows Server 2008 R2には、従来のグラフィックモードをお勧めします。ビルトインのCitrixポリシーテンプレートである「高サーバースケーラビリティ - レガシOS」と「WANの最適化 - レガシOS」を使用して、これらのユースケースに推奨されるポリシー設定の組み合わせを提供します。
- Thinwireの動作を制御する **[圧縮にビデオコーデックを使用する]** ポリシー設定は、XenAppおよびXenDesktop 7.6 FP3以降のVDAバージョンで利用できます。 **[選択された場合ビデオコーデックを使用する]** オプションは、VDAバージョンXenAppおよびXenDesktop 7.9以降のデフォルト設定です。
- ThinwireはすべてのCitrix Receiverでサポートされています。ただし一部のCitrix Receiverは、他でサポートされないThinwire機能（たとえば、帯域幅使用が低下した場合の8または16ビットグラフィック）をサポートする場合があります。そのような機能のサポートは、Citrix Receiverによって自動的にネゴシエートされます。
- Thinwireは、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwireが使用するリソース量は調整可能ですが、帯域幅の使用状況がその結果増大することがあります。
- 低帯域幅または高遅延のシナリオでは、8または16ビットグラフィックを有効化して対話操作性を改善することを検討でき

© 1999-2017 Citrix Systems, Inc. All rights reserved.

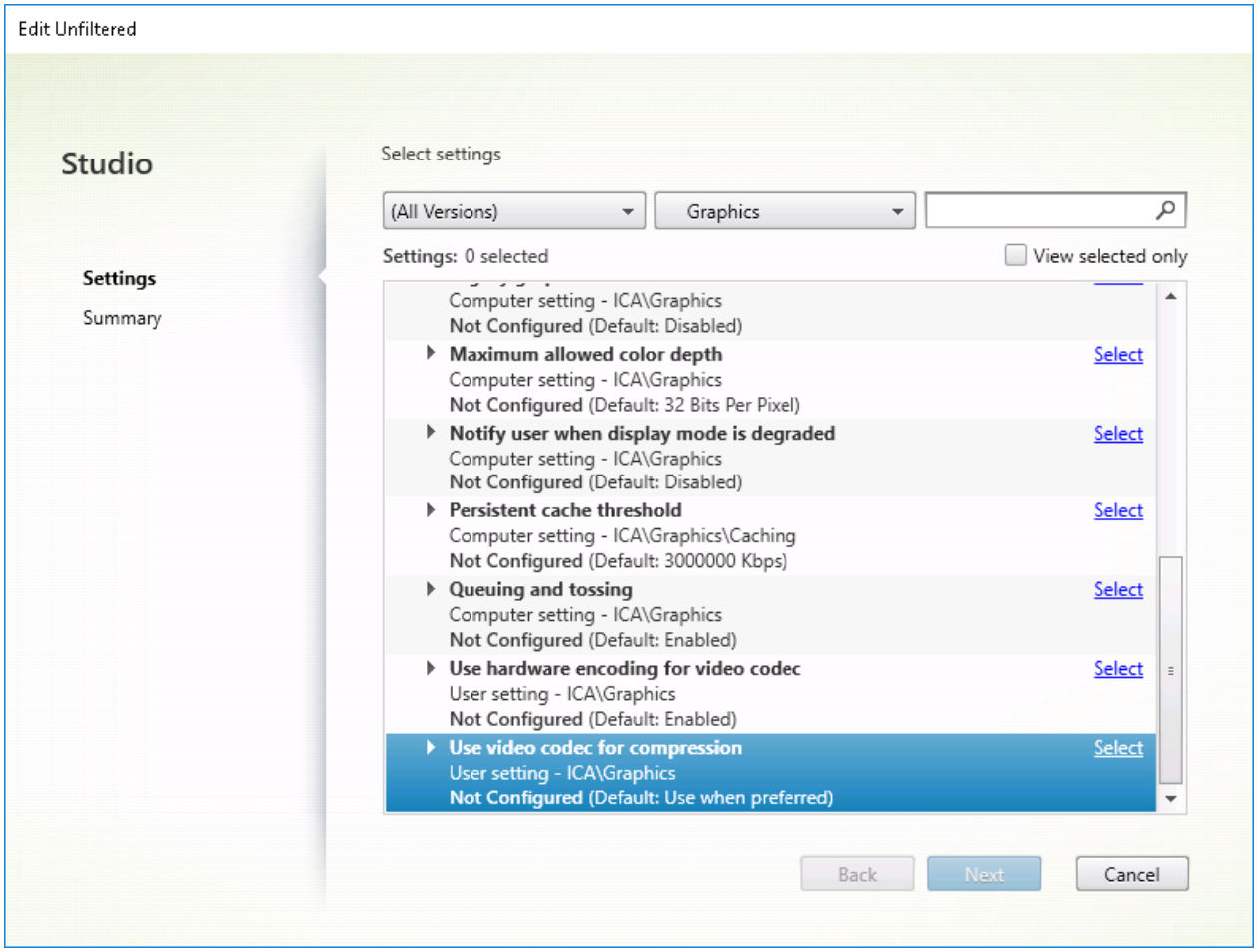
ますが、特に8ビットの色数で、表示品質が影響を受ける場合があります。

構成

Thinwireはデフォルトのディスプレイリモートテクノロジです。

次のグラフィックポリシー設定はデフォルトを設定し、さまざまなユースケースに代替選択肢を提供します。

- 圧縮にビデオコーデックを使用
  - **選択された場合ビデオコーデックを使用する**これがデフォルトの設定です。追加の構成は必要ありません。この設定をデフォルトとして保持することにより、すべてのCitrix接続でThinwireが選択され、デスクトップの一般的なワークロードで、スケーラビリティ、帯域幅、および優れた画質の点で、確実に最適化されます。
- このポリシー設定の他のオプションは、さまざまなユースケースでの他のテクノロジとの組み合わせでもThinwireを使用し続けます。次に例を示します。
  - **アクティブに変化する領域**。Thinwireのアダプティブ表示テクノロジは、動画（ビデオ、3Dインモーション）を識別し、画像が動く画面の部分でのみH.264を使用します。
  - **画面全体**。特に3Dグラフィックを多用する事例で、Thinwireを全画面H.264を使用して配信して、ユーザーエクスペリエンスと帯域幅の改善を最適化します。



次の視覚表示ポリシー設定など、いくつかの他のポリシー設定は、ディスプレイリモートテクノロジのパフォーマンスを微調整するために使用でき、また、Thinwireによってすべてサポートされます。

- シンプルなグラフィック用の優先色数

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ターゲットフレーム数
- 表示品質

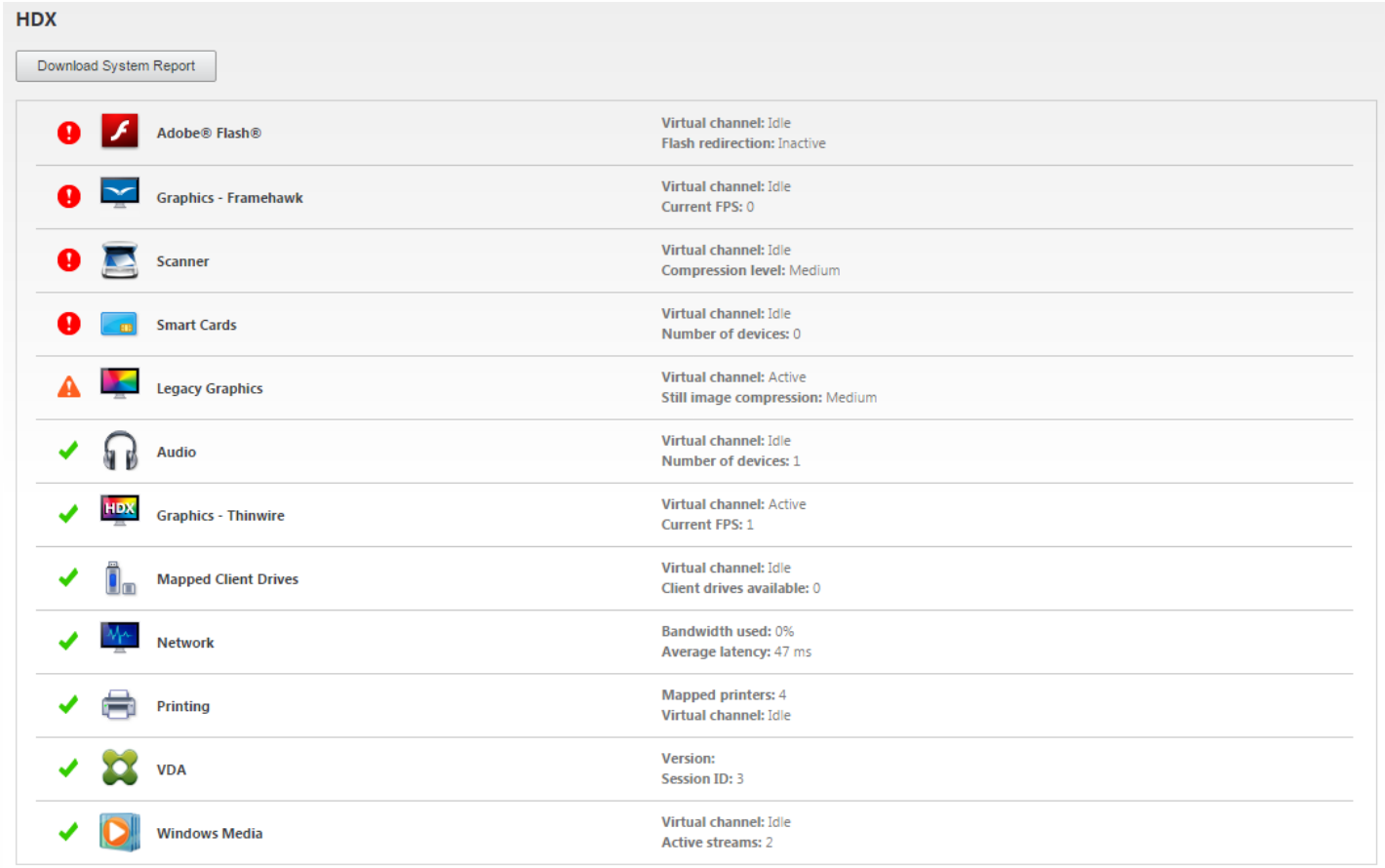
さまざまなビジネスユースケースに対してCitrixが推奨するポリシー設定の組み合わせを取得するには、組み込みのCitrixポリシーテンプレートを使用します。**高サーバースケーラビリティ**および**最高品位ユーザーエクスペリエンス**テンプレートはどちらも、組織の優先順位やユーザーの予期に最も適したポリシー設定との組み合わせでThinwireを使用します。

Thinwireのモニター

Citrix DirectorからThinwireの利用状況とパフォーマンスをモニターすることができます。HDX仮想チャネル詳細ビューには、あらゆるセッションで、Thinwireのトラブルシューティングやモニターに役立つ情報が表示されます。Thinwire関連の測定基準を表示するには：

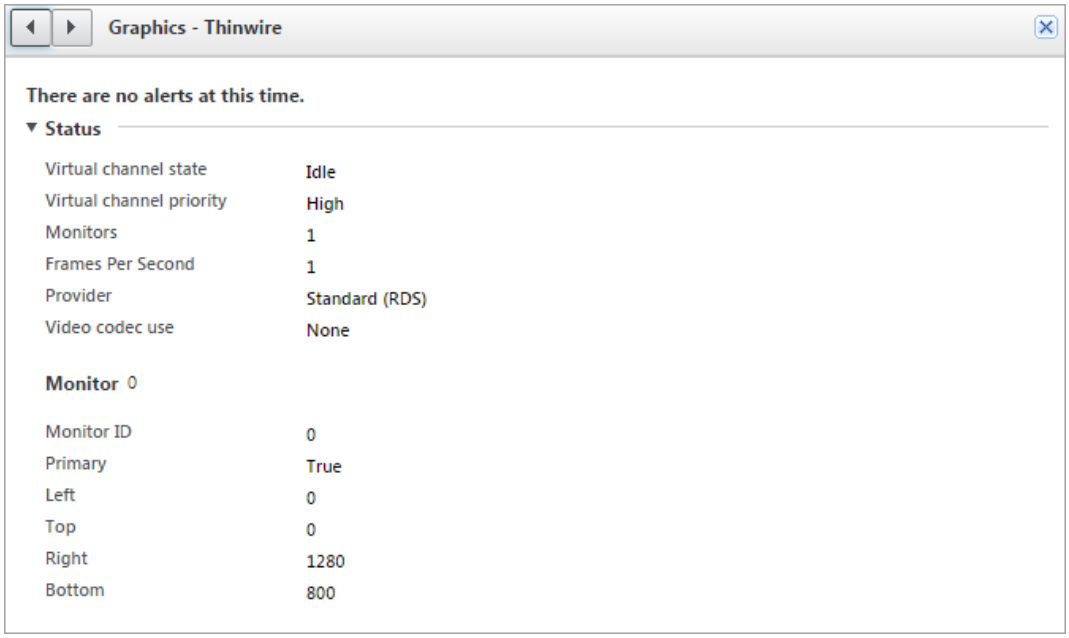
1. Directorで、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて、**[詳細]** をクリックします。または、 **[フィルター]** > **[セッション]** > **[すべてのセッション]** を選択し、アクティブなセッションを開いて **[詳細]** をクリックすることもできます。

2. **[HDX]** パネルまで下にスクロールします。



3. **[グラフィック - Thinwire]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

マルチメディア

Dec 05, 2017

HDX技術スタックは、マルチメディアアプリケーションの配信を次の2つの相補的なアプローチでサポートします。

- サーバー側でレンダリングするマルチメディア配信
- クライアント側でレンダリングするマルチメディアリダイレクト

これにより、良好なユーザーエクスペリエンスを保ちながら、サーバースケーラビリティを向上させ、ユーザーごとのコストを削減するあらゆる種類のマルチメディアフォーマットを配信できます。

サーバー側でレンダリングするマルチメディア配信で、オーディオとビデオコンテンツは、アプリケーションによってXenAppまたはXenDesktopサーバー上でデコードおよびレンダリングされます。コンテンツは圧縮され、ICAプロトコルでユーザーデバイス上のCitrix Receiverに配信されます。この方法は、さまざまなアプリケーションとメディア形式に対して、最大レートの互換性を提供します。ビデオ処理は数値計算であるため、サーバー側でレンダリングされたマルチメディア配信はオンボードのハードウェアアクセラレーションの利点を大幅に活かすことがきます。たとえば、DirectX Video Acceleration（DXVA）のサポートは 、H.264デコーディングを別のハードウェアで実行することで、CPUをオフロードします。Intel Quick SyncとNVIDIA NVENCの機能により、ハードウェアアクセラレーション用のH.264エンコーディングが利用できるようになりました。

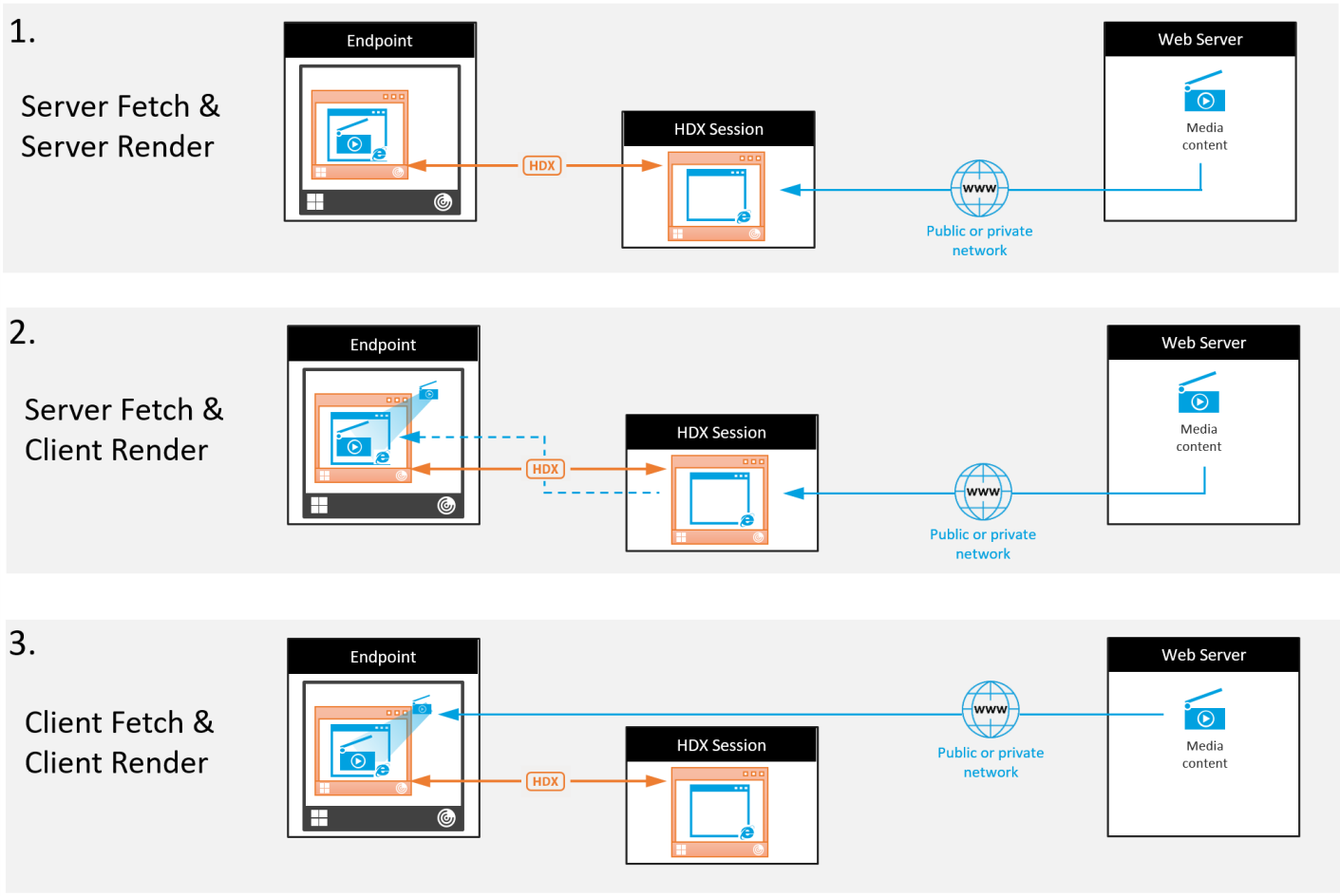
ほとんどのサーバーにビデオ圧縮用のハードウェアアクセラレーションがないため、すべてのビデオ処理をサーバーのCPUで実行する場合は、サーバースケーラビリティに悪影響を及ぼします。高サーバースケーラビリティを維持するために、多くのマルチメディア形式をユーザーデバイスにリダイレクトして、ローカル側でレンダリングできます。Windows Mediaリダイレクトは、一般的にWindows Media Playerに関連した、さまざまな種類のメディア形式に対してサーバーをオフロードします。

Flashリダイレクトは、ユーザーデバイス上でローカルに実行されるFlash PlayerにAdobe Flashビデオコンテンツをリダイレクトします。
HTML5ビデオが一般的になり、Citrixではこの種類のコンテンツに対するリダイレクト機能が導入されています。
また、一般的なアドレス帳リダイレクト機能である、ホストからクライアントへのリダイレクトとローカルアプリケーションアクセスを、マルチメディアコンテンツに適用できます。

これらの機能を含めて、リダイレクトを構成しない場合は、HDXはサーバー側でのレンダリングを実行します。
リダイレクトを構成する場合、HDXはサーバー側でフェッチし、クライアント側でレンダリング、またはクライアント側でフェッチし、クライアント側でレンダリングのいずれかを実行します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側でのレンダリングにフォールバックし、フォールバック防止ポリシーの対象になります。

サンプルシナリオ

© 1999-2017 Citrix Systems, Inc. All rights reserved.



シナリオ1.（サーバー側でフェッチし、サーバー側でレンダリング）

1. サーバーはメディアファイルをソースからフェッチし、デコードし、コンテンツをオーディオデバイスまたはディスプレイデバイスに対して再生します。
2. サーバーは再生されたイメージまたはサウンドをディスプレイデバイスまたはオーディオデバイスからそれぞれ抽出します。
3. オプションとしてサーバーが抽出されたファイルを圧縮し、クライアントに送信します。

このアプローチでは、（抽出されたイメージやサウンドが効率的に圧縮されていない場合は）高CPUコストと高帯域幅コストを負担することになり、サーバースケーラビリティは低くなります。

Thinwireとオーディオの仮想チャネルがこのアプローチを処理します。このアプローチの利点により、クライアントのハードウェアとソフトウェアの要件が削減されます。このアプローチでは、デコーディングはサーバーで実行され、より多くの種類のデバイスとフォーマットに対応します。

シナリオ2.（サーバー側でフェッチし、クライアント側でレンダリング）

このアプローチは、オーディオまたはディスプレイデバイスに対してデコードおよび再生される前に、メディアコンテンツをインターセプトできることを前提としています。圧縮されたオーディオ/ビデオコンテンツは、クライアントに送信され、ローカルでデコードおよび再生されます。このアプローチの利点により、デコーディングとプレゼンテーションはクライアントデバイスにオフロードされ、サーバーのCPUサイクルが節約されます。

ただし、このアプローチでは、クライアントにハードウェアとソフトウェアの要件が一部追加されます。クライアントは、受

© 1999-2017 Citrix Systems, Inc. All rights reserved.

信する可能性のあるそれぞれのフォーマットをデコードできる必要があります。

シナリオ3.（クライアント側でフェッチし、クライアント側でレンダリング）

このアプローチは、ソースからフェッチされる前に、メディアコンテンツのURLをインターセプトできることを前提としています。URLは、メディアコンテンツがローカルでフェッチ、デコード、および再生されたクライアントに送信されます。このアプローチは概念的に単純です。この利点により、制御コマンドのみがサーバーから送信されるため、サーバーのCPUサイクルと帯域幅の両方が節約されます。ただし、メディアコンテンツは、クライアントに常にアクセスできるわけではありません。

フレームワークとプラットフォーム

デスクトップオペレーティングシステム（Windows、Mac OS X、およびLinux）は、マルチメディアアプリケーションのよりすばやく簡単な開発を可能にする、マルチメディアフレームワークを提供します。次の表に、より一般的なマルチメディアフレームワークの一部を示します。各フレームワークはメディア処理を複数の段階に分割して、パイプラインベースのアーキテクチャを使用します。

Framework	Platform
DirectShow	Windows（98以降）
Media Foundation	Windows（Vista以降）
Gstreamer	Linux：
Quicktime	Mac OS X

メディアリダイレクト機能によるダブルホップのサポート

HDX Flashリダイレクト	なし
Windows Mediaリダイレクト	はい
HTML5ビデオリダイレクト	はい
オーディオリダイレクト	なし

関連情報

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Audio features
- Flash redirection
- HTML5 multimedia redirection
- Windows Media redirection
- General content redirection

© 1999-2017 Citrix Systems, Inc. All rights reserved.

オーディオ機能

Dec 05, 2017

ポリシーに以下の設定項目を追加して、HDXのオーディオ機能を最適化できます。これらの設定項目の使用方法、およびほかのポリシー設定項目との依存関係について詳しくは、「オーディオのポリシー設定」、「帯域幅のポリシー設定」および「マルチストリーム接続のポリシー設定」を参照してください。

> **Important**
>
> TCPではなくユーザーデータグラムプロトコル（UDP）を使ってオーディオを配信するのが最も良いのですが、DTLSを使ったUDPオーディオ暗号化はNetScaler GatewayとCitrix Receiver間でのみ有効です。そのため、TCPトランスポートが望ましい場合もあります。TCPは、VDAとCitrix Receiver間の、エンドツーエンドのTLS暗号化をサポートします。

音質

一般的に、音質を高くするほど、オーディオデータの転送に必要な帯域幅が大きくなり、サーバーのCPUにも負担がかかります。オーディオデータを圧縮すると、セッションのパフォーマンスと音質とのバランスを考慮しながら、ユーザーの操作感を最適化できます。これを行うには、サウンドファイルに適用する圧縮レベルを制御するには、Citrixポリシーを使用します。

デフォルトでは、TCPトランスポート使用時の「音質」ポリシー設定は［高 - 高品位オーディオ］に設定されており、UDPトランスポート使用時（推奨）は［中 - スピーチに最適化］に設定されています。高品位オーディオ設定ではHiFiステレオオーディオが提供されますが、ほかの品質設定よりも多くの帯域幅が消費されます。最適化されていないボイスチャットアプリケーションやビデオチャットアプリケーション（ソフトフォンなど）でこの設定を使用すると、リアルタイムの音声通信に不適切な遅延が発生することがあります。「スピーチに最適化」ポリシー設定は、選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオにお勧めです。

衛星、ダイヤルアップ接続など帯域幅が制限されている場合、音質を**低**に設定することで、帯域幅の消費を最少にすることができます。この状況では、低帯域幅接続のユーザーに対して別のポリシーを作成し、高帯域幅接続のユーザーに影響しないようにします。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。詳しくは、「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

クライアントオーディオリダイレクト

サーバー上で実行しているアプリケーションからユーザーデバイス上のスピーカーまたはヘッドフォンなどのサウンドデバイスでオーディオが再生されるようにするには、［クライアントオーディオリダイレクト］設定をデフォルトのまま（［許可］）にします。

クライアントオーディオマッピングによりサーバーおよびネットワークの負荷が増大しますが、［クライアントオーディオリダイレクト］設定で［禁止］を指定するとHDXのすべてのオーディオ機能が無効になります。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［Client audio settings］が有効になっていることを確認してください。詳しくは、「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

クライアントマイクリダイレクト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーデバイス上のマイクなどのサウンド入力デバイスを使って録音できるようにするには、[クライアントマイクリダイレクト] 設定をデフォルトのまま（ [許可] ）にします。

ユーザーデバイスとの信頼関係が設定されていないサーバー上のセッションでマイクを使用しようとすると、セキュリティに関する警告がユーザーに表示されます。この場合、クライアント側のマイクへのアクセスを許可するかどうかをユーザーが選択できます。この警告は、ユーザーがCitrix Receiver側で無効にできます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の [Client audio settings] が有効になっていることを確認してください。詳しくは、「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

オーディオプラグアンドプレイ

ポリシーの [オーディオプラグアンドプレイ] 設定では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。この設定項目は、デフォルトで **[有効]** になっています。 [オーディオプラグアンドプレイ] を使用すると、ユーザーのセッションが確立されるまでプラグを差し込まなくても、オーディオデバイスが認識されるようにできます。

この設定項目は、WindowsサーバーOSマシンのみに適用されます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。

オーディオリダイレクトの最大帯域幅（Kbps）とオーディオリダイレクトの最大帯域幅（%）

ポリシーの [オーディオリダイレクトの最大帯域幅（Kbps）] 設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。ポリシーの [オーディオリダイレクトの最大帯域幅（%）] 設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。これらの設定には、デフォルトで0が指定されており、帯域幅に制限はありません。両方の設定を構成した場合、より高い制限（より小さい値）の設定が適用されます。

設定について詳しくは、「帯域幅のポリシー設定」を参照してください。ユーザーデバイス側の [Client audio settings] が有効になっていることを確認してください。詳しくは、「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

UDPでのオーディオリアルタイムトランスポートとオーディオUDPポートの範囲

ポリシーの [UDPでのオーディオリアルタイムトランスポート] 設定は、デフォルトで [有効] が選択されています（インストール時に選択した場合）。これにより、サーバーのUDPポートが開き、 [UDPでのオーディオリアルタイムトランスポート] 設定が有効な接続でそのポートが使用されます。ネットワークで輻輳やパケット損失などが生じる環境で最適なユーザーエクスペリエンスを提供するため、オーディオのUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオでは、EDTよりUDPオーディオが優先されます。UDPは再送のないパケット損失が認められており、パケット損失が頻繁な場合でも接続に遅延が発生しません。

重要： NetScaler Access Gatewayがパス上にない場合、UDPで転送されるオーディオデータは暗号化されません。NetScaler Access GatewayがXenAppおよびXenDesktopのリソースにアクセスするよう構成されている場合、エンドポイントデバイスとNetScaler Access Gateway間のオーディオトラフィックはDTLSプロトコルで保護されます。

ポリシーの [オーディオUDPポートの範囲] 設定では、Virtual Delivery Agent（VDA）でユーザーデバイスとのオーディオパケットデータの送受信に使用されるポート番号の範囲を指定します。
デフォルトでは、16500～16509の範囲が指定されています。

[UDPでのオーディオリアルタイムトランスポート] 設定については「オーディオのポリシー設定」を、 [オーディオUDP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポートの範囲］設定については「マルチストリーム接続のポリシー設定」を参照してください。ユーザーデバイス側の［Client audio settings］が有効になっていることを確認してください。詳しくは、「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

ユーザーデバイス側のオーディオ設定ポリシー

1. 「グループポリシーオブジェクトテンプレートによるReceiverの構成」の手順に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、［管理用テンプレート］>［Citrix Components］>［Citrix Receiver］>［User Experience］の順に開きます。
3. ［Client audio settings］を開き、［未構成］、［有効］、または［無効］をクリックします。
   - **未構成**：デフォルトでは、オーディオリダイレクトは高品質オーディオ、または以前に構成したカスタムのオーディオ設定で有効になります。
   - **有効**：オーディオリダイレクトは、選択したオプションで有効になります。
   - **無効**：オーディオリダイレクトは無効化されます。
4. **［有効］**をクリックした場合は、音質を選択します。UDPオーディオでは、**［中］**（デフォルト）を使用してください。
5. UDPオーディオでは、**［リアルタイム転送を有効にします］**チェックボックスをオンにして、ローカルのWindowsファイアウォールを通過するための着信ポートの範囲を指定します。
6. NetScaler Access GatewayでUDPオーディオを使用するには、**［ゲートウェイ経由でのリアルタイムトランスポートを許可する］**チェックボックスをオンにします。NetScaler Access GatewayはDTLSで構成する必要があります。詳しくは、「UDP Audio Through a Netscaler Gateway」を参照してください。

エンドポイントデバイスで上記の変更を行う制御権を持っていない場合（BYODの場合や家庭用コンピューターの場合など）、管理者としてStoreFrontのdefault.ica属性を使用してUDPオーディオを有効にします。

1. StoreFrontマシンで、メモ帳などのエディターを使用してC:\inetpub\wwwroot\Citrix\<ストア名>\App_Data\default.icaを開きます。
2. ［Application］セクションに以下の項目を記入します。

コマンド　コピー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

ユーザーデータグラムプロトコル（UDP）オーディオは、default.icaの編集で有効になっている場合、そのストアを使用するすべてのユーザーに対して有効化されます。

マルチメディア会議でのエコーの解消

オーディオまたはビデオ会議にユーザーが参加したときに、音声にエコーがかかって聞こえることがあります。通常、この問題はスピーカーとマイクが近すぎる場合に発生します。このため、オーディオまたはビデオ会議ではヘッドセットを使用することをお勧めします。

HDXには、会議中のエコーを最小限に抑えるためのエコーキャンセル機能が用意されており、デフォルトで有効になっています。エコーキャンセル機能の効果は、スピーカーとマイクとの距離により異なります。デバイスは、近すぎず、かつ遠すぎないところに配置してください。

エコーキャンセル機能を無効にするには、レジストリ設定を変更します。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. ユーザーデバイス上でレジストリエディターを開き、以下のレジストリキーを選択します。
   - 32ビットシステム：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
- 64ビットシステム：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation

2. ［値のデータ］ボックスの値をFALSEに変更します。

ソフトフォン

ソフトフォンは、電話インターフェイスとして動作するソフトウェアです。コンピューターや他のスマートデバイスからインターネット経由で電話するには、ソフトフォンを使用します。ソフトフォンを使うことにより、画面を使って電話番号をダイヤルしたり、他の電話関連の機能を実行したりできます。

XenAppおよびXenDesktopは、ソフトフォンの配信に対するいくつかの代替手段をサポートします。

- **制御モード**。ホストされたソフトフォンが物理的な電話セットを制御します。このモードでは、XenAppまたはXenDesktopサーバーを通過するオーディオトラフィックはありません。
- **HDX RealTimeに最適化されたソフトフォンのサポート**。このメディアエンジンはユーザーデバイス上で実行され、ボイスオーバーIP（VoIP）トラフィックがピアツーピアで流れます。たとえば、以下を参照してください。
  - Microsoft Skype for BusinessとLyncの配信を最適化するHDX RealTime Optimization Pack。
  - Jabber用のCisco Virtualization Experience Media Engine（VXME）。
  - one-X CommunicatorおよびOne-X Agent用のAvaya VDI Communicator。
- **ローカルアプリケーションアクセス**。XenAppおよびXenDesktopの機能により、ソフトフォンなどのアプリケーションは、エンドユーザーのWindowsデバイス上ではローカルで実行されますが、その仮想/公開デスクトップとはシームレスに統合されています。これにより、ユーザーデバイスへのすべてのオーディオ処理の負荷が軽減されます。詳しくは、「ローカルアプリケーションアクセスとURLリダイレクト」を参照してください。
- **HDX RealTimeの汎用ソフトフォンのサポート**。VoIP-over-ICA。

汎用ソフトフォンのサポート

汎用ソフトフォンのサポートにより、データセンターのXenAppまたはXenDesktop上に、未変更のソフトフォンをホストすることができます。オーディオトラフィックは、Citrix ICAプロトコルを介して（UDP/RTPを優先的に使用して）、Citrix Receiverを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンのサポートは、HDX RealTimeの機能です。ソフトフォンの配信に対するこのアプローチは、以下の場合に特に有効です。

- ソフトフォンの配信に最適なソリューションがなく、ローカルアプリケーションアクセスが可能なWindowsデバイス上にユーザーがいない。
- ソフトフォンの最適化された配信に必要とされるメディアエンジンが、ユーザーデバイスにインストールされていないか、ユーザーデバイス上で実行しているオペレーティングシステムのバージョンで利用できない。このシナリオでは、汎用HDX RealTimeが価値のあるフォールバックソリューションを提供します。

XenAppおよびXenDesktopを使用したソフトフォンの配信には、考慮事項が2つあります。

- ソフトフォンアプリケーションがどのように仮想/公開デスクトップに配信されるか。
- エンドユーザーのヘッドセット、マイクロフォン、およびスピーカー、またはUSB電話セット間でオーディオがどのように配信されるか。

XenAppおよびXenDesktopには、汎用ソフトフォンの配信をサポートする多くのテクノロジが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅の効率性のための、スピーチに最適化されたコーデック。
- 遅延の少ないオーディオスタック。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ネットワーク遅延が変動する場合、オーディオをスムーズにするサーバー側のジッターバッファー。
- QoSのパケットのタグ付け（DSCPおよびWMM）
  - RTPパケットのDSCPタグ付け（レイヤー3）
  - WiFiのWMMタグ付け

Windows、Linux、Chrome、およびMac用のCitrix Receiverバージョンは、VoIPにも対応しています。Citrix Receiver for Windowsは以下の機能を提供します。

- クライアント側のジッターバッファー - ネットワーク遅延が変動する場合でもオーディオを確実にスムーズにします。
- エコーキャンセル - ヘッドセットを使用しないユーザー向けに、マイクとスピーカの距離を調整します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッション開始前にプラグインする必要はありません。いつでもプラグインできます。
- オーディオデバイスルーティング - ユーザーはヘッドセットの音声通信以外に、スピーカーに着信音を直接送信できます。
- マルチストリームICA - ネットワーク上で柔軟なQoS（サービス品質）ベースのルーティングを有効にします。
- ICAは、4つのTCPと2つのUDPストリームをサポートします。UDPストリームの1つは、RTP上でリアルタイムオーディオをサポートします。

Citrix Receiverの機能の概要については、『Citrix Receiver Feature Matrix』を参照してください。

システム構成の推奨事項

クライアントのハードウェアとソフトウェア：
音質の最適化のために、最新バージョンのCitrix ReceiverとアコースティックエコーキャンセルAEC付きの高品質なヘットセットをお勧めします。Windows、Linux、およびMac用のCitrix ReceiverバージョンはVoIPをサポートします。また、Dell WyseはThinOS（WTOS）のVoIPサポートを提供します。

CPU検討事項：
VDA上のCPU使用率を監視して、それぞれの仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを決定します。リアルタイムの音声およびビデオはデータ量が多いです。2つの仮想CPUを構成すると、スレッドの切り替え遅延を減らすことができます。そのため、XenDesktop VDI環境で2つのvCPUを構成することをお勧めします。

物理CPUはセッションを超えて共有できるため、2つの仮想CPUを持つことは、必ずしも物理CPUの数を倍にすることではありません。

セッション画面の保持機能に使われるCitrix Gateway Protocol（CGP）により、CPUの消費も増加します。高品質のネットワーク接続では、この機能を無効にして、VDAのCPU消費を削減することができます。前述のいずれの手順も、強力なサーバーでは必要ないかもしれません。

UDPオーディオ：
UDPによるオーディオは、ネットワークの輻輳やパケット損失に対する強力な耐性を提供します。利用できるのであれば、TCPから代えることをお勧めします。

LAN/WANの設定：
ネットワークの適切な設定は、リアルタイムオーディオの高い品質には極めて重要です。通常、過度のブロードキャストパケットはジッターを発生させる場合があるため、仮想LANVLANを構成する必要があります。IPv6が有効なデバイスでは、大量のブロードキャストパケットが発生する場合があります。IPv6のサポートが不要な場合は、それらのデバイスでIPv6を無効にできます。QoSサービス品質をサポートするように構成してください。

WAN接続使用時の設定：
ローカルエリアネットワークLANおよびワイドエリアネットワークWAN接続を経由したボイスチャットを使用でき

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ます。WAN接続では、音質は接続の遅延、パケット損失、およびジッターにより異なります。WAN接続を経由してソフトフォンを配信する場合、高いQoS（サービス品質）を保つため、データセンターとリモートオフィス間にはNetScaler SD-WANを使用することをお勧めします。NetScaler SD-WANは、UDPを含むマルチストリームICAをサポートします。また、単一のTCPストリームの場合は、さまざまなICA仮想チャネルの優先度を識別し、優先度の高いリアルタイムの音声データを優先的に扱うことができます。

HDX構成を検証するには、DirectorまたはHDX Monitorを使用してください。

リモートユーザーの接続：
NetScaler Gateway 11はDTLSをサポートし、UDP/RTPトラフィックをネイティブに（TCPでカプセル化せずに）送信します。
ポート443を介したUDPトラフィックに対してファイアウォールを双方向に開く必要があります。

コーデックの選択と帯域幅の消費：
ユーザーデバイスとデータセンターのVirtual Delivery Agent（VDA）間には、中品質オーディオとも呼ばれる、スピーチに最適化されたコーデック設定を使用することをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。次に例を示します。

- G711の音質は極めて高いものの、通話あたり80～100キロビットの帯域幅（ネットワークのレイヤー2のオーバーヘッドにより異なる）が必要になります。
- G729の音質は高く、通話あたり30～40キロビットの低帯域幅（ネットワークのレイヤー2のオーバーヘッドにより異なる）が必要になります。

ソフトフォンアプリケーションの仮想デスクトップへの配信

XenDesktop仮想デスクトップにソフトフォンを配信するには、次の2つの方法があります。

- アプリケーションは、仮想デスクトップイメージにインストールできます。
- アプリケーションは、Microsoft App-Vを使用して、仮想デスクトップにストリーム配信できます。このアプローチでは、仮想デスクトップイメージに手が加えられないため、管理上の利点があります。仮想デスクトップにストリーム配信された後、アプリケーションはその環境で、通常の方法でインストールされたかのように実行します。すべてのアプリケーションがApp-V互換であるわけではありません。

ユーザーデバイスとのオーディオの配信

汎用HDX RealTimeは、ユーザーデバイスとのオーディオの配信を次の2つの方法でサポートします。

- **Citrixオーディオ仮想チャネル**。具体的にオーディオ転送のために設計されているため、通常はCitrixオーディオ仮想チャネルをお勧めします。
- **汎用USBリダイレクト**。ユーザーデバイスがXenAppまたはXenDesktopサーバーへのLANまたはLANのような接続上にある場合は、ボタンやディスプレイといったヒューマンインターフェイスデバイス（HID）を持つオーディオデバイスのサポートに有効です。

Citrixオーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）は、ネットワーク上でオーディオを効率的に配信することができます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからオーディオを取り出して圧縮し、ICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力も圧縮され、ユーザーのヘッドセットまたはスピーカーにむけて反対方向に送信されます。この圧縮は、ソフトフォン自体で使われる圧縮（G.729、G.711など）とは関係ありません。スピーチに最適化されたコーデック（中品質）で行われます。その特性はボイスオーバーIP（VoIP）に最適です。高速エンコード機能を備え、ピーク時でもおよそ1秒間に56キロビット（それぞれの方向で28Kbpsす

© 1999-2017 Citrix Systems, Inc. All rights reserved.

つ）しかネットワーク帯域幅を消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studioのコンソールで明示的に選択する必要があります。デフォルトは、HDオーディオコーデック（高品質）です。このコーデックはHiFiステレオ録音には最適ですが、スピーチに最適化されたコーデックと比較してエンコードが遅くなります。

汎用USBリダイレクト

Citrix汎用USBリダイレクトテクノロジ（CTXGUSB仮想チャネル）は、複合デバイス（オーディオプラスHID）とアイソクロナスUSBデバイスを含む、USBデバイスのリモート処理に一般的な手段を提供します。USBプロトコルはネットワークの遅延に影響を受けやすく、相当量のネットワーク帯域幅を必要とするため、このアプローチはLAN接続のユーザーに制限されます。ソフトフォンによっては、アイソクロナスUSBリダイレクトが有効です。このリダイレクトは優れた音質と少ない遅延を提供しますが、オーディオトラフィックに最適化されているため、Citrixオーディオ仮想チャネルが優先されます。主な例外は、データセンターにLAN接続されているユーザーデバイスに取り付けられたUSB電話など、ボタンが付いたオーディオデバイスを使う場合です。この場合は、汎用USBリダイレクトが、信号をソフトフォンに送ることで機能を制御する電話セットまたはヘッドセットのボタンをサポートします。これは、デバイス上でローカルに動作するボタンでの問題ではありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Flashリダイレクト

Dec 05, 2017

Important

2017年7月25日、AdobeはFlashの製品終了（EOL）を発表しました。Flash Playerのアップデートおよび配布は、2020年末に停止される予定です。

Microsoftは、Adobeの発表した終了日より前にInternet ExplorerでのFlashのサポートから撤退していくことを発表しました。2020年末までに、FlashはWindowsから削除されます。これによって、ユーザーはInternet ExplorerでFlashを有効にしたり、実行したりすることができなくなります。

Citrixは、Microsoftポリシーに合わせて、2020年末までHDX Flashリダイレクトの保守およびサポートを継続します。Flashリダイレクトコードが除外されるXenAppおよびXenDesktopのバージョンは決定していませんが、可能な限り速やかにHTML5ビデオリダイレクションに切り替えることをお勧めします。HTML5ビデオリダイレクションは、マルチメディアコンテンツの制御に最適です。例えば、企業のコミュニケーションビデオ、トレーニングビデオ、またはサードパーティがコンテンツをホストする時などに使用できます。

HTML5ビデオリダイレクションについて詳しくは、「HTML5マルチメディアリダイレクト」を参照してください。

Flashリダイレクト機能を有効にすると、ほとんどのAdobe Flashコンテンツ（アニメーション、ビデオ、アプリケーションなど）がLANまたはWANで接続されたユーザー側のWindowsデバイスおよび32ビットLinux x86デバイス上で処理（レンダリング）され、サーバーリソースおよびネットワークの負荷が軽減されます。これにより、スケーラビリティおよびユーザーエクスペリエンスが向上します。Flashリダイレクトを構成するには、サーバー側およびクライアント側の設定が必要です。
注意： Flashリダイレクトでは、ユーザーデバイスとサーバー間で頻繁な相互通信が行われます。ユーザーデバイスとサーバー間でセキュリティ境界による分離が不要な環境でのみ、この機能を使用してください。また、ユーザーデバイスでは、信頼するサーバーでのみこの機能を使用するように設定する必要があります。Flashリダイレクトを使用するにはユーザーデバイス上にAdobe Flash Playerをインストールする必要があるため、ユーザーデバイス上のFlash Playerの安全性が確認されている場合にのみFlashリダイレクトを有効にしてください。

Flashリダイレクトは、クライアント側およびサーバー側でサポートされます。クライアント側で第2世代のFlashリダイレクトがサポートされる場合、Flashコンテンツはクライアント側でレンダリングされます。Flashリダイレクト機能では、以下で説明するWAN接続、インテリジェントフォールバック、URL互換性リストがサポートされます。

Flashリダイレクトは、サーバー上のWindowsイベントログを使用してFlashイベントのログを記録します。このイベントログには、Flashリダイレクトが使用されたかどうか、および問題に関する詳細が記録されます。Flashリダイレクトのすべてのイベントで、以下の共通の情報が記録されます。

- Flashリダイレクトのイベントは、アプリケーションログに記録されます。
- Windows 10、Windows 8およびWindows 7が動作するコンピューターでは、Flashリダイレクトのログは［アプリケーションとサービスログ］ノードに記録されます。
- ソースには「Flash」と記録されます。
- 分類には「なし」と記録されます。

HDX Flashの互換性に関する最新の更新については、CTX136588を参照してください。

サーバー側でのFlashリダイレクトの構成

サーバー側でFlashリダイレクト機能を構成するには、Citrixポリシーで以下の設定項目を使用します。詳しくは、「Flashリダイレクトのポリシー設定」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- デフォルトでは、Flashリダイレクトは有効になっています。特定のWebページのFlashコンテンツでこのデフォルト設定を上書きするには、［Flash URL 互換性リスト］設定を使用します。
- ［Flash インテリジェント フォールバック］設定により、小さいFlashムービー（広告で使用されるものなど）が検出され、それらがユーザーデバイスではなくサーバー側でレンダリングされます。この最適化を使用しても、WebページやFlashアプリケーションのロード時に中断や障害は発生しませんデフォルトでは、Flashインテリジェントフォールバックは有効になっています。サイズにかかわらずすべてのFlashコンテンツがユーザーデバイス側でレンダリングされるようにするには、この設定項目を無効にします。一部のFlashコンテンツが正常にリダイレクトされない場合がある点に注意してください。
- ［Flash サーバー側でのコンテンツ取得 URL リスト］設定を使用すると、特定のWebサイトのFlashコンテンツがいったんサーバー上にダウンロードされ、それがユーザーデバイスに転送されてレンダリングされるようになります。（Flashリダイレクトのデフォルトでは、Flashコンテンツがクライアント側フェッチでユーザーデバイス上に直接ダウンロードされます）。 Flashリダイレクトのデフォルトでは、Flashコンテンツがユーザーデバイス上にダウンロードされ、そこでレンダリングされます。この設定項目を使用する場合はユーザーデバイス側の［サーバー側のコンテンツの取得を有効にする］設定が必要で、イントラネット上の内部用Flashアプリケーションで使用されます。詳しくは、後述の説明を参照してください。この機能はほとんどのインターネットサイトでも動作するため、ユーザーデバイスが直接インターネットに接続できない環境（XenApp/XenDesktopサーバー経由でインターネットに接続している場合など）で使用できます。
  注： サーバー側でのコンテンツ取得機能は、RTMP（Real Time Messaging Protocol）を使用したFlashアプリケーションをサポートしません。この場合、サーバー側でのレンダリングが使用され、HTTPおよびHTTPSがサポートされます。
- ［Flash URL 互換性リスト］設定では、特定のWebサイト上のFlashコンテンツをクライアント側でレンダリングするか、サーバー側でレンダリングするか、またはブロックするかを指定します。
- ［Flash 背景色リスト］設定では、WebページとFlashインスタンスの表示色を一致させて、Flashリダイレクトを使用しているときのWebページの表示を改善させることができます。

ユーザーデバイス側でのFlashリダイレクトの構成

ユーザーデバイス側でFlashリダイレクト機能を使用するには、Citrix Receiverに加えてAdobe Flash Playerをインストールする必要があります。ユーザーデバイス上でこれ以外の特別な構成は必要ありません。

デフォルトの設定は、Active Directoryグループポリシーオブジェクトを使用して変更できます。HDX MediaStream Flashリダイレクトのクライアント管理テンプレート（HdxFlashClient.adm）をインポートして追加します。このテンプレートは、以下の場所からインポートできます。

- 32ビットコンピューターの場合： %Program Files%\Citrix\ICA Client\Configuration\language
- 64ビットコンピューターの場合： %Program Files (x86)%\Citrix\ICA Client\Configuration\language

［管理用テンプレート］> ［従来の管理用テンプレート（ADM）］> ［HDX MediaStream Flashリダイレクト - クライアント］を開きます。Active Directoryグループポリシーオブジェクトおよびテンプレートについて詳しくは、Microsoft社のドキュメントを参照してください。

Flashリダイレクトの動作を変更する

Adobe Flashコンテンツをユーザーデバイス側にリダイレクトしてローカルで処理されるようにするには、サーバー側での設定に加えて、［このユーザー デバイスでの HDX MediaStream Flash リダイレクトを有効にする］ポリシーを設定します。Flashリダイレクトはデフォルトで有効になっており、検出されたネットワークの状態に応じて自動的にユーザーデバイス上でFlashコンテンツが再生されます（インテリジェントネットワーク検出）。

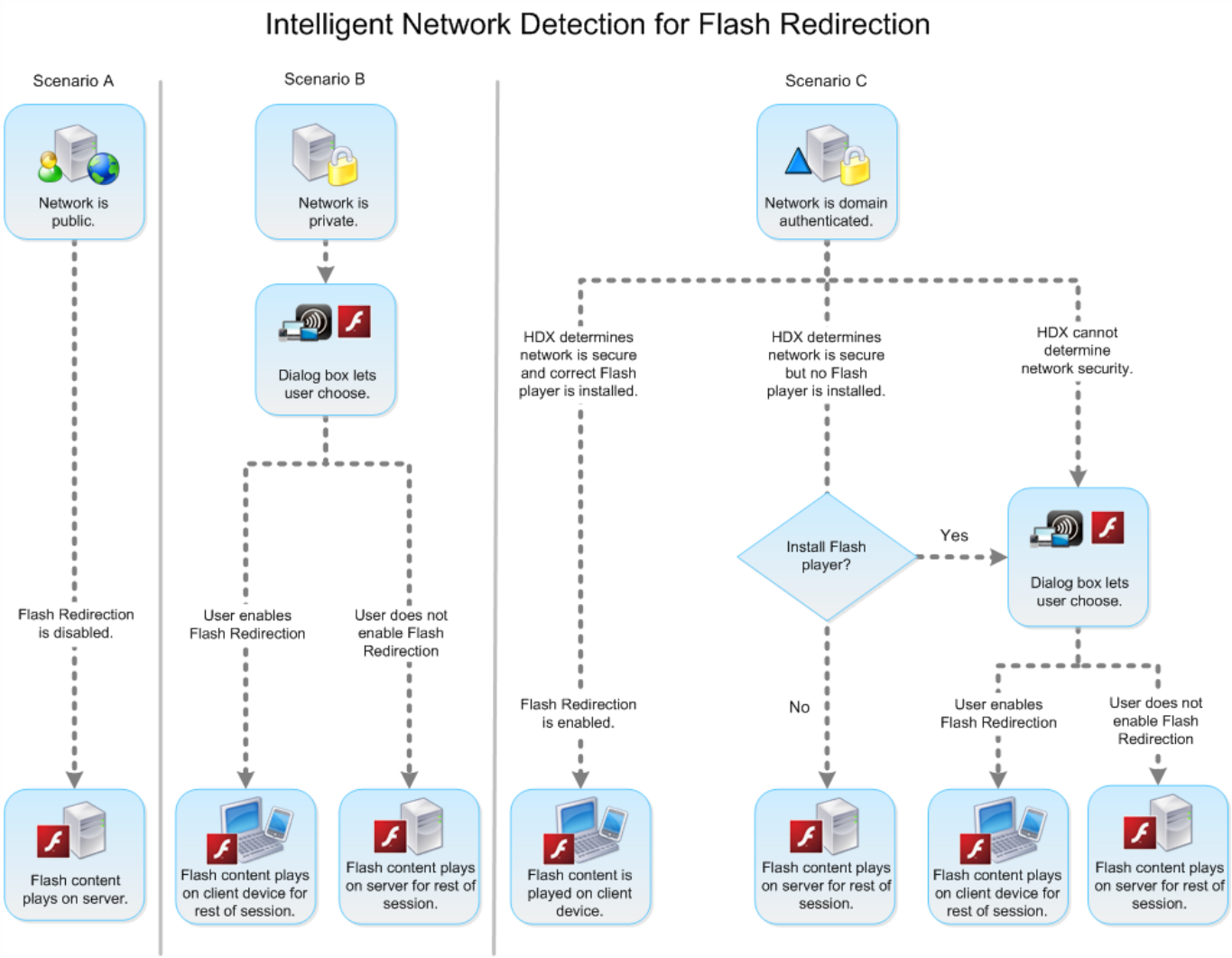
ポリシー設定が未構成である場合、Desktop Lock環境ではデフォルトでFlashリダイレクトが有効になります。

Flashリダイレクトの動作を変更したり、リダイレクト機能を無効にしたりするには、以下の手順に従います。

1. ［設定］の一覧で［このユーザーデバイスでの HDX MediaStream Flash リダイレクトを有効にする］を選択して［ポリシー設定］をクリックします。

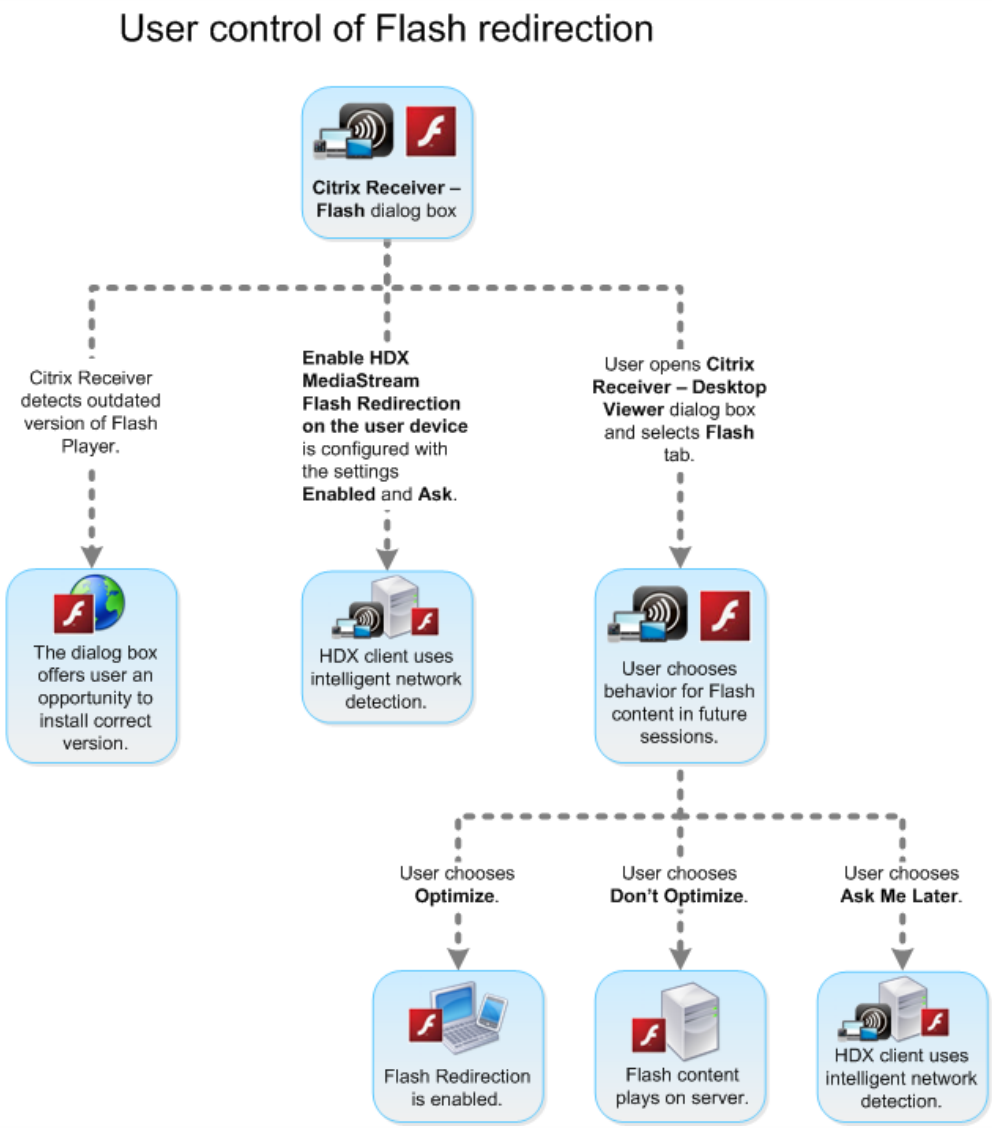
© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. ［未構成］、［有効］（デフォルト）、または［無効］を選択します。
3. ［有効］を選択する場合は、［HDX MediaStream Flash リダイレクトを使用する］一覧で以下のいずれかのオプションを選択します。
   - 最新のFlashリダイレクト機能（第2世代のFlashリダイレクト）を使用するには、［第 2 の生成でのみ有効］（第2世代Flashリダイレクトのこと）を選択します。これにより、要件が満たされる場合はFlashコンテンツがユーザーデバイス側で処理され、満たされない場合はサーバー側で処理されます。
   - 常にFlashリダイレクトを行うには、［常に有効］を選択します。これにより、Flashコンテンツが常にユーザーデバイス側で処理されます。
   - Flashリダイレクトを無効にするには、［常に無効］を選択します。これにより、Flashコンテンツが常にサーバー側で処理されます。
   - クライアント側のネットワークのセキュリティレベルを検出してFlashリダイレクトの使用を決定するには、［確認］（デフォルト）を選択します。ネットワークのセキュリティレベルを検出できない場合は、Flashリダイレクト機能を使用するかどうかを確認するメッセージがユーザーに表示されます。ネットワークのセキュリティレベルを検出できない場合は、Flashリダイレクト機能を使用するかどうかを確認するメッセージがユーザーに表示されます。
     次の図は、さまざまなネットワークでFlashリダイレクトがどのように処理されるかを示しています。



インテリジェントネットワーク検出機能は、ユーザー側で有効または無効にすることができます。これを行うには、［Citrix Receiver - Desktop Viewer 基本設定］ダイアログボックスの［Flash］タブで、［最適化する］または［最適化しない］を選択します。ここに表示されるオプションは、次の図のように、ユーザーデバイスでのFlashリダイレクトの構成により異なります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



クライアント側とサーバー側のHTTP Cookieを同期する

クライアント側とサーバー側のHTTP Cookieの同期機能は、デフォルトで無効になっています。この同期機能を有効にすると、サーバー側からクライアント側にHTTP Cookieがダウンロードされます。ダウンロードされたHTTP Cookieはクライアント側でのコンテンツ取得に使用され、そのFlashコンテンツのWebサイトがそのCookieを必要に応じて使用できるようになります。

注： この同期処理が発生しても、クライアント側のCookieは上書きされません。後で同期機能が無効になった場合は、元のクライアント側のCookieが使用されます。

1. ［設定］の一覧で［クライアント側の HTTP Cookie とサーバー側の Cookie の同期化を有効にする］を選択し、［ポリシー設定］をクリックします。
2. ［未構成］、［有効］、または［無効］（デフォルト）を選択します。

サーバー側でのコンテンツ取得を有効にする

Flashリダイレクトのデフォルトでは、Adobe Flashコンテンツがユーザーデバイス上に直接ダウンロードされ、そこで処理されます。サーバー側でのコンテンツ取得を有効にすると、Flashコンテンツがサーバー上にダウンロードされ、その後でユーザーデバイスに転送されます。［Flash URL 互換性リスト］設定によりブロックされるサイトなどの上書きポリシーがない限り、Flashコンテンツはユーザーデバイス側で処理されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通常、サーバー側でのコンテンツ取得は、ユーザーデバイスがNetScaler Gatewayを介して社内サイトに接続する場合や、ユーザーデバイスがインターネットに直接アクセスできない場合に使用されます。

注： サーバー側でのコンテンツ取得機能は、RTMP（Real Time Messaging Protocol）を使用したFlashアプリケーションをサポートしません。このようなサイトは、サーバー側で処理されます。
Flashリダイレクトでは、サーバー側でのコンテンツ取得を有効にする3つのオプションがサポートされています。これらの中には、サーバー側で取得したコンテンツをユーザーデバイス上にキャッシュするためのものが含まれています。これにより、再使用されるコンテンツがユーザーデバイス上にキャッシュされるため、パフォーマンスが向上します。このキャッシュコンテンツは、ユーザーデバイス上でキャッシュされるほかのHTTPコンテンツとは別に保存されます。

いずれかの有効オプションが選択されている場合に、クライアント側でのSWFファイル取得に失敗すると自動的にサーバー側コンテンツ取得にフォールバックされます。

サーバー側でのコンテンツ取得を有効にするには、クライアントデバイス側およびサーバー側での設定が必要です。

1. ［設定］の一覧で、［サーバー側のコンテンツの取得を有効にする］を選択して［ポリシー設定］をクリックします。
2. ［未構成］、［有効］、または［無効］（デフォルト）を選択します。［有効］を選択する場合は、［サーバー側のコンテンツの取得の状態］一覧で以下のいずれかのオプションを選択します。

オプション	説明
無効	サーバー側でのコンテンツ取得を無効にします。サーバー上の［Flash サーバー側でのコンテンツ取得 URL リスト］設定は無視されます。サーバー側でのコンテンツ取得へのフォールバックも無効になります。
有効	［Flash サーバー側でのコンテンツ取得 URL リスト］で指定したWebページおよびFlashアプリケーションに対するサーバー側でのコンテンツ取得を有効にします。サーバー側でのコンテンツ取得へのフォールバックは使用可能になりますが、Flashコンテンツはキャッシュされません。
有効（永続キャッシュ）	［Flash サーバー側でのコンテンツ取得 URL リスト］で指定したWebページおよびFlashアプリケーションに対するサーバー側でのコンテンツ取得を有効にします。サーバー側でのコンテンツ取得へのフォールバックが使用可能になります。サーバー側で取得されたコンテンツはユーザーデバイス上でキャッシュされ、そのセッションを終了しても保持されます。
有効（一時キャッシュ）	［Flash サーバー側でのコンテンツ取得 URL リスト］で指定したWebページおよびFlashアプリケーションに対するサーバー側でのコンテンツ取得を有効にします。サーバー側でのコンテンツ取得へのフォールバックが使用可能になります。サーバー側で取得されたコンテンツはユーザーデバイス上でキャッシュされますが、そのセッションの終了時に削除されます。

3. サーバー上で、ポリシーの［Flash サーバー側でのコンテンツ取得 URL リスト］設定を有効にして、URLを一覧に追加します。

クライアント側でのコンテンツ取得でユーザーデバイスをほかのWebサイトにリダイレクトする

Flashコンテンツの取得をリダイレクトするには、第2世代のFlashリダイレクト機能であるURL［クライアント側のコンテンツの取得の URL 書き換え規則］設定を使用します。この機能を構成する場合、2つのURLのパターンを指定します。ユーザーデバイスが最初のパターン（「一致パターン」）と一致するWebサイトからコンテンツを取得しようとすると、2つ目のパターン（「置換パターン」）により指定されたWebサイトにリダイレクトされます。

この設定を使って、コンテンツ配信ネットワーク（CDN）の機能を補うことができます。Flashコンテンツを配信する一部のWebサイトでは、ユーザーからのコンテンツ要求が、そのユーザーに最も近いWebサイトにリダイレクトされます。これを、「CDNリダイレクト」と呼びます。Flashリダイレクトによるクライント側でのコンテンツ取得を使用する場合、Flashコンテ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンツはユーザーデバイスから要求され、それ以外のWebページの内容はサーバーから要求されます。CDNを使用しているWeサイトでは、サーバーからの要求が最も近いWebサイトにリダイレクトされるため、ユーザーデバイスからの要求も同じ場所にリダイレクトされます。ただし、この場所はユーザーデバイスに最も近い場所ではない可能性があります。このため、WeページとFlashコンテンツの読み込みに距離による差が生じることがあります。

1. ［設定］の一覧で、［クライアント側のコンテンツの取得の URL 書き換え規則］を選択して［ポリシー設定］をクリックします。
2. ［未構成］、［有効］、または［無効］を選択します。［未構成］がデフォルトで選択されています。［無効］を選択すると、次の手順で指定するURL書き換え規則がすべて無視されます。
3. この設定を有効にした場合は、［表示］をクリックします。Perl正規表現構文を使って［値の名前］ボックスに一致パターンを入力し、［値］ボックスに置換パターンを入力します。

Flashリダイレクトの最小バージョンチェック。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix Receiver for WindowsまたはCitrix Receiver for Linuxを使ってVDAにアクセスするクライアントデバイスに対するFlashリダイレクトに必要な最小バージョンを指定するためのレジストリ設定を追加できます。このセキュリティ機能により、古いFlashバージョンが使用されないことが保証されます。

ServerFlashPlayerVersionMinimumは、ICAサーバー（VDA）上で必要なFlash Playerの最小バージョンを指定する文字列値です。

ClientFlashPlayerVersionMinimumは、ICAクライアント（Citrix Receiver）上で必要なFlash Playerの最小バージョンを指定する文字列値です。

これらのバージョン文字列は、「10」、「10.2」、または「10.2.140」のように指定できます。メジャーおよびマイナーのビルド番号のみ比較されます。レビジョン番号は無視されます。たとえば、メジャー番号のみ「10」と指定されたバージョン文字列の場合、マイナーおよびビルド番号は0であるという前提になります。

FlashPlayerVersionComparisonMaskは、DWORD値です。0と設定すると、ICAサーバー上のFlash Playerに対するICAクライアント上のFlash Playerのバージョンの比較が無効になります。比較マスクにはほかの値がありますが、0以外のマスクの意味は変わることがあるため、それらを使用するべきではありません。必要なクライアント対して比較マスクを0に設定することを推奨します。クライアント不明な設定について比較マスクを設定することはお勧めしません。比較マスクを指定しない場合、Flashリダイレクトを実行するにはICAクライアントにICAサーバー上のFlash Playerのバージョンと同じまたはそれ以上のバージョンのFlash Playerがある必要があります。この場合、Flash Playerのメジャーバージョン番号のみが比較の対象となります。

リダイレクトを実行するには、比較マスクを使ったチェックに加えてクライアントとサーバーの最小チェックにも成功する必要があります。

サブキーClientID0x51はCitrix Receiver for Linuxを指定します。サブキーClientID0x1はCitrix Receiver for Windowsを指定します。このサブキーには、文字列"ClientID"に16進数のクライアント製品ID（0で始まるものがない）を付けて名前が付けられます。

32ビットVDAのレジストリ構成例

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] クライアント不明の設定

"ClientFlashPlayerVersionMinimum"="13.0" ICAクライアントに必要な最小バージョン
"ServerFlashPlayerVersionMinimum"="13.0" ICAサーバーに必要な最小バージョン
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows ICAクライアント設定

"ClientFlashPlayerVersionMinimum"="16.0.0" Windowsクライアントに必要なFlash Playerの最小バージョンを指定します
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux ICAクライアント設定

"FlashPlayerVersionComparisonMask"=dword:00000000 Linuxクライアントのバージョン比較検査を無効にします（クライアントにサーバーよりも新しいFlash Playerがあるか確認します） "ClientFlashPlayerVersionMinimum"="11.2.0" LinuxクライアントのFlash Playerの最小バージョンを指定します。

64ビットVDAのレジストリ構成例

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HTML5マルチメディアリダイレクト

Jan 05, 2018

HTML5マルチメディアリダイレクションは、HDX MediaStreamのマルチメディアリダイレクト機能を拡張し、HTML5のオーディオとビデオを含むようにしたものです。マルチメディアコンテンツのオンライン配信の拡大、特にモバイルデバイスへの拡大により、ブラウザー業界はオーディオやビデオを再生するより効率的な方法を開発してきました。

Flashが標準となりましたが、 Flashはプラグインが必要で、すべてのデバイスで稼働するわけではなく、また、モバイルデバイスでは大量のバッテリーを消費します。Youtube、NetFlix.comなどの企業やMozilla、Google、Microsoftのブラウザーの新バージョンはHTML5に移行しており、これが新しい標準になっています。

HTML5ベースのマルチメディアには、専用プラグインを超える以下のような多数の利点があります。

- 企業非依存型の標準（W3C）
- 簡素化されたデジタル著作権管理（DRM）ワークフロー
- プラグインが原因のセキュリティの問題がないことによる優れたパフォーマンス

HTTPプログレッシブダウンロード

HTTPプログレッシブダウンロードは、HTML5をサポートする、HTTPベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、（単一品質でエンコードされた）1つのファイルがHTTP Webサーバーからダウンロードされている間に、ブラウザーがそれを再生します。ビデオは、受け取られるとハードドライブに保存され、ハードドライブから再生されます。ビデオを再度視聴する場合、ブラウザーがキャッシュからビデオをロードします。

プログレッシブダウンロードの例については、「HTML5ビデオリダイレクションのテストページ」を参照してください。使用するブラウザーの開発者ツールを使用して、Webページ内のビデオエレメントを調べ、以下のようなHTML5ビデオタグ内のソース（MP4コンテナーフォーマット）を探します。

HTML5とFlashの比較

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Feature	HTML5	Flash
専用のプレーヤーが必要	なし	はい
モバイルデバイスで実行	はい	一部
異なるプラットフォームでの実行速度	高	低速
iOSでサポート	はい	なし
リソース使用率	低い	追加
より高速なロード	はい	なし

要件

MP4フォーマットでのプログレッシブダウンロードのリダイレクトのみがサポートされます。WebM、およびDASH/HLSなどのアダプティブビットレートストリーミングのテクノロジーはサポートされません。

サポート対象：

- サーバー側でレンダリング
- サーバー側でフェッチし、クライアント側でレンダリング
- クライアント側でフェッチ

これらはポリシーを使って制御されます。詳しくは、「マルチメディアのポリシー設定」を参照してください。

Citrix Receiverの最小バージョン：

- Citrix Receiver for Windows 4.5
- Citrix Receiver for Linux 13.5

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Minimum VDA browser version	Windows OS version/build/SP
Internet Explorerバージョン11.0	Windows 10 x86（1607 RS1）およびx64（1607 RS1） Windows 7 x86およびx64 Windows Server 2016 RTM 14393（1607） Windows Server 2012 R2
Firefox 47 Firefox証明書ストアに証明書を手動で追加するか、 Windowsの信頼できる証明書ストアで 証明書を探すように Firefoxを構成します。詳しくは、https://wiki.mozilla.org/CA:AddRootToFirefox を参照してください。	Windows 10 x86（1607 RS1）およびx64（1607 RS1） Windows 7 x86およびx64 Windows Server 2016 RTM 14393（1607） Windows Server 2012 R2
Chrome 51	Windows 10 x86（1607 RS1）およびx64（1607 RS1） Windows 7 x86およびx64 Windows Server 2016 RTM 14393（1607） Windows Server 2012 R2

HTML5ビデオリダイレクションソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドを傍受するJavaScriptフック。HdxVideo.jsは、セキュアWebSocket（SSL/TLS）を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    場所：［証明書 - ローカルコンピューター］>［信頼されたルート証明機関］>［証明書］。
  - エンドエンティティ（リーフ）：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    場所：［証明書 - ローカルコンピューター］>［個人］>［証明書］。
- **WebSocketService.exe** - ローカルシステムで稼働し、SSLの終了とユーザーセッションマッピングを実行します。127.0.0.1ポート9001でリスンするTLS Secure WebSocketです。
- **WebSocketAgent.exe** - ユーザーセッションで稼働し、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HTML5ビデオリダイレクションを有効にするには

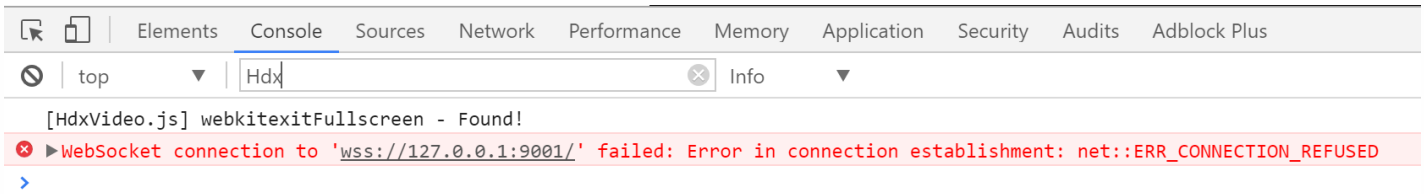
このリリースでは、この機能は管理対象Webページでのみ利用できます。HTML5マルチメディアコンテンツが利用可能なWebページにHdxVideo.js JavaScript（XenDesktopおよびXenAppのインストールメディアに含まれています）を追加する必要があります。たとえば、社内研修サイトのビデオなどです。

youtube.comのようにアダプティブビットレート技術（HTTPライブストリーミング（HLS）、Dynamic Adaptive Streaming over HTTP（DASH）など）をベースにしたWebサイトは、サポートされていません。

詳しくは、「*マルチメディアのポリシー設定*」を参照してください。

トラブルシューティングのヒント

WebページでHdxVideo.jsを実行しようとすると、エラーが発生する場合があります。JavaScriptが読み込みに失敗した場合、HTML5リダイレクションメカニズムはエラーになります。使用するブラウザーの開発者ツールウィンドウでコンソールを調べて、HdxVideo.jsに関連するエラーがないことを確認してください。たとえば、以下のようなものです。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows Media リダイレクト

Dec 05, 2017

Windows Mediaリダイレクトは、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。サーバーではなくクライアントデバイスでメディアランタイムファイルを再生することで、Windows Mediaリダイレクトはマルチメディアファイルの再生に必要な帯域幅を減少させます。Windows Mediaリダイレクトは、仮想Windowsデスクトップで実行中のWindows Media Playerおよび互換プレーヤーのパフォーマンスを向上させます。

Windowsメディアのクライアント側でのコンテンツ取得の要件が満たされない場合、メディア配信は自動的にサーバー側での取得を使用します。その方法はユーザーにとって透過的です。XenDesktop Collectorを使用して、HostMMTransport.dllからCitrix Diagnosis Facility（CDF）トレースを実行すると、その使用方法を決定できます。

Windows Mediaリダイレクトは、ホストサーバーでのメディアパイプラインをインターセプトし、ネイティブの圧縮フォーマットでメディアデータをキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスはパイプラインを再作成し、ホストサーバーから受信したメディアデータの展開およびレンダリングを行います。Windows MediaリダイレクトはWindowsオペレーティングシステムを実行中のクライアントデバイスで正しく動作します。これらのデバイスは、ホストサーバーに存在したパイプラインを再構築するために必要なマルチメディアフレームワークを備えています。Linuxクライアントは、メディアパイプラインを再構築するために、同様のオープンソースメディアフレームワークを使用します。

Windows Mediaリダイレクトのポリシー設定は、この機能を制御します。デフォルトは **[許可]** です。この設定は、通常、セッション内で再生されるオーディオおよびビデオの品質が向上して、クライアントデバイス上のファイルを再生しているときの品質に近くなります。まれに、Windows Mediaリダイレクトによるメディアの再生品質が、基本的なICA圧縮および通常のオーディオ機能での品質よりも悪い場合があります。その場合は、**Windows Mediaリダイレクト**設定をポリシーに追加し、その値を **[禁止]** にして、機能を無効にすることができます。

ポリシーの設定について詳しくは、「マルチメディアのポリシー設定」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

一般コンテンツリダイレクト

Dec 05, 2017

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを
うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームがUNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをWindowsデスクトップデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト

一般的ではないユースケースでの、ホストからクライアントへのリダイレクト機能の使用を検討します。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。この種類のリダイレクト機能は、サーバーOSのVDAでのみサポートされ、デスクトップOSのVDAではサポートされません。

ローカルアプリケーションアクセスとURLリダイレクト

ローカルアプリケーションアクセスを有効にすると、ローカルにインストールされているWindowsアプリケーションが仮想デスクトップ環境にシームレスに統合されます。

USBとクライアント側ドライブの考慮事項

HDXテクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なとき**汎用USBリダイレクト**を提供します。

関連情報

- Client folder redirection
- Host to client redirection
- Local App Access and URL redirection
- USB and client drive considerations
- Multimedia

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントフォルダーのリダイレクト

Dec 05, 2017

クライアントフォルダーの リダイレクトは、クライアント側のファイルがホスト側の セッションへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の 全ボリュームがUNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、 ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリューム の一部がリダイレクトされます。

セッション内では、ユーザーデバイス上の すべてのファイルシステムの代わりに ユーザー指定のフォルダーのみがUNCリンクとして表示されます。 レジストリでUNCリンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。

クライアントフォルダーのリダイレクトはWindowsデスクトップOSマシンでのみサポートされます。

外部USBドライブに対するクライアントフォルダーのリダイレクトは、デバイスを解除して再接続しても保存されません。

サーバー側でクライアントフォルダーのリダイレクトを有効にします。次に、クライアントデバイス上でリダイレクト対象フォルダーを指定します。クライアントフォルダーオプションの指定に使用するアプリケーションは、このリリースで提供されるCitrix Receiverに含まれています。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. サーバー側で以下を行います。
    1. キー（HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection）を作成します。
    2. REG_DWORD値を作成します。
        - 値の名前：CFROnlyModeAvailable
        - 種類：REG_DWORD
        - データ：「1」に設定します。
2. ユーザーデバイス側で以下を行います。
    1. 最新バージョンのCitrix Receiverがインストールされていることを確認します。
    2. Citrix Receiverのインストール先ディレクトリで、CtxCFRUI.exeを実行します。
    3. ［Custom］ラジオボタンをクリックし、フォルダーを追加、編集、または削除します。
    4. セッションを切断してから再接続すると、変更が適用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ホストからクライアントへのリダイレクト

Dec 05, 2017

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

ホストからクライアントへのリダイレクトは コンテンツリダイレクト機能の一種です。この機能は、サーバーOSのVDAでのみサポートされ、デスクトップOSのVDAではサポートされません。

- ホストからクライアントへのリダイレクト機能を有効にすると、URLはサーバーVDAでインターセプトされてからユーザーデバイスに送信されます。これらのURLは、ユーザーデバイス上のWebブラウザーまたはマルチメディアプレーヤーで開かれます。
- ホストからクライアントへのリダイレクト機能を有効にしても、ユーザーデバイスからURLに接続できない場合は、そのURLがサーバーVDAに戻されます。
- ホストからクライアントへのリダイレクト機能が無効な場合、URLはサーバーVDA上のWebブラウザーまたはマルチメディアプレーヤーで開きます。
- ホストからクライアントへのリダイレクト機能が有効な場合、ユーザーがこの機能を無効にすることはできません。

ホストからクライアントへのリダイレクト機能は、以前は**サーバーからクライアントへのリダイレクト機能**と呼ばれていました。

ホストからクライアントへのリダイレクト機能の使用に適した状況

一般的ではない特定の状況では、パフォーマンス、互換性、コンプライアンスなどの理由から、ホストからクライアントへのリダイレクト機能の使用が必要となることがあります。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。

性能は、

ホストからクライアントへのリダイレクト機能を使用すると、ユーザーデバイスにアプリケーションがインストールされていれば、VDA上のアプリケーションではなくこのアプリケーションを使用することができ、パフォーマンスを改善できます。

ただし、VDAではAdobe Flashなどのマルチメディアコンテンツは既に最適化されているため、ホストからクライアントへのリダイレクト機能によりパフォーマンスが改善されるのは特定の状況に限られます。まず、ホストからクライアントへのリダイレクト機能ではなく、次の表に示した他のアプローチ（ポリシー設定）を使用することを検討してください。これらの設定は柔軟性が高く、特に低性能のユーザーデバイスでは、一般的にユーザーエクスペリエンスも向上します。

互換性

以下の場合、ホストからクライアントへのリダイレクト機能を使用して互換性を確保できます。

- HTMLおよびマルチメディア以外のコンテンツタイプを使用する場合（例：カスタムURLタイプ）
- VDAのマルチメディアプレーヤーのマルチメディアリダイレクト機能ではサポートされていない旧式のメディア形式を使用する場合（Real Mediaなど）
- 特定のコンテンツタイプのアプリケーションを使用するユーザーがごく少数であり、それらのユーザーがこのアプリケーションを各ユーザーデバイスにインストール済みの場合
- VDAでは特定のWebサイトにアクセスできない場合（例：内部Webサイトから別組織のWebサイトへのアクセス）

コンプライアンス

以下の場合、ホストからクライアントへのリダイレクト機能を使用してコンプライアンスを確保できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- アプリケーションまたはコンテンツのライセンス契約によりVDA経由の公開が許可されていない場合
- 組織のポリシーによりVDAへのドキュメントのアップロードが許可されていない場合

一部の状況は、環境が複雑な場合や、ユーザーデバイスとVDAを所有する組織が異なる場合に起こりやすくなります。

ユーザーデバイスに関する考慮事項

環境によっては、さまざまな種類のユーザーデバイスが存在する場合があります。

ユーザーデバイス	状況または環境	使用するコンテンツリダイレクト機能
タブレット	-	次表のすべての機能
ラップトップPC	-	次表のすべての機能
デスクトップPC	ユーザーがユーザーデバイスにインストール済みの多様なアプリケーションを使用する場合	次表のすべての機能
デスクトップPC	ユーザーが使用するのが、ユーザーデバイスにインストール済みである少数かつ既知のアプリケーションに限られている場合	ローカルアプリケーションアクセス
デスクトップPC	ユーザーがユーザーデバイスにインストール済みのアプリケーションを使用しない場合	マルチメディアリダイレクトまたはFlashリダイレクト
デスクトップアプライアンス	ベンダーがマルチメディアリダイレクトまたはFlashリダイレクトをサポートしている場合	マルチメディアリダイレクトまたはFlashリダイレクト
シンクライアント	ベンダーがマルチメディアリダイレクト、Flashリダイレクト、ホストからクライアントへのリダイレクトをサポートしている場合	次表のすべての機能
ゼロクライアント	ベンダーがマルチメディアリダイレクトまたはFlashリダイレクトをサポートしている場合	マルチメディアリダイレクトまたはFlashリダイレクト

使用するコンテンツリダイレクト機能を決める際は、次の例を参考にしてください。

URLのリンク	状況または環境	使用するコンテンツリダイレクト機能
Webページまたはドキュメント	VDAがURLにアクセスできない場合	ホストからクライアントへのリダイレクト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Webページ	WebページにAdobe Flashが含まれる場合	Flashリダイレクト
マルチメディアファイルまたはストリーム	互換性のあるマルチメディアプレーヤーがVDAにインストールされている場合	マルチメディアリダイレクト
マルチメディアファイルまたはストリーム	互換性のあるマルチメディアプレーヤーがVDAにインストールされていない場合	ホストからクライアントへのリダイレクト
ドキュメント	VDAに当該種類のドキュメント用のアプリケーションがインストールされていない場合	ホストからクライアントへのリダイレクト
ドキュメント	ユーザーデバイスへのドキュメントのダウンロードが禁止されている場合	リダイレクト不可
ドキュメント	VDAへのドキュメントのアップロードが禁止されている場合	ホストからクライアントへのリダイレクト
カスタムのURLタイプ	VDAにカスタムURLタイプ用のアプリケーションがインストールされていない場合	ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクト機能は、Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux、Citrix Receiver for HTML5、Citrix Receiver for Chromeでサポートされています。

ホストからクライアントへのリダイレクト機能を使用するには、ユーザーデバイスにWebブラウザー、マルチメディアプレーヤー、またはコンテンツに対応したその他のアプリケーションをインストールする必要があります。ユーザーデバイスがデスクトップアライアンス、シンクライアント、またはゼロクライアントである場合、適切なアプリケーションがインストールされていること、および性能が十分であることを確認してください。

ローカルアプリケーションアクセスを有効にしたユーザーデバイスでは別のコンテンツリダイレクトメカニズムが使用されるため、ホストからクライアントへのリダイレクト機能は必要ありません。

Citrixの各種ポリシーを使用して、不適切なデバイスについてホストからクライアントへのコンテンツリダイレクト機能を禁止できます。

ホストからクライアントへのリダイレクト機能が使用される状況

ホストからクライアントへのリダイレクト機能は、URLが以下の場合に使用されます。

- アプリケーションにハイパーリンクとして埋め込まれている場合（電子メールメッセージやドキュメントなど）
- VDAアプリケーションのメニューまたはダイアログボックスから選択された場合（アプリケーションでWindows ShellExecuteEx APIが使用されているとき）
- Windowsの［ファイル名を指して実行］ダイアログボックスに入力された場合

Webブラウザー内のURL（WebページのURL内およびWebブラウザーのアドレスバーに入力されたURLのどちらでも）に対しては、ホストからクライアントへのリダイレクト機能は使用されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> ユーザーが（［規定のプログラムを設定する］などを使用して）VDA上のデフォルトのWebブラウザーを変更した場合、この変更によりアプリケーションのホストからクライアントへのリダイレクト機能が影響を受ける可能性があります。

ホストからクライアントへのリダイレクト機能が有効な場合、URLを開くアプリケーションは、URLの種類とコンテンツの種類の両方に関するユーザーデバイスの設定で決まります。次に例を示します。

- コンテンツタイプがHTMLであるHTTP URLは、デフォルトのWebブラウザーで開かれます。
- コンテンツタイプがPDFであるHTTP URLは、デフォルトのWebブラウザーまたは別のアプリケーションのどちらかで開かれます。

ユーザーデバイスの設定は、ホストからクライアントへのコンテンツリダイレクト機能では制御できません。ユーザーデバイスの設定を制御しない場合は、ホストからクライアントへのコンテンツリダイレクト機能ではなく、Flashリダイレクトおよびマルチメディアリダイレクトを使用してください。

ホストからクライアントへのリダイレクト機能が有効な場合、次の種類のURLはユーザーデバイスでローカルに開かれます。

- HTTP（Hypertext Transfer Protocol）
- HTTPS（Secure Hypertext Transfer Protocol）
- RTSP（RealPlayerおよびQuickTime）
- RTSPU（RealPlayerおよびQuickTime）
- PNM（従来のRealPlayer）
- MMS（Microsoft Media Server）

ホストからクライアントへのリダイレクト機能のURLタイプのリストを変更して、カスタムURLタイプなどのURLタイプを削除および追加できます。

ホストからクライアントへのリダイレクト機能の有効化

ホストからクライアントへのリダイレクト機能を有効にするには、まずCitrixポリシー設定を有効にします。

ホストからクライアントへのリダイレクトポリシーの設定については、「ファイルリダイレクトのポリシー設定」に記載されています。デフォルトでは、無効になっています。

さらに、VDAのOSによっては、サーバーVDAのレジストリキーとグループポリシーの設定も必要になります。

- サーバーVDAがWindows Server 2008 R2 SP1である場合、レジストリキーとグループポリシーを設定する必要はありません。
- サーバーVDAがWindows Server 2012、Windows Server 2012 R2、またはWindows Server 2016である場合、レジストリキーとグループポリシーの設定が必要になります。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsのインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レジストリの変更

1. 以下の「**Reg file start**」と「**Reg file end**」の間にあるテキストをコピーして、メモ帳に貼り付けます。
2. ［名前を付けて保存］で［ファイルの種類］を［すべてのファイル］、［ファイル名］を「ServerFTA.reg」に指定して、メモ帳ファイルを保存します。
3. Active Directoryのグループポリシーを使用して、**ServerFTA.reg**ファイルをサーバーに配布します。

ServerFTA.reg コピー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
- Reg file start --

Windows Registry Editor Version 5.00



[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0"

"ApplicationName"="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"



[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

-- Reg file end --
```

グループポリシーの変更

XMLファイルを作成します。このXMLファイルに、以下の「xml file start」と「xml file end」の間にあるテキストをコピーしてxmlファイルに貼り付けて、**ServerFTAdefaultPolicy.xml**という名前で保存します。

ServerFTAdefaultPolicy.xml コピー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
-- xml file start --
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
</DefaultAssociations>
-- xml file end --
```

現在のグループポリシー管理コンソールで、**[コンピューターの構成]** > **[管理用テンプレート]** > **[Windowsコンポーネント]** > **[エクスプローラー]** > **[既定の関連付け構成ファイルの設定]** の順に開いて、作成したServerFTAdefaultPolicy.xmlファイルを指定します。

ホストからクライアントへのリダイレクト機能のURLタイプリストの変更

ホストからクライアントへのリダイレクト機能のURLタイプのリストを変更するには、サーバーVDAで次のレジストリキーを設定します。

キー: HKLM\Software\Wow6432Node\Citrix\SFTA

リストからURLタイプを削除するには、DisableServerFTAとNoRedirectClassesを設定します。

名前： DisableServerFTA
種類： REG_DWORD
データ： 1

名前： NoRedirectClasses
種類： REG_MULTI_SZ
データ： http、https、rtsp、rtspu、pnm、mmsのいずれかの組み合わせを指定します。1つの行に1つの値を入力してください。たとえば次のように入力します。

http

https

rtsp

リストにURLタイプを追加するには、ExtraURLProtocolsを設定します。

名前： ExtraURLProtocols
種類： REG_MULTI_SZ
データ： URLタイプの組み合わせを指定します。各URLタイプにはサフィックスとして「://」を追加し、複数の値はセミコロンで区切って入力します。以下に例を示します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

customtype1://;customtype2://

特定のWebサイトのセットについてホストからクライアントへのリダイレクト機能を有効にする

特定のWebサイトのセットについてホストからクライアントへのリダイレクト機能を有効にするには、サーバーVDAで次のレジストリキーを設定します。

キー: HKLM\Software\Wow6432Node\Citrix\SFTA

名前： ValidSites
種類： REG_MULTI_SZ
データ：完全修飾ドメイン名（Fully-Qualified Domain Name：FQDN）の組み合わせを指定します。1つの行に1つのFQDNを入力してください。FQDNには、左端にのみワイルドカードを含めることができます。 ワイルドカードを含むFQDNは単一レベルのドメインと照合されます。これはRFC 6125の規則に準拠しています。 たとえば次のように入力します。

www.example.com

*.example.com

Internet Explorer 9以降のバージョンでの構成

Internet Explorer 9以降のバージョンを公開ブラウザーとして使用するには、VDAサーバー上の以下のレジストリキー値を変更します。

キー：

HKEY_LOCAL_MACHINE\Software\Classes\htmlfile\shell\opennew

HKEY_LOCAL_MACHINE\Software\Classes\http\shell\open

HKEY_LOCAL_MACHINE\Software\Classes\https\shell\open

HKEY_CLASSES_ROOT\http\shell\open

HKEY_CLASSES_ROOT\https\shell\open

HKEY_CLASSES_ROOT\htmlfile\shell\opennew

変更元：

名前：CommandID

種類：REG_SZ

データ：IE.Protocol

目的：

名前：CommandID

© 1999-2017 Citrix Systems, Inc. All rights reserved.

種類：REG_SZ

データ：IE.ProtocolX

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ローカルアプリケーションアクセスとURLリダイレクト

Dec 05, 2017

ここでは次のことについて説明します。

- はじめに
- 要件、考慮事項、および制限事項
- Windows上での動作
- ローカルアプリケーションアクセスとURLリダイレクトの構成

はじめに

ローカルアプリケーションアクセスを有効にすると、ローカルにインストールされているWindowsアプリケーションが仮想デスクトップ環境にシームレスに統合されます。ローカルアプリケーションアクセスにより、以下の操作が可能になります。

- ラップトップやPCなどの物理コンピューター上にローカルにインストールされたアプリケーションに仮想デスクトップからアクセスする。
- フレキシブルなアプリケーション配信ソリューションをユーザーに提供する。仮想化できないアプリケーションやIT担当者が管理しないアプリケーションをユーザーのローカルにインストールして、仮想デスクトップ上にインストールされたアプリケーションのように使用できます。
- 仮想デスクトップ以外のホスト上で提供される公開アプリケーションのダブルホップによる遅延を解消するために、そのアプリケーションのショートカットをユーザーのWindowsデバイス上に配置する。
- 次のようなアプリケーションを使用する。
  - GoToMeetingなどのビデオ会議ソフトウェア。
  - 仮想化されていない特殊なアプリケーション。
  - DVDバーナーやTVチューナーなど、ユーザーデバイスとサーバー間で大量のデータ転送が発生するアプリケーションや周辺機器。

XenAppおよびXenDesktopでローカルアプリケーションアクセスが有効な場合、URLリダイレクトにより、ホストされるデスクトップセッションからローカルアクセスアプリケーションを起動できます。URLリダイレクトでは、複数のURLアドレスでアプリケーションを起動できます。デスクトップセッションで、Webブラウザー内に埋め込まれたリンクをクリックすると、WebブラウザーのURLブラックリストに基づいてローカルのWebブラウザーが起動します。ブラックリストにないURLをクリックすると、デスクトップセッション内のWebブラウザーが再度使用されます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できるリダイレクト機能は、サーバーFTA（File Type Association：ファイルタイプの割り当て）リダイレクトの1つである「ホストからクライアントへのコンテンツのリダイレクト」のみです。このFTAでは、http、http、rtsp、mmsなど、特定のプロトコルがクライアント側に転送されます。たとえば、httpの埋め込みリンクを開くときに、クライアント側のアプリケーションが使用されます。特定のURLのリダイレクトを有効にしたり無効にしたりすることはできません。

ローカルアプリケーションアクセスを有効にすると、ローカルで実行されるアプリケーション、ホストされるアプリケーション、またはデスクトップ上のショートカットからアクセスされたURLを、以下のいずれかの方法でリダイレクトできます。

- ユーザーのコンピューターから、ホストされているデスクトップへ
- XenApp/XenDesktopサーバーから、ユーザーのコンピューターへ
- 起動された環境内で処理（リダイレクトなし）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

特定のWebサイトでのリダイレクト方法を指定するには、Virtual Delivery Agent上のURLホワイトリストおよびURLブラックリストを構成します。これらのリストでは、URLリダイレクトのポリシー設定を指定する複数行文字列値を設定します。詳しくは、「ローカルアプリケーションアクセスのポリシー設定」を参照してください。

すべてのURLをVDA側のWebブラウザーで開くこともできますが、以下のURLについてはエンドポイント上のWebブラウザーで開くためのポリシーを構成できます。

- ジオ/ロケール情報 — ユーザーの現在位置の情報に基づいて適切なページを自動的に表示するmsn.comやnews.google.comなどのWebサイト。たとえば、イギリスにあるデータセンターで提供されるVDAにインドのクライアントから接続する場合、in.msn.comではなくuk.msn.comが表示されます。
- マルチメディアコンテンツ — メディアリッチなWebサイト。クライアント側で処理されるように設定すると、ユーザーエクスペリエンスが向上し、狭帯域幅接続での使用帯域幅や処理能力が改善されます。Flashリダイレクト機能を使用することもできますが、URLリダイレクトを使用するとSilverlightなどほかの種類のメディアにも対応できます。これにより、環境のセキュリティも向上します。つまり、管理者により許可されたURLだけがクライアント側で処理され、ほかのURLはすべてVDA側で処理されます。

URLリダイレクトに加えて、FTAリダイレクトも使用できます。この機能では、セッションで特定のファイルを開くときにローカルのアプリケーションが使用されます。ローカルアプリケーションでファイルを開くには、そのローカルアプリケーションがそのファイルにアクセスできる必要があります。つまり、ローカルアプリケーションで開くことができるのは、ネットワーク共有上またはクライアントドライブ上にあるファイル（クライアント側ドライブのマッピング機能）のみです。たとえば、PDFファイルを開く場合、ローカルにインストールされているPDFリーダーでファイルが表示されます。ローカルアプリケーションはファイルに直接アクセスできるため、ファイルを開くときにICAによるネットワーク転送は発生しません。

要件、考慮事項、および制限事項

ローカルアプリケーションアクセスはVDA for Windows Server OSおよびVDA for Windows Desktop OSでサポートされるオペレーティングシステムでサポートされ、Citrix Receiver for Windows Version 4.1（以降）が必要です。次のWebブラウザーがサポートされています。

- Internet Explorer 11以降。Internet Explorer 8、9、または10も使用できますが、MicrosoftはInternet Explorer 11をサポートしており、CitrixもInternet Explorer 11の使用を推奨しています。
- Firefox 3.5～21.0
- Chrome 10

ローカルアプリケーションアクセスやURLリダイレクトを使用するときは、以下の考慮事項および制限事項について確認してください。

- ローカルアプリケーションアクセスは全画面モード用に設計されています。このため、以下の制限事項があります。
  - ローカルアプリケーションアクセスをウィンドウ表示モードの仮想デスクトップで使用するなど、単一の仮想デスクトップをすべてのモニター上で表示しない場合、ユーザーエクスペリエンスに混乱が生じます。
  - マルチモニター環境でアプリケーションの表示を1つのモニターで最大化すると、それ以降のアプリケーションはほかのモニターに表示されず、すべてのアプリケーションがそのモニター上に表示されます。
  - この機能は、単一VDAでの使用を想定して設計されています。複数の同時接続VDAを対象とするものではありません。
- 一部のアプリケーションでは、以下の予期されない問題が発生する場合があります。
  - ユーザーが、仮想デスクトップのCドライブとローカルのCドライブを混同する場合があります。
  - 仮想デスクトップで使用できるプリンターは、ローカルアプリケーションでは使用できません。
  - 管理者特権が必要なアプリケーションは、ローカルアプリケーションアクセスでは起動できません。
  - 単一インスタンスアプリケーション（Windows Media Playerなど）もほかのアプリケーションと同等に処理されます。
  - ローカルアプリケーションはローカルマシンのWindowsテーマで表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 全画面アプリケーションはサポートされません。これには、PowerPointのスライドショーやデスクトップ全体で表示されるフォトビューアーなど、全画面で開くアプリケーションが含まれます。
- ローカルアプリケーションアクセスでは、ローカルアプリケーションのプロパティ（デスクトップや［スタート］メニューへのショートカットの配置など）が複製されます。ただし、ショートカットキーや読み取り専用属性などのそのほかのプロパティは複製されません。
- 一部のアプリケーションで、各ウィンドウが正しい重なり順で表示されない場合があります。これにより、一部のウィンドウが非表示になることがあります。
- マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブ、フォルダーなどのショートカットはサポートされません。
- カスタムのファイルタイプ、関連付けられたプログラムのないファイル、ZIPファイル、および隠しファイルはサポートされません。
- ビット数の異なるローカルアプリケーションとVDAアプリケーションのタスクバーでのグループ化はサポートされません。たとえば、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションは、タスクバーでグループ化されません。
- アプリケーションはCOMを使って起動できません。たとえば、Officeアプリケーション内に埋め込まれているOfficeドキュメントをクリックしても、プロセス起動が検出されないため、ローカルアプリケーション統合に失敗します。

- ユーザーが、仮想デスクトップセッション内から別の仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- 明示的なURLリダイレクトのみがサポートされます。つまり、Webブラウザーのアドレスバーに表示されるURLや、ブラウザー内ナビゲーションによるURLだけが正しくリダイレクトされます。
- URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーにユーザーが新しいファイルを作成することはできません。
- ローカルアプリケーションの複数のインスタンスのタスクバーアイコンは、仮想デスクトップのタスクバー設定に基づいて表示されます。ただし、ローカルで実行されているアプリケーションのショートカットは、このアプリケーションの実行インスタンスのアイコンとはグループ化されません。また、ホストされているアプリケーションの実行インスタンスや、のアプリケーションのピン留めアイコンともグループ化されません。タスクバー上のアイコンでは、ローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ローカルアプリケーションのショートカットをデスクトップタスクバーや［スタート］メニューに固定することもできますが、そのショートカットからアプリケーションを起動できなくなる場合があります。

Windows上での動作

ローカルアプリケーションアクセスは、Windows上で次のように動作します。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアント上にインストールされたWindowsストアアプリケーションは、ローカルアプリケーションアクセスのショートカットとして列挙されません。
  - 通常、イメージファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションで開かれます。ただし、ローカルアプリケーションアクセスでは、Windowsストアアプリケーションが列挙され、ショートカットがデスクトップアプリケーションで開かれます。
- Local Programsフォルダー
  - Windows 7の場合、［スタート］メニューにLocal Programsフォルダーが表示されます。
  - Windows 8の場合、ユーザーがスタート画面のカテゴリとして **[すべてのアプリ]** を選択した場合のみ、Local Programsフォルダーが表示されます。Local Programsフォルダーにすべてのサブフォルダーが表示されるわけではありません。
- アプリケーション用のWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限され、スタート画面およびWindows 8スタイルアプリケー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ションの背面に表示されます。
    - ローカルアプリケーションアクセスは、マルチモニターモードでデスクトップアプリケーションのようには動作しません。マルチモニターモードでは、スタート画面とデスクトップは別のモニター上で表示されます。
- Windows 8およびローカルアプリケーションアクセスのURLリダイレクト
    - Windows 8上のInternet Explorerではアドオンを使用できないため、URLリダイレクトを有効にする場合はデスクトップ版のInternet Explorerを使用する必要があります。
    - Windows Server 2012上のInternet Explorerでは、デフォルトでアドオンが無効になっています。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にしてください。標準ユーザーに対してアドオンが有効になるように、Internet Explorerのオプションを再設定して再起動します。

ローカルアプリケーションアクセスとURLリダイレクトの構成

Citrix Receiverでローカルアプリケーションアクセスと URLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Receiverをインストールします。Citrix Receiverのインストール時に両方の機能を有効にしたり、グループポリシーエディターを使ってローカルアプリケーションアクセステンプレートを有効にしたりできます。
- ポリシーの **[ローカルアプリケーションのアクセスを許可する]** 設定で **[許可]** を選択します。またURLリダイレクトのため、URLホワイトリストとブラックリストポリシー設定を構成できます。詳しくは、「ローカルアプリケーションアクセスのポリシー設定」を参照してください。

Citrix Receiverのインストール時におけるローカルアプリケーションアクセスとURLリダイレクトの有効化

すべてのローカルアプリケーションに対してローカルアプリケーションアクセスとURLリダイレクトを有効にするには

1. ポリシーの **[ローカルアプリケーションのアクセスを許可する]** 設定で **[許可]** を選択します。これにより、管理者が公開したアプリケーションおよびローカルアプリケーションアクセスのショートカットが有効かどうかがクライアントにより検出されます。（この設定が無効の場合、管理者が公開したアプリケーションおよびローカルアプリケーションアクセスのショートカットのいずれもVDAで機能しません。）このポリシー設定は、URLリダイレクトのポリシー設定だけではなく、マシン全体に適用されます。
2. Citrix Receiverのインストール時に、マシンのすべてのユーザーに対してローカルアプリケーションアクセスとURLリダイレクトを有効にします。この操作により、URLリダイレクト機能で使用されるWebブラウザーアドオンも登録されます。コマンドプロンプトで適切なコマンドを実行して、次のオプションと共にReceiverをインストールします。

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

グループポリシーエディターを使ってローカルアプリケーションアクセステンプレートを有効にするには

1. **gpedit.msc**を実行します。
2. **［コンピューターの構成］** を選択します。**［管理用テンプレート］** を右クリックし、**［テンプレートの追加と削除］ > ［追加］** の順に選択します。
3. Citrix ReceiverのConfigurationフォルダー（通常はc:\Program Files (x86)\Citrix\Online Plugin\Configuration）にあるicaclient.admテンプレートを追加します（icaclient.admテンプレートをコンピューターのConfigurationに追加した後、［ユーザーの構成］でそれを構成できます）。
4. **［管理用テンプレート］**、**［従来の管理用テンプレート（ADM）］**、**［Citrix Components］**、**［Citrix Receiver］**、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[**User Experience**] の順に開きます。

5. [**ローカルアプリケーションアクセス設定**] を選択します。
6. [**有効**] を選択し、 [**URLのリダイレクトを許可します**] チェックボックスをオンにします。URLリダイレクト機能を使用するには、以下を参照にしながらコマンドラインを使用してWebブラウザーにアドオンを登録する必要もあります。

公開アプリケーションへのアクセスのみを提供する

公開アプリケーションへのアクセスのみを提供するには

1. Delivery Controllerがインストールされたサーバー上で、**regedit.exe**を実行します。
   1. HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\DesktopStudioを開きます。
   2. REG_DWORD値ClientHostedAppsEnabledを追加して、1を設定します（0を設定するとローカルアプリケーションアクセスが無効になります）。
2. Delivery Controllerサーバーを再起動して、Studioを起動します。
3. ローカルアプリケーションアクセスのアプリケーションを公開します。
   1. Studioのナビゲーションペインで [**デリバリーグループ**] を選択し、［アプリケーション］タブを選択します。
   2. ［操作］ペインで、 [**ローカルアクセスアプリケーションの作成**] を選択します。
   3. デスクトップのデリバリーグループを選択します。
   4. ユーザーのローカルマシン上にあるアプリケーションの実行可能ファイルのフルパスを入力します。
   5. このローカルアプリケーションのショートカットを仮想デスクトップの［スタート］メニューやデスクトップに追加するかどうかを指定します。
   6. ［名前］ページでデフォルトの値をそのまま使用して、設定内容を確認します。
4. Citrix Receiverのインストール時に、マシンのすべてのユーザーに対してローカルアプリケーションアクセスとURLリダイレクトを有効にします。この操作により、URLリダイレクト機能で使用されるWebブラウザーアドオンも登録されます。コマンドプロンプトで以下のコマンドを実行してCitrix Receiverをインストールします。
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. ポリシーの [**ローカルアプリケーションのアクセスを許可する**] 設定で [**許可**] を選択します。これにより、管理者が公開したアプリケーションおよびローカルアプリケーションアクセスのショートカットが有効かどうかがクライアントにより検出されます。［禁止］を選択すると、管理者が公開したアプリケーションとローカルアプリケーションアクセスのショートカットが機能しなくなります。

Webブラウザーアドオンの登録

注： URLリダイレクト機能で使用されるWebブラウザーアドオンは、コマンドラインでCitrix Receiverをインストールするときに/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを指定すると自動的に登録されます。

以下のコマンドを実行して、適切なWebブラウザーにアドオンを登録したり登録解除したりできます。

- クライアントデバイス上でアドオンを登録する場合： *<client-installation-folder>*\redirector.exe /reg*<browser>*
- クライアントデバイス上でアドオンの登録を解除する場合： *<client-installation-folder>*\redirector.exe /unreg*<browser>*
- VDA上でアドオンを登録する場合： *<VDAinstallation-folder>*\VDARedirector.exe /reg*<browser>*
- VDA上でアドオンの登録を解除する場合： *<VDAinstallation-folder>*\VDARedirector.exe /unreg*<browser>*

ここで、*<browser>*にはIE、FF、Chrome、またはAllを指定します。

たとえば、Citrix Receiverを実行するデバイス上でInternet Explorer用のアドオンを登録するには、次のコマンドを実行します。

```
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

また、VDA for Windows Server OSが動作するサーバー上ですべてのアドオンを登録するには、次のコマンドを実行します。

```
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll
```

さまざまなWebブラウザーでのURLリダイレクト

- Internet Explorerでは、入力されたURLがデフォルトでリダイレクトされます。ブラックリストに追加されていないURLがWebブラウザーやWebサイトによりほかのURLにリダイレクトされた場合、最終的なURLはブラックリストに追加されていてもリダイレクトされません。

  URLリダイレクトが正しく機能するためには、Webブラウザーに表示されるメッセージに従ってアドオンを有効にする必要があります。インターネットオプションを使用するアドオンやメッセージで示されたアドオンが無効の場合、URLリダイレクトは正しく機能しません。

- Firefoxアドオンでは、URLが常にリダイレクトされます。

  Firefoxでは、アドオンのインストールを許可するかどうかを確認するメッセージが新しいタブに表示されます。URLリダイレクトが正しく機能するためには、アドオンのインストールを許可する必要があります。

- Chromeのアドオンでは、ユーザーがナビゲーションにより開いた最終的なURL（ユーザーが入力したものでないURL）は常にリダイレクトされます。

  拡張機能が外部的にインストールされます。この拡張機能を無効にすると、ChromeでURLリダイレクトが動作しなくなります。シークレットモードでURLリダイレクトを使用するには、Webブラウザーの設定でシークレットモードでの拡張機能の実行を許可する必要があります。

ログオフおよび切断時のローカルアプリケーションアクセスの動作の構成

1. ホストされたデスクトップ上で、**gpedit.msc**を実行します。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session Stateを開きます。64ビットシステムの場合、HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session Stateを開きます。
3. REG_DWORD値Terminateを追加して、以下のいずれかを値のデータとして設定します。
   - 1 — ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。
   - 3 — ユーザーが仮想デスクトップからログオフまたは切断した場合、ローカルアプリケーションが終了します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

USBとクライアント側ドライブの考慮事項

Dec 05, 2017

HDXテクノロジは、一般的なUSBデバイスのほとんどに**最適化されたサポート**を提供します。以下の仮想ディスクを移動できます。

- モニター
- マウス
- キーボード
- ボイスオーバーIP電話
- ヘッドセット
- Webカメラ
- スキャナー
- カメラ
- プリンター
- ドライブ
- スマートカードリーダー
- 描画用タブレット
- 署名パッド

最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDXテクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なとき**汎用USBリダイレクト**を提供します。

- USBデバイスに追加の高度な機能があり（追加ボタンがあるマウスやWebカメラなど）、それらの機能が最適化されたサポートに含まれていないとき。
- ユーザーが最適化されたサポートに含まれない機能（CDの書き込みなど）を必要とするとき。
- USBデバイスが特殊なデバイス（テスト用機器、測定用機器、工業用コントローラーなど）であるとき。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスする必要があるとき。
- USBデバイスでWindowsドライバーしか使用できないとき。たとえば、スマートカードリーダーにCitrix Receiver for Androidで使用できるドライバーがないことがあります。
- Citrix Receiverのバージョンが、該当するタイプのUSBデバイスに最適化されたサポートを提供しないとき。

汎用USBリダイレクトでは、

- ユーザーデバイスにデバイスドライバーをインストールする必要はありません。
- USBクライアントドライバーはVDAマシン上にインストールされます。

> ## 注意
>
> - 汎用USBリダイレクトは、最適化されたサポートと併用できます。汎用USBリダイレクトを有効にする場合は、整合性の不一致と予期しない動作を避けるために、CitrixのUSBデバイスのポリシー設定で汎用USBリダイレクトと最適化されたサポートの両方を構成します。
> - Citrixのポリシー設定クライアントUSBデバイス最適化規則は、一部のUSBデバイスでは、汎用USBリダイレクト固有の設定です。ここで説明したような最適化されたサポートではありません
> - クライアントUSBプラグアンドプレイデバイスリダイレクトは、Picture Transfer Protocol（PTP）やMedia Transfer Protocol（MTP）を使用するカメラやメディアプレーヤーなどのデバイスに、最適化されたサポートを提供する関連機能です。ク

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ライアントUSBプラグアンドプレイリダイレクトは汎用USBリダイレクトの一部ではありません。クライアントUSBプラグアンドプレイリダイレクトはサーバーOSでのみ使用できます。

USBデバイスのパフォーマンスに関する考慮事項

一部のタイプのUSBデバイスの汎用USBリダイレクトでは、ネットワークの遅延と帯域幅がユーザーエクスペリエンスとUSBデバイスの操作に影響を与えます。たとえば、遅延が多く低帯域幅のリンクでタイミングが重要なデバイスが正しく動作しないことがあります。可能な場合は、代わりに最適化されたサポートを使用してください。

3Dマウスなどの一部のUSBデバイスは、高い帯域幅を使用できる必要があります（通常、これも高帯域幅を必要とする3Dアプリとともに使用）。パフォーマンスの問題はCitrixポリシーを使って回避することができます。詳しくは、「帯域幅のポリシー設定」（クライアントUSBデバイスリダイレクトの場合）および「マルチストリーム接続のポリシー設定」を参照してください。

USBデバイスのセキュリティに関する考慮事項

スマートカードリーダーやフィンガープリントリーダー、署名パッドなどの一部のUSBデバイスは、もともとセキュリティを重視します。USBストレージデバイスなどの他のUSBデバイスは、機密扱いである可能性のあるデータの受け渡しに使用できます。

USBデバイスは、しばしばマルウェアの配信に使用されます。このようなUSBデバイスのリスクを、Citrix Receiver、XenApp、およびXenDesktopの構成で減らすことはできますが、すべて取り除くことはできません。このことは、汎用USBリダイレクを使用しているか最適化されたサポートを使用しているかにかかわらず当てはまります。

Important

セキュリティを重視するデバイスやデータを扱う場合は、TLSまたはIPSecのどちらかを使用して、常にHDX接続をセキュリティで保護してください。

必要なUSBデバイスのサポートのみを有効にしてください。汎用USBリダイレクトと最適化されたサポートの両方で、このニーズを満たしてください。

信用できるソースから入手したUSBデバイスのみを使用する、USBデバイスを人がいないオープンな環境に置きっぱなしにしない（例：インターネットカフェにFlashデバイスを置きっぱなしにしない）といった、USBデバイスの安全な使用についてのガイダンスをユーザーに提供してください。また、複数のコンピューターで1つのUSBデバイスを使用することのリスクを説明してください。

汎用USBリダイレクトの互換性

汎用USBリダイレクトは、USB 2.0以前のデバイスでサポートされます。USB 3.0デバイスをUSB 2.0またはUSB 3.0ポートに接続した場合も、汎用USBリダイレクトがサポートされます。汎用USBリダイレクトは、USB3.0に導入された超高速などのUSB機能はサポートしません。

次のCitrix Receiverは、汎用USBリダイレクトをサポートします。

- Citrix Receiver for Windows（「XenDesktop環境の構成」を参照）
- Citrix Receiver for Mac（「Citrix Receiver for Macの構成」を参照）
- Citrix Receiver for Linux（「最適化」を参照）
- Citrix Receiver for Chrome OS（「Citrix Receiver for Chrome 2.1について」を参照）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Receiverのバージョンについては、『Citrix Receiver feature matrix』を参照してください。

前のバージョンのCitrix Receiverを使用している場合は、Citrix Receiverのドキュメントを参照して、汎用USBリダイレクトがサポートされていることを確認してください。サポートされるUSBデバイスのタイプに関する制限事項については、Citrix Receiverのドキュメントを参照してください。

汎用USBリダイレクトはVDA for Desktop OSのバージョン7.6以上のデスクトップセッションでサポートされます。

汎用USBリダイレクトはVDA for Server OSのバージョン7.6以上のデスクトップセッションでサポートされますが、以下の制限事項があります。

- VDAはWindows Server 2012 R2または Windows Server 2016で動作している必要があります。
- シングルホップのシナリオだけがサポートされます。デスクトップでホストされるアプリケーションセッションでは、ダブルホップ汎用USBリダイレクトはサポートされません。
- USBデバイスドライバーは、完全仮想化サポートなど、Windows 2012 R2のリモートデスクトップセッションホスト（RDSH）と完全に互換性がある必要があります。

次のような一部のタイプのUSBデバイスは、リダイレクトしても役に立たないため、汎用USBリダイレクトをサポートしません。

- USBモデム。
- USBネットワークアダプター。
- USBハブ。USBハブに接続したUSBデバイスは、個別に扱われます。
- USB仮想COMポート。汎用USBリダイレクトではなく、COMポートリダイレクトを使用します。

汎用USBリダイレクトでテストされたUSBデバイスについては、CTX123569を参照してください。一部のUSBデバイスは、汎用USBリダイレクトを使用すると正しく動作しません。

汎用USBリダイレクトの設定

汎用USBリダイレクトを使用するUSBデバイスのタイプを制御できます。次の手段で別々に設定できます。

- Citrixポリシー設定を使ってVDAで設定します。詳しくは、「クライアント側のドライブやデバイスのリダイレクト」および「ポリシー設定リファレンス」の「USBデバイスのポリシー設定」を参照してください。
- Citrix ReceiverでCitrix Receiverに依存するメカニズムを使用します。たとえば、Citrix Receiver for Windowsは、管理用テンプレートで制御できるレジストリ設定で設定します。USBリダイレクトのデフォルトでは、特定のクラスのUSBデバイスてのみ許可され、ほかのクラスのデバイスはリダイレクトされません。詳しくは、Citrix Receiver for Windowsのドキュメントの「XenDesktop環境の構成」を参照してください。

別々に設定できることで柔軟性が提供されます。次に例を示します。

- 2つの異なる組織または部門がCitrix ReceiverとVDAを担当している場合に、それぞれが別に制御を実行できます。このことは、ある組織のユーザーが別の組織のアプリケーションにアクセスするときにも適用されます。
- USBデバイスを、特定のユーザーのみまたは（NetScaler Gateway経由ではなく）LAN経由で接続しているユーザーのみに許可する必要がある場合は、Citrixポリシー設定で制御できます。

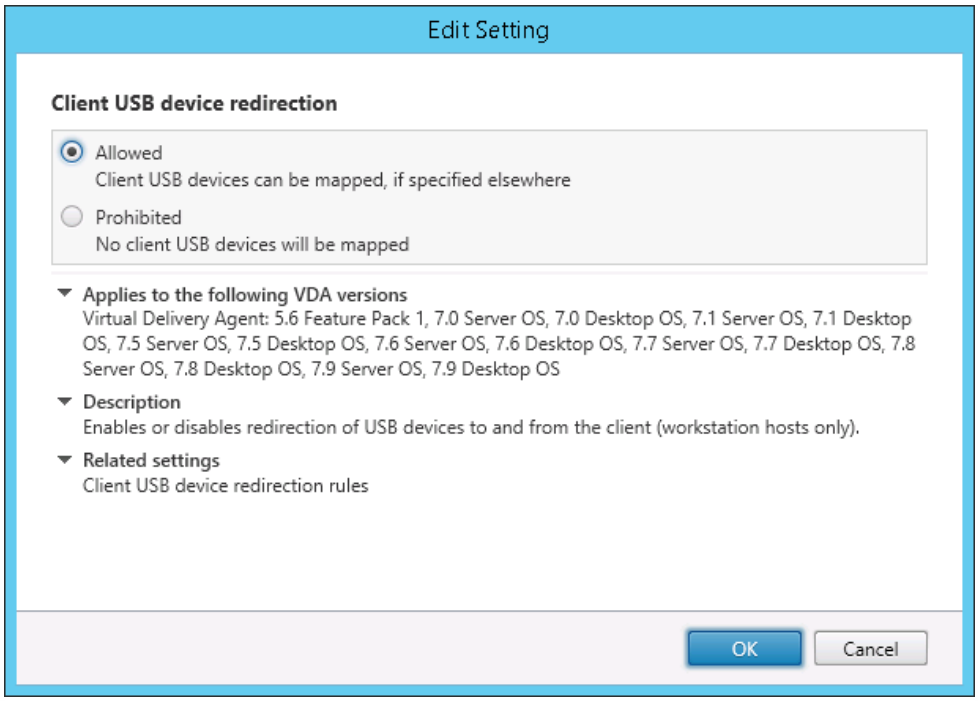
汎用USBリダイレクトの有効化

汎用USBリダイレクトを有効にするには、Citrixポリシー設定とCitrix Receiverの両方を設定します。

Citrixポリシー設定で、次の手順に従います。

1. 1.ポリシーに［クライアントUSBデバイスリダイレクト］を追加して、値に**［許可］**を設定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

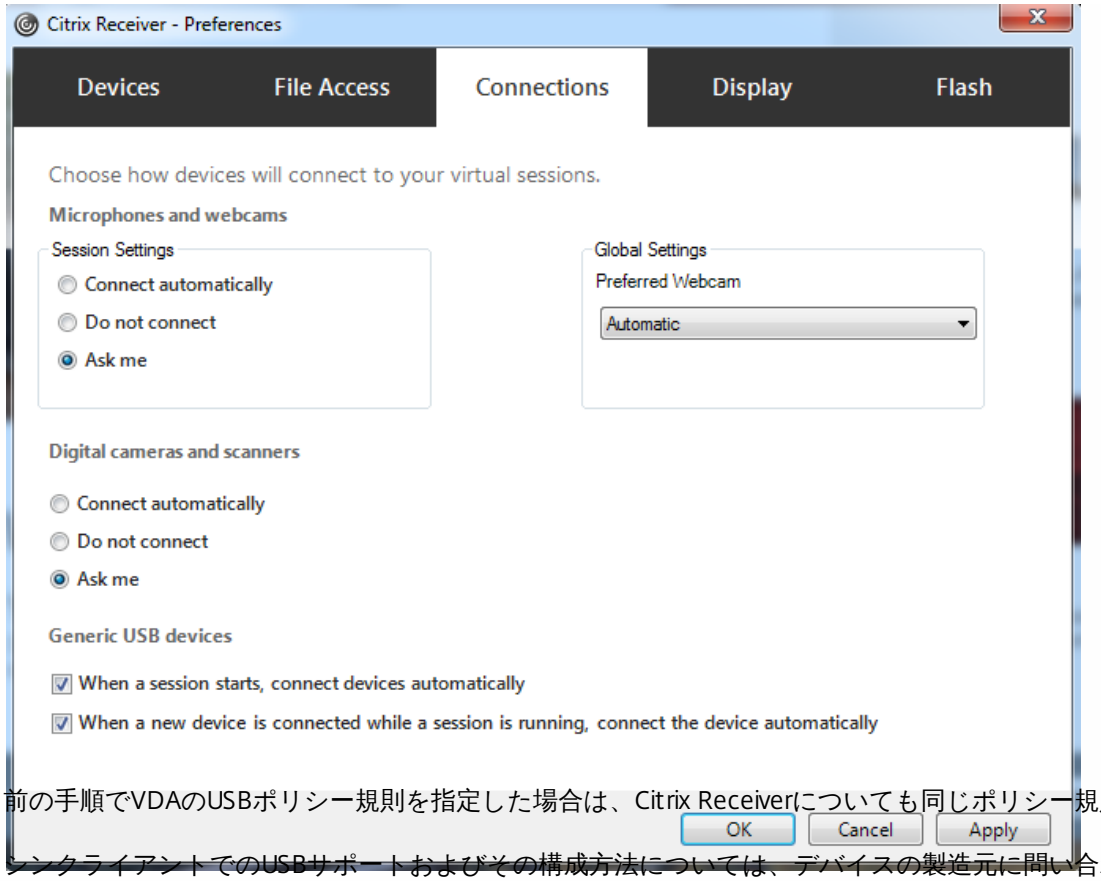


2. 必要な場合は、 [クライアントUSBデバイスリダイレクト規則]設定を追加して、リダイレクトするUSBデバイスの一覧を変更します。

Citrix Receiverで、次の手順に従います。

3. ユーザーデバイスにCitrix Receiverをインストールするときに、USBサポートを有効にします。この操作は、管理用テンプレートを使うか、［Citrix Receiver for Windows］>［基本設定］>［接続］で実行できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



前の手順でVDAのUSBポリシー規則を指定した場合は、Citrix Receiverについても同じポリシー規則を指定します。

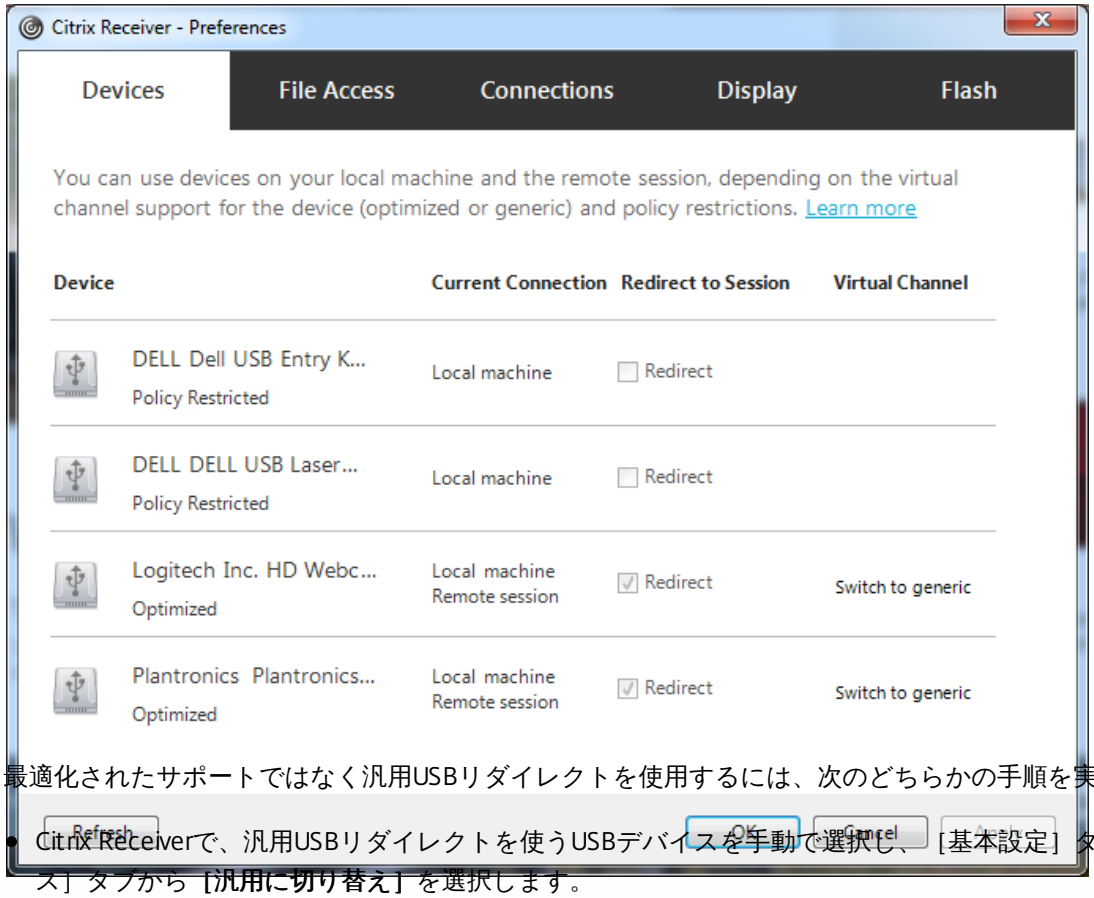
シンクライアントでのUSBサポートおよびその構成方法については、デバイスの製造元に問い合わせてください。

汎用USBリダイレクトで使用できるUSBデバイスタイプの設定

USBサポート機能が有効になっており、USB関連のユーザー設定でUSBデバイスに自動接続するように設定されている場合は、USBデバイスが自動的にリダイレクトされます。また、デスクトップアプライアンスモードで接続バーが表示されていない場合も、USBデバイスが自動的にリダイレクトされます。

ユーザーは、USBデバイスの一覧からデバイスを選択することによって、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。この手順について詳しくは、Citrix Receiver for Windowsのユーザーヘルプ「Desktop Viewerでのデバイスの表示」に説明されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



最適化されたサポートではなく汎用USBリダイレクトを使用するには、次のどちらかの手順を実行します。

- Citrix Receiverで、汎用USBリダイレクトを使うUSBデバイスを手動で選択し、［基本設定］ダイアログボックスの［デバイス］タブから**［汎用に切り替え］**を選択します。
- USBデバイスタイプの自動リダイレクトを設定することで（たとえばAutoRedirectStorage=1）、汎用USBリダイレクトを使うUSBデバイスを自動選択して、USBユーザー基本設定を自動接続USBデバイスに設定します。詳しくは、CTX123015を参照してください。

注： WebカメラとHDXマルチメディアリダイレクトの互換性がない場合は、Webカメラで使用する汎用USBリダイレクトのみを設定します。

USBデバイスを一覧に表示しないようにしたり、USBデバイスをリダイレクトできないようにしたりするには、Citrix ReceiveおよびVDAのデバイス規則を定義します。

汎用USBリダイレクトでは、少なくともUSBデバイスクラスとサブクラスを知っておく必要があります。すべてのUSBデバイスが明確なUSBデバイスクラスとサブクラスを持つわけではありません。次に例を示します。

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーはベンダー定義のクラスまたはHIDデバイスクラスを使用できます。

より正確な制御のためには、ベンダーID、製品ID、およびリリースIDも知っておく必要があります。この情報はデバイスベンダーから入手できます。

> ## Important
>
> 悪意のあるUSBデバイスが、意図された使用状況にマッチしないUSBデバイス特性を示すことがあります。デバイス規則は、この動作を防ぐことを目的としていません。

VDAとCitrix Receiver両方のUSBデバイスリダイレクト規則を指定し、デフォルトのUSBポリシー規則よりも優先することで、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

汎用USBリダイレクトを使用できるUSBデバイスを制御できます。

VDAの場合：

- グループポリシー規則を介して、サーバーOSマシン上のOSの管理者による上書き規則を編集します。グループポリシー管理コンソールは、インストールメディアにあります。
  - x64の場合：DVDルートの\os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - x86の場合：DVDルートの\os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Citrix Receiver for Windowsで

- ユーザーデバイス側のレジストリを編集します。インストールメディアに収録されている管理テンプレート（ADMファイル。\os\lang\Support\Configuration\icaclient_usb.adm）により、Active Directoryのグループポリシーを使用してユーザーデバイスを変更できます。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

製品のデフォルトの規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRulesに格納されています。このデフォルトの規則は変更しないでください。ただし、以下で説明しているように、製品のデフォルトの規則を参照して管理者による上書き規則を作成できます。管理者による上書き規則は、製品のデフォルトの規則よりも先に評価されます。

管理者による上書き規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRulesに格納されています。GPOポリシー規則は、**{Allow:|Deny:}**の後にスペースで区切った一連の=式の形式で設定します。

以下のタグがサポートされます。

タグ	説明
VID	デバイス記述子のベンダーID
PID	デバイス記述子の製品ID
REL	デバイス記述子のリリースID
クラス	デバイス記述子またはインターフェイス記述子のクラス。USB Webサイト（http://www.usb.org/）にあるUSBクラスコードを参照してください
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

© 1999-2017 Citrix Systems, Inc. All rights reserved.

新しいポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の末尾に、#で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切り文字にはスペースが使用されますが、番号または識別子の間には使用できません。たとえば、「Deny: Class = 08 SubClass=05」は有効ですが、「Deny: Class=0 Sub Class=05」は無効です。
- タグには等号（=）を使用する必要があります（VID=1230など）。
- 各規則を1行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。

> **注意**
>
> ADMテンプレートを使用する場合は、規則を単一行に（セミコロン区切りのリストとして）作成する必要があります。

例：

- 次の例は、ベンダーID（VID）および製品ID（PID）に対する管理者定義のUSBポリシー規則です。
  Allow: VID=046D PID=C626 # Logitech SpaceNavigator 3Dマウスを許可
  Deny: VID=046D # すべてのLogitech製品を禁止
- 次の例は、クラス、サブクラス、およびプロトコルに対する管理者定義のUSBポリシー規則です。
  Deny: Class=EF SubClass=01 Prot=01 # MS Active Syncデバイスを禁止
  Allow: Class=EF SubClass=01 # Syncデバイスを許可
  Allow: Class=EF # すべてのUSB-Miscellaneousデバイスを許可

USBデバイスの装着と取り外し

ユーザーは、仮想セッションの開始前および開始後にUSBデバイスを装着できます。

Citrix Receiver for Windowsでは、以下の点について考慮してください。

- セッションを開始した後で装着したデバイスは、Desktop Viewerの［USB］メニューに追加されます。
- USBデバイスが正しくリダイレクトされない場合、仮想セッションが開始されてからデバイスを装着することで問題が解決される場合があります。
- データの損失を避けるため、Windowsで推奨される手順（［ハードウェアの安全な取り外し］アイコンの使用など）に従ってUSBデバイスを取り外してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスでは最適化されたサポートが提供されます。これは、XenAppおよびXenDesktopクライアント側ドライブのマッピングに含まれています。ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップのドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。クライアント側ドライブのマッピングを構成するには、ポリシーの［ICA］>［ファイルリダイレクト］セクションの**［クライアント側リムーバブルドライブ］**設定を使用します。

USBマスストレージデバイスでは、Citrixポリシーによって制御されるClient側ドライブのマッピングまたは汎用USBリダイレクトのどちらか、またはこの両方を使用できます。主な違いは次のとおりです。

機能	クライアント側ドライブのマッピング	汎用USBリダイレクト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトで有効。	はい	なし
読み取り専用アクセスの構成が可能	はい	なし
デバイスアクセスが暗号化される	はい、デバイスをアクセスする前に暗号化のロックを解除した場合	なし
セッション中にデバイスを安全に取り外せる	なし	はい（ユーザーがオペレーティングシステムで推奨される手順に従う場合）

汎用USBリダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効な場合、セッション開始前または後に装着されたマスストレージデバイスがクライアント側ドライブのマッピングによりリダイレクトされます。汎用USBリダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効で、自動リダイレクト（http://support.citrix.com/article/CTX123015を参照）が構成されている場合、セッション開始前または後に装着されたマスストレージデバイスが汎用USBリダイレクトによりリダイレクトされます。

> **注意**
>
> USBリダイレクトはより低い帯域幅の接続（50Kbpsなど）でもサポートされますが、大きなファイルはコピーできません。

クライアント側ドライブのマッピングを使うファイルアクセスの制御

管理者は、ユーザーが仮想環境のファイルをユーザーデバイス上にコピーすることを許可したり禁止したりできます。デフォルトでは、マップされたクライアント側ドライブ上のフォルダーやファイルに対するセッション内での読み取りや書き込みが許可されます。

マップされたクライアント側ドライブ上のフォルダーやファイルの追加や変更を禁止するには、**[クライアント側ドライブへの読み取り専用アクセス]** 設定を有効にします。この設定項目をポリシーに追加するときは、**[クライアントドライブリダイレクト]** 設定も追加されており、 **[許可]** が選択されていることを確認してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷

Dec 05, 2017

環境でのプリンター管理には、 以下の複数の段階があります。

1. 印刷の概念を理解します。
2. 印刷アーキテクチャを計画します。これには、業務上のニーズや既存の印刷インフラストラクチャについての分析と、ユーザーやアプリケーションが現状でどのように印刷を行っているか、および理想的な印刷管理モデルは何かについての評価が含まれます。
3. プリンタープロビジョニングの方法を選択し、印刷設計を展開するためのポリシーを作成して印刷環境を構成します。新しい従業員またはサーバーが追加されたときにポリシーを更新します。
4. 新しい印刷環境を実務環境に展開する前に、その環境をテストします。
5. プリンタードライバーを管理し、印刷のパフォーマンスを最適化してCitrixの印刷環境を維持します。
6. 発生する問題をトラブルシューティングします。

印刷の概念

印刷環境の構築を計画する前に、Citrix環境での印刷処理の主な概念について理解しておく必要があります。

- 使用できるプリンタープロビジョニングの種類
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーの基本的な管理方法

印刷の概念は、Windowsの印刷概念上に構成されています。環境での印刷設定を正しく管理するには、Windowsでのネットワークやクライアント印刷のしくみについて熟知しており、それが実際の環境にどのように適用されるのかを理解する必要があります。

印刷プロセス

この環境では、ユーザーによる印刷はすべてアプリケーションをホストするマシン上で開始されます。印刷ジョブはネットワークプリントサーバーまたはユーザーデバイスを介して印刷装置にリダイレクトされます。

仮想デスクトップやアプリケーションのユーザーに提供されるワークスペースは永続的ではありません。ユーザーのセッションが終了すると、そのユーザーのワークスペースはサーバーから削除されます。このため、各セッションの開始時にすべての設定を再構築する必要があります。この結果、ユーザーが新しいセッションを開始するたびに、ユーザーのワークスペースが再構築されます。

ユーザーが印刷を実行すると、以下の処理が行われます。

- ユーザーに提供するプリンターを決定します。この処理は、プリンタープロビジョニングと呼ばれます。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

管理者は、プリンタープロビジョニング、印刷ジョブの送信経路、プリンタープロパティの保存、およびプリンタードライバー管理に関するオプションを変更して、上記の処理をカスタマイズできます。これらのオプションの変更によって環境での印刷パフォーマンスやユーザーエクスペリエンスがどのように変化するのかを検証してください。

プリンタープロビジョニング

セッション用のプリンターを準備する処理は、プリンタープロビジョニングと呼ばれます。通常、この処理は動的に行われます。つまり、セッションで提供されるプリンターは事前定義されておらず、非永続的です。プリンターは、セッションへの

© 1999-2017 Citrix Systems, Inc. All rights reserved.

グオン時または再接続時にポリシーに基づいて構成されます。このため、ポリシー、ユーザーの場所、およびネットワークに基づいて、異なるプリンターをユーザーに提供できます。つまり、ユーザーが別の場所に移動すると、そのユーザーの印刷環境が変更されます。

このCitrix製品の環境では、クライアント側のプリンターが監視され、クライアント側プリンターの追加、削除、および変更に応じてセッションの自動作成プリンターが動的に変更されます。この動的プリンター検出は、さまざまなデバイスを使用するモバイルユーザーにとって便利な機能です。

プリンターのプロビジョニングには、主に以下の方法があります。

- **Universal Print Server** — Citrix Universal Print Serverは、ネットワークプリンターでのユニバーサル印刷をサポートします。Universal Print Serverでは、ユニバーサルプリンタードライバーが使用されます。これにより、サーバーOSマシン上の単一のドライバーを使って、任意のデバイスからネットワーク印刷を実行できます。

  リモートの印刷サーバーを使う環境では、Citrix Universal Print Serverの使用をお勧めします。Universal Print Serverで送信される印刷ジョブは最適化および圧縮されるため、ネットワーク消費を抑えてユーザーエクスペリエンスを向上させることができます。

  Universal Print Serverの機能は以下のコンポーネントで構成されます。

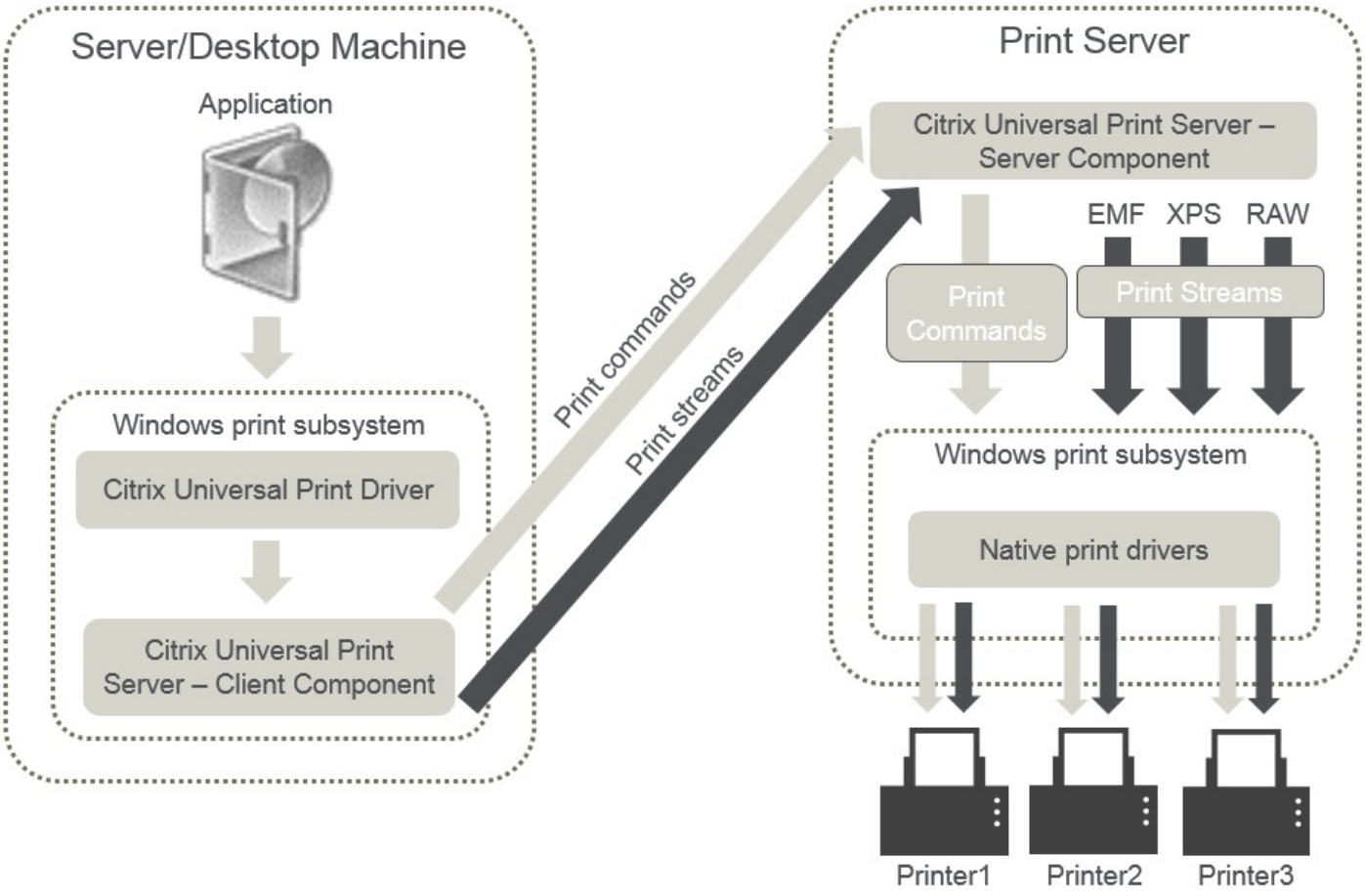
  クライアントコンポーネントの**UPClient** — サーバーOSマシンでユニバーサルプリンタードライバーを使用するセッションネットワークプリンターをプロビジョニングする場合は、そのマシン上のUPClientを有効にします。

  サーバーコンポーネントの**UPServer** — プリントサーバーでユニバーサルプリンタードライバーを使用するセッションネットワークプリンターをプロビジョニングする場合は（それらのセッションプリンターを集中管理的にプロビジョニングするかどうかに関係なく）、その印刷サーバー上にUPServerをインストールします。

Universal Print Serverの要件とセットアップ詳細については、システム要件およびインストールに関する説明を参照してください。

次の図は、Universal Print Serverを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Citrix Universal Print Serverを有効にすると、接続されているすべてのネットワークプリンターでUniversal Print Serverが自動検出されて使用されます。

注： Universal Print ServerはVDI-in-a-Box 5.3でもサポートされます。VDI-in-a-BoxでのUniversal Print Serverのインストールについて詳しくは、VDI-in-a-Boxのドキュメントを参照してください。

- **自動作成**-*自動作成とは、各セッションの開始時に自動的に作成されるプリンターを指します。*リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターだけが自動作成されるように構成することを検討します。自動作成するプリンターの数を最小限にすることで、サーバーOSマシンの負荷（メモリやCPU）を軽減できます。また、これによりユーザーログオン時間も短縮されます。
  以下の項目に基づいてプリンターが自動作成されます。

  - ユーザーデバイス上にインストールされたプリンター。
  - セッションに適用されるポリシー。
    管理者は、自動作成に関するポリシーを設定して、作成されるプリンターの数や種類を制御できます。デフォルトでは、ユーザーデバイス上で設定されているすべてのプリンター（ローカル接続のプリンターおよびネットワークプリンター）が自動作成され、ユーザーに提供されます。

  ユーザーがセッションを終了すると、これらのプリンターは削除されます。

  クライアントプリンターおよびネットワークプリンターの自動作成機能を使用する場合、保守作業が必要です。たとえば、プリンターを追加した場合は以下の設定が必要になります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ［セッションプリンター］ポリシー設定を更新します。
- ［プリンタードライバーのマッピングと互換性］ポリシー設定ですべてのサーバーOSマシンにドライバーを追加します。

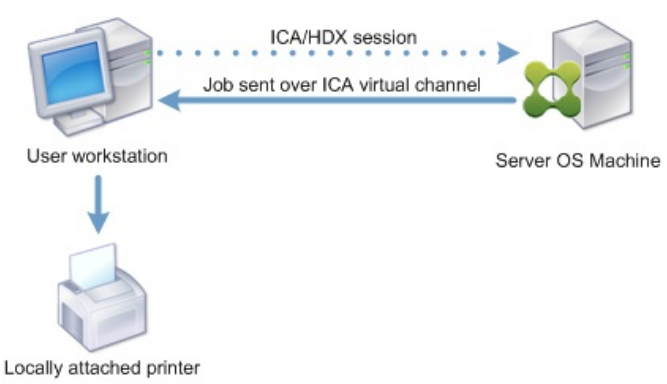
印刷ジョブの送信

印刷経路という語は、印刷ジョブがどのような経路で印刷装置に転送されるのか、および印刷ジョブがどこにスプールされるのかという概念を含んでいます。印刷環境を管理する場合、これらの概念を理解することは重要です。印刷ジョブのルーティング経路はネットワークトラフィックに影響し、スプール場所は印刷ジョブを処理するコンピューターの負荷に影響します。

この環境では、印刷装置への印刷ジョブの転送経路として、クライアント経由とネットワーク上のプリントサーバー経由の2つがあります。これらの転送経路は、「クライアント印刷経路」および「ネットワーク印刷経路」と呼ばれます。デフォルトでどちらの印刷経路が使用されるかは、使用されるプリンターの種類により異なります。

ローカル接続のプリンター

印刷ジョブは、サーバーOSマシンからクライアントに送信され、さらにローカル接続のプリンターに転送されます。この場合、ICAプロトコルにより最適化および圧縮された印刷ジョブがネットワーク上に送信されます。印刷装置がユーザーデバイスにローカルに接続されている場合、印刷ジョブがICA仮想チャネルで転送されます。



ネットワーク上のプリンター

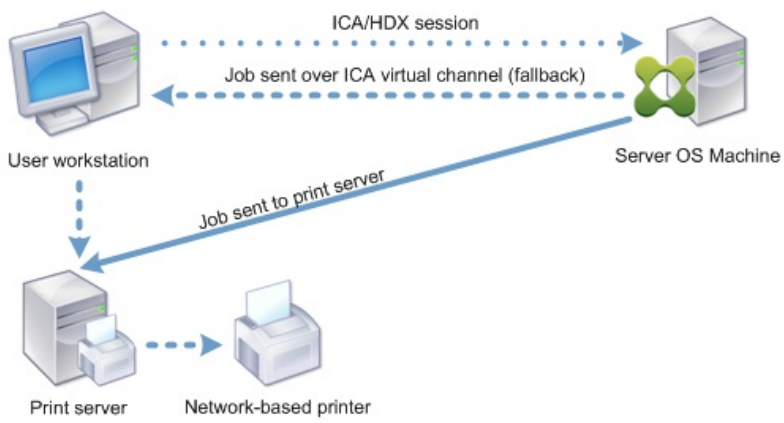
デフォルトでは、サーバーOSマシンからのすべての印刷ジョブがネットワークを介してプリントサーバーに直接転送されます。ただし、以下の状況では印刷ジョブが自動的にICA仮想チャネルで転送されます。

- 仮想デスクトップまたはアプリケーションがプリントサーバーにアクセスできない場合。
- プリンター固有のドライバーがサーバーOSマシン上にない場合。

Universal Print Serverが無効な場合、ICA仮想チャネルを介して送信される印刷ジョブは最適化および圧縮されるため、WANなどの狭帯域幅接続で隔たれたサーバーとクライアント間でクライアント印刷経路が使用されるように構成するとネットワークトラフィックへの負担が軽減されます。

また、クライアント印刷経路では、印刷ジョブに割り当てられる帯域幅を制限できます。印刷機能がないシンクライアントなど、ユーザーデバイスを介して印刷ジョブを転送できない場合は、QoS設定でICA/HDXトラフィックを優先させて、セッションで良好なユーザーエクスペリエンスが提供されるように構成してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



プリンタードライバーの管理

Citrixユニバーサルプリンタードライバー（UPD）は、デバイスに依存しないプリンタードライバーで、大部分のプリンターに対して互換性があります。Citrix UPDは、以下の2つのコンポーネントで構成されています。

サーバーコンポーネントCitrix UPDは、XenAppまたはXenDesktop VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに次のドライバーをインストールします：Citrixユニバーサルプリンター（EMFドライバー）およびCitrix XPSユニバーサルプリンター（XPSドライバー）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

印刷ジョブが開始されると、ドライバーは、エンドポイントデバイスをいっさい変更せずに、アプリケーションの出力を記録して送信します。

クライアントコンポーネントCitrix UPDは、Citrix Receiverのインストールの一部としてインストールされます。それによって、XenAppまたはXenDesktopセッションの着信する印刷ストリームがフェッチされます。印刷ストリームはローカルの印刷サブシステムに転送され、そこで印刷ジョブがデバイス固有のプリンタードライバーを使用してレンダリングされます。Citrix UPDのほか、Citrix PDFユニバーサルプリンタードライバーを、Citrix Receiver for HTML5およびCitrix Receiver for Chromeとともに別々にインストールできます。

Citrix UPDは次の印刷形式をサポートします。

- Enhanced Metafile Format（**EMF**）、デフォルト。EMFは32ビットバージョンのWindows Metafile（WMF）形式です。EMFドライバーは、Windowsベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーではXMLが使用され、Adobe PDFに似た、プラットフォームに依存しない「電子ペーパー」が作成されます。
- Printer Command Language（**PCL5c**および**PCL4**）。PCLは、もともとインクジェットプリンターのためにHewlett-Packardによって開発された印刷プロトコルです。基本的なテキストおよびグラフィックを印刷するために使用され、HP LaserJetおよび複合機で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストおよびベクターグラフィックスを印刷するために使用できるコンピューター言語です。ドライバーは、低コストのプリンターや複合機で広く使われています。

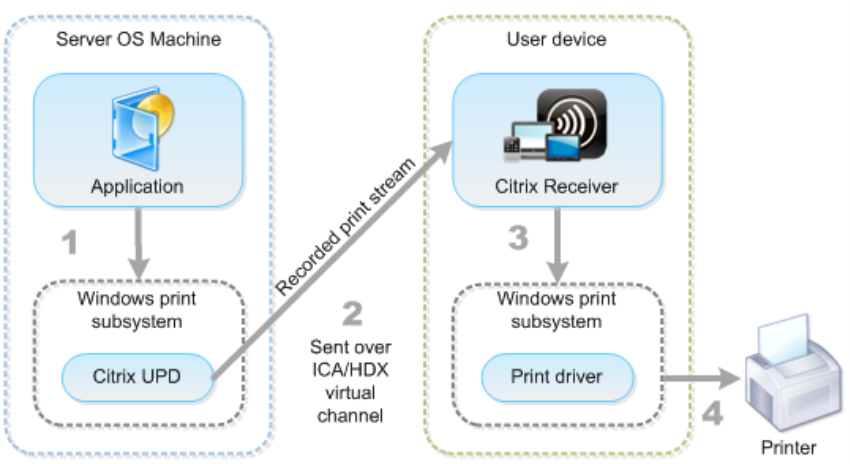
PCLおよびPSドライバーは、MacやUNIXクライアントなど、非Windowsベースのデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用する順序は、ユニバーサルドライバーの優先度ポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリンター機能をサポートします。これらの機能は、ネイティブドライバーがMicrosoftの印刷機能テクノロジを使用して利用可能としている場合にのみ、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

利用できます。ネイティブドライバーでは、印刷機能XMLで、標準化された印刷スキーマキーワードを使用する必要があります。標準化されていないキーワードを使用すると、Citrixのユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

次の図は、ユニバーサルプリンタードライバーコンポーネントとデバイスにローカル接続されたプリンターの一般的なワークフローを示しています。

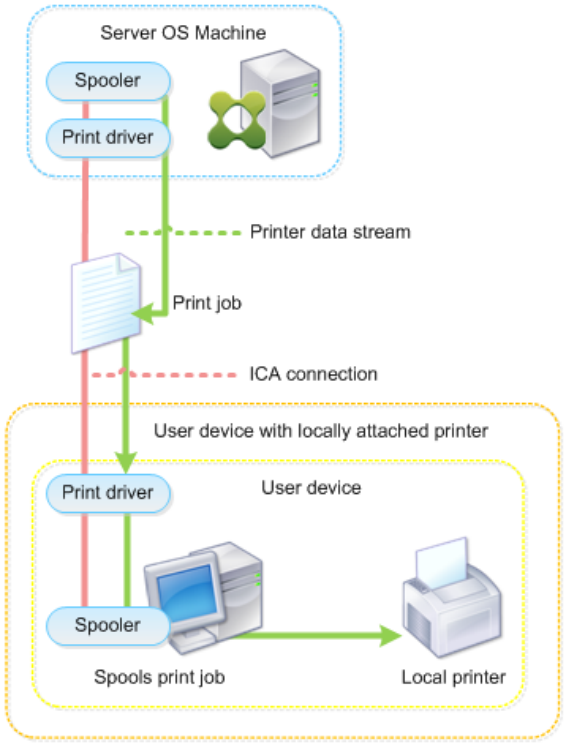


プリンタードライバーの管理方法を計画する場合、ユニバーサルプリンタードライバーを使用するか、デバイス固有のドライバーを使用するか、またはその両方を使用するかを決定する必要があります。標準ドライバーをサポートする場合は、以下の点を検討する必要があります。

プリンターの自動作成時に、ユーザーデバイスに接続された新しいローカルプリンターが検出されると、必要なプリンタードライバーについてサーバーOSマシンがチェックされます。デフォルトでは、Windowsネイティブドライバーが使用できない場合は、ユニバーサルプリンタードライバーが使用されます。

正しく印刷するには、サーバーOSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致する必要があります。次の図は、クライアント印刷経路でサーバーとクライアント上のプリンタードライバーがどのように使用されるかを示しています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- サポートするドライバーの種類。
- サーバーOSマシンにプリンタードライバーがない場合に自動的にインストールされるように設定するかどうか。
- プリンタードライバーの互換性リストを作成するかどうか。

関連トピック

- 印刷構成の例
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作
- 印刷に関するポリシーと設定
- プリンターのプロビジョニング
- 印刷環境の保守

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷構成の例

Mar 26, 2018

組織のコンピューティング環境やユーザーのニーズに適した印刷環境を設定すると、管理が容易になります。 通常、デフォルトの印刷構成でも正しく印刷できますが、ユーザーエクスペリエンスが低下したり、ネットワーク使用が最適化されなかったり、管理上のオーバーヘッドが生じたりする場合もあります。

印刷環境を設定するときは、以下の事項を考慮します。

- 業務上の ニーズと既存の印刷インフラストラクチャ。
  組織のニーズに基づいて、 印刷環境を設計します。既存の 印刷環境（ユーザーが自分でプリンターを追加できるかどうか、どのユーザーがどのプリンターに アクセスできるか、など）を確認し、それに沿って 印刷環境を構成できます。
- 組織のセキュリティポリシー。 人事部用のプリンターなど、特定のユーザー用に予約されたプリンターがあるかどうかを確認します。
- メインのワークステーションとは離れた場所で 印刷するユーザーがいるかどうか。たとえば、複数のワークステーション間を 移動しながら作業したり、出張先で印刷したりするユーザーがいるかどうかを確認します。

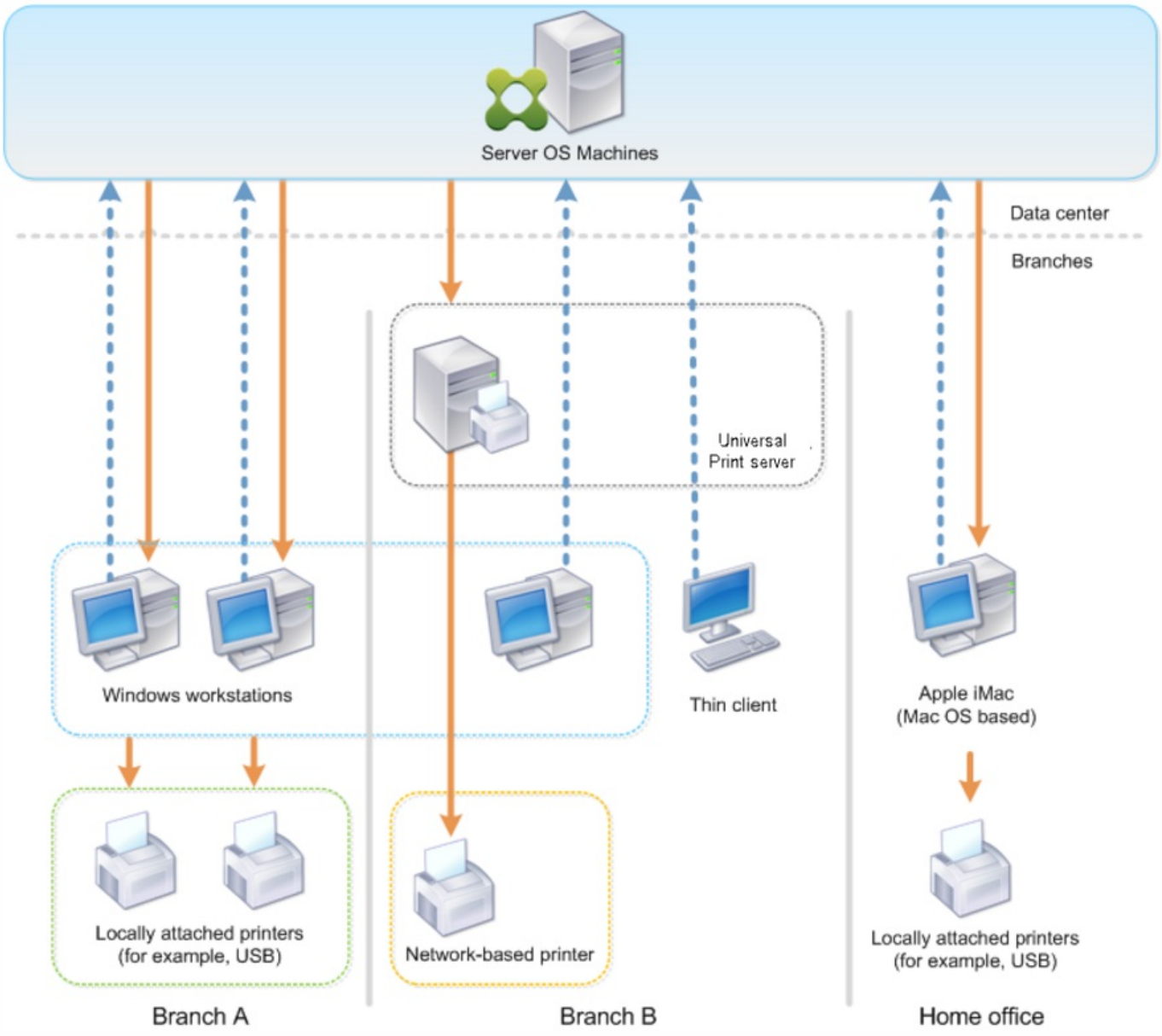
印刷環境を設計するにあたり、ユーザーがローカルのユーザーデバイス上で印刷する時と同様のユーザーエクスペリエンスを提供することを目標にします。

印刷展開の例

次の図は、以下の環境での印刷展開を示しています。

- **支社A -** 数台のWindowsワークステーションがある海外の小さな支社。すべてのユーザーワークステーションは共有されていないプリンターにローカルで接続されています。
- **支社B -** シンクライアントおよびWindowsベースのワークステーションがある大規模な支社。効率を上げるため、この支店のユーザーはネットワーク上のプリンターを（各階で1台）共有しています。支店内に置かれているWindowsベースのプリントサーバーが印刷キューを管理します。
- **社員の自宅 -** Mac OSベースのユーザーデバイスで自宅から会社のCitrixインフラストラクチャにアクセスしています。ユーザーデバイスはプリンターにローカルで接続されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



以降のセクションでは、各印刷環境をシンプルにして簡単に管理するための構成について説明します。

自動作成されるクライアントプリンターとCitrixユニバーサルプリンタードライバー

支社Aのすべてのユーザーは Windows ベースのワークステーションを使用しており、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。この構成には以下のメリットがあります。

- パフォーマンス - 印刷ジョブはICA印刷チャネル上で配信されます。このため、印刷データの圧縮により帯域幅を節約できます。
  サイズの大きなドキュメントを印刷しているユーザーがほかのユーザーのセッションパフォーマンスを低下させることがないように、最大印刷帯域幅を指定するCitrixポリシーを構成します。

  代替策として、マルチストリームICA接続を使用して、印刷トラフィックが優先度の低い専用のTCP接続で転送されるように構成することもできます。マルチストリームICAは、WAN接続にサービス品質（QoS）が実装されていない場合のオプションです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 柔軟性 - Citrixユニバーサルプリンタードライバーを使用して、新しいプリンタードライバーをデータセンターに追加する、となく、クライアントに接続されているすべてのプリンターを仮想デスクトップやアプリケーションのセッションでも使用できるように構成します。

Citrix Universal Print Server

支社Bのすべてのプリンターはネットワークに接続されており、その印刷キューはWindowsプリントサーバー上で管理されます。このため、Citrix Universal Print Serverが最も効果的な構成になります。

必要なすべてのプリンタードライバーは、ローカルの管理者によりプリントサーバー上にインストールされて管理されます。ネットワーク上のプリンターは、以下のように仮想デスクトップやアプリケーションセッションにマップされます。

- Windowsベースのワークステーションの場合 - ローカルのITチームの支援により、ユーザーのWindowsワークステーションを適切なネットワークプリンターに接続します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。
  仮想デスクトップやアプリケーションのセッションを開始すると、ローカルで構成されたプリンターがセッション内で自動作成されます。仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントが構成されているため、ネイティブのプリンタードライバーは不要です。ドライバーをアップデートしたりプリンターキューを変更したりしても、データセンターで何らかの構成を行う必要はありません。

- シンクライアントの場合 - シンクライアントデバイスのユーザーは、仮想デスクトップやアプリケーションのセッションでプリンターを接続する必要があります。ユーザーに最もシンプルな印刷構成を提供するには、管理者がCitrixポリシーの［セッションプリンター］設定を階ごとに構成して、各階のプリンターがデフォルトのプリンターとして接続されるようにします。
  ユーザーが階を移動しても正しいプリンターが接続されるようにするには、シンクライアントのサブセットまたは名前に基づいてポリシーが適用されるように構成します。この構成は「近接プリンター機能」と呼ばれ、ローカルプリンタードライバーのメンテナンスを委任管理モデルに基づいて実行できます。

  プリンターキューを変更または追加する必要がある場合は、Citrix管理者が環境内でそれぞれの[セッションプリンター]設定を変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネルの外側で送信されるため、サービス品質（QoS）が実装されます。ICA/HDXトラフィックにより使用されるポート上の送受信ネットワークトラフィックは、ほかのすべてのネットワークトラフィックよりも優先されます。この構成により、大きな印刷ジョブがユーザーセッションに影響を及ぼすことがなくなります。

自動作成されるクライアントプリンターとCitrixユニバーサルプリンター ドライバー

ユーザーが自宅で非標準的なワークステーションを使用し、管理されていない印刷 装置を使用する場合、 ユニバーサルプリンタードライバーを使用してクライアントプリンターを自動作成する構成が最適です。

展開の要約

要約すると、 展開例は以下のように構成されています。

- サーバーOSマシン上にはプリンター ドライバーがインストールされていません。Citrixユニバーサルプリンター ドライバのみを使用します。ネイティブの プリンタードライバーへのフォールバックおよびプリンタードライバーの自動インストールは無効です。
- すべてのクライアントプリンターを自動作成するためのポリシーがすべてのユーザーに 適用されます。サーバーOSマシンはデフォルトでプリントサーバーに 直接アクセスします。 必要な構成タスクは、Universal Print Serverコンポーネントの有

© 1999-2017 Citrix Systems, Inc. All rights reserved.

効化のみです。

- 支社Bの各階に個別の［セッション プリンター］設定が構成されており、その階のすべての シンクライアントに適用されます。
- 支社BにはQoSが 実装され、優れたユーザーエクスペリエンスが提供されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

Dec 05, 2017

ベストプラクティス

環境での最適な印刷ソリューションは、さまざまな要因により決定されます。以下のベストプラクティスの中には、特定のサイトに適用されない場合があります。

- Citrix Universal Print Serverを使用します。
- ユニバーサルプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- サーバーOSマシン上にインストールされるプリンタードライバー数を最小化します。
- ネイティブドライバーへのドライバーマッピングを使用します。
- 動作検証されていないプリンタードライバーを実稼働環境サイトにインストールしないようにします。
- ドライバーのアップデートインストールを避け、常にドライバーをアンインストールしてからプリントサーバーを再起動して、その後で新しいドライバーをインストールしてください。
- 未使用のドライバーをアンインストールするか、[プリンター ドライバーのマッピングと互換性] ポリシーを行使して、プリンターがそのドライバーで作成されないようにします。
- Version 2のカーネルモードドライバーを使用しないようにします。
- 特定のプリンターがサポートされるかどうかについては、製造元に問い合わせるか、Citrix Ready製品に関する情報（www.citrix.com/ready）を参照してください。
  一般的に、Microsoft社より提供されるプリンタードライバーはすべてTerminal Servicesでテストされ、Citrix環境での動作が確認されています。ただし、サードパーティ製のプリンタードライバーを使う前に、ターミナルサービスでの動作がWindows Hardware Quality Labs（WHQL）プログラムで認定されているかどうかをプリンタードライバーのベンダーに確認してください。Citrixではプリンタードライバーの動作を保証しません。

セキュリティに関する注意事項

Citrixの印刷ソリューションは、これ自体がセキュアに設計されています。

- Citrix Print Manager Serviceは、ログオンやログオフ、切断、再接続、およびセッション終了などのセッションイベントを常に監視してそれらに応答します。実際のセッションユーザーを偽装して、サービス要求を処理します。
- Citrixの印刷ソリューションでは、セッション内の一意な名前空間に各プリンターが割り当てられます。
- Citrixの印刷ソリューションでは、自動作成プリンターにデフォルトのセキュリティ記述子が設定されます。これにより、あるセッションで自動作成されたクライアントプリンターにほかのセッションのユーザーがアクセスできないようになります。デフォルトでは、クライアントプリンターのアクセス権を変更するための管理者権限を持つユーザーでも、ほかのセッションのクライアントプリンターに誤って出力してしまうということはありません。

デフォルトの印刷動作

印刷に関するポリシーを設定しない場合、デフォルトで次のように処理されます。

- Universal Print Serverが無効になります。
- ユーザーデバイス上で設定されているすべてのプリンターが、各セッションの開始時にサーバー上に自動作成されます。この動作は、Citrixポリシーの [クライアント プリンターを自動作成する] 設定で [すべてのクライアント プリンターを自動作成する] を構成した場合と同等です。
- クライアントデバイスにローカル接続されたプリンターへのすべての印刷ジョブは、ICAチャネルを介してユーザーデバイスに送信され、プリンターに転送されます（クライアント印刷経路）。
- ネットワークプリンターへのすべての印刷ジョブは、サーバーOSマシンからプリントサーバーに直送されます。印刷ジョ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ブをネットワーク上に送信できない場合は、ユーザーコンピューターを介して転送されます（リダイレクトされるクライアント印刷ジョブ）。
この動作は、Citrixポリシーの［プリント サーバーへの直接接続］設定で［無効］を選択した場合と同等です。

- デフォルトでは、印刷プロパティ（ユーザーの印刷設定とデバイス設定）はユーザーデバイス上に格納されます。クライアント側でこの処理がサポートされない場合、サーバーOSマシン上のユーザープロファイルに印刷プロパティが格納されます。
  この動作は、Citrixポリシーの［プリンター プロパティの保存］設定で［クライアントに保存できない場合にのみユーザープロファイルに保存する］を選択した場合と同等です。

- セッション内でプリンターが自動作成されるときに、そのサーバーOSマシン上にインストールされているWindowsバージョンのプリンタードライバーが使用されます。適切なドライバーがインストールされていない場合、Windowsオペレーティングシステムからドライバーがインストールされます。Windowsオペレーティングシステムから適切なドライバーをインストールできない場合、Citrixユニバーサルプリンタードライバーが使用されます。
  この動作は、Citrixポリシーの［付属のプリンター ドライバーの自動インストール］設定で［有効］を選択し、［ユニバーサル印刷］設定で［要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する］を選択した場合と同等です。

  ただし、［付属のプリンター ドライバーの自動インストール］を有効にすると、必要以上に多くのプリンタードライバーがインストールされる可能性があります。

注： 印刷に関するデフォルト設定を確認するには、新しいCitrixポリシーを作成し、印刷に関するすべての設定項目で［デフォルト値を使用する］チェックボックスをオンにします。これにより、デフォルトの設定が適用されます。

Always-Onログ

VDAにはプリントサーバーおよび印刷サブシステムのためのAlways-Onログ機能があります。

ログをZIPとしてまとめてメールで送信、または自動的にCitrix Insight Servicesにアップロードするには、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷に関するポリシーと設定

Dec 05, 2017

Citrixポリシーでは、ユーザーが公開アプリケーションからプリンターにアクセスするときの以下の動作を制御できます。

- どのようにプリンターを提供するか（どのようにセッションに追加するか）
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーをどのように管理するか

Citrixポリシーでは、ユーザーが使用するユーザーデバイスやユーザーアカウントなどの条件に応じて、異なる印刷環境を構成できます。

印刷機能の多くは、Citrixの「印刷のポリシー設定」で設定できます。 印刷の設定は、Citrixポリシーの標準的な動作に基づいて適用されます。

プリンター設定は、セッション終了時にプリンターオブジェクトまたは（ユーザーのネットワークアカウントに適切な権限がある場合は）クライアントの印刷装置に格納されます。Citrix Receiverのデフォルトでは、プリンターオブジェクトに格納された設定がまずチェックされ、見つからない場合はほかの場所に格納されている設定が使用されます。

デフォルトでは、ユーザーデバイス（デバイスがこれをサポートする場合）またはサーバーOSマシン上のユーザープロファイルにプリンターのプロパティが格納（または保持）されます。 セッションでの作業中にユーザーがプリンターのプロパティを変更すると、その内容はそのマシン上のユーザープロファイルに反映されます。 ユーザーがそのマシンに再ログオンしたり再接続したりすると、ユーザープロファイルに保持されたプロパティがユーザーデバイスに継承されます。 つまり、ユーザーデバイス上のプリンタープロパティの変更は、ユーザーの次回ログオン時まで反映されません。

印刷設定の場所

Windowsの印刷環境では、印刷設定に対する変更をローカルコンピューターに格納したり、ドキュメントファイルに格納したりできます。この環境では、ユーザーが変更した印刷設定を以下の場所に格納できます。

- **ユーザーデバイス上-**Windowsユーザーは、ユーザーデバイス側の印刷設定を自分で変更できます。これを行うには、コントロールパネルでプリンターを右クリックして、［印刷設定］を選択します。たとえば、印刷の方向として［横］を選択すると、そのプリンターのデフォルトの方向として横向きが設定されます。
- **ドキュメント内 -** ワードプロセッサやデスクトップパブリッシングのプログラムでは、印刷の向きなどのドキュメント設定はそのドキュメントファイル内に格納されます。たとえば、Microsoft Wordドキュメントを印刷キューに送ると、ユーザーが指定した印刷の向きやプリンター名などの印刷設定がそのドキュメントファイル内に格納されます。これらのオプションは、次回そのドキュメントを印刷するときのデフォルト設定として表示されます。
- **セッションでのユーザーによる変更 -** 自動作成されたプリンターでは、ユーザーがセッション内のコントロールパネルで変更したオプション、つまりサーバーOSマシン上で変更されたオプションだけが保持されます。
- **サーバーOSマシン上 -** サーバーOSマシン上の特定のプリンタードライバーに対するデフォルト設定は、そのマシン上に格納されます。

Windowsベースの環境で保持される設定は、ユーザーがどのようにその設定を変更したかにより異なります。つまり、スプレッドシートプログラムなどに表示される印刷設定が、ドキュメントなどほかの場所に格納されている設定と異なることがあります。この結果、特定のプリンターに適用される設定は、セッション内で変化することがあります。

ユーザーの印刷設定の階層構造

印刷に関するユーザー設定はさまざまな場所に格納されるため、特定の優先順位でそれらの設定が処理されます。 また、デバイス設定はドキュメント設定とは区別され、より優先されることに注意してください。

デフォルトでは、ユーザーがセッション内で変更したすべての印刷設定、つまり保持された設定が適用され、その後でそのに

© 1999-2017 Citrix Systems, Inc. All rights reserved.

かの設定がチェックされます。 ユーザーが印刷を行うと、サーバーOSマシン上に格納されたデフォルトの設定と、保持された設定やクライアントプリンター設定が統合されます。

ユーザーの印刷設定の保存

プリンタープロパティの格納場所を変更することは推奨されません。デフォルトの格納場所（つまりユーザーデバイス上）を使用すると、ユーザーの印刷に一貫したプロパティが適用されるようになります。ユーザーデバイス上にプロパティを保存できない場合は、自動的にサーバーOSマシン上のユーザープロファイルが格納場所として使用されます。

以下の環境では、［プリンタープロパティの保存］設定の内容を確認してください。

- ユーザーデバイス上へのプリンタープロパティの格納をサポートしない従来のプラグインソフトウェアが使用されている。
- 固定プロファイルを使用するWindowsネットワーク環境で、ユーザーのプリンタープロパティが保持されるように設定する。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

プリンターのプロビジョニング

Dec 05, 2017

プリンターのプロビジョニングには以下の3つの方法があります。

- Citrix Universal Print Server
- クライアントプリンターの自動作成
- 管理者によるセッションプリンターの割り当て

Citrix Universal Print Server

環境に最適の印刷ソリューションを決定するときは、以下の点について検討します。

- Universal Print Serverにより提供されるイメージとフォントのキャッシュ、高度圧縮、最適化、QoSサポートなどの機能は、Windowsの印刷プロバイダーでは提供されません。
- ユニバーサルプリンタードライバーでは、Microsoftによって定義されているパブリックな非デバイス依存の設定がサポートされます。ユーザーがプリンターの製造元固有のデバイス設定を使用する必要がある場合は、Universal Print ServerとWindowsネイティブドライバーの両方を提供します。この構成では、Universal Print Serverの長所を維持したままでユーザーに特殊なプリンター機能へのアクセスが提供されます。ここで考慮すべきことは、Windowsネイティブドライバーではメンテナンスが必要になるということです。
- Citrix Universal Print Serverは、ネットワークプリンターでのユニバーサル印刷をサポートします。Universal Print Serverではユニバーサルプリンタードライバーが使用されます。このドライバーはサーバーOSマシン上の単一のドライバーで、シンクライアントやタブレットを含むあらゆるデバイスからのローカル印刷またはネットワーク印刷が可能になります。

Universal Print ServerをWindowsネイティブドライバーと一緒に使うには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが使用可能な場合はそれが使用されます。使用できない場合は、ユニバーサルプリンタードライバーが使用されます。Windowsネイティブドライバーのみ、またはユニバーサルプリンタードライバーのみを使用するなど、ユニバーサル印刷機能の動作を変更するには、ポリシーの［ユニバーサル印刷の使用］設定を使用します。

Universal Print Serverのインストール

Universal Print Serverを使用するには、製品のインストールに関するドキュメントの説明に従って、プリントサーバー上にUpsServerコンポーネントをインストールして構成します。詳細は、「コアコンポーネントのインストール」および「コマンドラインを使ったインストール」を参照してください。

XenApp 6.5など、UPClientコンポーネントを別個に展開する環境の場合：

1. WindowsデスクトップOSまたはWindowsサーバーOS用のXenAppおよびXenDesktop Virtual Delivery Agent（VDA）スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使ったインストール」の説明に従って、コマンドラインを使ってVDAを展開します。
3. \Image-Full\Support\VcRedist_2013_RTMから前提条件をインストールします
   - Vcredist_x64 / vcredist_x86
     - 32ビット展開に対してはx86のみ、 64ビット展開に足しては両方を実行
4. \Image-Full\x64\Virtual Desktop Componentsまたは\Image-Full\x86\Virtual Desktop Componentsからcdf前提条件をインストールします。
   - Cdf_x64 / Cdf_x86
     - 32ビット展開に対してはx86、 64ビット展開に対してはx64
5. \Image-Full\x64\Virtual Desktop Componentsまたは\Image-Full\x86\Virtual Desktop ComponentsでUPClientコンポーネントを見つけます。
6. 展開してUPClientコンポーネントをインストールし、コンポーネントのMSIを実行します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. UPClientコンポーネントのインストール後には再起動する必要があります。

Universal Print ServerのCEIPからの登録解除

Universal Print Serverをインストールすると、自動的にCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に登録されます。インストール日時から7日後に最初のデータアップロードが行われます。

CEIPの登録を解除するには、レジストリキー**HKLM\Software\Citrix\Universal Print Server\CEIPEnabled**を編集して、**DWORD** 値を**0**に設定します。

もう一度参加するには、このDWORD値を1に設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

詳しくは、「Citrix Insight Services」を参照してください。

Universal Print Serverの構成

以下のCitrixポリシー設定を使用してUniversal Print Serverを構成します。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。

- **Universal Print Serverの有効化**： Universal Print Serverはデフォルトでは無効になっています。Universal Print Serverを有効にする場合、Universal Print Serverを使用できないときにWindows印刷プロバイダーにフォールバックするかどうかを選択できます。Universal Print Serverを有効にすると、Windows印刷プロバイダーとCitrixプロバイダーのインターフェイスを介してネットワークプリンターを追加して列挙できます。
- **Universal Print Server印刷データストリーム（CGP）ポート**。 Universal Print Server印刷データストリームCGP（Common Gateway Protocol）リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **Universal Print Server Webサービス（HTTP/SOAP）ポート**。 Universal Print Serverのリスナーで使用される、HTTP/SOAP要求の受信TCPポート番号を指定します。デフォルトは**8080**です。

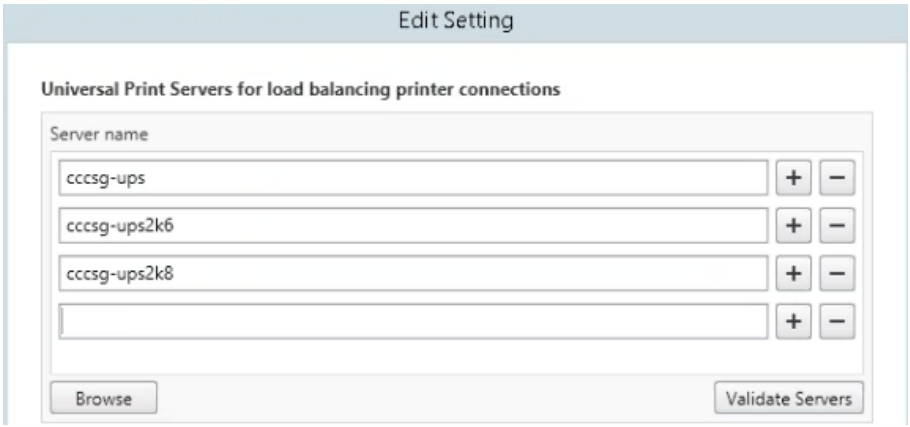
XenAppおよびXenDesktop VDAへのUniversal Print Server通信用のHTTP 8080のデフォルトポートを変更するには、次のレジストリを作成し、Universal Print Serverコンピューターでポート番号値を変更する必要があります：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
"UpsHttpPort"=DWORD:

このポート番号は、StudioでHDXポリシー、Universal Print Server Webサービス（HTTP/SOAP）ポートと一致する必要があります。

- **Universal Print Server入力データストリームの最大帯域幅（Kbps）**。 各印刷ジョブからUniversal Print ServerにCGPで配信される印刷データの転送速度の上限をキロビット/秒単位で指定します。デフォルトは0（無制限）です。
- **負荷分散のためのユニバーサルプリントサーバー**。この設定には、Citrixのほかの印刷ポリシー設定を評価した後、セッション起動時に確立されるプリンター接続の負荷分散に使用するUniversal Print Serverの一覧が表示されます。プリンターの作成時間を最適化するには、すべてのプリントサーバーに同じ共有プリンターを設定することをお勧めします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **ユニバーサルプリントサーバーのサービス停止のしきい値** ロードバランサーが、反応しないプリントサーバーの復旧を待機する時間を指定します。タイムアウト後、ロードバランサーはそのサーバーが永続的にオフラインであると判定し、その負荷をほかの利用可能なプリントサーバーに再分散します。デフォルト値は180秒です。

Delivery Controllerで印刷ポリシーを変更した後、そのポリシーの変更がVDAに適用されるまでに数分かかることがあります

ほかのポリシー設定との相互作用- Universal Print Serverは、ほかのCitrix印刷ポリシー設定とも相互作用します。次の表では、Universal Print Serverコンポーネントをインストールしてポリシーで有効にした場合に、ほかのポリシー設定がどのような影響を受けるかについて説明します。

ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターを自動作成する	Universal Print Serverが有効な場合、ネイティブドライバーの代わりにユニバーサルプリンタードライバーを使ってクライアントネットワークプリンターが作成されます。ユーザー側には、同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリンタードライバー関連のポリシー設定によりセッションプリンターが構成されます。
プリントサーバーへの直接接続	Universal Print Serverが有効で、［ユニバーサル印刷の使用］ポリシー設定で［ユニバーサル印刷のみを使用する］が構成されている場合、ユニバーサルプリンタードライバーでプリントサーバーに直接ネットワークプリンターの接続を作成できます。
ユニバーサルドライバーの優先度	EMFおよびXPSドライバーがサポートされます。

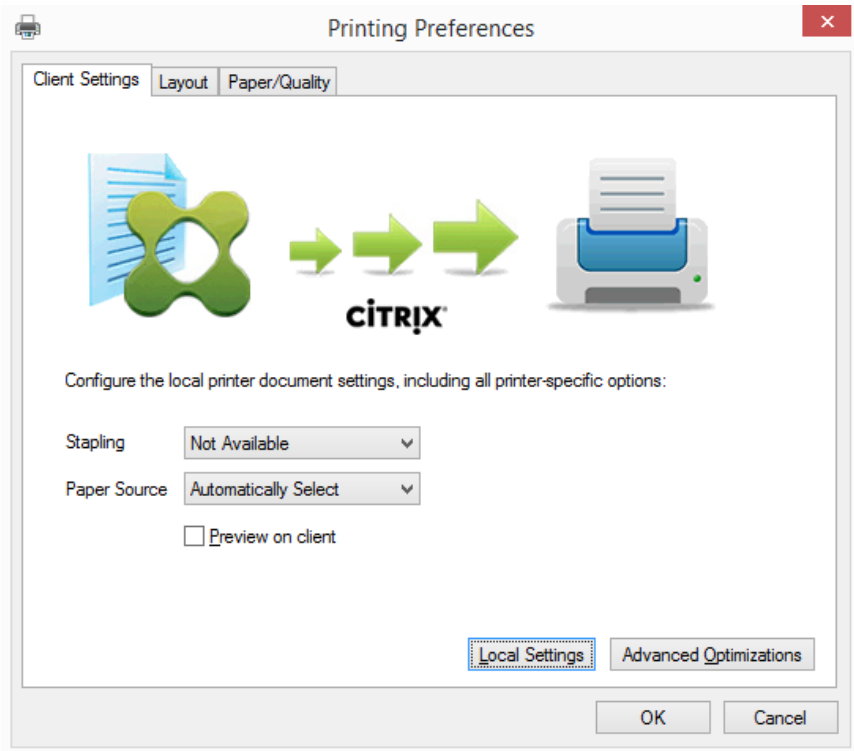
ユーザーインターフェイスに対する影響- Universal Print Serverにより使用されるCitrixユニバーサルプリンタードライバーにより、以下のユーザーインターフェイスコントロールが無効になります。

- ［プリンターのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタン
- ［ドキュメントのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタンおよび［クライアントでのプレビュー］ボタン

Citrixユニバーサルプリンタードライバー（EMFおよびXPSドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンター機能をサポートします。ホチキス留めや給紙方法などのオプションは、セッションのUPDにマップされるクライアントまたはネットワークプリンターがこれらの機能をサポートしている場合に、カスタムUPDの印刷ダイアログボックスから選択できます。



カスタムのUPD印刷ダイアログ

ホチキス留めや安全なPINなどの非標準のプリンター設定を設定するには、Citrix UPD EMFまたはXPSドライバーを使用するあらゆるクライアントマッピングされたプリンターに対して、カスタムのUPD印刷ダイアログで**[ローカル設定]**を選択します。マップされたプリンターの**[プリンターの設定]**ダイアログがクライアント上のセッションの外部に表示されるので、ユーザーはあらゆるプリンターオプションを変更でき、アクティブなセッションでそのドキュメントを印刷する場合、変更されたプリンター設定が使用されます。

これらの機能は、ネイティブドライバーがMicrosoftの印刷機能テクノロジを使用して利用可能としている場合にのみ、利用できます。ネイティブドライバーでは、印刷機能XMLで、標準化された印刷スキーマキーワードを使用する必要があります。標準化されていないキーワードを使用すると、Citrixのユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

Universal Print Serverを使用するときのCitrix印刷プロバイダーのプリンターの追加ウィザードは、Windows印刷プロバイダーのプリンターのものとほぼ同じです。ただし、以下の違いがあります。

- 名前またはアドレスを指定してプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。このポート番号は、プリンター名の一部として表示されます。
- Citrixユニバーサルプリンタードライバーに関するポリシーでユニバーサル印刷が常に使用されるように設定すると、プリンターを選択するときにユニバーサルプリンタードライバー名が表示されます。Windows印刷プロバイダーはユニバーサルプリンタードライバーを使用できません。

Citrix印刷プロバイダーはクライアント側でのレンダリングをサポートしません。

Universal Print Serverについて詳しくは、CTX200328を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントプリンターの自動作成

ユニバーサル印刷ソリューションにより、クライアントプリンターに以下の機能が提供されます。

- **Citrixユニバーサルプリンター -**セッションの開始時に作成される汎用プリンターで、特定の印刷装置に関連付けられるものではありません。Citrixユニバーサルプリンターを使用することでログオン時のクライアントプリンターの列挙が不要になるため、リソース負荷が軽減され、ユーザーが高速にログオンできるようになります。ユニバーサルプリンターでは、クライアント側のあらゆる印刷装置を使用できます。
  Citrixユニバーサルプリンターは、ユーザーが使用するユーザーデバイスやCitrix Receiverによっては正しく動作しない場合があります。CitrixユニバーサルプリンターはWindows環境で動作し、Citrix Offline Plug-inや、クライアント上にストリーム配信されるアプリケーションをサポートしません。このような環境では、クライアントプリンターの自動作成機能とユニバーサルプリンタードライバーの使用を検討してください。

  非Windows Citrix Receiverのユーザーにユニバーサル印刷ソリューションを提供するには、自動的にインストールされるPostScript/PCLベースのユニバーサルプリンタードライバーを使用してください。

- **Citrixユニバーサルプリンタードライバー -**デバイスに依存しないプリンタードライバー。Citrixユニバーサルプリンタードライバーを構成すると、デフォルトでEMFベースのユニバーサルプリンタードライバーが使用されます。
  Citrixユニバーサルプリンタードライバーによる印刷ジョブのサイズは、古いバージョンなどのプリンタードライバーのものよりも小さい場合があります。ただし、特殊なプリンターでの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成— 以下のCitrixポリシー設定を使用してユニバーサル印刷を構成します。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。

- ユニバーサル印刷の使用：ユニバーサル印刷を使用する条件を指定します。
- 汎用ユニバーサルプリンターを自動作成する：ユニバーサル印刷と互換性があるユーザーデバイスが使用されたセッションで、汎用的なCitrixユニバーサルプリンターオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。
- ユニバーサルドライバーの優先度：ユニバーサルプリンタードライバーの使用優先順位を指定します。一覧の上位にあるドライバーから順に使用されます。この一覧では、ドライバーを追加、編集、または削除したり、優先順位を変更したりできます。
- ユニバーサル印刷プレビューの設定：自動作成プリンターおよび汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード：Windowsユーザーデバイス上でのEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFスプールファイルがクライアント上のスプールキューに直接挿入されます。これにより、EMF形式の印刷を高速に実行でき、CPUリソースの消費も少なくなります。

ポリシーについて詳しくは、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色設定、両面印刷、部数などのデフォルト設定を変更する方法については、CTX113148を参照してください。

ユーザーデバイスからのプリンターの自動作成— デフォルトでは、セッションの開始時にユーザーデバイス上で設定されているすべてのプリンターが自動作成されます。管理者は、セッション内でユーザーに提供するプリンターの種類を制御して、自動作成を無効にできます。

自動作成機能を制御するには、Citrixポリシーの [クライアントプリンターを自動作成する] 設定を使用します。以下のオプションを選択できます。

- ローカル接続されているプリンターやネットワークプリンターを含め、ユーザーデバイス上で設定されているすべてのプリンターがセッション開始時に自動作成されるようにする（デフォルト）。
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動作成されるようにする。
- ユーザーデバイス上で設定されているデフォルトプリンターだけが自動作成されるようにする。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- すべてのクライアントプリンターに対する自動作成を無効にする。

［クライアントプリンターを自動作成する］設定を使用する場合は、［クライアントプリンターリダイレクト］設定を［許可］（デフォルト）にする必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、クライアントデバイス上で設定されているすべてのネットワークプリンターが、セッション開始時に自動作成されます。管理者は、列挙およびマップされるプリンターの数を最小限にするために、各セッションで特定のネットワークプリンターだけが作成されるように構成することができます。このようなプリンターをセッションプリンターと呼びます。

IPアドレスによりセッションプリンターポリシーをフィルターして、近接プリンター機能を提供できます。この機能を使用すると、ユーザーのIPアドレスの範囲に応じて、特定のネットワークプリンターが自動的に割り当てられるようになります。近接プリンター機能はCitrix Universal Print Serverにより提供され、このセクションで説明する構成は必要ありません。

近接プリンター機能は、以下の環境で使用できます。
- 企業の社内ネットワークでユーザーのIPアドレスがDHCPサーバーにより自動的に割り当てられる。
- 組織内のすべての部署で、それぞれ異なるIPアドレス範囲が割り当てられる。
- 各部署のIPアドレス範囲内にネットワークプリンターが存在する。

近接プリンター機能を構成すると、従業員がある部署から別の部署に移動する場合でも追加の印刷装置の構成は必要ありません。移動先の部署のIPアドレス範囲でユーザーデバイスが認識されると、その範囲内のすべてのネットワークプリンターへのアクセスが可能になります。

セッションで特定のプリンターがリダイレクトされるように構成する— 管理者割り当てのプリンターを作成するには、Citrixポリシーの［セッションプリンター］設定を構成します。この設定では、以下のいずれかの方法でネットワークプリンターを追加します。
- プリンターのUNCパスを\\<servername>\<printername>形式で入力します。
- ネットワーク上でプリンターの場所を参照します。
- 特定サーバー上のプリンターを参照します。サーバー名を\\<servername>形式で入力して［参照］をクリックします。

重要： 特定のセッションに複数のポリシーが適用される場合、それらのポリシー（優先度の高いものから低いものまですべて）の［セッションプリンター］設定で指定されているすべてのネットワークプリンターが自動作成されます。複数のポリシーにより同じプリンターの自動作成が適用される場合、最も優先度の高いポリシーの設定だけがそのプリンターのカスタムデフォルト設定として使用されます。
［セッションプリンター］設定を使用すると、サブネットなどの条件により異なるポリシーが適用されるように構成して、ユーザーがセッションを開始した場所によって異なるネットワークプリンターが自動作成されるように制御できます。

セッションのデフォルトネットワークプリンターを指定する— デフォルトでは、ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。セッションのデフォルトのクライアントプリンターとして設定するプリンターを指定するには、Citrixポリシーの［デフォルトプリンター］設定を構成します。
1. ［デフォルトプリンター］設定で、［デフォルトのクライアントプリンター］ボックスの一覧から、以下のいずれかのオプションを選択します。
   - Network printer nameではありません。［セッションプリンター］ポリシー設定で追加されたプリンターがこのメニューに表示されます。デフォルトプリンターとして指定するネットワークプリンターを選択します。
   - デフォルトプリンターの設定を変更しない。ターミナルサービスまたはWindowsのユーザープロファイルで設定されているデフォルトプリンターが使用されます。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。
2. このポリシーの適用先として、ユーザーグループ（またはそのほかのフィルターオブジェクト）を指定します。

近接プリンター機能を構成する— Citrix Universal Print Serverでは、近接プリンター機能も提供されます。この場合、ここで設

© 1999-2017 Citrix Systems, Inc. All rights reserved.

明されている構成は必要ありません。

1. 各サブネット（またはプリンターが設定されている場所）に応じて、異なるポリシーを作成します。
2. 各ポリシーの［セッションプリンター］設定で、そのサブネットの場所に設置されているプリンターを追加します。
3. ［デフォルトプリンター］設定で、［デフォルトプリンターの設定を変更しない］を選択します。
4. 各ポリシーの適用先として、クライアントのIPアドレスを指定します。DHCP IPアドレス範囲が変更された場合は、これらのポリシーも更新する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷環境の保守

Dec 05, 2017

印刷環境では、以下の保守作業を行います。

- プリンタードライバーを管理する。
- 印刷パフォーマンスを最適化する。
- プリンターを表示して印刷キューを管理する。

プリンタードライバーの管理

管理上のオーバーヘッドや潜在的な問題を最小化するため、Citrixユニバーサルプリンタードライバーの使用をお勧めします。

自動作成に失敗すると、デフォルトで、Windowsで提供されているWindowsネイティブのプリンタードライバーがインストールされます。ドライバーが使用できない場合は、ユニバーサルプリンタードライバーが使用されます。プリンタードライバーのデフォルトについて詳しくは、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

Citrixユニバーサルプリンタードライバーが適さない環境では、サーバーOSマシン上にインストールするドライバーの数を少なくするためにプリンタードライバーをマップします。プリンタードライバーをマップすることで、以下のことが可能になります。

- 特定のプリンターでCitrixユニバーサルプリンタードライバーだけが使用されるようにする
- 特定のドライバーによるプリンターの作成を許可または禁止する
- 問題が生じるプリンタードライバーの代わりに正しく動作するプリンタードライバーを割り当てる
- クライアント側のプリンタードライバーの代わりにWindowsサーバー上で使用可能なドライバーを割り当てる

プリンタードライバーの自動インストールを無効にする— サーバーOSマシン間で一貫したプリンター構成を保つため、プリンタードライバーの自動インストールを無効にします。これはCitrixのポリシー、Microsoftのポリシー、またはその両方で設定できます。Windowsネイティブドライバーが自動的にインストールされないようにするには、Citrixポリシーの［付属のプリンタードライバーの自動インストール］設定を無効にします。

クライアントプリンタードライバーのマップ— ユーザーがセッションにログオンするときに、プリンタードライバー名など、クライアント側のプリンターの情報が提供されます。クライアントプリンターの自動作成時に、クライアントから提供されたプリンターのモデル名に基づいて、Windowsサーバーのプリンタードライバーの名前が選択されます。次に、選択されたプリンタードライバーが自動作成プロセスで使用され、リダイレクトされるクライアント印刷キューが作成されます。

次の手順で、ドライバー置換規則を定義して、マップされたクライアントプリンタードライバーの印刷設定を編集します。

1. 自動作成クライアントプリンターのドライバー置換規則を指定するには、Citrixポリシーの[プリンタードライバーのマッピングと互換性］設定を構成して、クライアント側のプリンタードライバーの名前を追加し、それに割り当てるサーバー側プリンタードライバーを指定します（［サーバー側プリンタードライバー］を選択して［ドライバーの検索］をクリック）。ここでは、ワイルドカード文字を使用できます。たとえば、すべてのHP社製プリンターで特定のドライバーを使用する場合は、「HP*」と入力します。
2. プリンタードライバーの使用を禁止するには、ドライバー名を選択して[作成しない］を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、一覧のドライバーエントリの順位を変更したりできます。
4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、[設定］をクリックして印刷品質、印刷の向き、印刷カラーなどの設定を指定します。プリンタードライバーでサポートされないオプションを選択した場合、そのオプションは無視されます。ここで選択するオプションは、ユーザーが前回のセッションで指定し、保持されていた設定よりも優先されます。
5. 一部のプリンター機能は特定のドライバーでのみ使用可能であるため、ドライバーをマップした後でプリンターの動作を

© 1999-2017 Citrix Systems, Inc. All rights reserved.

細にテストすることをお勧めします。

ユーザーがログオンすると、クライアントプリンタードライバーの互換性一覧がチェックされ、その後でクライアントプリンターがセットアップされます。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print Serverとユニバーサルプリンタードライバーを使用します。以下のポリシー設定を構成して、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷最適化デフォルト：セッションで作成されるユニバーサルプリンターに適用されるデフォルト設定を指定します。
  - ［必要なイメージ品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを印刷できます。
  - ［ヘビーウェイト圧縮を有効にする］では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
  - ［イメージおよびフォントのキャッシュ］では、印刷ストリームで使用されているイメージやフォントをキャッシュするかどうかを指定します。キャッシュを有効にすると、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。デフォルトでは、埋め込みイメージおよびフォントがキャッシュされます。
  - ［非管理者によるこれらの設定の変更を許可する］では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。デフォルトでは、禁止されています。
- ユニバーサル印刷イメージ圧縮制限：ユニバーサルプリンタードライバーでのイメージ印刷で使用できる品質レベルの上限を指定します。デフォルトでは、イメージ品質の上限が［最高品質（無損失圧縮）］に設定されています。
- ユニバーサル印刷品質制限：セッションでの印刷出力で使用できる最大DPI値（インチあたりのドット数）を指定します。デフォルトでは、DPI値に上限はありません。

デフォルトでは、サーバーOSマシンからのすべての印刷ジョブがネットワークを介してプリントサーバーに直接転送されます。ネットワークで遅延が発生したり帯域幅に制限があったりする場合は、ICA仮想チャネルでの印刷ジョブの送信を検討します。これを行うには、Citrixポリシー設定の［プリントサーバーへの直接接続］設定で［無効］を選択します。ICA仮想チャネルで送信されるデータは圧縮されるため、データがWANを横断するときに消費される帯域幅が少なくなります。

印刷帯域幅を制限してセッションのパフォーマンスを改善する— サーバーOSマシンからユーザープリンターで印刷すると、帯域幅消費によりビデオなどほかの仮想チャネルのパフォーマンスが低下することがあります。この問題は、ユーザーが低速のネットワークを介してサーバーにアクセスする場合に顕著です。このような低下を防ぐために、ユーザープリンターでの印刷に使用される帯域幅を制限できます。転送される印刷データの量を制限すると、ビデオ、キーストローク、およびマウスデータ転送のためHDXデータストリームで使用できる帯域幅が大きくなります。

重要： プリンター帯域幅の制限設定は、ほかのチャネルが使用されていない場合でも常に適用されます。
Citrixポリシーで［帯域幅］カテゴリの以下の設定項目を使用して、セッションでの印刷帯域幅制限を構成します。サイトでの制限を設定するには、Studioを使ってポリシーを構成します。個々のサーバーでの制限を設定するには、各サーバーOSマシン上でローカルのWindowsグループポリシー管理コンソールを使ってポリシーを構成します。

- ［プリンターリダイレクトの最大帯域幅（Kbps）］設定で、印刷に使用される最大帯域幅をキロビット/秒（Kbps）で指定します。
- ［プリンターリダイレクトの最大帯域幅（%）］設定で、印刷に使用される最大帯域幅を、セッション全体に対する割合で指定します。
  注： ［プリンターリダイレクトの最大帯域幅（%）］設定を使って帯域幅をパーセンテージで指定する場合は、［セッション全体の最大帯域幅］設定でセッション全体で使用可能な総帯域幅の最大値をキロビット/秒（Kbps）で指定します。最大帯域幅をKbpsおよびセッション全体に対する割合（%）で指定した場合、より高い制限（より低い値）の設定が適用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷帯域幅に関する情報をリアルタイムに取得するには、Citrix Directorを使用します。

Universal Print Serverの負荷分散

Universal Print Serverソリューションは、負荷分散ソリューションにプリントサーバーを追加することによって拡張できます。VDAにはそれぞれ、印刷の負荷をすべてのプリントサーバーに分散する独自のロードバランサーがあるため、単一の障害点はありません。

負荷分散ソリューションでプリントサーバー全体の印刷負荷を分散するには、ポリシー設定「負荷分散のためのユニバーサルプリントサーバー」および「ユニバーサルプリントサーバーのサービス停止のしきい値」を使用します。

プリントサーバーで予期しない障害が発生した場合、各VDAのロードバランサーのフェールオーバーメカニズムにより、既存の受信セッションがすべてユーザーエクスペリエンスに影響せず管理者の介入も必要とせずに通常どおり機能するように、障害が発生したプリントサーバーに割り当てられているプリンター接続が他の使用可能なプリントサーバーに自動的に再分散されます。

管理者は、一連のパフォーマンスカウンターを使用してVDAの以下の項目を追跡し、負荷分散されたプリントサーバーのアクティビティを監視できます。

- VDA上の負荷分散されたプリントサーバーおよびそのステータス（使用可能、使用不可）の一覧
- 各プリントサーバーで許可されたプリンター接続の数
- 各プリントサーバー上で失敗したプリンター接続の数
- 各プリントサーバー上で有効なプリンター接続の数
- 各プリントサーバー上で保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、プリンターを表示したり印刷キューを管理したりするためのツールの一覧です。

	印刷経路	UACの有効/無効	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	オン	Microsoft管理コンソールの［印刷の管理］スナップイン
		電源 - オフ	Windows 8よりも前： コントロールパネル Windows 8： ［印刷の管理］スナップイン
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	オン	プリントサーバーのMicrosoft管理コンソール［印刷の管理］スナップイン
		電源 - オフ	プリントサーバーの［コントロールパネル］
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	クライアント印刷	オン	プリントサーバーのMicrosoft管理コンソール［印刷の管理］スナッ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	経路 印刷経路	UAC 電源 - 有効/無効	プイン 場所
			Windows 8よりも前： コントロールパネル Windows 8： ［印刷の管理］スナップイン
ローカルのネットワークサーバープリンター（サーバーOSマシンに追加されたネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	オン	プリントサーバーの［コントロールパネル］
		電源 - オフ	プリントサーバーの［コントロールパネル］

注： ネットワーク印刷経路で実行されたネットワークプリンターへの印刷キューは「プライベート」であり、システムで管理することはできません。

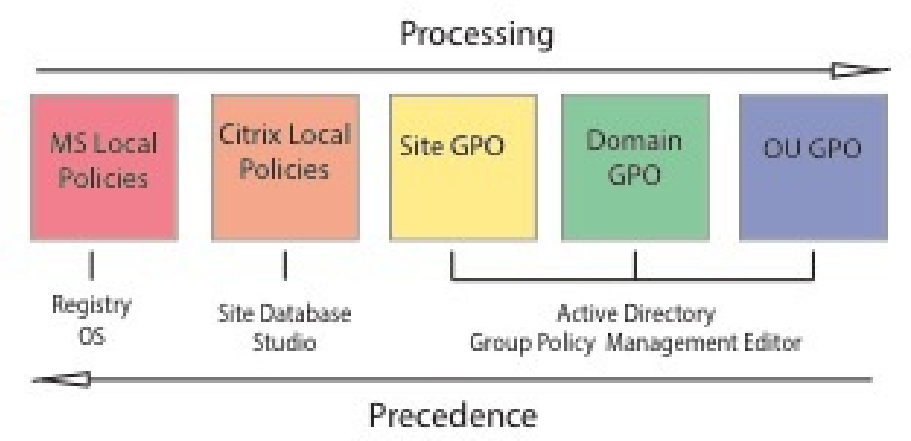
© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシー

Dec 05, 2017

ポリシーは構成可能な設定項目をグループ化したもので、特定のユーザー、デバイス、または接続の種類に対して特定のセッション、帯域幅、およびセキュリティ構成が適用されるように制御する目的で使用します。

これらのポリシーは、特定の物理マシン、仮想マシン、またはユーザーに割り当てることができます。ユーザーに適用する場合、ローカルレベルのアカウントを指定したりActive Directoryのセキュリティグループを指定したりできます。ポリシーに追加できる各設定項目では、特定の条件や規則を定義します。ポリシーを特定のオブジェクトに明示的に割り当てない場合、その設定はすべての接続に適用されます。



ポリシーは、ネットワークのさまざまなレベルに割り当てることができます。組織単位のGPOレベルに割り当てられたポリシーは、そのネットワークで最も優先されます。ドメインのGPOレベルのポリシーはサイトGPO レベルのポリシーよりも優先され、これらのポリシーはMicrosoftや Citrixのローカルポリシーよりも優先されます。

すべてのCitrixローカル ポリシーはCitrix Studio上で作成および管理され、 サイトデータベース内に格納されます。これに対し、グループポリシーは Microsoftグループポリシー管理コンソール（GPMC）上で作成および管理され、Active Directory内に格納されます。Microsoftローカルポリシーは Windows上で 作成され、レジストリ内に格納されます。

Studioの モデル作成ウィザードを使用すると、 複数のテンプレートやポリシーの設定項目とその構成内容を比較してポリシーの競合や重複 を避けることができます。また、GPMCを使用してGPOを設定して、 ネットワークのさまざまなレベルのユーザーにそれらを適用できます。

これらのGPOは Active Directory内に保存され、セキュリティ上の理由から、通常IT担当者のみが設定を 管理できます。

複数のポリシーの設定内容は、ポリシーの優先度や条件に 基づいて統合されます。優先度のより高いポリシーの設定で［無効］または［禁止］が選択されている場合、 優先度の低いポリシーで［有効］または［許可］が選択されていても、その設定内容は無視されます。未構成の設定項目は無視され、優先度の低いポリシーでの設定を 上書きすることはありません。

ローカルポリシーとActive Directoryのグループポリシーの設定内容が 競合する場合、優先されるポリシーは状況により異なります。

すべてのポリシーは、以下の順番で 処理されます。

1. エンドユーザーがドメインの資格情報を使用してマシンにログオンする。
2. 資格情報がドメインコントローラーに送信される。
3. Active Directoryによりすべてのポリシー（エンドユーザー、エンドポイント、組織単位、およびドメイン）が適用され

© 1999-2017 Citrix Systems, Inc. All rights reserved.

る。
4. エンドユーザーがReceiverにログオンしてアプリケーションまたはデスクトップにアクセスする。
5. そのエンドユーザー、およびアプリケーションまたはデスクトップのホストマシンに適用されるCitrixポリシーとMicrosofポリシーが処理される。
6. Active Directoryにより各ポリシー設定の優先度が決定され、エンドポイントデバイスのレジストリやリソースをホストしているマシンに適用されます。
7. エンドユーザーがアプリケーションまたはデスクトップからログオフする。そのエンドユーザー、およびアプリケーションまたはデスクトップのホストマシンに適用されるCitrixポリシーが非アクティブになる。
8. エンドユーザーがユーザーデバイスからログオフし、GPOユーザーポリシーが非アクティブになる。
9. エンドユーザーがユーザーデバイスをシャットダウンし、GPOマシンポリシーが非アクティブになる。

ユーザー、ユーザーデバイス、およびマシンのグループに割り当てる ポリシーを作成する場合、そのグループの一部のメンバーで要件が 異なるためにいくつかの設定項目で例外を設定しなければならない場合があります。この例外はStudioおよびGPMCでフィルターとして作成でき、これによりだれにどの ポリシーが適用されるのかが決定されます。

注： 1つのGPOにWindowsポリシーとCitrixポリシーを混在させることはできません。

関連トピック

- ポリシーの使用
- ポリシーテンプレート
- ポリシーの作成
- ポリシーの比較、優先度、モデル作成、およびトラブルシューティング
- デフォルトのポリシー設定
- ポリシー設定リファレンス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーの使用

Dec 05, 2017

ユーザーのアクセスやセッション環境を制御するには、Citrixポリシーを構成します。 Citrixポリシーを使用して、接続、セキュリティ、および帯域幅の設定を効率的に制御できます。 ポリシーは、特定のグループのユーザー、デバイス、または接続の種類を対象に適用できます。 1つのポリシーに複数の設定を選択して構成できます。

Citrixポリシーを構成するツール

Citrixポリシーは、以下のツールを使用して構成します。

- **Studio** - グループポリシーの管理権限が付与されていないCitrix管理者は、Studioを使ってサイトのポリシーを作成します。Studioを使って作成されたポリシーはそのサイトのデータベースに保存され、仮想デスクトップをブローカーに登録するとき、またはユーザーが仮想デスクトップに接続するときにその仮想デスクトップに適用されます。
- **ローカルグループポリシーエディター**（Microsoft管理コンソールのスナップイン） - ネットワーク環境でActive Directoryが使用されており、グループポリシーの管理権限が付与されている場合は、グループポリシーエディターを使用してサイトのポリシーを作成できます。ここでの設定内容は、グループポリシー管理コンソールで指定するグループポリシーオブジェクト（GPO）に反映されます。
  重要： VDAのControllerへの登録に関するものやMicrosoft App-Vサーバーに関するものなど、一部のポリシー設定を構成するには、グループポリシーエディターを使用する必要があります。

ポリシーの 処理順序と優先順位

グループポリシーの 設定は、以下の順で処理されます。

1. ローカルのGPO
2. XenApp/XenDesktopサイトの GPO（サイトのデータベースに格納される）
3. サイトレベルのGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、 設定内容に競合が発生すると、最後に処理されるポリシーの設定により、 先に処理されるポリシーの設定が上書きされることがあります。つまり、ポリシーの設定は 以下の順番で優先されます。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. XenApp/XenDesktopサイトの GPO（サイトのデータベースに格納される）
5. ローカルのGPO

たとえば、営業部のユーザーが クライアント側のファイルをセッション内で使用できるようにするポリシー（Policy A）をCitrix管理者がStudioで作成し、同じユーザーに対してこの機能を禁止するポリシー（Policy B）をほかの 管理者がグループポリシーエディターで作成したとします。 この場合、営業部のユーザーが仮想デスクトップに ログオンするとPolicy Bが適用され、Policy Aは無視されます。 これは、ドメインレベルで処理されるPolicy Bが、 XenApp/XenDesktopサイトのGPOレベルで処理されるPolicy Aよりも優先されるためです。

ただし、 ユーザーがICAまたはリモートデスクトッププロトコル（RDP）セッションを開始する場合は、 Active DirectoryやWindowsの リモートデスクトップセッションホストの構成ツールでの設定よりも、Citrixポリシーでの設定の方が優先されることに注意してください。これは、RDPクライアント接続で一般的に設定されている、 デスクトップの 壁紙、メニューのアニメーション化、ウィンドウの内容を表示したままドラッグする機能などにも当てはまります。

複数のポリシーを適用する場合は、競合する 設定項目が正しく処理されるように優先順位を設定できます。詳しくは、「ポ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リシーの比較、優先度、モデル作成、およびトラブルシューティング」を参照してください。

Citrixポリシーの設定工程

ポリシーを設定する工程は次のとおりです。
1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーを マシンやユーザーオブジェクトに割り当てます。
4. ポリシーの優先度を設定します。
5. Citrixグループポリシーモデル作成ウィザードを実行して、ポリシーの効果を確認します。

Citrixポリシーと設定の使用

ローカルグループポリシーエディターでは、ポリシーと設定項目が［コンピューターの構成］ノードと［ユーザーの構成］ノードに表示されます。これらのそれぞれに［Citrix Policies］ノードがあります。このスナップインの使用方法については、Microsoft社のドキュメントを参照してください。

Studioでは、ポリシーやテンプレートの設定項目が機能に基づいて分類されています。たとえば、［Profile Management］カテゴリには、Profile managementのポリシー設定が含まれています。

- 「コンピューター設定」（マシンに適用される設定項目）は仮想デスクトップの動作を制御し、仮想デスクトップの起動時に適用されます。これらの設定項目は、仮想デスクトップにアクティブなユーザーセッションがない場合でも適用されます。「ユーザー設定」は、仮想デスクトップにICA接続する場合のユーザーエクスペリエンスを制御します。これらの設定項目は、ユーザーがICAを使って接続または再接続するたびに適用されます。ユーザーがRDPを使って接続したりコンソールに直接ログオンしたりする場合は適用されません。

  ポリシー、設定項目、およびテンプレートを管理するには、Studioのナビゲーションペインで[ポリシー］を選択します。
  - **［ポリシー］**タブには、すべての既存のポリシーが表示されます。ここでポリシーを選択すると、右側に［概要］タブ（名前、優先度、有効/無効の状態、および説明）、［設定］タブ（構成済みの設定項目の一覧）、および［割り当て先］タブ（ポリシーの適用対象のユーザーおよびマシンオブジェクト）が表示されます。詳しくは、「ポリシーの作成」を参照してください。
  - **［テンプレート］**タブには、組み込みおよびカスタムのテンプレートが表示されます。ここでテンプレートを選択すると、右側に［説明］タブ（テンプレートの使用目的）、および［設定］タブ（構成済みの設定項目の一覧）が表示されます。詳しくは、「ポリシーテンプレート」を参照してください。
  - **［比較］**タブでは、複数のポリシーやポリシーテンプレートの設定項目を比較することができます。環境に適した設定項目が構成されているかどうかを確認するときに、この機能を使用できます。詳しくは、「ポリシーの比較、優先度、モデル作成、およびトラブルシューティング」を参照してください。
  - **［モデル作成］**タブでは、特定の接続シナリオでのCitrixポリシーの効果をシミュレートできます。詳しくは、 ポリシーの比較、優先度、モデル作成、およびトラブルシューティング」を参照してください。

  ポリシーやテンプレートの設定項目を検索するには、以下の手順に従います。
  1. ポリシーまたはテンプレートを選択します。
  2. ［操作］ペインの［ポリシーの編集］または［テンプレートの編集］を選択します。
  3. ［設定］ページで、設定項目の名前を入力します。

  特定の製品バージョンや設定項目のカテゴリ（［帯域幅］など）を選択することで、検索範囲を限定できます。また、［選択項目のみを表示する］チェックボックスをオンにすると、そのポリシーで選択済みの設定項目のみが表示されます。すべての設定項目を検索対象にするには、［すべての設定］を選択します。

- ポリシーの設定項目を検索するには、以下の手順に従います。
  1. ポリシーを選択します。
  2. ［設定］タブを選択し、設定項目の名前を入力します。

特定の製品バージョンや設定項目のカテゴリを選択することで、検索範囲を限定できます。すべての設定項目を検索対象にす

© 1999-2017 Citrix Systems, Inc. All rights reserved.

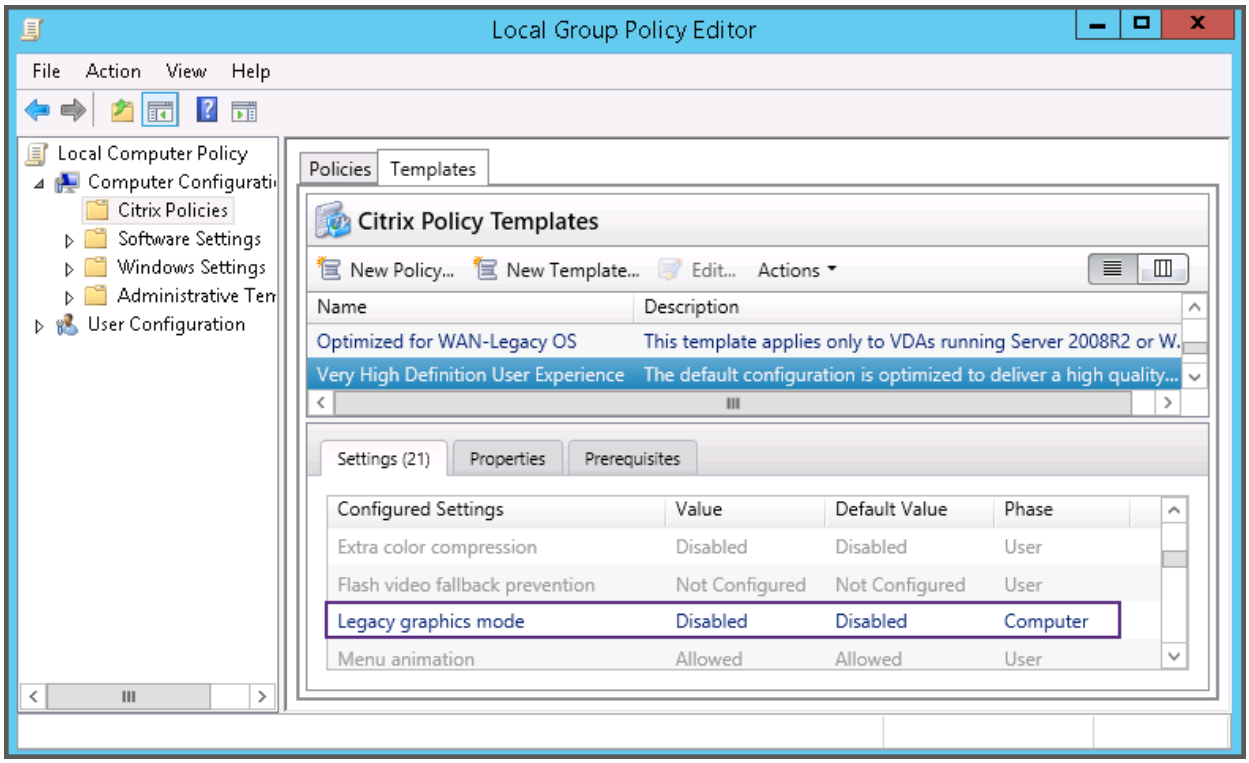
るには、［すべての設定］を選択します。

いったんポリシーを作成したら、それは使用されるテンプレートとは全く無関係です。新しいポリシーの説明フィールドを使って、使用されるソーステンプレートを監視し続けることができます。

Studioでは、ユーザー、コンピューター、または両方の種類の設定のいずれかを含んでいるかどうかにかかわらず、ポリシーとテンプレートは単一の一覧に表示され、ユーザーとコンピューターの両方のフィルターを使って適用することができます。

グループポリシーエディターでは、コンピューターとユーザーの両方の種類の設定を含むテンプレートから作成された場合でも、コンピューターとユーザーは別々に適用される必要があります。この例では、［コンピューターの構成］で［最高品位ユーザー エクスペリエンス］を使用することを選択しています。

- 従来のグラフィックモードは、このテンプレートから作成されるポリシーで使用されるコンピューター設定です。
- 灰色表示のユーザー設定は、このテンプレートから作成されるポリシーでは使用されません。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーテンプレート

Dec 05, 2017

テンプレートは、事前定義された開始ポイントからポリシーを作成するためのソースです。組み込みCitrixテンプレートは、特定の環境またはネットワーク状況に対して最適化され、次のように使用できます。

- サイト間で共有する自分のポリシーおよびテンプレートを作成するためのソース。
- 結果を引用できるようになるため、展開環境間で結果をより簡単に比較するためのリファレンス。例："..when using Citrix template x or y.."
- テンプレートをインポートまたはエクスポートすることにより、Citrixサポートまたは信頼するサードパーティとポリシーを通信するための手段。

ポリシーテンプレートをインポートまたはエクスポートできます。追加のテンプレートと組み込みテンプレートの更新については、Citrix Knowledge CenterのCTX202000を参照してください。

ポリシーの作成にテンプレートを使用するときの考慮事項については、CTX202330を参照してください。

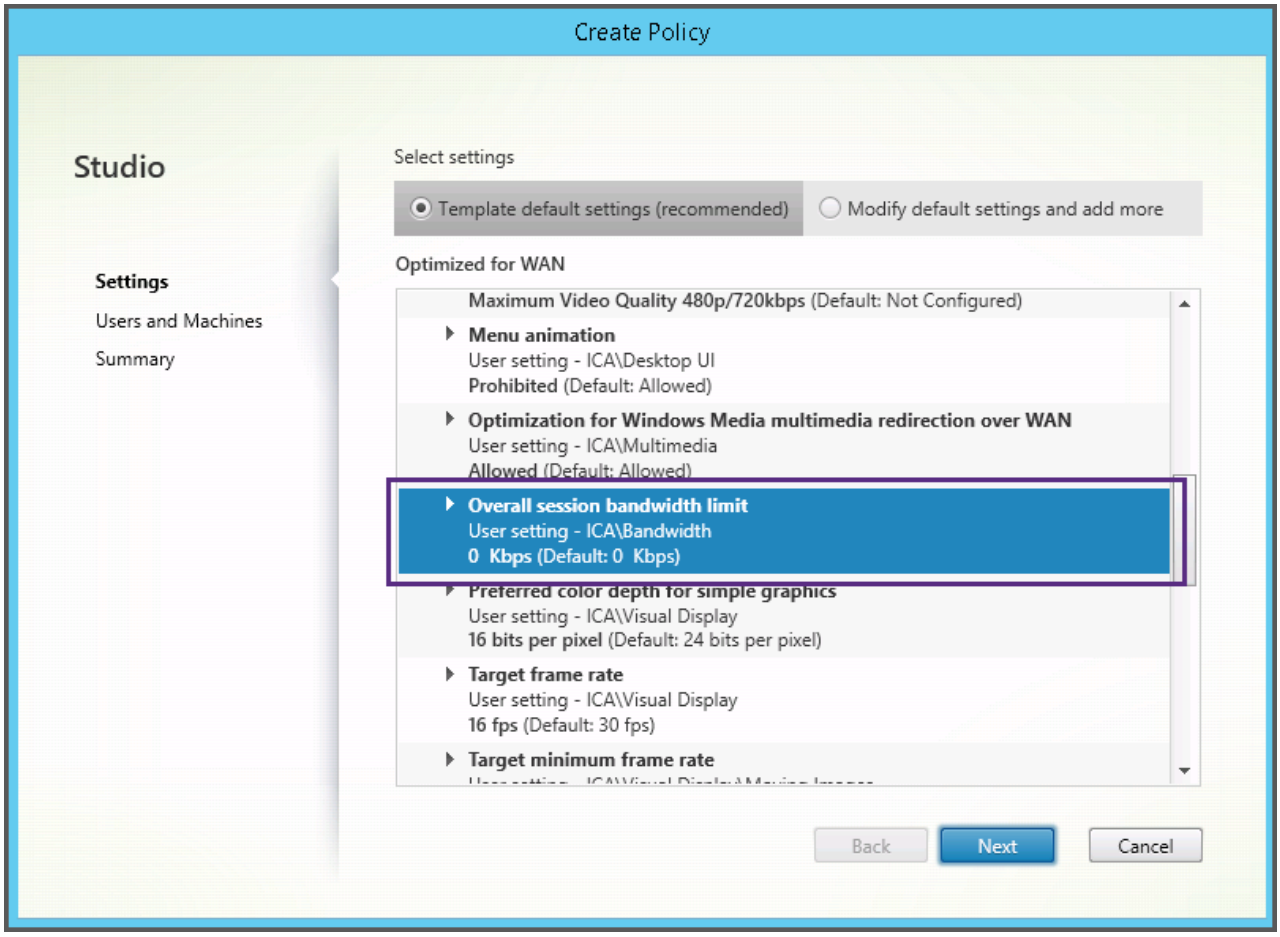
組み込みのCitrixテンプレート

使用できるポリシーテンプレートは以下のとおりです。

- **最高品位ユーザーエクスペリエンス**。このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。
- **高サーバースケーラビリティ**。サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増大させながら、良質のユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防ぎます。
- **高サーバースケーラビリティ - レガシOS**。この高サーバースケーラビリティテンプレートは、Windows Server 2008 R2またはWindows 7以前が動作するVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **NetScaler SD-WANに最適化**。これは、NetScaler SD-WANが展開された支店などのユーザーに適用してXenDesktopの配信を最適化するテンプレートです。（NetScaler SD-WANは、CloudBridgeの新しい名前です）。
- **WANの最適化**。このテンプレートは、共有WAN接続を使用している支店や、低帯域幅接続を実行する遠隔地にいて、マルチメディアコンテンツがほとんどない視覚的に簡素なユーザーインターフェイスのアプリケーションにアクセスするタスクワーカーを対象としたものです。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。
- **WANの最適化 - レガシ OS**。このWANの最適化テンプレートは、Server 2008 R2 またはWindows 7以前が動作するVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **セキュリティと制御**。許容率が低い環境でのこのテンプレートの使用にはリスクがあります。XenAppおよびXenDesktopではデフォルトで有効な機能が最小化することになります。このテンプレートには、印刷、クリップボード、周辺デバイス、ドライブマッピング、ポートのリダイレクト、およびユーザーデバイス上のFlashアクセラレーションへのアクセスを無効にする設定があります。このテンプレートを適用すると、より多くの帯域幅が消費され、サーバーごとのユーザー密度が減ります。

組み込みCitrixテンプレートはそのデフォルトの設定のままで使用することをお勧めしますが、特定の推奨値がない設定があります（WANの最適化テンプレートに含まれるセッション全体の最大帯域幅など）。この場合、テンプレートにより設定が公開され、これによって管理者はこの設定がそのシナリオに適用されようとしていることを理解します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



XenAppおよびXenDesktop 7.6 FP3より前のバージョン（ポリシー管理およびVDA）を使用していて、高サーバースケーラビリティおよびWANの最適化テンプレートを必要とする場合、これらのテンプレートを適用するときはそのレガシOSバージョンを使用してください。

> **注意**
>
> 組み込みテンプレートは、Citrixにより開発およびアップデートされます。これらのテンプレートを変更したり削除したりすることはできません。

Studio使ったテンプレートの作成と管理

テンプレートをベースにした新しいテンプレートを作成するには：

1. Studioのナビゲーションペインで **[ポリシー]** を選択します。
2. **[テンプレート]** タブを選択し、作成元のテンプレートを選択します。
3. ［操作］ペインの **[テンプレートの作成]** を選択します。
4. テンプレートのポリシー設定を選択して構成します。また、新しいテンプレートに不要な既存の設定は削除します。テンプレートの名前を入力します。

[完了] をクリックすると、新しいテンプレートが **[テンプレート]** タブに表示されます。

ポリシーをベースに新しいテンプレートを作成するには：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Studioのナビゲーションペインで **[ポリシー]** を選択します。
2. **[ポリシー]** タブを選択し、作成元のポリシーを選択します。
3. ［操作］ペインの **[テンプレートとして保存]** を選択します。
4. テンプレートに含める新しいポリシー設定を追加して構成します。また、新しいテンプレートに不要な既存の設定は削除します。新しいテンプレートの名前と説明を入力し、 **[完了]** をクリックします。

テンプレートをインポートするには：

1. Studioのナビゲーションペインで **[ポリシー]** を選択します。
2. **[テンプレート]** タブを選択し、 **[テンプレートのインポート]** を選択します。
3. インポートするテンプレートを選択して、 **[開く]** をクリックします。既存のものと同じ名前のテンプレートをインポートすると、既存のものを上書きするか、別名（自動的に生成されます）でインポートするかを選択できます。

テンプレートをエクスポートするには：

1. Studioのナビゲーションペインで **[ポリシー]** を選択します。
2. **[テンプレート]** タブを選択し、 **[テンプレートのエクスポート]** を選択します。
3. テンプレートの保存先を指定して、 **[保存]** をクリックします。

指定した場所にテンプレートファイル（拡張子.gpt）がエクスポートされます。

グループポリシーエディターでテンプレートを作成および管理する

グループポリシーエディターの ［コンピューターの構成］または ［ユーザーの構成］を開きます。 ［ポリシー］ノードを開き、 ［Citrix ポリシー］を選択します。 以下の操作を行います。

目的	手順
既存の ポリシーから新しいテンプレートを作成する	［ポリシー］タブでポリシーを選択して ［操作］> ［テンプレートとして保存］を選択する
既存の テンプレートから新しいポリシーを作成する	［テンプレート］タブでテンプレート を選択して ［新規ポリシー］をクリックする
既存の テンプレートから新しいテンプレートを作成する	［テンプレート］タブでテンプレート を選択して ［新規テンプレート］をクリックする
テンプレートをインポートする	［テンプレート］タブで ［操作］> ［インポート］の順に選択する
テンプレートをエクスポートする	［テンプレート］タブで、 ［操作］> ［エクスポート］の順に選択する
テンプレートに構成済みの設定項目を確認する	［テンプレート］タブでテンプレート を選択して［設定項目］タブをクリックする
テンプレートのプロパティを確認する	［テンプレート］タブでテンプレート を選択して［プロパティ］タブをクリックする
テンプレートの必須条件を確認する	［テンプレート］タブでテンプレート を選択して［必須条件］タブをクリックする

管理者の委任機能とテンプレート

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーテンプレートは、ポリシー管理パッケージがインストールされたマシン上に格納されます。このマシンは、Delivery Controllerマシンかグループポリシーオブジェクト管理マシンのいずれかで、XenAppおよびXenDesktopサイトのデータベースではありません。これはつまり、ポリシーテンプレートファイルへのアクセスはWindowsの管理アクセス許可により制御され、サイトの委任された管理タスクの委任機能や管理スコープは考慮されません。

このため、たとえばサイトの読み取りのみの管理権限を持つ管理者がテンプレートを作成できます。ただし、テンプレートはローカルファイルであるため、ほかのマシン上のStudioには反映されません。

カスタムテンプレートは、それを作成するユーザーアカウントでのみ表示可能で、ユーザーのWindowsプロファイルに格納されます。これ以外のユーザーアカウントに対してもカスタムテンプレートを公開するには、そこからポリシーを作成するか、または共有の場所にエクスポートします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーの作成

Dec 05, 2017

ポリシーを作成する前に、そのポリシーの適用先となるユーザーまたはデバイスのグループを決定します。ユーザーの担当業務、接続の種類、ユーザーデバイス、または作業場所に応じてポリシーを適用できます。または、WindowsのActive Directoryのグループポリシーと同じ基準を使用できます。

グループに適用するポリシーを作成済みの場合は、別のポリシーを作成するのではなく、既存のポリシーの設定内容を編集することを検討してください。特定の設定内容を変更するため、または特定のユーザーを適用対象から除外するためだけに新しいポリシーを作成することは避けてください。

既存のポリシーテンプレートを基に新しいポリシーを作成し、必要に応じて設定項目をカスタマイズします。または、テンプレートを使用せずにポリシーを作成して、必要な設定項目を選択して構成します。

Citrix Studioでは、新しいポリシーを作成すると、［ポリシーの有効化］チェックボックスが明示的にオンになっていない限り［無効］に設定されます。

ポリシー設定（一般的な「設定」と区別するためにここでは「設定項目」という語を使用します）

ポリシーを設定するには、適用するポリシー設定を選択して値を構成します。 デフォルトでは、ポリシーに追加されている設定項目はありません。 設定を適用するには、ポリシーに追加する必要があります。

ポリシーのいくつかの設定では、次のオプションを指定します。

- ［許可］または［禁止］を選択して、その設定項目により制御されるアクションを許可または禁止します。これらのアクションには、セッション内でのユーザーによる管理を許可したり禁止したりできるものがあります。 たとえば、 ［メニューを アニメーション化する］設定で［許可］を選択した場合、ユーザーがクライアント環境内でメニューのアニメーション化を制御できるようになります。
- ［有効］または［無効］を選択して、その設定項目の機能を有効または無効にします。 ここで無効にすると、より優先度の低いポリシーで［有効］を選択しても、その設定は有効になりません。

また、一部の設定は、それに依存する設定の効果を制御します。 たとえば、 ［クライアント ドライブリダイレクト］設定により、クライアントデバイス側のドライブへのアクセスが制御されます。 ユーザーがネットワーク ドライブにアクセスできるようにするには、この設定と ［クライアント側 ネットワークドライブ］設定の両方で［許可］が選択されている必要があります。この場合、 ［クライアント ドライブリダイレクト］設定で［禁止］を選択すると、 ［クライアント側 ネットワークドライブ］設定で［許可］を選択しても、ユーザーが ネットワークドライブにアクセスできなくなります。

通常、マシンの動作を制御するポリシー設定に対する変更内容は、仮想デスクトップが再起動したときまたはユーザーがログオンしたときに適用されます。 また、ユーザーの機能を制御する設定項目は、そのユーザーの次回ログオン時に適用されます。 Active Directory環境では、ポリシーが90分間隔で再評価され、仮想デスクトップが再起動したときまたはユーザーがログオンしたときに適用されます。

一部の設定項目では、ポリシーに追加するときに値を入力または選択します。 ［デフォルト値を使用する］チェックボックスをオンにすると、その設定項目のデフォルト値が適用され、 ほかの値を設定できなくなります。 ［デフォルト値を使用する］チェックボックスをオンにする前に設定した値は無視されます。

ベストプラクティス：

- ポリシーの適用先として、個々のユーザーアカウントではなくグループアカウントを使用します。 ポリシーの対象ユーザーを個々に追加したり削除したりするよりも、そのユーザーがグループアカウントに属しているかどうかで管理した方が効率的です。
- Windowsのリモートデスクトップセッションホストの構成ツールと重複または競合する設定を使用しないでください。 リ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

モートデスクトップセッションホストの構成ツールとCitrixポリシーで、同様の機能に対して異なる動作が設定されていると、予期せぬ問題が生じる場合があります。 設定の有効/無効をできる限り統一しておくと、問題解決が容易になります。
- 使用しないポリシーは無効にしておきます。 ポリシーに設定を追加しない場合でも、そのポリシーにより不要な処理が行われます。

ポリシーの割り当て

ポリシーを作成したら、それを特定のユーザーやマシンオブジェクトに割り当てます。これにより、設定した条件や規則に基づいてポリシーが接続に適用されます。通常、1つのポリシーに複数の割り当てを指定して、複数の条件を組み合わせることができます。割り当てを指定しない場合、そのポリシーはすべての接続に適用されます。

次の表は、使用可能な割り当ての一覧です。

割り当て名	ポリシーの適用対象
アクセス制御	セッションに接続するときのアクセス制御条件。 ● 接続の種類 - 接続がNetScaler Gateway経由かどうかを指定します。 ● NetScaler Gatewayファーム名 - NetScaler Gateway仮想サーバーの名前を指定します。 ● アクセス条件 - 使用するエンドポイント解析ポリシーまたはセッションポリシーの名前を入力します。
Citrix CloudBridge	ユーザーセッションがCitrix CloudBridge経由で起動されたかどうか。 注： ポリシーに追加できる［Citrix CloudBridge］割り当ては1つのみです。
クライアントのIPアドレス	セッションに接続するクライアントデバイスのIPアドレス。 ● IPv4の例：12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 ● IPv6の例：2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。 ● 完全一致：ClientABCName ● 使用するワイルドカード：Client*Name
デリバリーグループ	所属するデリバリーグループ。
デリバリーグループの種類	実行されるデスクトップまたはアプリケーションの種類。プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーションから選択します。
組織単位（OU）	組織単位。
タグ	マシンのタグ。 **注：** タグを使用する場合にポリシーを確実に正しく適用するには、CTX142439からHotfixを入手してインストールしてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

割り当て名またはグループ	ポリシーの適用対象ユーザーまたはグループ名。

ユーザーがログオンするときに、その接続の条件に一致するすべてのポリシーが検出されます。検出されたポリシーは優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。たとえば、優先度の高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーの同じ設定で［有効］が選択されていても、その設定には［無効］が適用されます。構成されていないポリシー設定は無視されます。

重要： グループポリシー管理コンソールを使ってActive DirectoryポリシーとCitrixポリシーの両方を構成する場合、割り当ておよび設定が意図したとおりに適用されない場合があります。詳しくは、CTX127461を参照してください。
「Unfiltered」という名前のポリシーはデフォルトで提供されています。

- Studioを使用してCitrixポリシーを管理する場合は、Unfilteredポリシーに追加する設定がそのサイトのすべてのサーバー、仮想デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用してCitrixポリシーを管理する場合は、そのポリシーのグループポリシーオブジェクト（GPO）スコープに属するすべてのサイトおよび接続にUnfilteredポリシーの設定が適用されます。たとえば、営業部署の組織単位に大阪支社のすべての営業メンバーを含んでいるSales-OSKというGPOがある場合に、いくつかのユーザーポリシー設定を追加したUnfilteredポリシーをSales-OSKに設定します。ここで大阪支社の営業部長がサイトにログオンすると、この部長はSales-OSK GPOのメンバーなので、Unfilteredポリシーのすべての設定がセッションに適用されます。

割り当ての［モード］によっても、そのポリシーの適用先が異なります。割り当てのモードとして[許可］（デフォルト）が設定されている場合、その割り当て条件にマッチした接続にのみポリシーが適用されます。割り当てのモードとして［禁止］が設定されている場合、その割り当て条件にマッチしない接続にのみポリシーが適用されます。以下の例では、複数の割り当てを追加したCitrixポリシーで、割り当てのモードがどのように適用されるかについて説明します。

- **例： 同じ種類の割り当てでモードが異なる場合**- ポリシーに同じ種類の割り当てを追加し、一方を［許可］にしてもう一方を［禁止］にした場合、［禁止］を設定した割り当てが優先されます。次に例を示します。
  Policy 1に以下の割り当てを追加します。
  - Assignment Aは営業部署のグループアカウントに適用される割り当てで、［許可］を設定します。
  - Assignment Bは営業部長のアカウントに適用される割り当てで、［禁止］を設定します。

  ここで営業部長がログオンした場合、営業部長が営業部署のグループアカウントに属していても、Assignment Bが[禁止］モードなのでこのPolicy 1は適用されません。

- **例： 異なる種類の割り当てでモードが同じ場合**- ポリシーに異なる種類の複数の割り当てを追加し、すべての割り当てに［許可］を設定した場合、すべての種類の割り当てに一致しないとポリシーは適用されません。次に例を示します。
  Policy 2に以下の割り当てを追加します。
  - Assignment Cは営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てで、[許可］を設定します。
  - Assignment Dは10.8.169.*（企業ネットワーク）を指定するクライアントIPアドレス割り当て です。モードは[許可］に設定されます。

  ここで営業部長が社内のオフィスからログオンした場合、上記2つの割り当てに合致するので、このPolicy 2が適用されます。

  Policy 3に以下の割り当てを追加します。
  - Assignment Eは営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てで、[許可］を設定します。
  - Assignment Fは特定のNetScaler Gateway接続に適用される［アクセス制御］割り当てで、［許可］を設定します。

  ここで営業部長が社内のオフィスからログオンした場合、Assignment Fに合致しないので、このPolicy 3は適用されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Studioでテンプレートから新しい ポリシーを作成する

1. Studioのナビゲーションペインで ［ポリシー］ を選択します。
2. ［テンプレート］ タブを選択し、テンプレートを選択します。
3. ［操作］ ペインの ［テンプレートからのポリシーの作成] を選択します。
4. デフォルトでは、テンプレートで指定されているすべての設定項目が新しいポリシーに追加されます（［テンプレートのデフォルトの 設定項目］ が有効）。設定項目を変更する場合は、 ［デフォルトの設定項目を変更および追加する] をクリックして、 必要に応じて設定項目を追加または削除します。
5. ポリシーの割り当て先として、以下のいずれかを選択します。
   - ［選択したユーザーおよびマシンオブジェクト] をクリックして、ポリシーを適用するユーザーおよびマシンオブジェクトを選択します。
   - ［サイト内のすべてのオブジェクトに割り当てる] をクリックします。これにより、サイト内のすべてのユーザーやマシンオブジェクトにこのポリシーが適用されます。
6. 「新しいポリシーの名前を入力するか、デフォルトの名前を使用します。経理部」や「リモートユーザー」など、ポリシーの適用対象に基づいて名前を付けると便利です。 また、必要に応じて説明を入力します。
   新しいポリシーはデフォルトで有効になりますが、無効にすることもできます。 ポリシーを作成して有効にすると、新たにログオンするユーザーに直ちに適用されます。既存のセッションには適用されません。 無効にしたポリシーは適用されません。 作成済みのポリシーに優先度を設定したり、設定項目を追加したりするときは、そのポリシーを一時的に無効にすることを検討してください。

Studioで新しいポリシーを作成する

1. Studioのナビゲーションペインで ［ポリシー］ を選択します。
2. ［ポリシー］ タブをクリックします。
3. ［操作］ ペインの ［ポリシーの作成］ を選択します。
4. 必要な設定項目を追加して構成します。
5. ポリシーの割り当て先として、以下のいずれかを選択します。
   - ［選択したユーザーおよびマシンオブジェクト] をクリックして、ポリシーを適用するユーザーおよびマシンオブジェクトを選択します。
   - ［サイト内のすべてのオブジェクトに割り当てる] をクリックします。これにより、サイト内のすべてのユーザーやマシンオブジェクトにこのポリシーが適用されます。
6. 「新しいポリシーの名前を入力するか、デフォルトの名前を使用します。経理部」や「リモートユーザー」など、ポリシーの適用対象に基づいて名前を付けると便利です。 また、必要に応じて説明を入力します。
   新しいポリシーはデフォルトで有効になりますが、無効にすることもできます。 ポリシーを作成して有効にすると、新たにログオンするユーザーに直ちに適用されます。既存のセッションには適用されません。 無効にしたポリシーは適用されません。 作成済みのポリシーに優先度を設定したり、設定項目を追加したりするときは、そのポリシーを一時的に無効にすることを検討してください。

グループポリシーエディターでポリシーを作成および管理する

グループ ポリシーエディターの ［コンピューターの構成］ または ［ユーザーの構成］ を開きます。 ［ポリシー］ ノードを開き、 ［Citrix ポリシー］ を選択します。 以下の操作を行います。

目的	手順
新しいポリシーを作成する	［ポリシー］ タブの ［新規］ をクリックする
既存のポリシーを編集する	［ポリシー］ タブでポリシーを選択して ［編集］ をクリックする

© 1999-2017 Citrix Systems, Inc. All rights reserved.

目的	手順
既存のポリシーの優先度を変更する	［ポリシー］タブでポリシーを選択して ［上げる］または ［下げる］をクリックする
ポリシーの要約情報を表示する	［ポリシー］タブでポリシーを選択して ［情報］タブをクリックする
ポリシーの設定項目を表示して変更する	［ポリシー］タブでポリシーを選択して ［設定］タブをクリックする
ポリシーの割り当て先を表示して変更する	［ポリシー］タブでポリシーを選択して ［フィルター］タブをクリックする
ポリシーを有効または無効にする	［ポリシー］タブでポリシーを選択して ［操作］> ［有効］または ［操作］> ［無効］の順に選択する
既存のテンプレートから新しいポリシーを作成する	［テンプレート］タブでテンプレートを選択して ［新規ポリシー］をクリックする

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーの比較、優先度、モデル作成、およびトラブルシューティング

Dec 05, 2017

ユーザーの担当業務、作業場所、または接続の種類などのユーザーのニーズに応じて、複数のポリシーを作成できます。たとえば、セキュリティ上の理由から、機密性の高いデータを日常的に取り扱うユーザーグループのアクセスに、一定の制限を適用したい場合があります。この場合、ユーザーがローカルのクライアントドライブ上にファイルを保存することを禁止するポリシーを作成できます。また、そのユーザーグループの中にローカルドライブへのアクセスが必要なユーザーがいる場合は、そのユーザー専用のポリシーを作成してほかのポリシーよりも高い優先度を設定します。同じユーザーに複数のポリシーが適用される場合は、それらのポリシーに優先度を設定して、適用される設定内容を制御できます。

複数のポリシーを使用するときは、どのように優先度を設定するか、どのように特定のユーザーを対象から除外するか、およびポリシーが競合した場合にどの設定内容が最終的に適用されるかについて確認する必要があります。

通常、Citrixポリシーの設定は、サイト全体、またはDelivery Controllerやユーザーデバイス側で構成されている同様の設定よりも優先されます。ただし、暗号化レベルとシャドウ機能の設定については、オペレーティングシステムでの設定を含み、最も高い制限が適用されます。

Citrixポリシーは、オペレーティングシステム側で設定されているほかのポリシーとも関連して機能します。Citrix環境では、Active DirectoryやWindowsのリモートデスクトップセッションホストの構成ツールでの設定よりも、Citrixポリシーでの設定の方が優先されます。これは、RDP（Remote Desktop Protocol）クライアント接続で一般的に設定されている、デスクトップの壁紙、メニューのアニメーション化、ウィンドウの内容を表示したままドラッグする機能などにも当てはまります。また、［SecureICAの最低暗号化レベル］など、オペレーティングシステム側の設定と合致していなければならないものもあります。Citrixポリシー以外の機能でより高い暗号化レベルが設定されている場合、［SecureICAの最低暗号化レベル］設定やアプリケーションやデスクトップごとに指定されている配信設定は無視されます。

たとえば、デリバリーグループを作成するときに指定する暗号化レベルは、その環境全体に対して設定されているレベルと同じである必要があります。

注： ダブルホップ環境における2つ目のホップにおいて、デスクトップOSのVDAがサーバーOSのVDAに接続すると、デスクトップOSのVDA上のCitrixポリシーがユーザーデバイスのように機能します。たとえば、ユーザーデバイス上のイメージをキャッシュするようポリシーが設定されると、ダブルホップ環境における2つ目のホップに対してキャッシュされたイメージはデスクトップOSのVDAマシンでキャッシュされます。

ポリシーおよびテンプレートの比較

Studioでは、複数のポリシーやポリシーテンプレートの設定項目を比較することができます。たとえば、環境に適した設定項目が構成されているかどうかを確認するときに、この機能を使用できます。また、そのポリシーやテンプレートの各設定項目の設定値を、デフォルトの値と比較することもできます。

1. Studioのナビゲーションペインで［ポリシー］を選択します。
2. ［比較］タブをクリックし、［選択］をクリックします。
3. 比較するポリシーまたはテンプレートのチェックボックスをオンにします。[設定項目のデフォルト値と比較する］チェックボックスをオンにすると、各設定項目のデフォルト値が比較結果に追加されます。
4. ［比較］をクリックすると、構成された設定項目とその設定値が一覧表示されます。
5. すべての設定項目を表示するには、［すべての設定項目を表示］を選択します。元の表示に戻るには、［共通の設定項目を表示］を選択します。

ポリシーの優先度

© 1999-2017 Citrix Systems, Inc. All rights reserved.

複数のポリシーで設定内容が競合することを防ぐために、ポリシーに優先度を設定できます。 ユーザーがログオンするときに、その接続の条件に一致するすべてのポリシーが検出されます。 検出されたポリシーは 優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。

Studioでは、ポリシーの優先度が数値で示されます。 デフォルトでは、新しいポリシーに最低の優先度が設定されます。 複数のポリシーで設定内容に矛盾が生じた場合は、優先度の高いポリシー（最高の優先度は「1」です）の設定が適用されます。 同じ条件の接続に対して複数のポリシーが合致する場合は、各ポリシーに追加されている設定がポリシーの優先度、および各設定内容により統合され、「最終的に適用されるポリシー」が決定されます。 優先度のより高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーで［有効］が選択されていても、その設定内容は無視されます。ただし、［設定しない］が選択されたポリシー設定は無視されるため、優先度の高いポリシーで［設定しない］が設定されている場合、その設定内容は無視され、優先度の低いポリシーの内容が適用されます。

1. Studioのナビゲーションペインで ［ポリシー］を選択します。 ［ポリシー］タブが選択されていることを確認します。
2. ポリシーを選択します。
3. ［操作］ペインの ［優先度を 低く］または ［優先度を 高く］を選択します。

例外

ユーザー、ユーザーデバイス、またはマシンに対して作成したポリシーの中に、そのグループの特定のユーザーに適用したくない設定内容が含まれている場合は、 以下の方法で 例外を設定します。

- 例外処理が必要なグループメンバー用に新しいポリシーを作成して、ほかのポリシーより高い優先度を設定します。
- ポリシーに追加する割り当てのモードとして ［禁止］を選択します。

割り当ての モードとして ［禁止］を選択すると、その条件にマッチしない接続にのみポリシーが適用されます。 たとえば、

- ［クライアントのIP アドレス］割り当てで「208.77.88.*」を指定して ［許可］モードを選択
- ［ユーザーまたはグループ］割り当てで特定のユーザーアカウントを指定して ［禁止］モードを選択

この2つのフィルターが設定されたポリシーは、Assignment Aで 指定した範囲のIPアドレスを持つサイトにログオンするすべてのユーザーに 適用されます。ただし、Assignment Bで指定したユーザーアカウントを使用してこのサイトにログ オンするユーザーには、IPアドレスが Assignment Aで指定した範囲内で あってもこのポリシーは適用されません。

接続に適用されるポリシーの確認

複数のポリシーが適用されるために、意図した設定が接続に反映されないことがあります。 作成したポリシーよりも優先度の高いポリシーがあると、意図した設定内容が上書きされてしまいます。 管理者は、ポリシーの優先度や追加されている 設定を基に、最終的に適用される設定を確認することができます。

最終的に適用される設定を確認するには、以下の方法を使用します。

- Citrixグループポリシー モデル作成ウィザードを使用して、接続シナリオをシミュレートしてCitrix ポリシーがどのように適用されるかを確認する。接続シナリオ条件 （ドメインコントローラー、ユーザー、Citrixポリシーの割り当て、低速ネットワーク接続などの 環境設定）を指定します。すると、その条件に基づいて、そのシナリオに適用されるCitrixポリシーの内容についてのレポートが生成されます。 ドメインユーザーとしてControllerにログオンしている場合は、 サイトポリシー設定 とActive Directoryグループポリシーオブジェクト（GPO）の両方を使ってポリシーの結果セットが算出されます。
- グループポリシーの結果ウィザードで、特定のユーザーや Controllerに適用されるCitrixポリシーのレポートを作成する。グループポリシーの結果ウィザードでは、現在の環境のGPOの状態を評価して、特定のユーザーやControllerにこれらのオブジェクト（Citrixポリシーを含む）がどのように適用されるかについてのレポートが生成されます。

Citrixグループポリシーモデル作成ウィザードは、Studioの［操作］ペインから起動できます。これらのツールは、Windows のグループポリシー管理コンソールから起動できます。

グループポリシー管理コンソールから Citrixポリシーモデル作成ウィザードまたはグループ ポリシーの結果ウィザードを実行する場合は、Studioで作成したサイトポリシー設定はポリシーの結果セットに含まれません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシーの管理にグループポリシー管理コンソールのみを使用している場合を除き、 最も包括的なポリシーの結果セットを取得するには、Studioから Citrixグループポリシーモデル作成ウィザードを起動することをお勧めします。

Citrix グループポリシーモデル作成ウィザードの使用

Citrix グループポリシーモデル作成ウィザードを開くには、以下のいずれかを行います。

- Studioのナビゲーションペインで ［ポリシー］を選択し、 ［モデル作成］タブを選択して［操作］ペインの ［モデル作成ウィザードの 起動］を選択します。
- グループポリシー管理コンソール（gpmc.msc）を起動して、コンソールツリーの ［Citrix グループポリシーモデル作成］ノードを右クリックして ［Citrix グループポリシーモデル作成ウィザード］を選択します。

ウィザードの 指示に従って、シミュレーションで使用するドメインコントローラー、ユーザー、コンピューター、環境 設定、およびCitrixフィルター条件を選択します。 ［完了］をクリックすると、モデル作成の 結果のレポートが作成されます。 Studioでは、中央ペインの［モデル作成］ タブにレポートが表示されます。

レポートを表示するには、 ［モデル作成レポートの表示］を選択します。

ポリシーのトラブルシューティング

複数のポリシーで、適用先として同じ割り当て（ユーザーアカウントやクライアントのIPアドレスなど）を指定することも可能です。 この場合、これらのポリシーでの設定が競合すると、ポリシーが意図したとおりに適用されません。 最終的に適用されるポリシーを確認するためにCitrixグループポリシーモデル作成ウィザードやグループ ポリシーの結果ウィザードを使用する場合、ユーザー 接続にいずれのポリシーも適用されないことが判明することがあります。この場合、そのポリシーの割当て条件に合致するユーザー接続が発生しても、いずれのポリシー設定も適用されません。 以下の状況では、いずれのポリシーも適用されません。

- 割り当て条件に合致するポリシーがない場合。
- 割り当て条件に合致したポリシーに設定項目が追加されていない場合。
- 割り当て条件に合致したポリシーが無効になっている場合。

指定した条件の接続にポリシーが適用されるようにするには、以下の内容を確認します。

- そのポリシーが有効になっている。
- そのポリシーに追加した設定項目の内容が適切である。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトのポリシー設定

Dec 05, 2017

次の表は、ポリシーの各設定項目のデフォルト設定と、適用されるVirtual Delivery Agent（VDA）のバージョンの一覧です。

ICA

名前	デフォルト設定	VDA
クライアントクリップボードリダイレクト	許可	すべてのバージョンのVDA
デスクトップの起動	禁止	VDA for Server OS 7以降
EDT	電源 - オフ	VDA 7.13 「アダプティブトランスポート」を参照してください。
ICAリスナー接続タイムアウト	120,000 ミリ秒	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
ICAリスナーポートの番号	1494	すべてのバージョンのVDA
クライアント接続での非公開アプリケーションの起動	禁止	VDA for Server OS 7以降
クライアントクリップボードに書き込みを許可する形式	形式の指定なし	VDA 7.6以降
クライアントクリップボードの書き込み制限	禁止	VDA 7.6以降
セッションクリップボードの書き込み制限	無効	VDA 7.6以降
セッションクリップボードに書き込みを許可する形式	形式の指定なし	VDA 7.6以降

ICA/Adobe Flashデリバリー/Flashリダイレクト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
Flashビデオフォールバック防止	未構成	VDA 7.6 FP3以降
Flashビデオフォールバック防止エラー*.swf		VDA 7.6 FP3以降

ICA/オーディオ

名前	デフォルト設定	VDA
オーディオプラグアンドプレイ	許可	VDA for Server OS 7以降
音質	高 - 高品位オーディオ	すべてのバージョンのVDA
クライアントオーディオリダイレクト	許可	すべてのバージョンのVDA
クライアントマイクリダイレクト	許可	すべてのバージョンのVDA

ICA/クライアントの自動再接続

名前	デフォルト設定	VDA
クライアントの自動再接続	許可	すべてのバージョンのVDA
クライアントの自動再接続時の認証	認証を必要としない	すべてのバージョンのVDA
クライアントの自動再接続のログ	自動再接続イベントをログに記録しない	すべてのバージョンのVDA

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンのVDA
オーディオリダイレクトの最大帯域幅（%）	0	すべてのバージョンのVDA
USBデバイスリダイレクトの最大帯域幅（Kbps）	0Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
USBデバイスリダイレクトの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
クリップボードリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンのVDA
クリップボードリダイレクトの最大帯域幅（%）	0	すべてのバージョンのVDA
COM ポート リダイレクトの最大帯域幅 (Kbps)	0Kbps	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
COM ポート リダイレクトの最大帯域幅 (%)	0	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
ファイルリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンのVDA
ファイルリダイレクトの最大帯域幅（%）	0	すべてのバージョンのVDA
HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（Kbps）	0Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、およびVDA for Desktop OS 7以降
HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
LPTポートリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
LPTポートリダイレクトの最大帯域幅（%）	0	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
セッション全体の最大帯域幅	0Kbps	すべてのバージョンのVDA
プリンターリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンのVDA
プリンターリダイレクトの最大帯域幅（%）	0	すべてのバージョンのVDA
TWAINデバイスリダイレクトの最大帯域幅（Kbps）	0Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
TWAINデバイスリダイレクトの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
クライアントデバイスの位置情報をアプリケーションで使用する	禁止	VDA 5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効（7.6 FP3以降） 有効（5.6～7.6 FP2）	VDA 5.6、VDA for Desktop OS 7以降
デスクトップコンポジションの画質	中	VDA 5.6、VDA for Desktop OS 7以降
デスクトップの壁紙	許可	すべてのバージョンのVDA
メニューをアニメーション化する	許可	すべてのバージョンのVDA
ドラッグ中にウィンドウの内容を表示する	許可	すべてのバージョンのVDA

ICA/エンドユーザー モニタリング

名前	デフォルト設定	VDA
ICA往復測定	有効	すべてのバージョンのVDA
ICA往復測定間隔	15秒	すべてのバージョンのVDA
アイドル接続のICA往復測定	無効	すべてのバージョンのVDA

ICA/デスクトップエクスペリエンス拡張

名前	デフォルト設定	VDA
デスクトップエクスペリエンス拡張	許可	VDA for Server OS 7以降

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブに自動接続する	許可	すべてのバージョンのVDA
クライアントドライブリダイレクト	許可	すべてのバージョンのVDA
クライアント側固定ドライブ	許可	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前 クライアント側フロッピードライブ	デフォルト設定	VDA すべてのバージョンのVDA
クライアント側ネットワークドライブ	許可	すべてのバージョンのVDA
クライアント側光学式ドライブ	許可	すべてのバージョンのVDA
クライアント側リムーバブルドライブ	許可	すべてのバージョンのVDA
ホストからクライアントへのリダイレクト	無効	VDA for Server OS 7以降
クライアント側のドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
クライアント側ドライブへの読み取り専用アクセス	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
ユーザーフォルダーのリダイレクト	許可	Web Interface環境でのみ。VDA for Server OS 7以降
非同期書き込みを使用する	無効	すべてのバージョンのVDA

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的無損失の圧縮を使用する	無効	VDA 7.6以降
表示メモリの制限	65536KB	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
メモリが不足したときの表示モード	色数を下げる	すべてのバージョンのVDA
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
従来のグラフィックモード	無効	VDA for Server OS 7以降、VDA for

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		Desktop OS 7以降
許可される最大表示色数	32ビット/ピクセル	すべてのバージョンのVDA
メモリ不足による表示品質の低下をユーザーに通知する	無効	VDA for Server OS 7以降
キューイメージの破棄	有効	すべてのバージョンのVDA
圧縮にビデオコーデックを使用	選択された場合ビデオコーデックを使用する	VDA 7.6 FP3以降
ビデオコーデックへのハードウェアエンコーディングの使用	有効	VDA 7.11以降

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
固定キャッシュしきい値	3000000bps	VDA for Server OS 7以降

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawkディスプレイチャネル	無効	VDA 7.6 FP2以降
Framehawkディスプレイチャネルポートの範囲	3224,3324	VDA 7.6 FP2以降

ICA/Keep Alive

名前	デフォルト設定	VDA
ICA Keep-Aliveタイムアウト	60秒	すべてのバージョンのVDA
ICA Keep-Alive	ICA Keep-Aliveメッセージを送信しない	すべてのバージョンのVDA

ICA/ローカルアプリケーションアクセス

名前	デフォルト設定	VDA
ローカルアプリケーションのアクセスを許可	禁止	VDA for Server OS 7以降、VDA for Desktop OS 7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
URLリダイレクトのブラックリスト	サイトの指定なし	VDA for Server OS 7以降、VDA for Desktop OS 7以降
URLリダイレクトのホワイトリスト	サイトの指定なし	VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/モバイルデバイスでの動作

名前	デフォルト設定	VDA
キーボードの自動表示	禁止	VDA 5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
タッチパネルでの操作に最適化されたデスクトップ	許可	VDA 5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降 この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは使用できません。
コンボボックスをデバイス側で表示する	禁止	VDA 5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	VDA for Server OS 7以降、VDA for Desktop OS 7以降
マルチメディア会議	許可	すべてのバージョンのVDA
WAN接続でのWindows Mediaマルチメディアリダイレクトの最適化	許可	VDA for Server OS 7以降、VDA for Desktop OS 7以降
WAN接続でのWindows Mediaマルチメディアリダイレクトでの GPUの使用	禁止	VDA for Server OS 7以降、VDA for Desktop OS 7以降
Windows メディア フォールバック防止	未構成	VDA 7.6 FP3以降
Windows Mediaのクライアント側でのコンテンツ取得	許可	VDA for Server OS 7以降、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		VDA for Desktop OS 7以降
Windows Mediaリダイレクト	許可	すべてのバージョンのVDA
Windows Mediaリダイレクトのバッファーサイズ	5秒	VDA 5、5.5、5.6 FP1
Windows Mediaリダイレクトのバッファーサイズ使用	無効	VDA 5、5.5、5.6 FP1

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDPを使用したオーディオ	許可	VDA for Server OS 7以降
オーディオUDPポートの範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
マルチポートポリシー	プライマリポート（2598）に優先度［高］	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアント COM ポートを自動接続する	無効	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
クライアントLPTポートを自動接続する	無効	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
クライアントCOMポートリダイレクト	禁止	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。
クライアントLPTポートリダイレクト	禁止	すべてのバージョンのVDA。VDA 7.0から7.8ではレジストリで構成します。

ICA/印刷

名前	デフォルト設定	VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのバージョンのVDA
デフォルトプリンター	クライアントのメインプリンターをデフォルトに設定する	すべてのバージョンのVDA
プリンター割り当て	ユーザーの現在のプリンター	すべてのバージョンのVDA
プリンター自動作成イベントログの設定	エラーおよび警告をログに記録する	すべてのバージョンのVDA
セッションプリンター	プリンターの指定なし	すべてのバージョンのVDA
プリンターの自動作成を待機する（デスクトップ）	無効	すべてのバージョンのVDA

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成する	すべてのクライアントプリンターを自動作成する	すべてのバージョンのVDA
汎用ユニバーサルプリンターを自動作成する	無効	すべてのバージョンのVDA
クライアントプリンター名	標準のプリンター名	すべてのバージョンのVDA
プリントサーバーへの直接接続	有効	すべてのバージョンのVDA
プリンタードライバーのマッピングと互換性	規則の指定なし	すべてのバージョンのVDA
プリンタープロパティの保存	クライアントに保存できない場合にのみユーザープロファイルに保存する	すべてのバージョンのVDA
クライアントプリンターの保持と復元	許可	VDA 5、5,5、5.6 FP1

ICA/印刷/ドライバー

名前	デフォルト設定	VDA
付属のプリンタードライバーの自動インストール	有効	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
ユニバーサルドライバーの優先度	EMF; XPS; PCL5c; PCL4; PS	すべてのバージョンのVDA
ユニバーサル印刷の使用	要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する	すべてのバージョンのVDA

ICA/印刷/Universal Print Server

名前	デフォルト設定	VDA
Universal Print Serverの有効化	無効	すべてのバージョンのVDA
Universal Print Server印刷データストリーム（CGP）ポート	7229	すべてのバージョンのVDA
Universal Print Server入力データストリームの最大帯域幅（Kbps）	0	すべてのバージョンのVDA
Universal Print Server Webサービス（HTTP/SOAP）ポート	8080	すべてのバージョンのVDA
負荷分散のためのユニバーサルプリントサーバー		VDAバージョン7.9以降
ユニバーサルプリントサーバーのサービス停止のしきい値	180（秒）	VDAバージョン7.9以降

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷EMF処理モード	EMFスプールファイルを直接挿入する	すべてのバージョンのVDA
ユニバーサル印刷イメージ圧縮制限	最高品質（無損失圧縮）	すべてのバージョンのVDA
ユニバーサル印刷最適化デフォルト	イメージ圧縮 • 必要なイメージ品質：標準品質 • ヘビーウェイト圧縮を有効にする：オフ イメージおよびフォントキャッシュ	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
	• 埋め込みイメージのキャッシュを許可する：オン • 埋め込みフォントのキャッシュを許可する：オン	
	非管理者によるこれらの設定の変更を許可する：オフ	
ユニバーサル印刷プレビューの設定	自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューを使用しない	すべてのバージョンのVDA
ユニバーサル印刷品質制限	制限なし	すべてのバージョンのVDA

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最低暗号化レベル	基本	VDA for Server OS 7以降

ICA/サーバーの制限

名前	デフォルト設定	VDA
サーバーのアイドルタイマーの間隔	0 ミリ秒	VDA for Server OS 7以降

ICA/セッションの制限

名前	デフォルト設定	VDA
切断セッションタイマー	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
切断セッションタイマーの間隔	1,440分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
セッション接続タイマーの間隔	1,440分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降
セッションアイドルタイマーの間隔	1,440分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7以降

ICA/セッション画面の保持

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
セッション画面の保持	許可	すべてのバージョンのVDA
セッション画面の保持のポート番号	2598	すべてのバージョンのVDA
セッション画面の保持のタイムアウト	180秒	すべてのバージョンのVDA

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカルタイムゾーンを検出する	有効	VDA for Server OS 7以降
クライアントのローカルタイムゾーンを使用する	サーバーのタイムゾーンを使用する	すべてのバージョンのVDA

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアント TWAIN デバイス リダイレクト	許可	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化規則	有効（VDA 7.6 FP3以降） 無効（VDA 7.11以降） デフォルトでは、規則は指定されていません。	VDA 7.6 FP3以降
クライアントUSBデバイスリダイレクト	禁止	すべてのバージョンのVDA
クライアントUSBデバイスリダイレクト規則	規則の指定なし	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/視覚表示

名前	デフォルト設定	VDA
シンプルなグラフィック用の優先色数	24ビット/ピクセル	VDA 7.6 FP3以降
ターゲットフレーム数	30fps	すべてのバージョンのVDA
表示品質	中	VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/視覚表示/動画

名前	デフォルト設定	VDA
画質の下限レベル	通常	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
動画圧縮	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
プログレッシブ圧縮のレベル	なし	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
プログレッシブ圧縮のしきい値	2147483647Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降
保持する最低フレーム数	10fps	VDA 5.5、5.6 FP1、VDA for Server OS 7以降、VDA for Desktop OS 7以降

ICA/視覚表示/静止画

名前	デフォルト設定	VDA
エクストラ色圧縮	無効	すべてのバージョンのVDA
エクストラ色圧縮しきい値	8192Kbps	すべてのバージョンのVDA
ヘビーウェイト圧縮	無効	すべてのバージョンのVDA
非可逆圧縮のレベル	中	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
非可逆圧縮のしきい値	2147483647Kbps	すべてのバージョンのVDA

ICA/WebSocket

名前	デフォルト設定	VDA
WebSocket接続	禁止	VDA for Server OS 7以降、VDA for Desktop OS 7以降
WebSocketポート番号	8008	VDA for Server OS 7以降、VDA for Desktop OS 7以降
WebSocket信頼される接続元サーバー一覧	*（すべてのReceiver for WebサイトURLが信頼されます）	VDA for Server OS 7以降、VDA for Desktop OS 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオントレランス	2	VDA for Server OS 7以降
CPU使用率	無効	VDA for Server OS 7以降
CPU使用率から除外するプロセスの優先順位	通常以下および低	VDA for Server OS 7以降
ディスク使用率	無効	VDA for Server OS 7以降
最大セッション数	250	VDA for Server OS 7以降
メモリ使用率	無効	VDA for Server OS 7以降
基本メモリ使用量	負荷なし：768MB	VDA for Server OS 7以降

Profile Management/上級設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのバージョンのVDA
問題が発生する場合にユーザーをログオフ	無効	すべてのバージョンのVDA
ロックされたファイルにアクセスする場合の試行数	5	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
ログオフ時のインターネットCookieファイルの処理	無効	すべてのバージョンのVDA

Profile Management/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのバージョンのVDA
Profile managementの有効化	無効	すべてのバージョンのVDA
除外グループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンのVDA
オフラインプロファイルサポート	無効	すべてのバージョンのVDA
ユーザーストアへのパス	Windows：	すべてのバージョンのVDA
ローカル管理者のログオン処理	無効	すべてのバージョンのVDA
処理済みグループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンのVDA

Profile Management/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。（［処理済みグループ］で指定したすべてのユーザーグループのプロファイルが処理されます）	すべてのバージョンのVDA
クロスプラットフォーム設定の有効化	無効	すべてのバージョンのVDA
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのバージョンのVDA
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのバージョンのVDA
クロスプラットフォーム設定を作成するためのソース	無効	すべてのバージョンのVDA

Profile Management/ファイルシステム/除外

名前	デフォルト設定	VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
除外の一覧 - ディレクトリ	無効。ユーザープロファイルのすべてのフォルダーが同期されます。	すべてのバージョンのVDA
除外の一覧 - ファイル	無効。ユーザープロファイルのすべてのファイルが同期されます。	すべてのバージョンのVDA

Profile Management/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのバージョンのVDA
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのバージョンのVDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可	無効	すべてのバージョンのVDA
ドメイン名を包含	無効	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/AppData（Roaming）

名前	デフォルト設定	VDA
AppData（Roaming）パス	無効。パスは指定されていません。	すべてのバージョンのVDA
AppData（Roaming）のリダイレクト設定	［AppData（Roaming）パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/アドレス帳

名前	デフォルト設定	VDA
アドレス帳パス	無効。パスは指定されていません。	すべてのバージョンのVDA
アドレス帳のリダイレクト設定	［アドレス帳パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/デスクトップ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
デスクトップパス	無効。パスは指定されていません。	すべてのバージョンのVDA
デスクトップのリダイレクト設定	［デスクトップ パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。パスは指定されていません。	すべてのバージョンのVDA
ドキュメントのリダイレクト設定	［ドキュメント パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。パスは指定されていません。	すべてのバージョンのVDA
ダウンロードのリダイレクト設定	［ダウンロード パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。パスは指定されていません。	すべてのバージョンのVDA
お気に入りのリダイレクト設定	［お気に入りパス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。パスは指定されていません。	すべてのバージョンのVDA
リンクのリダイレクト設定	［リンク パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/ミュージック

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
ミュージックパス	無効。パスは指定されていません。	すべてのバージョンのVDA
ミュージックのリダイレクト設定	［ミュージック パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。パスは指定されていません。	すべてのバージョンのVDA
ピクチャのリダイレクト設定	［ピクチャ パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/保存したゲーム

名前	デフォルト設定	VDA
保存したゲームパス	無効。パスは指定されていません。	すべてのバージョンのVDA
保存したゲームのリダイレクト設定	［保存したゲームパス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。パスは指定されていません。	すべてのバージョンのVDA
検索のリダイレクト設定	［検索パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。パスは指定されていません。	すべてのバージョンのVDA
スタートメニューのリダイレクト設定	［スタート メニュー パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/フォルダーのリダイレクト/ビデオ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
ビデオパス	無効。パスは指定されていません。	すべてのバージョンのVDA
ビデオのリダイレクト設定	［ビデオ パス］で指定したUNCパスにリダイレクト	すべてのバージョンのVDA

Profile Management/ログ設定

名前	デフォルト設定	VDA
Active Directory操作	無効	すべてのバージョンのVDA
一般的な情報	無効	すべてのバージョンのVDA
一般的な警告	無効	すべてのバージョンのVDA
ログの有効化	無効	すべてのバージョンのVDA
ファイルシステム操作	無効	すべてのバージョンのVDA
ファイルシステム通知	無効	すべてのバージョンのVDA
ログオフ	無効	すべてのバージョンのVDA
ログオン	無効	すべてのバージョンのVDA
ログファイルの最大サイズ	1048576	すべてのバージョンのVDA
ログファイルへのパス	無効。%SystemRoot%\System32\Logfiles\UserProfileManagerに生成されます	すべてのバージョンのVDA
個人用ユーザー情報	無効	すべてのバージョンのVDA
ログオンおよびログオフ時のポリシー値	無効	すべてのバージョンのVDA
レジストリ操作	無効	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名前	デフォルト設定	VDA
ログオフ時のレジストリ差分	無効	すべてのバージョンのVDA

Profile Management/プロファイル制御

名前	デフォルト設定	VDA
キャッシュしたプロファイルを削除する前の待ち時間	0	すべてのバージョンのVDA
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	すべてのバージョンのVDA
ローカルプロファイル競合の制御	ローカルプロファイルを使用	すべてのバージョンのVDA
既存のプロファイルの移行	ローカルおよび移動	すべてのバージョンのVDA
テンプレートプロファイルへのパス	無効。ユーザーが最初にログオンするコンピューター上のデフォルトのユーザープロファイルから新しいユーザープロファイルが作成されます。	すべてのバージョンのVDA
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのバージョンのVDA
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのバージョンのVDA
すべてのログオンでCitrix固定プロファイルとして使用されるテンプレートプロファイル	無効	すべてのバージョンのVDA

Profile Management/レジストリ

名前	デフォルト設定	VDA
除外の一覧	無効。HKEY_CURRENT_USERハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンのVDA
包含の一覧	無効。HKEY_CURRENT_USERハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Profile Management/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常時キャッシュ	無効	すべてのバージョンのVDA
常時キャッシュサイズ	0MB	すべてのバージョンのVDA
プロファイルストリーム配信	無効	すべてのバージョンのVDA
ストリーム配信ユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルが処理されます。	すべてのバージョンのVDA
待機領域のロックファイルのタイムアウト（日数）	1日	すべてのバージョンのVDA

Receiver

名前	デフォルト設定	VDA
StoreFrontアカウント一覧	ストアの指定なし	VDA for Server OS 7以降、VDA for Desktop OS 7以降

Virtual Delivery Agent

名前	デフォルト設定	VDA
コントローラー登録のIPv6ネットマスク	ネットマスクの指定なし	VDA for Server OS 7以降、VDA for Desktop OS 7以降
コントローラー登録ポート	80	すべてのバージョンのVDA
コントローラーSID	SIDの指定なし	すべてのバージョンのVDA
Controller	Controllerの指定なし	すべてのバージョンのVDA
コントローラーの自動更新を有効にする	有効	VDA for Server OS 7以降、VDA for Desktop OS 7以降
IPv6コントローラー登録のみを使用する	無効	VDA for Server OS 7以降、VDA for Desktop OS 7以降
サイトGUID	GUIDの指定なし	すべてのバージョンのVDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent/HDX 3D Pro

名前	デフォルト設定	VDA
無損失を有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質レベル		VDA 5.5、5.6 FP1

Virtual Delivery Agent/Monitoring

名前	デフォルト設定	VDA
プロセス監視の有効化	無効	VDA 7.11以降
リソース監視の有効化	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6以降
仮想IPループバックプログラム一覧	なし	VDA 7.6以降

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシー設定リファレンス

Dec 05, 2017

ポリシーには、対象のセッションを制御するための設定項目（規則）を追加します。ここでは、その設定項目が依存するほかの設定項目や、関連する設定項目についても説明します。

クイック リファレンス

次の各表は、ポリシーに追加できる設定の一覧です。これらの表では、左側の列がポリシーで制御するセッションの機能を示し、右側の列がその機能に対応する設定を示します。

オーディオ

目的	使用するポリシー設定
複数オーディオデバイスの使用を制御する	オーディオプラグアンドプレイ
クライアント側のマイクからのオーディオ入力を制御する	クライアントマイクリダイレクト
クライアント側のオーディオの音質を制御する	音質
クライアント側のスピーカーの使用を制御する	クライアントオーディオリダイレクト

帯域幅の制限

目的	使用するポリシー設定
クライアントオーディオマッピングで使用される帯域幅を制限する	オーディオリダイレクトの最大帯域幅（Kbps）、または オーディオリダイレクトの最大帯域幅（%）
クリップボードマッピングで使用される帯域幅を制限する	クリップボードリダイレクトの最大帯域幅（Kbps）、または クリップボードリダイレクトの最大帯域幅（%）
クライアント側ドライブへのアクセスで使用される帯域幅を制限する	ファイルリダイレクトの最大帯域幅（Kbps）、または ファイルリダイレクトの最大帯域幅（%）
HDX MediaStreamマルチメディアアクセラレーション	HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（Kbps）、または HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（%）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントセッションで使用される帯域幅を制限する	セッション全体の最大帯域幅
印刷	プリンターリダイレクトの最大帯域幅（Kbps）、または プリンターリダイレクトの最大帯域幅（%）
カメラやスキャナーなどのTWAINデバイスで使用される帯域幅を制限する	TWAINデバイスリダイレクトの最大帯域幅（Kbps）、または TWAINデバイスリダイレクトの最大帯域幅（%）
USBデバイスで使用される帯域幅を制限する	USBデバイスリダイレクトの最大帯域幅（Kbps）、または USBデバイスリダイレクトの最大帯域幅（%）

クライアント側のドライブやデバイスのリダイレクト

目的	使用するポリシー設定
ログオン時にクライアント側ドライブに接続する機能を制御する	クライアントドライブに自動接続する
サーバーとローカルのクリップボード間でのデータ転送を制御する	クライアントクリップボードリダイレクト
クライアント側ドライブのマッピングを制御する	クライアントドライブリダイレクト
クライアント側ハードディスクドライブの使用を制御する	クライアント側固定ドライブ、および クライアントドライブリダイレクト
クライアント側フロッピーディスクドライブの使用を制御する	クライアント側フロッピードライブ、および クライアントドライブリダイレクト
クライアント側ネットワークドライブの使用を制御する	クライアント側ネットワークドライブ、および クライアントドライブリダイレクト
クライアント側CD、DVD、およびブルーレイドライブの使用を制御する	クライアント側光学式ドライブ、および クライアントドライブリダイレクト

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアント側リムーバブルドライブの使用を制御する	クライアント側リムーバブルドライブ、および クライアントドライブリダイレクト
デジタルカメラやスキャナーなどのクライアント側TWAINデバイスの使用および転送されるイメージデータの圧縮レベルを制御する	クライアント TWAIN デバイス リダイレクト TWAIN圧縮レベル
クライアント側USBデバイスの使用を制御する	クライアントUSBデバイスリダイレクト、および クライアントUSBデバイスリダイレクト規則
WANを介した接続でのクライアント側ドライブへの書き込み速度を改善する	非同期書き込みを使用する

コンテンツリダイレクト

目的	使用するポリシー設定
サーバーからユーザーデバイス側にコンテンツをリダイレクトするかどうかを制御する	ホストからクライアントへのリダイレクト

デスクトップ UI

目的	使用するポリシー設定
セッションでの壁紙の表示を制御する	デスクトップの壁紙
ウィンドウの内容を表示したままドラッグする機能を制御する	ドラッグ中にウィンドウの内容を表示する

グラフィック/マルチメディア

目的	使用するポリシー設定
仮想デスクトップがクライアント側に送信されるときの、1秒あたりのフレームの最大数を設定する	ターゲットフレーム数
ユーザーデバイス側に表示されるイメージの表示品質を制御する	表示品質
セッションでのFlashコンテンツのレンダリングを制御する	Flashアクセラレーションのデフォルトの動作

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションで特定のWebページ上のFlashコンテンツを表示するかどうかを制御する	• Flashサーバー側でのコンテンツ取得URLリスト • Flash URL互換性リスト • Flashビデオフォールバック防止ポリシー設定 • Flashビデオフォールバック防止エラー*.swf
サーバー側でレンダリングするビデオの圧縮の制御	• 圧縮にビデオコーデックを使用 • ビデオコーデックへのハードウェアエンコーディングの使用
HTML5マルチメディアWebコンテンツのユーザーへの配信の制御	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先度

目的	使用するポリシー設定
マルチストリーム接続のICAトラフィックのポートを指定して、各ポートのネットワーク 優先度を定義する	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にする	マルチストリーム（コンピューターポリシーおよびユーザーポリシー）

印刷

目的	使用するポリシー設定
ログオン時のクライアントプリンターの自動作成を制御する	クライアントプリンターを自動作成する、および クライアントプリンターリダイレクト
プリンタープロパティの保存先を制御する	プリンタープロパティの保存
印刷ジョブをサーバーから直接プリンターに送信するか、クライアント経由で送信するかを制御する	プリントサーバーへの直接接続
クライアント側プリンターの使用を制御する	クライアントプリンターリダイレクト
クライアントプリンターおよびネットワークプリンターの自動作成時に、Windowsに付属のプリンタードライバーを自動的にインストールするかどうかを制御する	付属のプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーの使用を制御する	ユニバーサル印刷の使用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ローミングユーザーの接続方法に応じて自動作成されるプリンターを制御する	デフォルトプリンター
負荷を分散し、Universal Print Serverのフェールオーバーしきい値を設定する	負荷分散のためのユニバーサルプリントサーバー Universal Print Serverのサービス停止のしきい値

注： デスクトップまたはアプリケーションセッションでは、ポリシーを使用してスクリーンセーバーを有効にすることはできません。スクリーンセーバーが必要なユーザーの場合は、ユーザーデバイスにスクリーンセーバーを実装できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICAのポリシー設定

Dec 05, 2017

［ICA］カテゴリには、ICAリスナーの接続とクリップボードのマッピングに関する設定項目が含まれています。

アダプティブトランスポート

この設定では、EDT上のデータトランスポートをプライマリとし、TCPにフォールバックすることを許可または禁止します。

デフォルトでは、アダプティブトランスポートは無効（**オフ**）になっており、常にTCPが使用されます。

1. Studioで、ポリシー設定「HDXアダプティブトランスポート」を有効にします（デフォルトでは無効）。また、この機能を、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。
2. ポリシー設定を有効にするには、値を **[優先]** に設定し、 **[OK]** をクリックします。

    [優先] 。可能な場合、Adaptive transport over EDTが使用され、TCPにフォールバックします。

    [診断モード] 。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングでのみお勧めします。

    [オフ] 。TCPが強制的にオンになり、EDTが無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

アプリケーションの起動待機タイムアウト

この設定では、セッションで最初のアプリケーションの起動を待機する待機タイムアウトの値をミリ秒単位で指定します。この時間を超えた後にアプリケーションが起動されると、セッションは終了します。

デフォルトの時間（1万ミリ秒）を選択するか、数値をミリ秒単位で指定できます。

クライアントクリップボード リダイレクト

この設定項目では、 クライアント側のクリップボードをサーバーのクリップボードにマップすることを許可または 禁止します。

デフォルトでは クリップボードリダイレクトは許可されます。

セッションとローカルの クリップボード間でデータを転送できなくるすには、 ［禁止］を選択します。ただし、セッション内で動作する アプリケーション間でのクリップボードを介したデータ転送は無効になりません。

この 設定を許可したら、 ［クリップボード リダイレクトの最大帯域幅（Kbps）］設定または ［クリップボード リダイレクトの最大帯域幅（%）］設定を使用して、 クライアント接続でクリップボードが使用できる帯域幅の上限を設定します。

クライアントクリップボードに書き込みを許可する形式

［クライアント クリップボードの書き込み制限］設定が有効な場合、ホスト側のクリップボードデータがクライアントエンドポイント側に共有されません。この［クライアント クリップボードに書き込みを許可する形式］設定では、特定の種類のクリップボードデータの共有を許可します。これを行うには、この設定項目を有効にして、許可するデータ形式を追加します。

以下のシステム定義のクリップボードデータ形式を追加できます。

- CF_TEXT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

また、以下のXenAppおよびXenDesktop用のカスタム定義のデータ形式を追加できます。
- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML形式

HTML形式はデフォルトで無効になっています。この機能を有効にするには、以下の手順に従います。

- **[クライアントクリップボードリダイレクト]**が許可されていることを確認します。
- **[クライアント クリップボードの書き込み制限]**が有効になっていることを確認します。
- **[クライアント クリップボードに書き込みを許可する形式]**で、**[HTML 形式]**（およびサポートを希望するほかの形式）のエントリを追加します。

注： HTML形式のクリップボードコピーのサポート（HTML形式）を有効にすると、コピーされたコンテンツのソースのあらゆるスクリプト（存在する場合）が、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルをHTMLファイルとして保存して実行する場合に限り、ライブになります。

カスタム定義のデータ形式を追加することもできます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

[クライアント クリップボードリダイレクト]設定または[クライアント クリップボードの書き込み制限]設定で[禁止]が設定されている場合、この設定項目は無視されます。

デスクトップの起動

この設定により、VDAのDirect Access Usersグループの非管理者ユーザーによるICAコネクションを使ったVDA上のセッションへの接続を許可または禁止します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、管理者以外のユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAのDirect Access Usersグループの非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっているかに関わらずVDAに接続できます。この設定は、VDAのDirect Access Usersグループではない非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっているかに関わらずVDAに接続できません。

ICAリスナー接続タイムアウト

注： この設定は、Virtual Delivery Agent 5.0、5.5、および5.6 Feature Pack 1にのみ適用されます。

この設定では、ICAプロトコルによる接続が完了するまでの最大待機時間を指定します。

デフォルトの最大待機時間は、120000ミリ秒（2分）です。

ICAリスナーポートの番号

この設定では、サーバー上のICAプロトコルで使用されるTCP/IPポートを指定します。

デフォルトのポート番号は、1494に設定されています。

ほかのポートを指定する場合は、0から65535の範囲で、ほかのウェルノウンポート番号と競合しない番号を使用してください。変更したポート番号を有効にするには、サーバーを再起動する必要があります。サーバー上のポート番号を変更した場合は、そのサーバーに接続するCitrix Receiverやプラグインソフトウェア側でもポート番号を変更する必要があります。

クライアント接続での非公開アプリケーションの起動

この設定項目では、サーバー上のリモートデスクトップを介した開始アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上のリモートデスクトップを介した開始アプリケーションの起動は許可されません。

ログオフチェッカー起動遅延

この設定では、ログオフチェッカー起動の遅延時間を指定します。このポリシーを使用して、クライアントセッションがセッション切断を待機する時間（秒単位）を設定します。

この設定により、ユーザーがサーバーからログオフするのにかかる時間を長くすることもできます。

クライアントクリップボードの書き込み制限

この設定項目を有効にすると、ホスト側のクリップボードデータがクライアントエンドポイント側に共有されなくなります。この場合、特定のデータの共有を許可するには、［クライアントクリップボードに書き込みを許可する形式］設定を使用します。

デフォルトでは、禁止に設定されています。

セッションクリップボードの書き込み制限

この設定項目を有効にすると、クライアント側のクリップボードデータがユーザーセッション側に共有されなくなります。この場合、特定のデータの共有を許可するには、［セッションクリップボードに書き込みを許可する形式］設定を使用します。

デフォルトでは、禁止に設定されています。

セッションクリップボードに書き込みを許可する形式

© 1999-2017 Citrix Systems, Inc. All rights reserved.

［セッション クリップボードの書き込み制限］設定が有効な場合、クライアント側のクリップボードデータはセッション内のアプリケーション側に共有されません。この［セッション クリップボードに書き込みを許可する形式］設定では、特定の種類のクリップボードデータの共有を許可します。

以下のシステム定義のクリップボードデータ形式を追加できます。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

また、以下のXenAppおよびXenDesktop用のカスタム定義のデータ形式を追加できます。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML形式

HTML形式はデフォルトで無効になっています。この機能を有効にするには、以下の手順に従います。

- **［クライアントクリップボードリダイレクト］**が許可されていることを確認します。
- **［セッション クリップボードの書き込み制限］**が有効になっていることを確認します。
- **［セッション クリップボードに書き込みを許可する形式］**で、**［HTML 形式］**（およびサポートを希望するほかの形式）のエントリを追加します。

注： HTML形式のクリップボードコピーのサポート（HTML形式）を有効にすると、コピーされたコンテンツのソースのあらゆるスクリプト（存在する場合）が、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルをHTMLファイルとして保存して実行する場合に限り、ライブになります。

カスタム定義のデータ形式を追加することもできます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

［クライアント クリップボード リダイレクト］設定または［セッション クリップボードの書き込み制限］設定で［禁止］が設定されている場合、この設定項目は無視されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントの自動再接続のポリシー設定

Dec 05, 2017

［クライアントの自動再接続］カテゴリには、セッションの自動再接続の制御に関する設定項目が含まれています。

クライアントの自動再接続

この設定では、接続が中断した後で同じクライアントから自動再接続することを許可または禁止します。

Citrix Receiver for Windows 4.7以降のクライアントの自動再接続では、Citrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、サーバーからクライアントにクライアントの自動再接続が同期されます。以前のバージョンのCitrix Receiver for Windowsでは、クライアントの自動再接続を構成するのには、Studioポリシーを使用してレジストリまたはdefault.icaファイルを変更します。

クライアントの自動再接続を許可すると、ユーザーは接続が切断された時点の状態に戻って作業を再開できます。自動再接続機能では、切断された接続が検出されてそのセッションにユーザーが再接続されます。

セッションIDと資格情報のキーが含まれているCitrix ReceiverのCookieを使用していない場合は、自動再接続によって新しいセッションが開始されることがあります。つまり、既存のセッションに再接続されるのではありません。再接続に時間がかかってCookieの有効期限が切れた場合や、ユーザーが資格情報を入力する必要がある場合には、Cookieは使用されません。また、ユーザーが自分で切断した場合、クライアントの自動再接続はトリガーされません。

再接続中は、セッションウィンドウが灰色になります。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。セッションがタイムアウトになると、接続は切断されます。

アプリケーションセッションで自動再接続が許可されている場合は、セッションが再接続するまでの残り時間を指定するカウントダウンタイマーが通知領域に表示されます。Citrix Receiverによる再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。

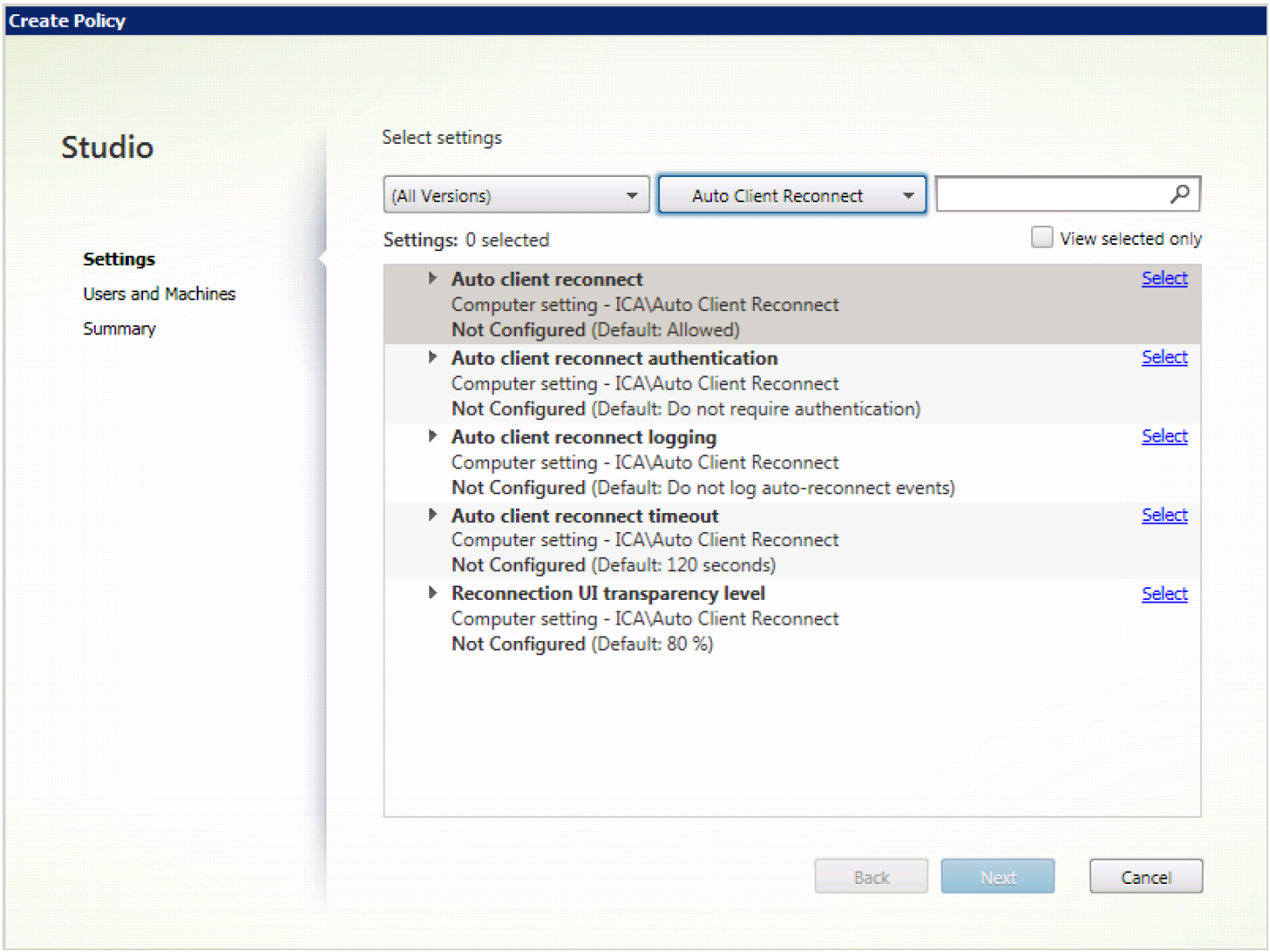
ユーザーセッションでは、自動再接続が許可されている場合、Citrix Receiverは、指定された時間、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。デフォルトでは、この時間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、クライアントの自動再接続が許可されます。

クライアントの自動再接続を無効にするには

1. Citrix Studioを開始します。
2. **［クライアントの自動再接続］**ポリシーを開きます。
3. ポリシーを**［禁止］**に設定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



クライアントの自動再接続時の認証

この設定では、自動再接続時に認証処理を必要とするかどうかを制御します。［認証を必要とする］を選択すると、クライアントの自動再接続時に認証のためのダイアログボックスが開きます。

ユーザーが最初にログオンすると、そのユーザーの資格情報は暗号化されてメモリに格納され、その暗号キーを含んだCookieが作成されます。このCookieは、Citrix Receiverに送信されます。この設定項目を構成して［認証を必要とする］を選択すると、Cookieは使用されなくなります。その代わりに、切断セッションへの再接続時に、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

デフォルトでは、認証は要求されません。

クライアントの自動再接続時の認証を変更するには

1. Citrix Studioを開始します。
2. **［クライアントの自動再接続時の認証］**ポリシーを開きます。
3. 認証を有効または無効にします。
4. **［OK］**をクリックします。

クライアントの自動再接続のログ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定では、クライアントの自動再接続イベントをログに記録するかどうかを制御します。

ログを有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。これらのイベントは、そのイベントが発生した個々のサーバーのシステムログに記録されます。

デフォルトでは、ログは無効になっています。

クライアントの自動再接続時のロギングを変更するには

1. Citrix Studioを開始します。
2. **[クライアントの自動再接続のログ]** ポリシーを開きます。
3. ロギングを有効または無効にします。
4. **[OK]** をクリックします。

クライアントの自動再接続のタイムアウト

デフォルトでは、クライアントの自動再接続タイムアウトは120秒に設定されます。自動クライアント接続の構成可能なタイムアウトの最大値は300秒です。

クライアントの自動再接続のタイムアウトを変更するには

1. Citrix Studioを開始します。
2. **[クライアントの自動再接続のタイムアウト]** ポリシーを開きます。
3. タイムアウト値を編集します。
4. **[OK]** をクリックします。

再接続UIの透過レベル

Studioポリシーを使用すると、セッション画面の保持の再接続時に、XenAppまたはXenDesktopのセッションウィンドウに適用される不透明度レベルを構成できます。

デフォルトでは、再接続UIの透明度は、80に設定されています。

再接続ユーザーインターフェイスの不透明度レベルを変更するには

1. Citrix Studioを開始します。
2. **再接続UIの透明度レベル**ポリシーを開きます。
3. 値を編集します。
4. **[OK]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

オーディオのポリシー設定

Dec 05, 2017

［オーディオ］カテゴリには、ユーザーデバイスがパフォーマンスを低下させずにセッションでオーディオを送受信するこ
を許可するための設定項目が含まれています。

UDPでのオーディオ リアルタイムトランスポート

この設定 では、ホストと ユーザーデバイス間のユーザーデータグラムプロトコル（UDP）を使用したオーディオリアルタイ
ムトランスポート（RTP）でのオーディオ転送を許可または禁止します。この設定を 無効にすると、オーディオがTCP上で送
受信されます。

デフォルトでは 許可されます。

オーディオプラグアンド プレイ

この設定 では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。

デフォルトでは 許可されます。

この設定項目 は、WindowsサーバーOSマシンのみに適用されます。

音質

この設定では、ユーザーセッション内で受信されるサウンドの品質を指定します。

デフォルトでは、［高 - 高品位オーディオ］が指定されています。

音質を制御するには、次のオプションから1つを選択します。

- 狭帯域接続には［低 - 低速接続用］を選択します。この設定では、サウンドデータが最大16Kbpsまで圧縮されてから転送されます。圧縮により、再生または録音される音質は著しく低下しますが、モデム接続などの狭帯域幅接続に最適です。
- VoIP（Voice over IP）アプリケーションを配信する場合、512Kbps未満の低速なネットワーク接続回線でメディアアプリケーションを配信する場合、または輻輳やパケット損失が生じる環境では、［中 - スピーチに最適化］を選択します。高速にエンコーディングされるため、ソフトフォンや統合コミュニケーションアプリケーションなどのメディア処理をサーバー側で行う場合に適しています。
  この音質レベルでは、オーディオデータが最大64Kbpsまで圧縮されてからユーザーデバイスに転送されます。この圧縮により、ユーザーデバイス上でのオーディオ再生の品質はやや低下しますが、遅延は少なくなり、帯域幅の消費も少なくなります。VoIPアプリケーションで十分な音質が得られない場合は、［UDPでのオーディオリアルタイムトランスポート］設定で［許可］を選択します。

  現在、この音質が設定されている場合のみ、UDP上のリアルタイムトランスポート（RTP）がサポートされています。この音質は、非常に低速なネットワーク接続（512Kbps未満）や、ネットワークで輻輳やパケット損失などが生じる環境で使用します。

- 帯域幅が十分で、サウンドの音質が重要である場合は、［高 - 高品位オーディオ］を選択します。この設定では、ネイティブのサウンドデータを再生または録音できます。サウンドデータは、CDレベルの音質が維持される112Kbpsの高品質レベルで圧縮されます。ただし、大量のネットワークデータ転送が要求されるため、CPUおよびネットワークに負担がかかる場合があります。

録音と再生を同時に行った場合、消費帯域幅は2倍になります。

帯域幅の上限を指定するには、［オーディオリダイレクトの最大帯域幅（Kbps）］設定または［オーディオリダイレクトの最

© 1999-2017 Citrix Systems, Inc. All rights reserved.

大帯域幅（%）］設定を使用します。

クライアントオーディオ リダイレクト

この設定では、サーバーでホストされているアプリケーションから、ユーザーデバイスにインストールされている サウンドバイスを介してサウンドを再生したり、 オーディオ入力を録音したりすることを許可または禁止します。

デフォルトでは 許可されます。

この設定を許可したら、 オーディオの再生や録音で使用できる帯域幅の上限を設定します。これにより、 アプリケーションのパフォーマンスが向上しますが、音質が低下することがあります。 録音と再生を同時に行った場合、 消費帯域幅は2倍になります。 帯域幅の上限を指定するには、 ［オーディオ リダイレクトの最大帯域幅（Kbps）］設定または ［オーディオ リダイレクトの最大帯域幅（%）］設定を使用します。

Windowsサーバー OSマシンで複数のオーディオデバイスをサポートするには、 ［オーディオ プラグアンドプレイ］設定で［有効］が選択されていることも確認してください。

重要： ［クライアントオーディオリダイレクト］設定で［禁止］を選択すると、すべてのHDXオーディオ 機能が無効になります。

クライアント マイクリダイレクト

この設定 では、クライアント側のマイクのリダイレクトを有効または無効にします。この設定を有効にすると、セッション内でクライアント側の マイクを使ってオーディオを録音できるようになります。

デフォルトでは 許可されます。

セキュリティの設定により、 ユーザーデバイスに信頼されていないサーバーからユーザーデバイス側のマイクに アクセスしたときに、警告メッセージが表示されます。ユーザーは、このメッセージに対してアクセスを許可したり拒否したりできます。この警告は、ユーザーがCitrix Receiver側で 無効にできます。

Windowsサーバー OSマシンで複数のオーディオデバイスをサポートするには、 ［オーディオ プラグアンドプレイ］設定で［有効］が選択されていることも確認してください。

ユーザーデバイス側で ［クライアント オーディオリダイレクト］設定が無効になっている場合、この設定 は無視されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

帯域幅のポリシー設定

Dec 05, 2017

［帯域幅］カテゴリには、クライアントセッションでの消費帯域幅に関する問題を避けるための設定項目が含まれています。

重要： これらのポリシー設定を ［マルチストリーム］設定と一緒に使用すると、意図したとおりに動作しなくなる場合があります。 ポリシーで［マルチストリーム］設定を使用する場合は、帯域幅を 制限するポリシー設定を追加しないようにしてください。

オーディオ リダイレクトの最大帯域幅（Kbps）

この設定では、クライアント側デバイスによるオーディオの再生や 録音で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［オーディオ リダイレクトの最大帯域幅（%）］設定 の両方を指定した場合、より高い制限（より小さい値）の 設定が適用されます。

オーディオ リダイレクトの最大帯域幅（%）

この設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［オーディオ リダイレクトの最大帯域幅（Kbps）］設定 の両方を指定した場合、より高い制限（より小さい値）の 設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］ 設定も使用する必要があります。

USB デバイスリダイレクトの最大帯域幅（Kbps）

この設定項目では、クライアント側のUSBデバイスに アクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［USBデバイスリダイレクトの最大帯域幅（%）］設定の 両方を指定した場合、より高い 制限（より小さい値）の設定が適用されます。

USB デバイスリダイレクトの最大帯域幅（%）

この設定では、 クライアント側のUSBデバイスにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［USBデバイスリダイレクトの最大帯域幅（Kbps）］設定の 両方を指定した場合、より高い 制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］ 設定も使用する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クリップボード リダイレクトの最大帯域幅（Kbps）

この設定項目では、セッションとローカルのクリップボード間でのデータ 転送で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［クリップボードリダイレクトの最大帯域幅（%）］ 設定の 両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

クリップボード リダイレクトの最大帯域幅（%）

この設定項目では、セッションと ローカルのクリップボード間でのデータ転送で使用可能な最大帯域幅を、セッション全体に対する割合で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［クリップボードリダイレクトの最大帯域幅（Kbps）］設定の 両方を指定した場合、 より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］ 設定も使用する必要があります。

COM ポート リダイレクトの最大帯域幅 (Kbps)

注： Virtual Delivery Agent 7.0～7.8では、レジストリを使ってこの設定を構成します。「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。
この設定では、クライアント側COMポートにアクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。この設定および［COMポートリダイレクトの最大帯域幅（%）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

COM ポート リダイレクトの最大帯域幅 (%)

注： Virtual Delivery Agent 7.0～7.8では、レジストリを使ってこの設定を構成します。「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。
この設定では、クライアント側COMポートにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［COMポートリダイレクトの最大帯域幅（Kbps）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する［セッション全体の最大帯域幅］設定も使用する必要があります。

ファイル リダイレクトの最大帯域幅（Kbps）

この設定では、 クライアント側ドライブにアクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［ファイル リダイレクトの最大帯域幅（%）］ 設定の 両方を指定した場合、より高い制限（より小さい値）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

の 設定が適用されます。

ファイル リダイレクトの最大帯域幅（%）

この設定では、クライアント側ドライブにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する 割合で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［ファイル リダイレクトの最大帯域幅（Kbps）］の 両方を指定した場合、より高い制限 （より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］ 設定も使用する必要があります。

HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（Kbps）

この設定では、HDX MediaStreamマルチメディア アクセラレーションによりストリーム 配信されるオーディオやビデオで使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（%）］ 設定の 両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

HDX MediaStreamマルチメディアアクセラレーションの最大帯域幅（%）

この設定では、HDX MediaStreamマルチメディアアクセラレーションによりストリーム配信されるオーディオや ビデオで使用可能な最大帯域幅を、 セッション全体に対する割合で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および［HDX MediaStreamマルチメディア アクセラレーションの最大帯域幅（%）］設定の 両方を指定した場合、より高い制限（ より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を 指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

LPTポートリダイレクトの最大帯域幅（Kbps）

注： Virtual Delivery Agent 7.0～7.8では、レジストリを使ってこの設定を構成します。「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。
この設定では、クライアント側LPTポートを使用する印刷ジョブで使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［LPTポートリダイレクトの最大帯域幅（%）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

LPTポートリダイレクトの最大帯域幅（%）

注： Virtual Delivery Agent 7.0～7.8では、レジストリを使ってこの設定を構成します。「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。
この設定では、クライアント側LPTポートを使用する印刷ジョブで使用可能な最大帯域幅を、セッション全体に対する割合で

© 1999-2017 Citrix Systems, Inc. All rights reserved.

指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［LPTポートリダイレクトの最大帯域幅（Kbps）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する［セッション全体の最大帯域幅］設定も使用する必要があります。

セッション全体の最大帯域幅

この設定では、 セッションで使用可能な総帯域幅の最大値を、キロビット/秒（Kbps）単位で 指定します。

適用できる帯域幅の上限は、10Mbps（10,000Kbps）です。デフォルトでは、上限なし （0）が指定されています。

狭帯域幅接続で、セッションでの 使用帯域幅が原因でほかのアプリケーションでのデータ転送パフォーマンスが低下する 場合に、この設定を使用します。

プリンター リダイレクトの最大帯域幅（Kbps）

この設定では、 クライアント側プリンターにアクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［プリンターリダイレクトの最大帯域幅（%）］設定の 両方を指定した場合、 より高い制限（より小さい値）の設定が適用されます。

プリンター リダイレクトの最大帯域幅（%）

この設定では、クライアント側プリンターにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する 割合で指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［プリンターリダイレクトの最大帯域幅（Kbps）］設定の 両方を指定した場合、 より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を 指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

TWAINデバイス リダイレクトの最大帯域幅（Kbps）

この設定では、 クライアント側TWAINデバイスにアクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトでは、 上限なし（0）が指定されています。

この設定および ［TWAIN デバイスリダイレクトの最大帯域幅（%）］設定の 両方を指定した場合、より高い 制限（より小さい値）の設定が適用されます。

TWAINデバイスリダイレクトの最大帯域幅（%）

この設定では、クライアント側TWAINデバイスにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割

© 1999-2017 Citrix Systems, Inc. All rights reserved.

合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［TWAINデバイスリダイレクトの最大帯域幅（Kbps）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する［セッション全体の最大帯域幅］設定も使用する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

双方向のコンテンツリダイレクトのポリシー設定

Dec 05, 2017

双方向のコンテンツリダイレクトの設定セクションには、クライアントからホスト（およびホストからクライアント）へのURLリダイレクトを有効にするか無効にするかのポリシー設定が含まれています。サーバーポリシーはCitrix Studioで設定し、クライアントポリシーは、Citrix Receiverグループポリシーオブジェクト管理用テンプレートで設定します。

URLリダイレクトに関しては、ホストからクライアントへのリダイレクトおよびクライアント用のローカルアプリケーションアクセスが利用可能ですが、ドメインに参加しているWindowsクライアントに関しては、双方向のコンテンツリダイレクトを使用することをお勧めします。

双方向のコンテンツリダイレクトを利用するには、XenAppまたはXenDesktop 7.13以降に加えて、Citrix Receiver for Windows 4.7以降が必要です。

Important

- リダイレクト規則によってループが構成されないように注意してください。たとえば、VDAのクライアント規則で「https://www.citrix.com」に設定され、クライアントのVDA規則で同じURLが設定されていると無限ループになる可能性があります。
- サポート対象は、ドメイン参加のエンドポイントのみです。
- 明示的なURLリダイレクトのみがサポートされます（Webブラウザーのアドレスバーに表示されるURLや、ブラウザによっては、ブラウザー内ナビゲーションで発見できるURLだけが正しくリダイレクトされます）。短縮URLはサポートされていません。
- 双方向のコンテンツリダイレクトに対応しているのは、Internet Explorer 8から11のみです。Internet Explorerは、ユーザーデバイスとVDAの双方で使用する必要があります。
- 双方向のコンテンツリダイレクトには、Internet Explorerブラウザー用のアドオンが必要です。詳しくは、「Webブラウザーアドオンの登録」を参照してください。
- セッションの起動に関する問題でリダイレクトが失敗した場合のフォールバックメカニズムはありません。
- 2つのアプリケーションが複数のStoreFrontアカウントで同じ表示名に設定されていた場合、プライマリStoreFrontアカウントの表示名が起動に使用されます。
- Citrix Receiver for Windowsのみがサポートされます。
- 新しいWebブラウザーのウィンドウが表示されるのは、URLがクライアントにリダイレクトされた場合だけです。Webブラウザーを開いている状態でURLがVDAにリダイレクトされると、リダイレクトされたURLが新しいタブで開かれます。
- ドキュメント、メール、PDFなどのファイルの埋め込みリンクをサポートしています。
- この機能は、デスクトップセッションでもアプリケーションセッションでも使用できますが、これとは異なり、ローカルアプリケーションアクセスのURLリダイレクトは、デスクトップセッションでしか使用できません。
- URLリダイレクトでローカルアプリケーションアクセスが有効になっている場合（VDAまたはクライアントにおいて）、双方向のコンテンツリダイレクトは無効です。

ホストからクライアントおよびホストからホストへのリダイレクト

Citrix Studioを使用して、ホストからクライアント（クライアント側）とホストからホスト（VDA側）のリダイレクトポリシーを構成します。

デフォルトでは、双方向のコンテンツリダイレクトは**禁止されています**。

双方向のコンテンツリダイレクトを有効化するには

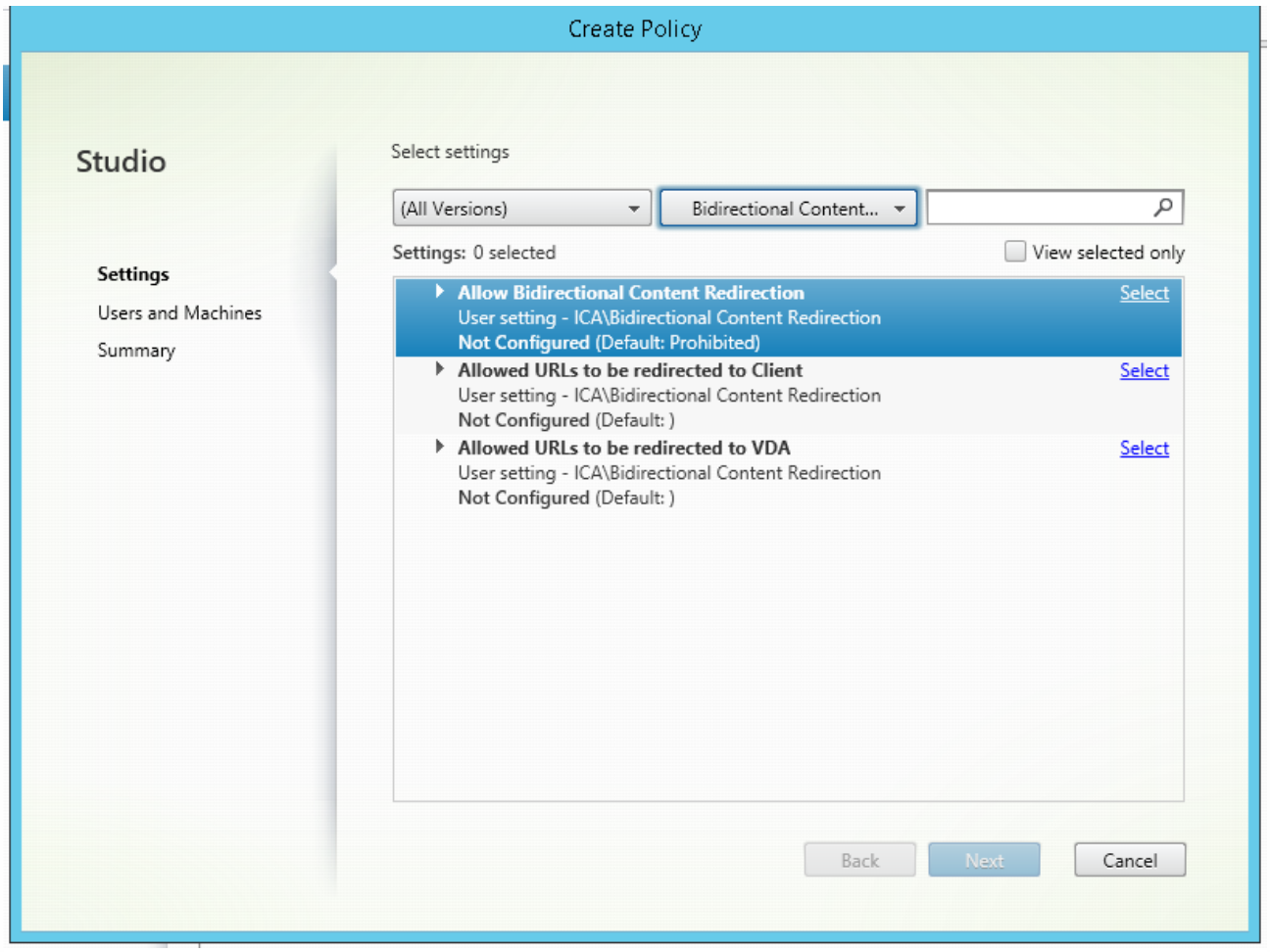
URLが複数ある場合、URLを1つずつ指定してもよいですし、セミコロンで区切ったURLの一覧で指定しても構いません。ワィ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ルドカード文字としてアスタリスク（*）をドメイン名に使用できます。次に例を示します。

http://*.citrix.com; http://www.google.com

1. Citrix Studioを起動します。
2. **[双方向のコンテンツリダイレクト]** ポリシーを開きます。
3. **[双方向のコンテンツリダイレクトを許可する]** を選択し、 **[許可]** を選んで、 **[OK]** をクリックします。このオプションを許可しないと、この手順を完了できません。
4. **[クライアントへのリダイレクトを許可するURL]** を選択し、URLまたはURLの一覧を指定するか、またはデフォルト値から選択します。
5. **[VDAへのリダイレクトを許可するURL]** を選択し、URLまたはURLの一覧を指定するか、またはデフォルト値から選択します。



クライアントからホスト（VDA）およびクライアントからクライアントへのリダイレクト

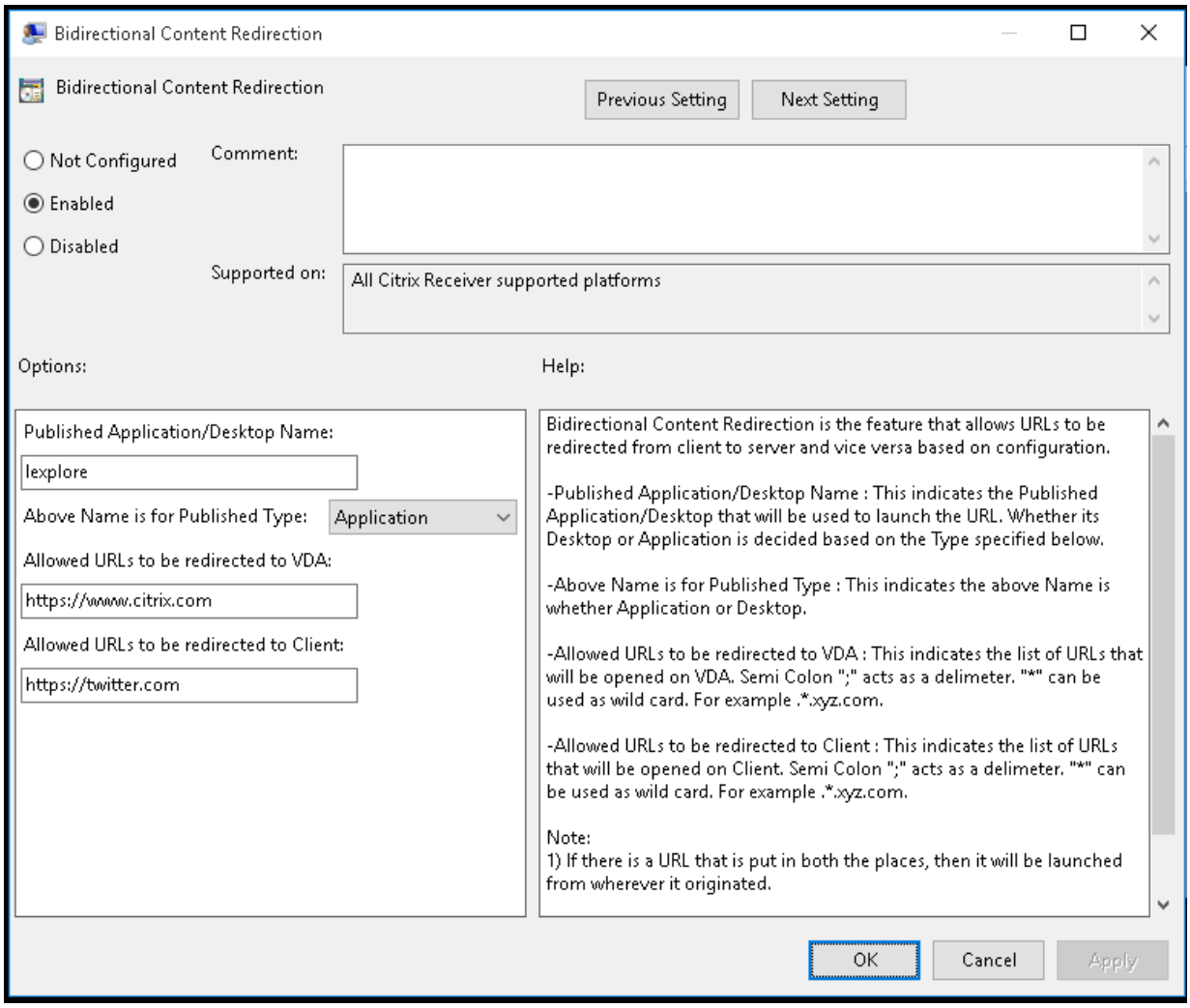
Citrix Receiverグループポリシーオブジェクト管理テンプレートを使って、クライアントからホスト（VDA側）およびクライアントからクライアント（クライアント側）へのリダイレクトを構成します。

双方向のコンテンツリダイレクトを有効化するには

URLが複数ある場合、URLを1つずつ指定してもよいですし、セミコロンで区切ったURLの一覧で指定しても構いません。ワイルドカード文字としてアスタリスク（*）を使用できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

詳しくは、Citrix Receiverドキュメントの「双方向のコンテンツリダイレクトの構成」を参照してください。



Webブラウザーアドオンの登録

双方向のコンテンツリダイレクトには、Internet Explorerブラウザー用のアドオンが必要です。

以下のコマンドを実行して、Internet Explorer用のアドオンを登録したり登録解除したりできます。

- クライアントデバイス上でアドオンを登録する場合： \redirector.exe /regIE
- クライアントデバイス上でアドオンの登録を解除する場合： \redirector.exe /unregIE
- VDA上でアドオンを登録する場合： \VDARedirector.exe /regIE
- VDA上でアドオンの登録を解除する場合： \VDARedirector.exe /unregIE

たとえば、Citrix Receiverを実行するデバイス上でInternet Explorer用のアドオンを登録するには、次のコマンドを実行します。

```
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
```

また、VDA for Windows Server OSが動作するサーバー上でInternet Explorer用のアドオンを登録するには、次のコマンドを実行します。

```
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regIE
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントセンサーのポリシー設定

Dec 05, 2017

クライアントセンサーセクションには、ユーザーセッションでのモバイルデバイスのセンサー情報の制御に関するポリシー設定が含まれています。

クライアントデバイスの位置情報をアプリケーションで使用する

この設定では、セッション内のアプリケーションをモバイルデバイス上で使用する場合に、そのモバイルデバイスの位置情報をアプリケーションで使用することを許可または禁止します。

デフォルトでは、禁止されます。

位置情報の使用が禁止されている場合、アプリケーションからの位置情報の取得要求に対して「アクセス拒否」が返されます。

位置情報の使用が許可されている場合でも、Citrix Receiverからの位置情報の要求を拒否することで、位置情報の使用をユーザーが拒否できます。AndroidおよびiOSデバイスでは、そのセッションで最初に位置情報への要求が発生したときにメッセージが表示されます。

[クライアントデバイスの位置情報をアプリケーションで使用する]設定をサポートするアプリケーションを開発する場合は、以下の点に注意してください。

- 位置情報が常に使用可能であるとは限りません。これは、以下の理由によります。
  - 位置情報の使用をユーザーが拒否する可能性がある。
  - アプリケーションを実行している間に位置情報が提供されない、または位置が変化する可能性がある。
  - 位置情報の提供をサポートしないほかのデバイスからアプリケーションに再接続する可能性がある。
- 位置情報をサポートするアプリケーションの設定として、以下の点を考慮してください。
  - 位置情報の使用をデフォルトで無効にする。
  - アプリケーションの実行時にユーザーが位置情報の使用を許可したり禁止したりできる。
  - アプリケーションでキャッシュされた位置情報データをユーザーが消去できる（ただし、Citrix Receiverは位置情報データをキャッシュしません）。
- そのアプリケーションでの目的に適したデータが取得されるように、位置情報の精度を管理できなければなりません。また、位置情報の使用について、すべての関連法域の法規に準拠しなければなりません。
- 位置情報を使用するときは、保護された接続（TLSやVPNによる接続など）が使用されるようにします。Citrix Receiverで接続するサーバーは、信頼されたものである必要があります。
- 位置情報サービスの使用に関して法的なアドバイスを得ることを検討してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デスクトップUIのポリシー設定

Dec 05, 2017

［デスクトップUI］カテゴリには、クライアント接続での視覚効果を制御して使用帯域幅を管理するための設定項目が含まれています。視覚効果に含まれるのは、デスクトップの壁紙、メニューのアニメーション、およびドラッグ中にウィンドウの内容を表示する機能です。WANなどの狭帯域幅接続で視覚効果を無効にすると、公開アプリケーションのパフォーマンスが向上します。

デスクトップコンポジションリダイレクト

この設定では、ローカルのDirectXグラフィック処理をユーザーデバイス側のGPU（Graphics Processing Unit）またはIGP（Integrated Graphics Processor）で行い、より滑らかなWindowsデスクトップ操作を提供するかどうかを指定します。デスクトップコンポジションリダイレクトを有効にすると、Windowsデスクトップの操作レスポンスが向上し、サーバーの高いスケーラビリティが維持されます。

デフォルトでは無効になっています。

デスクトップコンポジションリダイレクトを無効にしてユーザーセッションに必要な帯域幅を減らすには、この設定項目で［無効］を選択します。

デスクトップ コンポジションの画質

この設定では、デスクトップコンポジションリダイレクトで使用される画質を指定します。

デフォルトでは、［高］に設定されています。

［高］、［中］、［低］、または［無損失］から選択します。

デスクトップの壁紙

この設定では、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザー セッションで壁紙を表示できます。

デスクトップの 壁紙を非表示にしてユーザーセッションに必要な帯域幅を減らすには、ポリシーにこの設定を追加して［禁止］をクリックします。

メニューをアニメーション化する

この設定では、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは許可されます。

メニューアニメーションは、アクセスを簡単にするためのMicrosoftの個人優先設定です。 これが有効な場合、スクロールまたはフェードインによってメニューが表示されるのが少し遅れることとなります。 矢印アイコンはメニュー下部に表示されます。そのアイコン上にマウスポインターを置くと、メニューの内容が表示されます。

この設定項目が［許可］に設定されている場合、デスクトップでメニューアニメーションが有効で、またメニューアニメーションMicrosoft 個人優先設定が有効です。

注： メニューアニメーションMicrosoft個人優先設定への変更がデスクトップに変更されます。 これにより、セッションの終了時に変更を破棄するようデスクトップが設定されます。セッションでメニューアニメーションを有効にしたユーザーは、デスクトップ上の以降のセッションではメニューアニメーションを使用できない可能性があります。 メニューアニメー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ションが必要なユーザーについては、デスクトップのマスターイメージのMicrosoft設定を有効にするか、またはデスクトップでユーザーの変更を維持する必要があります。

ドラッグ中にウィンドウの内容を表示する

この設定では、ウィンドウをドラッグするときにウィンドウの内容を表示する機能を許可または禁止します。

デフォルトでは許可されます。

［許可］を選択すると、ウィンドウをドラッグするときに内容が表示されたままになります。［禁止］を選択すると、ドロップするまでウィンドウの外枠のみが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

エンドユーザーモニタリングのポリシー設定

Dec 05, 2017

エンドユーザーモニタリングセクションには、セッショントラフィックの測定に関するポリシー設定が含まれています。

ICA往復 測定

この設定では、 アクティブな 接続に対してICA往復測定を実行するかどうかを決定します。

デフォルトでは、 ICA往復測定が実行されます。

デフォルトでは、 ユーザーの操作によるいくつかのトラフィックが発生するまで、 ICA往復測定の開始は遅延されます。このため、ユーザーが操作していないにもかかわらず ICA往復測定による ICAトラフィックが発生することはありません。

ICA往復測定 間隔

この設定では、 ICA往復測定を実行する頻度を秒単位で 指定します。

デフォルトでは、 15秒ごとに測定が実行されます。

アイドル接続の ICA往復測定

この設定では、 アイドル状態の 接続に対してICA往復測定を実行するかどうかを決定します。

デフォルトでは、 アイドル接続に対してICA往復測定は実行されません。

デフォルトでは、 ユーザーの操作によるいくつかのトラフィックが発生するまで、 ICA往復測定の開始は遅延されます。このため、ユーザーが操作していないにもかかわらず ICA往復測定による ICAトラフィックが発生することはありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デスクトップエクスペリエンス拡張のポリシー設定

Dec 05, 2017

この設定項目では、ローカルでWindows 7デスクトップを実行しているユーザーに対して、サーバーオペレーティングシステム上のセッションにWindows 7デスクトップテーマを適用するかどうかを構成します。

デフォルトでは、この設定は許可されています。

Windowsクラシックテーマが選択されたユーザープロファイルが存在する仮想デスクトップでは、この設定を有効にしてもデスクトップエクスペリエンス拡張が提供されません。 この設定項目が未構成または無効の場合、Windows 7テーマのユーザーがWindows Server 2012上の仮想デスクトップにログオンすると、テーマの適用に失敗したことを示すエラーメッセージが表示されます。

これらの問題は、ユーザープロファイルをリセットすることで解決されます。

実行中のユーザーセッションが存在する仮想デスクトップでこの設定項目を有効から無効に変更すると、Windows 7テーマおよびWindowsクラシックテーマでの表示に問題が発生します。 この問題を避けるには、この設定項目の構成を変更した後で仮想デスクトップを再起動してください。 また、管理者は仮想デスクトップの移動プロファイルを削除する必要もあります。 さらに、プロファイル間の一貫性の問題を避けるため、仮想デスクトップの他のユーザープロファイルもすべて削除することをお勧めします。

移動プロファイルが使用される環境では、プロファイルを共有するすべての仮想デスクトップでデスクトップエクスペリエンス拡張機能の有効/無効を統一してください。

サーバーOSを実行する仮想デスクトップとクライアントOSを実行する仮想デスクトップで移動プロファイルを共有することは推奨されません。 サーバーOSとクライアントOSのプロファイルは異なるため、移動プロファイルを共有するとプロファイル内のプロパティの整合性に問題が生じることがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ファイルリダイレクトのポリシー設定

Dec 05, 2017

ファイルリダイレクトセクションには、クライアント側ドライブのマッピングと最適化に関するポリシー設定が含まれていま す。

クライアントドライブに自動接続する

この設定では、 ログオン時にクライアント側のドライブに自動的にマップすることを許可または禁止します。

デフォルトでは 許可されます。

この 設定項目をポリシーに追加する場合は、 ドライブの種類別の設定項目についても確認してください。たとえば、クライアント側の CD-ROMドライブへの自動接続を許可するには、この設定および ［クライアント 側光学式ドライブ］設定を許可します。

関連する設定項目は以下のとおりです。

- クライアントドライブリダイレクト
- クライアント側フロッピードライブ
- クライアント側光学式ドライブ
- クライアント側固定ドライブ
- クライアント側ネットワークドライブ
- クライアント側リムーバブルドライブ

クライアントドライブ リダイレクト

この設定では 、ファイルのクライアント側ドライブへのリダイレクトおよびクライアント側ドライブからのリダイレクトを効または無効にします。

デフォルトでは 有効になっています。

この設定を有効にすると、 ユーザーはクライアント側のすべてのドライブにファイルを保存できるようになります。この設定を無効にすると、ファイルの リダイレクトがいっさいできなくなります。このとき、 ［クライアント側 フロッピー ドライブ］設定や ［クライアント側 ネットワーク ドライブ］設定などの個々のファイル リダイレクト設定の内容は考慮されません。

関連する設定項目 は以下のとおりです。

- クライアント側フロッピードライブ
- クライアント側光学式ドライブ
- クライアント側固定ドライブ
- クライアント側ネットワークドライブ
- クライアント側リムーバブルドライブ

クライアント側固定 ドライブ

この設定では、 クライアント側の固定ドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは 許可されます。

この設定を ポリシーに追加する場合、 ［クライアント ドライブ リダイレクト］設定で ［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側 固定ドライブはマップされず、ユーザーが手作業でそれらのドライ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

にアクセスすることもできなくなります。 このとき、 ［クライアント側 固定ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときに固定 ドライブに自動接続できるようにするには、 ［クライアント ドライブに自動 接続する］設定を使用します。

クライアント側フロッピー ドライブ

この設定 では、 クライアント側のフロッピードライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは 許可されます。

この 設定をポリシーに追加するときは、 ［クライアント ドライブ リダイレクト］設定で ［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側 フロッピードライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。 このとき、 ［クライアント側 フロッピー ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときにフロッピー ドライブに自動接続できるようにするには、 ［クライアント ドライブに 自動接続する］設定を使用します。

クライアント側ネットワーク ドライブ

この設定 では、クライアント側でマップ済みのネットワークドライブ（リモートドライブ） にアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは 許可されます。

この 設定をポリシーに追加するときは、 ［クライアント ドライブ リダイレクト］設定で ［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側 ネットワークドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。 このとき、 ［クライアント側 ネットワーク ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときにネットワーク ドライブに自動接続できるようにするには、 ［クライアント ドライブに 自動接続する］設定を使用します。

クライアント側光学式 ドライブ

この設定 では、クライアント側のCD-ROM、DVD-ROM、および BD-ROMドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは 許可されます。

この 設定をポリシーに追加するときは、 ［クライアント ドライブ リダイレクト］設定で ［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側 光学式ドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。 このとき、 ［クライアント側 光学式ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときに光学式 ドライブに自動接続できるようにするには、 ［クライアント ドライブに 自動接続する］設定を使用します。

クライアント側 リムーバブルドライブ

この設定 により、 クライアント側のUSBドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは 許可されます。

この 設定をポリシーに追加するときは、［クライアント ドライブ リダイレクト］設定で［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側 リムーバブルドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。 このとき、［クライアント側 リムーバブル ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときに リムーバブルドライブに自動接続できるようにするには、［クライアント ドライブに 自動接続する］設定を使用します。

ホストからクライアントへの リダイレクト

この設定 では、URLや特定のメディアコンテンツ をクライアント側で開くためのファイルタイプの関連付けを有効または無効にします。この設定を無効にすると、コンテンツはサーバー上で開きます。

デフォルトでは 無効になっています。

この設定を有効にすると、次の種類のURL がクライアント側のアプリケーションで開きます。

- Hypertext Transfer Protocol （HTTP）
- Secure Hypertext Transfer Protocol（HTTPS）
- Real PlayerおよびQuickTime （RTSP）
- Real PlayerおよびQuickTime （RTSPU）
- 従来のRealPlayer（PNM）
- Microsoft Media Server （MMS）

クライアント側のドライブ文字を保持する

この設定 では、クライアント側ドライブを セッション内でマップするときに、元のドライブ文字を保持するかどうかを指定します。

デフォルトでは クライアント側のドライブ文字列は保持されません。

この 設定をポリシーに追加するときは、［クライアント ドライブ リダイレクト］設定で［許可］が選択されていることを確認してください。

クライアント側ドライブへの読み取り専用アクセス

この設定 では、マップされたクライアントドライブ上にユーザーやアプリケーションがファイルや フォルダーを作成したり変更したりすることを許可または禁止します。

デフォルトでは 許可されます。

［有効］に設定すると、ファイルやフォルダーへの 読み取り専用アクセスが許可されます。

この 設定をポリシーに追加するときは、［クライアント ドライブ リダイレクト］設定で［許可］が選択されていることを確認してください。

ユーザーフォルダーのリダイレクト

この設定では、Citrix ReceiverやWeb Interfaceを使用するユーザーに対して、セッション内でクライアント側の［ドキュメント］や［デスクトップ］などのローカルフォルダーに簡単にアクセスするための機能を許可または禁止します。

デフォルトでは許可されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定では、この機能の有効/無効をポリシーの適用条件に基づいて制御できます。この設定が禁止されている場合、ユーザーフォルダーのリダイレクトに関するStoreFront、Web Interface、またはCitrix Receiverのすべての設定が無視されます。

ユーザーフォルダーのリダイレクトを許可するユーザーを定義するには、この設定項目で[許可] を選択し、ポリシーの適用先としてそのユーザーを指定します。この設定は、ユーザーフォルダーのリダイレクトに関するほかの設定よりも優先されます。

ユーザーフォルダーのリダイレクトによりクライアント側のドライブがアクセスされるため、クライアント側のハードドライブへのアクセスや書き込みを禁止するとユーザーフォルダーのリダイレクトも禁止されます。

この設定をポリシーに追加するときは、[クライアント側固定ドライブ] 設定で [許可] が選択されていることを確認してください。

非同期書き込みを使用する

この設定 では、クライアント側のディスクへの非同期書き込みを有効または無効にします。

デフォルトでは 無効になっています。

非同期 書き込みを有効にすると、 WAN接続を介したサーバーからクライアント側へのディスク書き込みおよびファイル転送の 遅延が改善されます。ただし、非同期転送時にセッションが切断されたりクライアント側のディスク容量が不足したりしてファイル書き込みが中断された場合に、クライアント側のファイルが破損することがあります。この問題が発生した場合、ポップアップ ウィンドウが開き、影響を受けたファイルがユーザーに通知されます。ユーザーは 問題を解決した後でファイル転送を やり直すことができます。

WAN 接続でのファイル転送速度の改善が重要で、クライアント側のデータが破損しても ユーザーが容易に復元できる場合のみ、非同期書き込みを有効にしてください 。

この 設定をポリシーに追加するときは、 [クライアント ドライブ リダイレクト] 設定で [許可] が選択されていることを確認してください。この設定が無効の場合、非同期 書き込みは行われません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Flashリダイレクトのポリシー設定

Dec 05, 2017

Flashリダイレクトセクションには、ユーザーセッションでのFlashコンテンツの処理に関するポリシー設定が含まれています。

Flash アクセラレーション

この設定では、 Flashコンテンツのレンダリングを サーバー上ではなくクライアント側で行う機能を有効または無効にします。デフォルトでは、クライアント側でのFlashコンテンツのレンダリングが有効になっています。

注： この設定は、 Citrix Online Plug-in 12.1でサポートされる従来のFlashリダイレクト機能について使用します。
この機能を有効にすると、 Flashコンテンツがユーザー デバイス上でレンダリングされるため、ネットワークおよびサーバーへの負荷が軽減されます。特定の WebサイトのFlashコンテンツを強制的にサーバー上でレンダリングするには、 ［Flash URL互換性リスト］設定を使用します。

この機能を使用するには、ユーザー デバイス側でも ［このユーザーデバイスでの HDX MediaStream Flash リダイレクトを有効にする］を有効にする 必要があります。

Flashアクセラレーションを無効にすると、 すべてのWebサイトのFlashコンテンツが サーバー上でレンダリングされます。特定のWebサイトのFlashコンテンツのみをユーザー デバイス上でレンダリングするには、 ［Flash URL 互換性リスト］設定を使用します。

Flash背景色リスト

この設定では、特定のURLのFlashコンテンツの背景色を指定します。

デフォルトでは、背景色は指定されていません。

この背景色は、クライアント側でレンダリングされるFlashコンテンツの背景に表示され、これにより表示領域を判別しやすくなります。表示領域を判別しやすくするために、非一般的な色を指定する必要があります。

このリストには、URL（先頭および末尾にワイルドカード文字を使用可）と24ビットRGBの16進カラーコードをスペースで区切って入力します例：http://citrix.com 000003。

指定されるURLはFlashコンテンツのURLである必要があります。これはWebサイトのURLとは異なることがあります。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsのインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Windows 8またはWindows 2012が動作するVDAでは、この設定によりURLのキー色の設定に失敗することがあります。この場合、VDAマシンでレジストリを編集します。

32ビットマシンの場合は、このレジストリ設定を使用します：

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

© 1999-2017 Citrix Systems, Inc. All rights reserved.

64ビットマシンの場合は、このレジストリ設定を使用します：

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

Flash アクセラレーションの後方互換

この設定は、 以前のバージョンのCitrix Receiver（旧称「Citrix Online Plug-in」）用の第1世代（従来モード）のFlashリダイレクト機能を 使用できるようにするかどうかを制御します。

デフォルトでは、 有効になっています。

この機能を使用するには、ユーザー デバイス側でも ［このユーザーデバイスでの HDX MediaStream Flash リダイレクトを有効にする］を 有効にする必要があります。

第2世代の Flashリダイレクト機能は、Citrix Receiver 3.0で使用できます。第1世代（従来モード）のFlash リダイレクト機能は、Citrix Online Plug-in 12.1でサポートされています。 第2世代のFlashリダイレクト機能を使用するには、 サーバー側およびユーザーデバイス側で第2世代のFlashリダイレクト機能 を有効にする必要があります。サーバー側またはユーザー デバイス側で従来モードのFlashリダイレクト機能が有効になっている場合は、従来モードのFlashリダイレクト機能が使用されます。

Flashアクセラレーションのデフォルトの動作

この設定では、第2世代のFlashリダイレクト機能のデフォルトの動作を設定します。

デフォルトでは、Flashアクセラレーションは有効になっています。

この設定を構成するには、次のいずれかのオプションを選択します。

- Flashアクセラレーションを有効にする：Flashリダイレクトが使用されます。
- Flash Playerをブロックする： Flashリダイレクトおよびサーバー側でのレンダリングが行われません。これにより、ユーザーはFlashコンテンツを表示できなくなります。
- アクセラレーションを無効にする：Flashリダイレクトは使用されません。適切なバージョンのFlash Player for Windows Internet Explorerがサーバーにインストールされている場合、ユーザーはサーバー側で処理されたFlashコンテンツを表示できます。

この設定は、［Flash URL 互換性リスト］設定に追加した特定のWebページやFlashインスタンスでは無視されます。また、Flashリダイレクト機能を使用するには、ユーザーデバイス側でも［このユーザーデバイスでの HDX MediaStream Flash リダイレクトを有効にする］を有効にする必要があります。

Flashイベントの ログ

この設定では、 FlashイベントをWindowsのアプリケーションイベントログに記録するかどうかを指定します。

デフォルトでは、 ログは有効になっています。

Windows 7またはWindows Vistaが動作するコンピューターでは、 Flashリダイレクトのログは ［アプリケーションとサービスログ］ノードに記録されます。

Flash インテリジェントフォールバック

この設定は、 Flashコンテンツのクライアント側でのレンダリングが不要または 低速な場合に、サーバー側でのレンダリングに自動的に切り替える機能を有効または無効にします。

デフォルトでは、 有効になっています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Flash遅延 しきい値

この設定では、 Flash コンテンツのレンダリングをサーバー側で行うかどうかを決定する遅延時間のしきい値を、0～30ミリ秒で指定します。

デフォルトの しきい値は、30ミリ秒です。

HDX MediaStream for Flashでは、起動時にサーバーと クライアント間の遅延時間が計測されます。計測値がしきい値未満の場合、HDX MediaStream for Flash 機能によりクライアント側でFlashコンテンツがレンダリングされます。遅延が しきい値を超える場合は、サーバー側でFlashコンテンツがレンダリングされます（そのサーバー上にAdobe Flash Playerが インストールされている場合）。

この 設定を有効にするときは、 ［Flash アクセラレーションの 後方互換］設定で ［有効］が選択されていることを確認してください。

注： HDX MediaStream Flashリダイレクトを従来モードで使用する場合のみ適用されます。

Flashビデオフォールバック防止

この設定は、「小さな」Flashコンテンツがレンダリングされてユーザーに表示されるのかどうか、されるならどのようにさるのかを指定します。

デフォルトでは、この設定は構成されていません。

この設定を構成するには、次のいずれかのオプションを選択します。

- **小さなコンテンツのみ。**サーバー上でインテリジェントフォールバックコンテンツのみレンダリングされます。ほかのFlashコンテンツはエラー*.swfと置き換えられます。
- **サポートされたクライアントがある小さなコンテンツのみ。**クライアントが現在Flashリダイレクトを使用している場合に、サーバー上でインテリジェントフォールバックコンテンツのみレンダリングされます。ほかのFlashコンテンツはエラー*.swfと置き換えられます。
- **サーバー側コンテンツなし。**サーバー上のすべてのコンテンツは、エラー*swfと置き換えられます。

このポリシー設定を使用するには、エラー*.swfファイルを指定する必要があります。このエラー*.swfは、VDA上でレンダリングしない任意のコンテンツを置き換えます。

Flashビデオフォールバック防止エラー*.swf

この設定は、サーバー負荷管理ポリシーが使用されている場合にFlashインスタンスを置き換えるためユーザーに表示されるエラーメッセージのURLを指定します。次に例を示します。

http://domainName.tld/sample/path/error.swf

Flash サーバー側でのコンテンツ取得URLリスト

この設定の リストに追加したWebサイトのFlashコンテンツは、サーバーにより取得され、 ユーザーデバイスに転送されます。

デフォルトでは、サイトは指定されて いません。

サーバー側での コンテンツ取得は、インターネットに直接アクセスできないユーザーデバイスに対して 有効にします。また、ユーザーデバイス側でも ［サーバー側のコンテンツの取得を有効にする ］設定を有効にする必要があります。

第2世代のFlashリダイレクトには、 FlashのSWFファイルをサーバー側でダウンロードするフォールバック機能 が含まれています。ユーザーデバイスがWeb サイトからFlashコンテンツをフェッチできず、WebサイトがFlashサーバー側コンテンツ

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

フェッチ URL一覧で指定されている場合、サーバー側コンテンツのフェッチは自動的に発生します。

対象のURLを リストに追加する場合、以下の点に注意してください。
- Flash Playerを開始する上位レベルのHTMLページのURLではなく、FlashコンテンツのURL を追加します。
- URLの 最初または最後にワイルドカード文字としてアスタリスク（*）を使用できます。
- URLの最後にワイルドカード文字を使うと、 すべての子URLを指定できます（http://www.citrix.com/*など）。
- 冒頭の「http://」や 「https://」は正しく認識されますが、省略することもできます。

Flash URL 互換性リスト

この設定項目では、 特定のWebサイト上の Flashコンテンツをクライアント側でレンダリングするか、サーバー側でレンダリングするか、またはブロックするかを指定します。

デフォルトでは、 規則は指定されていません。

対象のURLを リストに追加する場合、以下の点に注意してください。
- リスト上位の URLやアクションが優先されます。
- URLの 最初または最後にワイルドカード文字としてアスタリスク（*）を使用できます。
- URLの最後にワイルドカード文字を使うと、 すべての子URLを指定できます（http://www.citrix.com/*など）。
- 冒頭の「http://」や 「https://」は正しく認識されますが、省略することもできます。
- ユーザーデバイス上で正しくレンダリングされないFlashコンテンツのサイトをこのリストに追加して、 ［サーバー側でレンダリング］または ［ブロック］オプションを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

グラフィックのポリシー設定

Dec 05, 2017

グラフィックセクションには、ユーザーセッションでの画像処理の制御に関するポリシー設定が含まれています。

視覚的無損失の圧縮を使用する

この設定により、グラフィックに対して、真の無損失圧縮の代わりに視覚的に無損失の圧縮を使用できるようになります。視覚的無損失では、真の無損失よりもパフォーマンスは向上しますが、見た目にはわからない程度の軽微な損失が発生します。この設定によって、表示品質設定の値の使用方法が変更されます。

デフォルトでは、無効になっています。

表示メモリの制限

この設定では、セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。

デフォルトの表示メモリ制限は、65536キロバイトに設定されます。

セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。キロバイト単位の容量指定は、128から4,194,303です。最大値4,194,303によって表示メモリが制限されることはありません。デフォルトでは、65536キロバイトに設定されます。ウィンドウサイズを大きくしたり、表示色数を多くしたりすると、必要なメモリの量が増えます。従来のグラフィックモードでは、この最大値に達すると、［メモリが不足したときの表示モード］設定に基づいて色数または解像度が低下します。

高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は、次の式で算出できます。

必要とされるメモリ（バイト単位）＝（1ピクセルあたりのビット数を8で割った色数）×（垂直方向のピクセル単位の解像度）×（水平方向のピクセル単位の解像度）

たとえば、ウィンドウの高さ600、ウィンドウの幅800、32ビットの色数の場合、必要なメモリの最大量は（32bpp÷8）×（600ピクセル）×（800ピクセル）＝1920000バイトであるため、［表示メモリの制限］設定で1920KBを指定します。

32ビット以外の色数は、［従来のグラフィックモード］設定が有効な場合のみ使用できます。

HDXでは、各セッションで必要な表示メモリ量だけが割り当てられます。このため、デフォルト値よりも多くのメモリが必要なユーザーが一部だけの場合にこの設定項目で表示メモリの制限を増やしても、スケーラビリティは低下しません。

メモリが不足したときの表示モード

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、セッション 表示用のメモリが上限に達したときに、色数と解像度のどちらを下げるかを 指定します。

デフォルトでは、最初に色数 が低下します。

セッション表示用の メモリが上限に達したときに、表示品質を下げることでメモリ不足による問題の発生を防ぐことができます。色数 を下げることを選択すると、表示用のメモリが上限に達したときに、まずより少ない色でのイメージ表示に切り替わります。解像度を 下げることを選択すると、まず1インチあたりのピクセル数が少なくなります。

色数または解像度の低下をユーザーに通知するには、 ［メモリ不足による表示品質の低下を ユーザーに通知する］設定を使用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

動的ウィンドウ プレビュー

この設定では、フリップ、フリップ3D、タスクバープレビュー、 およびピークウィンドウプレビューモードにおけるシームレスウィンドウの表示の有効 /無効を切り替えます。

Windows Aeroプレビューオプション	説明
タスクバープレビュー	Windowsタスクバー上のアイコン上にマウスポインターを合わせると、そのウィンドウの縮小版がプレビューとして表示されます。
ピークウィンドウプレビュー	Windows タスクバー上に開いた縮小版上にマウスポインターを合わせると、そのウィンドウがフルサイズで表示されます。
フリップ	Alt+Tabキーを押すと、開いているすべてのウィンドウの縮小版が一覧表示されます。
フリップ3D	Tab+Windowsロゴキーを押すと、 開いているすべてのウィンドウが立体的に重なって一覧表示されます。

デフォルトでは、 有効になっています。

イメージ キャッシュ

注： Virtual Delivery Agent 7.xでは、 [従来の グラフィックモード] 設定が有効な場合のみこの設定項目が適用されます。
この設定項目では、 セッション内のイメージのセクションキャッシュおよび取得を有効または無効にします。必要な場合にセクションのイメージをキャッシュし、そのセクションを取得すると、 スクロールがよりスムーズになり、ネットワーク上のデータ伝送量が減少して、 ユーザーデバイス上で必要とされる処理が少なくなります。

デフォルトでは、 イメージのキャッシュ設定は有効になっています。

注： イメージの キャッシュ設定は、イメージがどのようにキャッシュおよび取得されるかを制御します。イメージが キャッシュされるかどうかについては制御しません。従来のグラフィック モード設定が有効な場合は、イメージがキャッシュされます。

従来のグラフィックモード

この設定では、リッチなグラフィック表示が無効になります。この設定を使用すると、従来のグラフィック表示が取り消され、WANやモバイル接続での帯域幅の使用量が削減されます。XenAppおよびXenDesktop 7.13に導入された帯域幅の削減によって、このモードは廃止されます。

この設定はデフォルトで無効になっており、リッチなグラフィック表示が提供されます。

Windows 7およびWindows Server 2008 R2 VDAでは、従来のグラフィックモードがサポートされます。

Windows 8.x、10、またはWindows Server 2012、2012 R2、2016では、従来のグラフィックモードはサポートされていません。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードおよびポリシーの最適化について詳しくは、CTX202687を参照してください。

許可される最大表示色数

注： Virtual Delivery Agent 7.xでは、 [従来のグラフィックモード] 設定が有効な場合のみこの設定項目が適用されます。
この設定では、セッションで許可される最大表示色数を指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、1ピクセルあたり32ビットまでの色数が許可されます。

この設定はThinWireドライバーおよび接続にのみ適用されます。これは、プライマリディスプレイドライバーとしてWindow Display Driver Model（WDDM）ドライバーを使用するVDAのような、非ThinWireドライバーがプライマリディスプレイドライバーのVDAには適用されません。プライマリディスプレイドライバーとしてWindows Display Driver Model（WDDM）ドライバーを使用するデスクトップOS VDA（Windows 8など）には、この設定は効果がありません。 WDDMドライバーを使用するWindowsサーバーOS VDA（Windows Server 2012 R2など）の場合、この設定によりユーザーがVDAに接続できない可能性があります。

高い表示色数をサポートするには、より多くのメモリが必要です。メモリ不足時に自動的に色数を減らすには、[メモリが不足した時の表示モード］設定を使用します。この設定で色数を下げるオプションを選択すると、イメージの表示色数が少なくなります。

メモリ不足による表示品質の低下をユーザーに通知する

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、 色数または解像度が 低下するときにユーザーに簡単なメッセージを表示するかどうかを指定します。

デフォルトでは、 メッセージは表示されません。

キューイメージの 破棄

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、 ほかのイメージで置換される中間イメージを破棄するかどうかを指定します。

デフォルトでは、キューイメージの 破棄は有効になっています。

有効にすると、 グラフィックがユーザーデバイス側に送信されるときのレスポンスが向上します。ただし、中間フレームが脱落するため、アニメーションの動きがスムーズでなくなる 場合があります。

圧縮にビデオコーデックを使用

エンドポイントでビデオのデコードを使用できる場合は、グラフィックの圧縮にビデオコーデック（H.264）を使用できます。 **［画面全体］**が選択された場合、ビデオコーデックにはすべてのデフォルトコーデックが適用されます。**［アクティブに変化する領域］**が選択された場合、画面上に変更が定期的にある領域にビデオコーデックが使用され、他のデータでは静止画圧縮およびビットマップのキャッシュが使用されます。エンドポイントでビデオのデコードを使用できない、または**使用しない**ように指定すると、静止画像圧縮とビットマックキャッシュの組み合わせが使用されます。**［選択された場合ビデオコーデックを使用する］**が指定されている場合、選択はさまざまな要素に基づいて行われます。選択方法が拡張されているため、結果はバージョンによって異なる場合があります。

現在のシナリオに最適な設定が自動的に選択されるようにするには、**［選択された場合ビデオコーデックを使用する］**を選択します。

ユーザーエクスペリエンスと帯域幅の改善のために最適化する場合、特にサーバー側でレンダリングするビデオや3Dグラフィックを多用する場合は、 **［画面全体］**を選択します。

ビデオパフォーマンス、特に低帯域幅が改善されるように最適化しつつ、コンテンツが静的かつ徐々に変更されるようにするためにスケーラビリティを維持するには **［アクティブに変化する領域］**を選択します。この設定は、マルチモニターの展開でサポートされます。

サーバーCPUの負荷を最適化する場合、およびサーバー側でレンダリングするビデオやその他の画像処理に多くのリソースを消費するアプリケーションがほとんどない場合は、 **［ビデオコーデックを使用しない］**を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、**[選択された場合ビデオコーデックを使用する]** に設定されています。

ビデオのハードウェアエンコーディングの使用

この設定によりグラフィックハードウェア（搭載している場合）を利用して、画面要素をH.264ビデオコーデックで圧縮できます。 該当するハードウェアが利用可能でない場合、VDAはソフトウェアビデオコーデックを使用してCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトのオプションは **[有効]** です。

複数のモニターがサポートされます。

H.264デコーディングをサポートするCitrix Receiverは、NVENCハードウェアエンコーディングで使用できます。

非可逆圧縮（4:2:0）と視覚的無損失圧縮（4:4:4）がサポートされます。 視覚的無損失（グラフィックポリシー設定、視覚的無損失の圧縮を使用する）にはReceiver for Windows 4.5が必要です。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコーディングは、HDX 3D Pro モードの VDA for Desktop OSでサポートされています。

NVIDIA GPUは、NVENCハードウェアエンコーディングをサポートする必要があります。サポートされているGPUの一覧については、「NVIDIAビデオコーデックSDK」を参照してください。

NVIDIA GRIDには、ドライバーのバージョン3.1以上が必要です。NVIDIA Quadroには、ドライバーのバージョン362.56以上が必要です。NVIDIAリリースR361ブランチからのドライバーをお勧めします。

VDAが（HDX 3D Proではなく）標準モードで構成された場合の機能である無損失テキストには、NVENCハードウェアエンコーディングとの互換性はありません。HDX 3D Proモードで有効になっている場合、無損失テキストはNVENCハードウェアエンコーディングよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的使用はサポートされません。

Intel

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコーディングは、VDAs for Desktop OS（標準モードまたはHDX 3D Pro モード）およびVDA for Server OSでサポートされています。

サポート対象は、Intel BroadwellプロセッサファミリのIntel Iris Proグラフィックプロセッサ以降です。Intel Iris Proハードウェアエンコーダー SDKは必須で、IntelのWebサイト「Remote Displays SDK」からダウンロードできます。

無損失テキストがサポートされています。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的使用がサポートされています。

対応は、Windows 10およびWindows Server 2012以降です。

3D Pro モードのVDAで、Intel エンコーダーは最大で8つのエンコーディングセッションを可能にする優れたユーザーエクスペリエンスをもたらします（たとえば、1人のユーザーが8つのモニターを使ったり、8人のユーザーが各自モニターを使用するなど）。8つ以上のエンコーディングセッションが必要な場合は、仮想マシンが接続するモニター数を確認してください。優れたユーザーエクスペリエンスを維持するために、管理者はこのポリシー設定をユーザー単位またはマシン単位に構成できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

キャッシュのポリシー設定

Dec 05, 2017

［キャッシュ］カテゴリには、狭帯域幅のクライアント接続でイメージデータをユーザーデバイス上にキャッシュする機能を有効にするための設定項目が含まれています。

固定 キャッシュしきい値

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。この設定では 、ビットマップをユーザーデバイスのハードドライブ上にキャッシュするときの帯域幅しきい値を指定します。この機能により 、サイズの大きな、頻繁に使用されるイメージがキャッシュされ、以降のセッションで再使用されます。

デフォルトの しきい値は、3000000bpsです。

帯域幅が このしきい値を下回る場合、固定キャッシュ機能が 有効になります。つまり、デフォルトの設定では、接続帯域幅が3,000,000bpsを下回る場合に、ビットマップがユーザーデバイスのハード ドライブ上にキャッシュされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Framehawkのポリシー設定

Dec 05, 2017

Framehawkセクションには、サーバーでFramehawkディスプレイチャネルを有効化し、構成するためのポリシー設定が含まれます。

Framehawkディスプレイチャネル

この機能を有効にすると、サーバーはFramehawkディスプレイチャネルを使用して、ユーザーのグラフィックスおよび入力リモート処理を試行します。この表示チャネルは、UDPを使用して、高い損失および遅延特性を示すネットワークにより快適なユーザーエクスペリエンスを提供します。ただし、使用するサーバーのリソースや帯域幅は他のグラフィックモードより多くなります。

デフォルトでは、Framehawkディスプレイチャネルは無効になっています。

Framehawkディスプレイチャネルポートの範囲

このポリシー設定項目では、VDAでユーザーデバイスとのFramehawkディスプレイチャネルデータの送受信に使用されるUDPポート番号の範囲を「,」の形式で指定します。VDAは、各ポートの使用を試行します。まず、最小のポート番号から始めて、2回目以降の試行では1つずつ番号を増やしていきます。ポートは、受信トラフィックと送信トラフィックに使用されます。

デフォルトでは、ポートの範囲は3224、3324です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Keep-Aliveのポリシー設定

Dec 05, 2017

Keep-Aliveセクションには、ICA Keep-Aliveメッセージの管理に関するポリシー設定が含まれています。

ICA Keep-Alive タイムアウト

この設定では、ICA Keep-Aliveメッセージの送信間隔を秒単位で 指定します。

デフォルトでは、 ICA Keep-Aliveメッセージが60秒おきに送信されます。

ICA Keep-Aliveメッセージの 送信間隔として設定可能な範囲は、1～3600秒です。ただし、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に 閉じるように設定している環境では、この設定を使用 しないでください。

ICA Keep -Alive

この設定では、ICA Keep-Aliveメッセージを定期的に送信するかどうかを 指定します。

デフォルトでは、ICA Keep-Aliveメッセージは送信されません。

この 設定を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。また、サーバー側でセッションのアイドル状態が 検出されたときに、リモートデスクトップサービス（RDS）によりセッションが 切断されることを防ぐことができます。サーバーは、 定期的にKeep-Aliveメッセージを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、 サーバーにより「切断」状態として認識されます。

ICA Keep-Aliveは、セッション画面の保持機能を使用する環境では正しく 動作しません。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Aliveを 有効にしてください。

関連する設定項目： セッション画面の保持。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ローカルアプリケーションアクセスのポリシー設定

Dec 05, 2017

［ローカルアプリケーションアクセス］カテゴリには、ホストされるデスクトップ環境で、ユーザーデバイス上にインストールされたローカルアプリケーションとホスト上のアプリケーションをシームレスに使用できるようにするための設定項目が含まれています。

ローカル アプリケーションのアクセスを許可する

この設定では、ホストされるデスクトップ環境で、 ローカルアプリケーションとホスト上のアプリケーションの統合を許可または禁止します。

ユーザーが ローカルのアプリケーションを起動すると、そのアプリケーションが 仮想デスクトップ上で動作しているかのように表示されます。

デフォルトでは、ローカル アプリケーションへのアクセスは禁止されます。

URL リダイレクトのブラックリスト

この設定では、 ユーザーデバイス上のローカルのWeb ブラウザーで開くWebサイトを指定します。通常、ユーザーの現在位置の情報を使用するWebサイト （msn.comやnewsgoogle.comなど）や、クライアント側で処理した方が効率的なマルチメディアコンテンツサイト などのURLを指定します。

デフォルトでは、 サイトは指定されていません。

URL リダイレクトのホワイトリスト

この設定では、 ユーザーデバイス側にリダイレクトしないWebサイトを指定します。

デフォルトでは、 サイトは指定されていません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

モバイルデバイスでの動作のポリシー設定

Dec 05, 2017

モバイルデバイスでの動作セクションには、Citrix Mobility Packの動作を制御するためのポリシー設定が含まれています。

キーボードの自動表示

この設定 では、モバイルデバイス 画面上におけるキーボードの自動表示を有効または無効にします。

デフォルトでは、 無効になっています。

タッチパネルでの操作に最適化されたデスクトップ

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定では、タッチパネルでの操作に最適化されたデスクトップの起動を許可または禁止して、全体的なCitrix Receiverインターフェイスの動作を指定します。

デフォルトでは、タッチパネルでの操作に最適化されたデスクトップが起動します。

通常のWindowsインターフェイスのデスクトップを起動する場合は、［禁止］を選択します。

コンボボックスをデバイス側で表示する

この設定では、モバイルデバイスでのセッションで表示するコンボボックスの種類を指定します。モバイルデバイス側のコンボボックスコントロールを表示するには、［許可］を選択します。管理者がこの設定で許可を選択しても、Citrix Receiver for iOSのユーザーは、セッション設定で通常のWindowsコンボボックスの表示を選択できます。

デフォルトでは、コンボボックスをデバイス側で表示する機能は禁止されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マルチメディアのポリシー設定

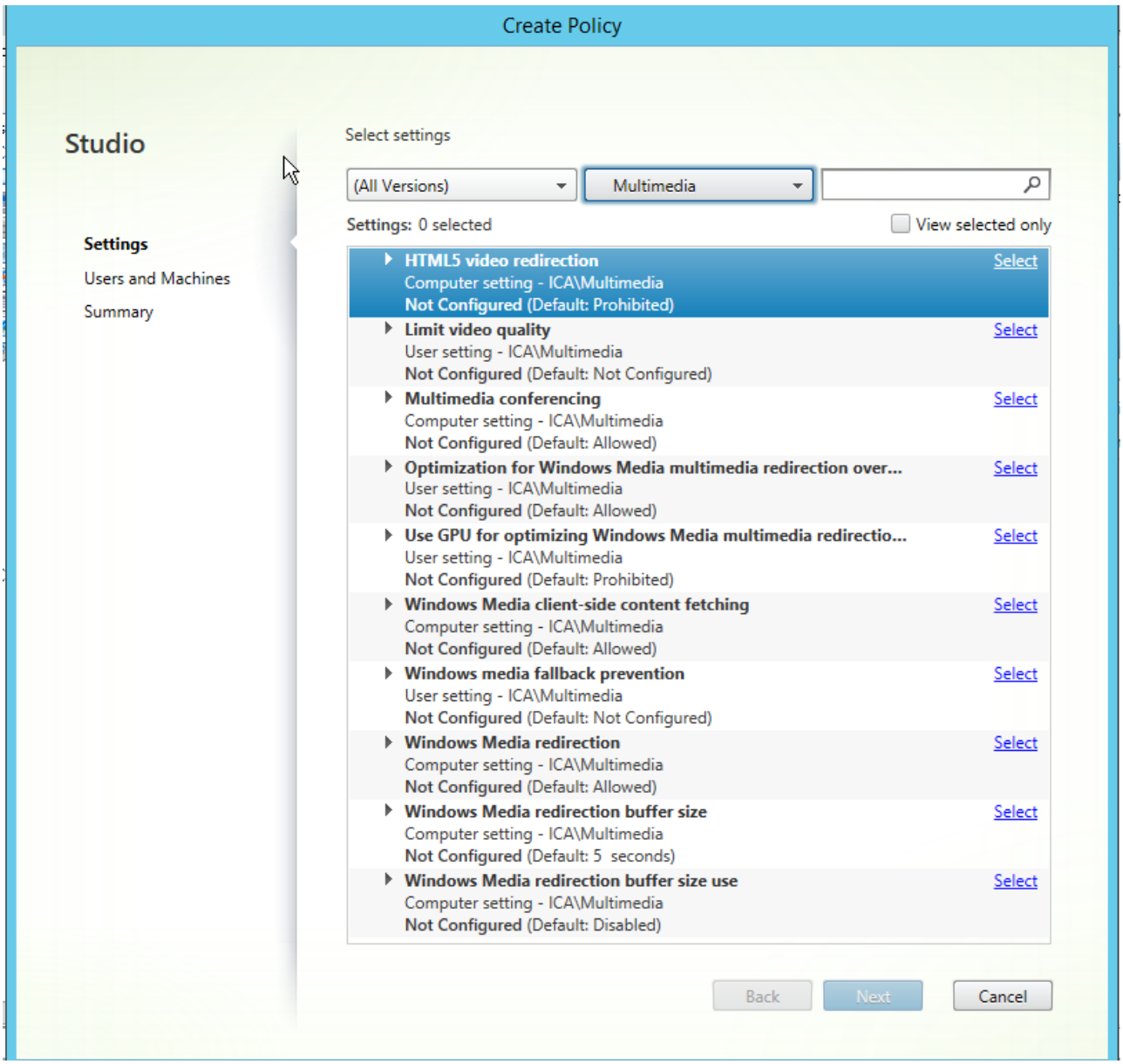
Jan 05, 2018

［マルチメディア］セクションには、ユーザーセッションでのHTML5およびWindowsのオーディオとビデオのストリーム配信の管理に関するポリシー設定があります。

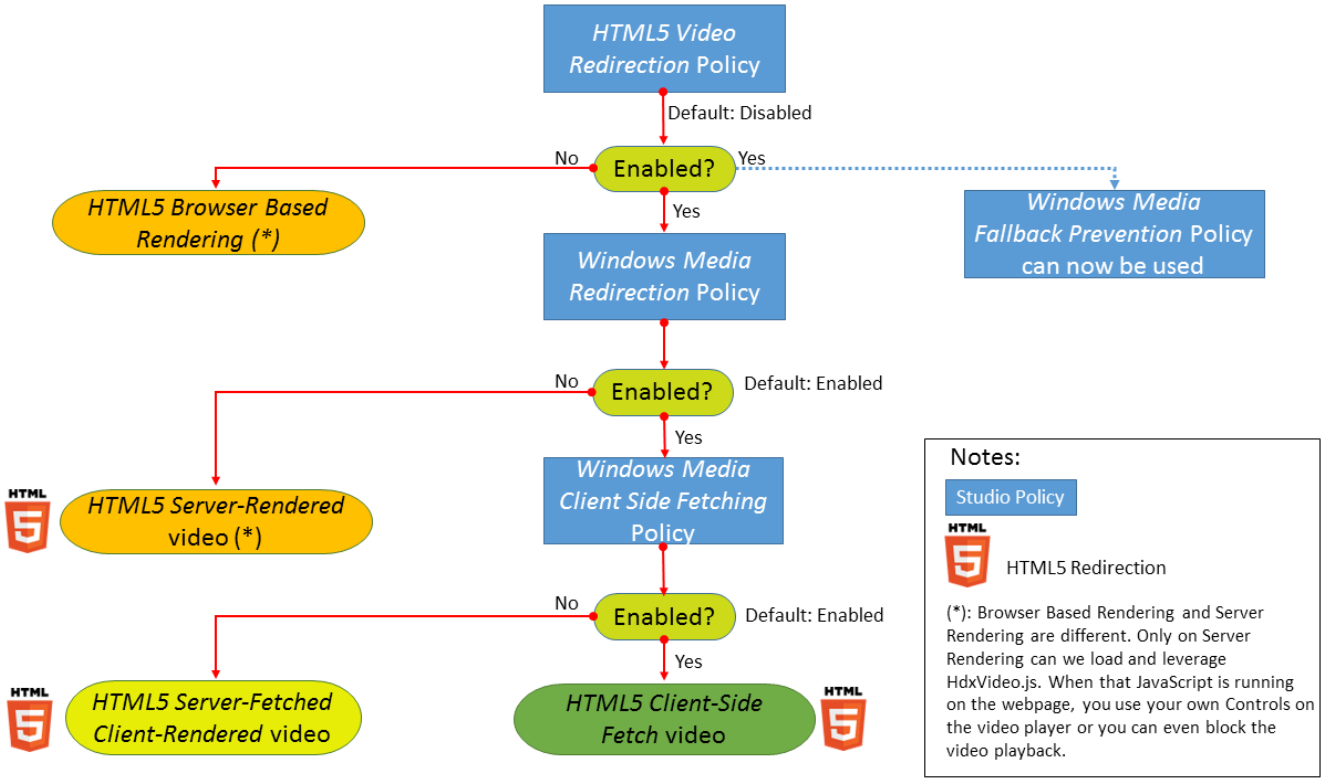
HTML5ビデオリダイレクション

XenAppおよびXenDesktopサーバーがユーザーにHTML5マルチメディアWebコンテンツを提供する方法を制御、最適化します。

デフォルトでは、無効になっています。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



このリリースでは、この機能は管理対象Webページでのみ利用できます。HTML5マルチメディアコンテンツが利用できるWebページ（たとえば、社内研修サイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクションを構成するには：

1. **HdxVideo.js**ファイルを、VDAがインストールされた%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionから社内Webページの場所にコピーします。
2. 次の行をWebページに挿入します（Webページに別のスクリプトが設定されている場合、**HdxVideo.js**をそのスクリプトの前に追加します）。

注： HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使ってHdxVideo.jsへのフルパスを指定します。

管理対象のWebページにJavaScriptが追加されていない場合、ユーザーがHTML5ビデオを再生すると、XenAppおよびXenDesktopはサーバー側レンダリングにデフォルト設定されます。

Windows Mediaリダイレクトを許可しないと、HTML5ビデオリダイレクションは機能しません。このポリシーは、サーバー側フェッチ/クライアント側レンダリングでは必須であり、クライアント側フェッチでも必要とされます（この場合、 *[Windows Mediaのクライアント側でのコンテンツ取得]*を［許可］に設定する必要があります）。

Microsoft Edgeではこの機能はサポートされていません。

HdxVideo.jsにより、ブラウザーのHTML5プレーヤーのコントローラーが独自のものに置き換えられます。特定のWebサイトでHTML5ビデオリダイレクションが有効であるかどうかを確認するには、プレーヤーのコントローラーを ***[HTML5ビデオリダイレクション]*** ポリシーが［禁止］に設定されている場合のシナリオと比較します。

（このポリシーが［許可］に設定されている場合のCitrixのカスタムコントローラー）

© 1999-2017 Citrix Systems, Inc. All rights reserved.



（このポリシーが［禁止］に設定されているか未構成の場合のネイティブのWebページコントローラー）



次のビデオコントロールがサポートされます。

- 再生
- 一時停止
- シーク
- リピート
- オーディオ
- 全画面

https://www.citrix.com/virtualization/hdx/html5-redirect.htmlで、HTML5ビデオリダイレクションのテストページを表示できます。

TLSおよびHTML5ビデオリダイレクション

HTML5ビデオリダイレクションを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されたJavaScriptは、VDAで動作するCitrix HDX HTML5ビデオリダイレクションサービス（WebSocketService.exe）へのTLS接続を確立する必要があります。このリダイレクションを実現し、WebページのTLS整合性を維持するために、Citrix HDX HTML5ビデオリダイレクションサービスはVDAの証明書ストアで2つのカスタム証明書を生成します。

HdxVideo.jsは、セキュアWebSocketを使用してVDAで動作するWebSocketService.exeと通信します。このプロセスはローカルシステムで動作し、SSLの終了とユーザーセッションマッピングを実行します。

WebSocketService.exeは127.0.0.1ポート9001でリスンします。

ビデオ品質の制限

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定を使用するには、*［WAN接続でのWindows Mediaマルチメディアリダイレクトの最適化］*を有効化する必要があります。

この設定では、HDX接続で許可される最大ビデオ品質レベルを指定します。最大ビデオ品質を指定すると、マルチメディアコンテンツに対する一定レベルのQoS（Quality of Service）を保証できます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを指定するには、次のいずれかのオプションを選択します。

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

© 1999-2017 Citrix Systems, Inc. All rights reserved.

単一サーバー上で複数のビデオを同時に再生すると多くのリソースが消費され、サーバーのスケーラビリティが低下するこ
があります。

マルチメディア会議

この設定では、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクションテクノロジの使用を許可また
は禁止します。

デフォルトでは、許可されます。

この設定をポリシーに追加するときは、［Windows Mediaリダイレクト］設定で［許可］（デフォルト）が選択されている
ことを確認してください。

マルチメディア会議を使用する場合、次の条件を満たしていることを確認してください。

- マルチメディア会議に使用するWebカメラの製造元が提供するドライバーが、クライアントにインストール済みである。
- ビデオ会議セッションの開始前にWebカメラをユーザーデバイスに接続している。サーバーで、複数のWebカメラを同時
に使用することはできません。ユーザーデバイス上に複数のWebカメラが装着されている場合、サーバーでは、最初に検
出されたものから接続が試行されます。

このポリシーは、汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合は必要ありません。その場合は、VD
にWebカメラドライバーをインストールします。

WAN接続でのWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定によりリアルタイムマルチメディアトラ
ンスコードが有効になります。これにより、オーディオやビデオのメディアコンテンツを劣化ネットワーク経由でモバイル
デバイスにストリーム配信することができるようになり、またWAN通信経由でのWindows Mediaコンテンツの配信方法を改
善することでユーザーエクスペリエンスが向上します。

デフォルトでは、WANを介したWindows Mediaコンテンツの配信が最適化されます。

この設定をポリシーに追加するときは、**［Windows Mediaリダイレクト］**設定で**［許可］**が選択されていることを確認して
ください。

この設定を有効にすると、メディアのストリーム配信を有効にするリアルタイムマルチメディアトランスコードが必要に応
て自動的に適用され、ネットワーク条件が悪い場合でもシームレスなユーザーエクスペリエンスが提供されます。

WAN接続でのWindows Mediaマルチメディアリダイレクトでの GPUの使用

この設定はWindows Mediaにのみ適用され、Virtual Delivery Agent（VDA）上のグラフィック処理ユニット（GPU）でリアル
タイムマルチメディアトランスコード処理を行うことができるようになります。これにより、サーバースケーラビリティが
善されます。GPUでのトランスコード処理は、VDA側にハードウェアアクセラレーションをサポートするGPUが搭載されて
る場合にのみ可能になります。適切なGPUがない場合は、CPUがトランスコード処理を行います。

注：GPUでのトランスコード処理は、NVIDIA社のGPUでのみサポートされます。

デフォルトでは、WANを介したWindows MediaコンテンツVDA側のGPUを使用して最適化する機能は禁止されていま
す。
この設定をポリシーに追加するときは、［Windows Mediaリダイレクト］設定および［WAN接続でのWindows Mediaマルチ
メディアリダイレクトの最適化］設定で［許可］が選択されていることを確認してください。

Windowsメディアフォールバック防止

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定はHTML5とWindows Mediaの両方に適用されます。この設定をHTML5で使用するには、***[HTML5ビデオリダイレクション]*** ポリシーを **[許可]** に設定します。

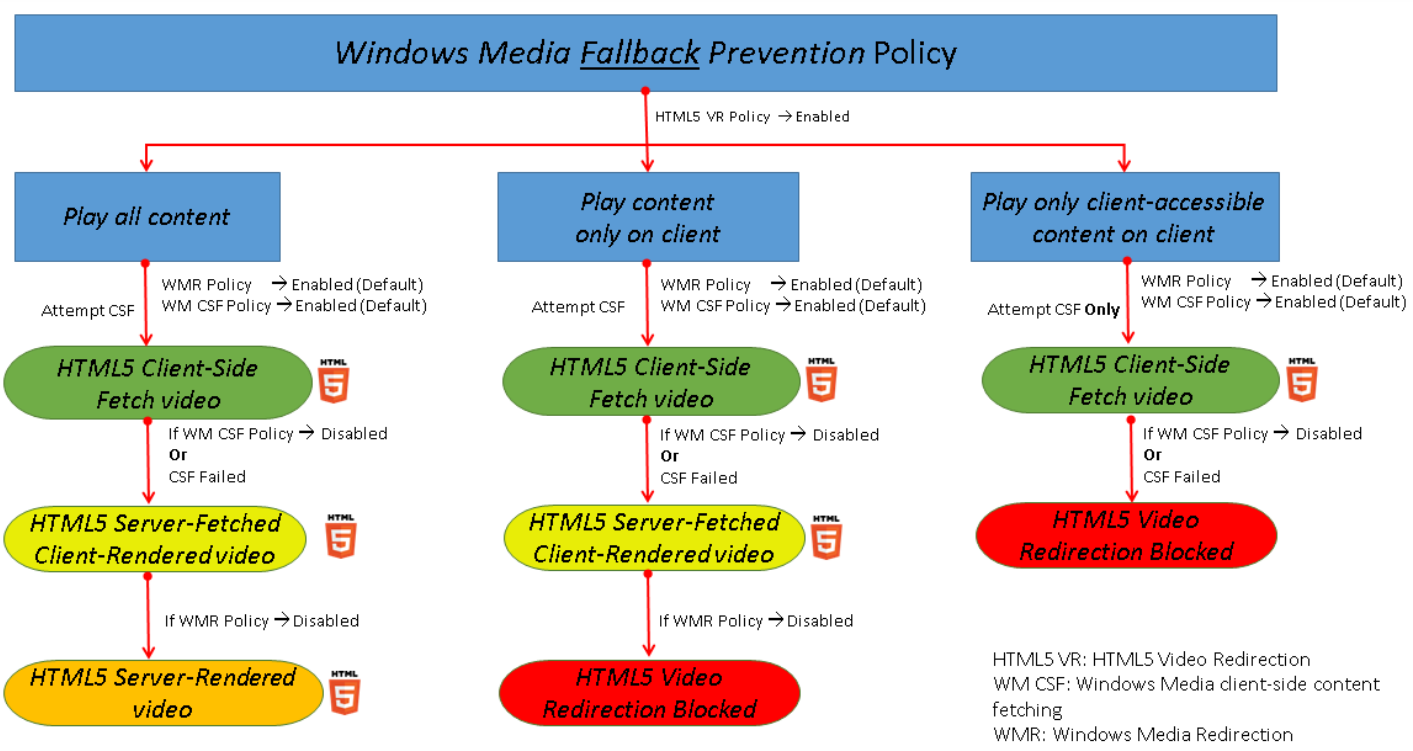
管理者はこのWindowsメディアバック防止ポリシー設定を使って、ユーザーへのストリーム配信コンテンツの配信方法を指定できます。

デフォルトでは、この設定は構成されていません。この設定が［未構成］に設定されている場合の動作は、**[すべてのコンテンツを再生]** のものと同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生**: クライアント側でのコンテンツ取得、Windows Mediaリダイレクトの順に試行します。失敗した場合、サーバー上でコンテンツを再生します。
- **クライアントにあるすべてのコンテンツのみを再生**: クライアント側でのフェッチ、Windows Mediaリダイレクトの順に試行します。失敗した場合、コンテンツは再生されません。
- **クライアント上のクライアントがアクセスできるコンテンツのみを再生** クライアント側でのフェッチのみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツを再生しない場合、プレーヤーのウィンドウにエラーメッセージ「Company has blocked video because of lack of resources」が表示されます（デフォルトの期間は5秒間）。



エラーメッセージが表示される期間は、VDAの次のレジストリキーでカスタマイズできます。レジストリにエントリがない場合は、期間はデフォルトで5秒間になります。

> ### 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と

© 1999-2017 Citrix Systems, Inc. All rights reserved.

判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

レジストリパスは、VDAのアーキテクチャによって異なります。

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前：VideoLoadManagementErrDuration

種類：DWORD

範囲：1からDWORD制限まで（デフォルト = 5）

単位：秒

Windows Mediaのクライアント側でのコンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定では、インターネットまたはイントラネット上のマルチメディアファイルを、XenAppやXenDesktopのホストサーバーを介さずにソースプロバイダーからユーザーデバイスへ直接ストリーム配信することを許可または禁止します。

デフォルトでは、**[許可]**に設定されています。この設定を許可すると、マルチメディアファイルがホストサーバーではなくユーザーデバイス上で処理されるため、ネットワーク消費が効率化され、サーバースケーラビリティが向上します。また、ユーザーデバイス上にMicrosoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをインストールする必要もなくなり、ユーザーデバイスではURLからファイルを再生することだけできればよくなります。

この設定をポリシーに追加するときは、**[Windows Mediaリダイレクト]**設定で**[許可]**が選択されていることを確認してください。**[Windows Mediaリダイレクト]**設定を無効にすると、Windows Mediaのクライアント側でのコンテンツ取得機能も無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。

デフォルトでは、**[許可]**に設定されています。HTML5の場合、***[HTML5ビデオリダイレクション]***ポリシーが**[禁止]**に設定されているとこの設定は適用されません。

この設定を許可すると、セッション内で再生されるオーディオおよびビデオの品質が向上して、ユーザーデバイス上のファイルを再生しているときの品質に近くなります。マルチメディアデータはサーバーからユーザーデバイスに、元の圧縮されたままの形で配信され、ユーザーデバイス側でメディアの展開およびレンダリングが行われます。

Windows Mediaダイレクトでは、Microsoft社のDirectShow、DirectX Media Objects（DMO）、およびMedia Foundation規格に準拠するコーデックでエンコードされたマルチメディアファイルが最適化されます。ユーザーデバイス側でメディアファイルの展開およびレンダリングを行うため、そのファイルのエンコーディング形式をサポートするコーデックがユーザーデバイス上にインストールされている必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、Citrix Receiverでオーディオサポートは無効になっています。ユーザーがICAセッション内でマルチメディアアプリケーションを実行できるようにするには、管理者がオーディオのサポートを有効にして、ユーザーがCitrix Receiverのオーディオ機能を有効にする必要があります。

Windows Mediaリダイレクトによるメディアの再生品質が、基本的なICA圧縮および通常のオーディオ機能での品質よりも悪い場合は、**[禁止]**を選択します。キーフレームの周波数が著しく低いメディアデータを狭帯域幅接続で再生する場合などで、この機能による問題がまれに生じることがあります。

Windows Mediaリダイレクトのバッファーサイズ

この設定は古いものであり、HTML5には適用されません。

この設定では、マルチメディアアクセラレーションのバッファーサイズを1～10秒の間で指定します。

デフォルトのバッファーサイズは5秒です。

Windows Mediaリダイレクトのバッファーサイズ使用

この設定は古いものであり、HTML5には適用されません。

この設定では、**[Windows Mediaリダイレクトのバッファーサイズ]**設定で指定したバッファーサイズを有効または無効にします。

デフォルトでは、指定されているデフォルトバッファーサイズが使用されません。

この設定が無効の場合、またはWindows Mediaリダイレクトバッファーサイズ設定が構成されていない場合、サーバーではデフォルトのバッファーサイズ値（5秒）が使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マルチストリーム接続のポリシー設定

Dec 05, 2017

マルチストリーム接続セクションには、単一セッションでの複数ICA接続のQoS（Quality of Service）優先度の管理に関するポリシー設定が含まれます。

UDP を使用したオーディオ

この設定 では、サーバーのUDPを使用したオーディオを許可または禁止します。

デフォルトでは 許可されます。

この機能を有効にすると、 サーバー上のUDPポートが開き、［UDPでのオーディオリアルタイムトランスポート］設定 が有効なすべての接続でそのポートが使用されます。

オーディオUDP ポートの範囲

この設定項目 では、Virtual Delivery Agent（VDA）でユーザーデバイスとのオーディオパケットデータの送受信に使用されるポート番号の範囲を「 lowest port number,highest port number」形式で 指定します。VDAでは、 オーディオデータの送受信に各UDPポートペアの使用が試行されます。 まず最小のポート番号が使用され、以降の試行では2ずつ番号を増やしていきます。各ポートは、受信トラフィックと送信トラフィックの 両方に使用されます。

デフォルトでは、 「16500,16509」に設定されています。

マルチポート ポリシー

この設定 では、ICAトラフィックで使用されるTCPポートおよび各ポートのネットワーク 優先度を指定します。

デフォルトでは、 プライマリポート（2598）に優先度［高］が設定されています。

ポートには 、以下の優先度を設定できます。

- 最高 - Webカメラ を使ったビデオ会議など、リアルタイムプロセスに適しています。
- 高 - 画面、キーボード 、マウスなど、インタラクティブなトラフィックに適しています。
- 中 - クライアント側 ドライブのマッピング機能など、バルクプロセスに適しています。
- 低 - 印刷など、 バックグラウンドプロセスに適しています。

各ポートには 異なる優先度を設定する必要があります。つまり、CGPポート1とCGPポート3の両方で 優先度に［最高］を設定することはできません。

ポートの優先度 設定を削除するには、ポート番号として「0」を入力します。プライマリポートの 優先度設定を削除したり変更したりすることはできません。

この設定項目 をポリシーに追加したら、サーバーを再起動します。この設定は、 ［マルチストリーム］ポリシー設定が 有効な場合のみ適用されます。

マルチストリームコンピューター設定

この設定では、サーバーのマルチストリーム機能を有効または無効にします。

デフォルトでは、無効になっています。

Citrix NetScaler SD-WANでマルチストリーム機能をサポートする場合は、この設定項目を使用する必要はありません。このポリシー設定は、サードパーティ製のルーターや従来のBranch Repeaterを使用する環境でQoS（Quality of Service）優先度を

© 1999-2017 Citrix Systems, Inc. All rights reserved.

指定するときに使用できます。

この設定の変更を反映させるには、サーバーを再起動する必要があります。
重要： このポリシー設定を、帯域幅を制限するポリシー設定（［セッション全体の最大帯域幅］など）と一緒に使用すると、意図したとおりに動作しなくなる場合があります。ポリシーでこの設定を使用する場合は、帯域幅を制限する設定を構成しないでください。

マルチストリーム ユーザー設定

この設定 では、ユーザーデバイスのマルチストリーム機能を有効または無効にします。

デフォルトでは、 すべてのユーザーに対して無効になっています。

この設定は、 ［マルチストリームコンピューター設定］ポリシー設定が 有効なホストに対してのみ適用されます。
重要： このポリシー設定を、帯域幅を制限するポリシー設定 （ ［セッション全体の最大帯域幅］など）と一緒に使用すると、 意図したとおりに動作しなくなる場合があります。ポリシーでこの設定を使用する場合は、 帯域幅を制限する設定を構成しないでください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポートリダイレクトのポリシー設定

Dec 05, 2017

ポートリダイレクトセクションには、クライアント側のLPTポートおよびCOMポートのマッピングに関するポリシー設定が含まれています。

7.0より前のバージョンのVirtual Delivery Agentの場合は、次のポリシー設定を使用してポートリダイレクトを構成します。**7.0から8.0**のバージョンのVDAの場合は、このような設定はレジストリを使って行います。詳しくは、「レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合は、次のポリシー設定を使用します。

クライアント COM ポートを自動接続する

この設定では、ユーザーのログオン時にクライアント側のCOMポートに自動的に接続する機能を有効または無効にします。

デフォルトでは無効になっています。

クライアントLPTポートを自動接続する

この設定では、ユーザーのログオン時にクライアント側のLPTポートに自動的に接続する機能を有効または無効にします。

デフォルトでは無効になっています。

クライアントCOMポートリダイレクト

この設定では、COMポートのクライアント側へのリダイレクトを許可または禁止します。

デフォルトでは禁止されます。

関連する設定項目は以下のとおりです。
- COM ポート リダイレクトの最大帯域幅 (Kbps)
- COM ポート リダイレクトの最大帯域幅 (%)

クライアントLPTポートリダイレクト

この設定では、LPTポートのクライアント側へのリダイレクトを許可または禁止します。

デフォルトでは禁止されます。

LPTポートは、印刷ジョブをユーザーデバイス上のプリンターオブジェクトではなくLPTポートに送信するレガシーアプリケーションでのみ使用されます。最近のアプリケーションでは、LPTポートではなくプリンターオブジェクトに印刷ジョブを送信されます。このポリシー設定は、LPTポートへの出力を行うレガシーアプリケーションをホストするサーバーに対してのみ使用します。

クライアントのCOMポートのリダイレクトは双方向ですが、LPTポートのリダイレクトは出力のみでICAセッション内の\\client\LPT1と\\client\LPT2に制限されていることに注意してください。

関連する設定項目は以下のとおりです。
- LPTポートリダイレクトの最大帯域幅（Kbps）
- LPTポートリダイレクトの最大帯域幅（%）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

印刷のポリシー設定

Dec 05, 2017

印刷セクションには、クライアントからの印刷の管理に関するポリシー設定が 含まれています。

クライアントプリンター リダイレクト

この設定項目では、ユーザーのログオン時にクライアントプリンターをサーバーに自動的にマップすることを 許可または禁止します。

デフォルトでは 許可されます。この設定項目が無効の場合、PDFプリンターは セッションで自動作成されません。

関連する 設定項目：クライアントプリンターを自動作成する

デフォルト プリンター

この設定では、 セッションのデフォルトのクライアントプリンターとして設定するプリンターを 指定します。

デフォルトでは、 ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。

［デフォルトプリンターの設定を 変更しない］を選択すると、 リモートデスクトップサービスまたはWindowsのユーザープロファイルで設定されているデフォルト プリンターが使用されます。このオプションを選択すると、 デフォルトプリンターはプロファイルに保存されず、 ほかのセッションやクライアント側のプロパティにより変更されなくなります。このオプションでは、セッションで 最初に自動作成されたプリンターがセッションのデフォルトプリンターになります。つまり、以下のどちらかのプリンターになります。

- Windowsサーバーの コントロールパネルの［デバイスとプリンター］で ローカルに追加された最初のプリンター。
- サーバーにローカルプリンターが追加されていない場合は、最初に自動作成された プリンター。

プロファイルの設定に基づいてユーザーに最も近いプリンターを提供する （近接プリンター機能を使用する）場合に、このオプションを使用できます。

プリンター 割り当て

この設定は、 ［デフォルト プリンター］設定および ［セッション プリンター］設定の代わりに 使用します。特定のサイト、大規模グループ、 または組織単位用のポリシーを構成する場合は、 ［デフォルト プリンター］設定および ［セッション プリンター］設定を使用します。［プリンター割り当て］設定は、多くの プリンターのグループを複数のユーザーに割り当てる場合に使用します。

この設定では、ユーザーデバイスを一覧に追加して、そのユーザーデバイス上のデフォルトプリンターが セッションでどのように使用されるかを 指定します。

デフォルトでは、 ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。

また、各ユーザーデバイスに対してセッションで自動作成する ネットワークプリンターを指定します。デフォルトでは、プリンターは指定されていません。

- デフォルト プリンター値は、以下のように設定します。
  ユーザーデバイスの 現在のデフォルトプリンターを使用する場合は、 ［変更しない］ を選択します。

  現在のリモートデスクトップサービスまたはWindowsのユーザープロファイルで設定されているデフォルト プリンターを

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用する場合は、［変更しない］を選択します。このオプションを選択すると、デフォルト プリンターはプロファイルに保存されず、ほかのセッションやクライアント側のプロパティにより変更されなくなります。このオプションでは、セッションで最初に 自動作成されたプリンターがセッションのデフォルトプリンターになります。つまり、以下のどちらかのプリンターになります。

- Windowsサーバーの コントロールパネルの［デバイスとプリンター］で ローカルに追加された最初のプリンター。
- サーバーにローカルプリンターが追加されていない場合は、最初に自動作成された プリンター。

- セッション プリンター値を設定するには、自動作成するプリンターのUNCパスを入力します。この一覧の設定は、ユーザーがログオンするたびに適用できます。

プリンター 自動作成イベントログの設定

この設定では、プリンターの自動作成処理中にログに記録するイベントを 指定します。エラーおよび 警告をログに記録しない、エラーのみを記録する、またはエラーおよび警告を記録することを選択できます。

デフォルトでは、エラー および警告がログに記録されます。

たとえば、プリンターのネイティブドライバーをインストールできず、代わりにユニバーサルプリンタードライバーがインストールされた場合は、警告がログに記録されます。このような状況でユニバーサルプリンター ドライバーを使用できるようにするには、［ユニバーサル印刷の使用］設定で［ユニバーサル印刷のみを使用する］または［要求されたドライバーを使用できない場合にのみ ユニバーサル印刷を使用する］を選択します。

セッション プリンター

この設定では、セッションで自動作成するネットワークプリンターを 指定します。

デフォルトでは、プリンターは指定されていません。

自動作成するプリンターを追加するには、そのプリンターのUNCパスを入力します。この一覧の設定は、ユーザーが ログオンするたびに適用できます。

プリンターの自動作成を待機する（サーバーデスクトップ）

この設定では、サーバーデスクトッププリンターが自動作成されるまでセッションへの接続を遅延させるかどうかを指定します。

デフォルトでは、プリンターの作成を待機せずに接続します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クライアントプリンターのポリシー設定

Dec 05, 2017

クライアントプリンターセクションには、クライアントプリンターに関するポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保存、およびプリントサーバーへの接続のための設定が含まれています。

クライアントプリンターを自動作成する

この設定では、自動作成するクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定より優先されます。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、［クライアントプリンターリダイレクト］設定で［許可］が選択されている場合にのみ適用されます。

この設定では、次のオプションを選択します。

- ［すべてのクライアントプリンターを自動作成する］では、ユーザーデバイス上のすべてのプリンターが自動作成されます。
- ［デフォルトのクライアントプリンターのみを自動作成する］では、ユーザーデバイス上のデフォルトプリンターのみが自動作成されます。
- ［ローカル（ネットワークを介さない）クライアントプリンターのみを自動作成する］では、ユーザーデバイスのローカルポート（LPTポート、COMポート、USBポート、TCP/IPポートなど）に直接接続されているプリンターのみが自動作成されます。
- ［クライアントプリンターを自動作成しない］では、ユーザーがログオンするときのすべてのクライアントプリンターの自動作成が無効になります。リモートデスクトップサービス（RDS）で設定されているクライアントプリンターの自動作成オプションが適用されるようにするには、このオプションを選択して、そのポリシーの優先度をほかのポリシーよりも高くします。

汎用ユニバーサルプリンターを自動作成する

注： このポリシー設定問題を解決するためのHotfixがCitrix Knowledge Center のCTX141565およびCTX141566で提供されています。
この設定では、UDPをサポートするクライアントのセッションで Citrixユニバーサルプリンターの汎用印刷オブジェクトを自動作成する機能を有効または無効にします。

デフォルトでは、 汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連する設定項目は以下のとおりです。

- ユニバーサル印刷の使用
- ユニバーサルドライバーの優先度

クライアントプリンター名

この設定では、自動作成されるクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

［標準のプリンター名］を選択すると、「セッション3のクライアント名のHP LaserJet 4」などのプリンター名が作成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MetaFrame Presentation Server 3.0またはそれ以前のバージョンと互換性のある命名規則でクライアントプリンターを作成するには、［従来のプリンター名］を選択します。この場合、「Client/clientname#/HPLaserJet 4」などの名前が使用されます。このオプションは安全性に欠けます。
注： このオプションは、以前のバージョンのXenAppやXenDesktopとの互換性を保持する場合に使用します。

プリントサーバーへの直接 接続

この設定では、 ネットワーク共有上のクライアントプリンターを使用するときに、クライアントを経由せずに仮想デスクトップやホスト サーバーからプリントサーバーに直接接続することを有効または無効にします。

デフォルトでは 有効になっています。

仮想 デスクトップやホストサーバーとネットワークプリントサーバーが同一LAN上にあり、WANで隔たれていない場合に直接 接続を有効にします。この場合、仮想デスクトップやホストサーバーからLANを介してプリントサーバーに直接印刷データが転送されるため、処理が高速になります。

仮想デスクトップやホストサーバーとネットワークプリントサーバーがWANで隔たれていたり、遅延や 帯域幅の問題が生じたりする場合は、直接 接続を無効にできます。直接接続を無効にすると、印刷ジョブがユーザーデバイスに送信され、 そこからネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは 圧縮されるため、データがWANを横断するときに消費される帯域幅が少なくなります。

同じ名前を持つネットワークプリンターが2つ存在する場合は、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定では、自動作成されるクライアントプリンターのドライバー置換規則を指定します。

この設定は、自動作成されるクライアントプリンターの一覧からMicrosoft OneNoteとXPS Document Writerを除外して構成されます。

ドライバー置換規則を定義すると、プリンターの自動作成時に特定のドライバーの使用を許可したり、ユニバーサル印刷の使用を指定したりできます。ドライバーの置換規則では、サーバーとクライアント間でドライバー名をマップして、ユーザーデバイスから提供されるプリンタードライバーではなくサーバー上のドライバーが使用されるように設定します。これにより、サーバー側のドライバーとクライアント側のドライバーの名前が異なっていても、サーバー上のアプリケーションからクライアントプリンターに出力できるようになります。

ドライバー置換規則の一覧では、ドライバーマッピングの追加、既存のマッピングの編集、マッピングに対するカスタム設定の上書き、マッピングの削除、および一覧のドライバーエントリの順序の変更を実行できます。マッピングを追加するには、クライアント側プリンタードライバーの名前を入力し、それを置換するサーバー側プリンタードライバーを選択します。

プリンター プロパティの保存

この設定では、ユーザーが変更したクライアントプリンターのプロパティをどこに保存するかを 指定します。

デフォルトでは、 システムの判定により、クライアントデバイスに保存できない場合にのみ ユーザープロファイルにプリンタープロパティが保存されます。

この 設定では、次のオプションを選択します。

- ［クライアントデバイスにのみ保存する］ は、更新されないユーザープロファイル（固定プロファイルや移動プロファイル）を使用する環境で選択します。 このオプションは、サーバーファーム内のすべてのサーバーで XenApp 5以降が動作しており、ユーザーがCitrix Online Plug-in Versions 9～12.x、またはCitrix Receiver 3.xを使用する場合にのみ選択してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ［ユーザープロファイルにのみ保存する］ は、使用帯域幅とログオン速度に制限があるユーザーデバイス（このオプションではネットワークトラフィックが軽減されます）、または古いプラグインソフトウェアを使用するユーザーのためのオプションです。 このオプションでは、サーバー上のユーザープロファイルにプリンタープロパティを保存し、 ユーザーデバイス上のプロパティを使用しません。このオプションは、 Presentation Server 3.0またはそれ以前のバージョンと、 Presentation Server クライアント8.x以前が使用される環境で選択してください。ただし、このオプションはリモートデスクトップ サービス（RDS）の移動プロファイルにのみ適用されます。
- ［クライアントに保存できない場合にのみユーザープロファイルに保存する］ では、システムによりプリンタープロパティの保存先が決定されます。 ユーザーデバイスに保存できない場合にのみ、 ユーザープロファイルにプリンタープロパティが保存されます。 さまざまな環境やクライアントの条件に対応できるオプションですが、 システムチェック処理が行われるため、ログオン時に遅延が生じたり使用帯域幅が増えたりすることがあります。
- ［プリンタープロパティを保持しない］ を選択した場合、プリンタープロパティは保持されません。

クライアントプリンターの保持と復元

この設定では、 ユーザーデバイス上のプリンターをセッション間で保持および再作成する機能を有効または無効にします。 デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

「保持されるプリンター」とは、 ユーザーが作成し次回セッションの開始時に再作成されるプリンターを指します。 保持されるプリンターがXenAppにより再作成されるときは、 ［クライアントプリンターを自動作成する］設定以外の すべてのポリシー設定が考慮されます。

「復元されるプリンター」とは、 管理者がカスタマイズしクライアントポートに永続的に接続された状態で保存されるプリンターを指します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ドライバーのポリシー設定

Dec 05, 2017

ドライバーセクションには、プリンタードライバーに関するポリシー設定が含まれています。

付属のプリンター ドライバーの自動 インストール

この設定項目 では、 Windowsに付属のドライバーセットや、 pnputil.exe /aによりホスト上にステージングされたドライバーパッケージから、プリンタードライバーを必要に応じて自動的にインストールする機能を有効または無効にします。

デフォルトでは、 自動インストールが有効になっています。

ユニバーサル ドライバーの優先度

この設定項目 では、ユニバーサルプリンタードライバーの使用優先順位を指定します。 一覧の上位にあるドライバーから順に使用されます。

デフォルトの 優先順位は以下のとおりです。

- EMF
- XPS
- PCL5c
- PCL4
- PS

この一覧では、ドライバーを追加、編集、 または削除したり、優先順位を変更したりできます。

ユニバーサル 印刷の使用

この設定 では、どのような状況でユニバーサル印刷を使用するかを指定します。

デフォルトでは、要求されたドライバーを使用できない場合にのみ ユニバーサル印刷を使用します。

ユニバーサル印刷 では、プリンター固有の標準ドライバー の代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理がシンプルになります。ユニバーサルプリンタードライバーを 使用できるかどうかは、ユーザー デバイス、ホスト、およびプリントサーバーソフトウェアにより決定されます。構成によっては、ユニバーサル 印刷を使用できない場合があります。

この設定 では、次のオプションを選択します。

- ［プリンター 固有のドライバーのみを使用する］では、クライアントプリンターの自動作成時に、そのプリンター固有の標準プリンタードライバーが使用されます。 必要なプリンタードライバーがサーバーにない場合、そのクライアントプリンターは自動作成されません。
- ［ユニバーサル印刷 のみを使用する］を有効にすると、プリンター固有の標準ドライバーは使用されません。 ユニバーサルプリンタードライバーのみを使用してプリンターが作成されます。
- ［要求されたドライバーを使用できない場合にのみ ユニバーサル印刷を使用する］では、可能な場合はプリンター固有の標準ドライバーが使用されます。 プリンター固有のドライバーがサーバーに ない場合は、 最適なユニバーサルドライバーを使用してクライアントプリンターが自動作成されます。
- ［ユニバーサル印刷を使用できない場合にのみ プリンター固有のドライバーを使用する］では、可能な場合はユニバーサルプリンタードライバーが使用されます。 ユニバーサルプリンタードライバーが サーバーにない場合は、適切な プリンター固有の標準ドライバーを使用してクライアントプリンターが自動作成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Universal Print Serverのポリシー設定

Dec 05, 2017

Universal Print Serverセクションには、Universal Print Serverの動作を制御するためのポリシー設定が含まれています。

Universal Print Serverの有効化

この設定項目 では、仮想デスクトップや公開アプリケーションでの Universal Print Server機能を有効または無効にします。この設定項目を仮想デスクトップまたはアプリケーションのホストサーバーを含んでいる組織 単位（OU）に割り当てます。

デフォルトでは、 Universal Print Serverは無効になっています。

この設定 では、以下のいずれかのオプションを選択します。

- **有効。Windowsのリモート印刷機能にフォールバックする** 。ネットワークプリンターへの接続時に Universal Print Server が使用されます。Universal Print Serverを使用 できない場合は、Windowsの印刷プロバイダーが使用されます。Windows印刷プロバイダーにより作成されたすべてのプリンターは、 引き続きWindows印刷 プロバイダーによって処理されます。
- **有効。Windows のリモート印刷機能にフォールバックしない** 。ネットワークプリンターへの接続時に Universal Print Serverのみが使用されます。Universal Print Serverを 使用できない場合は、ネットワークプリンターの接続に失敗します。この設定により、 Windowsの印刷プロバイダーを使用したネットワーク印刷を禁止できます。Windows印刷プロバイダーにより作成されたプリンターは、この設定が構成された ポリシーがアクティブな間は作成されなくなります。
- **無効**：Universal Print Server機能が無効になります。UNC名のネットワークプリンターに接続するときに、 Universal Print Serverによる接続は試行されません。 リモートプリンターへの接続では、Windowsのリモート印刷機能が 引き続き使用されます。

Universal Print Server印刷データストリーム（CGP）ポート

この設定 では、Universal Print Server印刷データ ストリームCGP（Common Gateway Protocol）リスナーが使用するTCPポート番号を指定します。このポリシー設定を構成したポリシーは、 プリントサーバーを含んでいる組織単位に割り当てます。

デフォルトのポート番号は、 7229に設定されています。

ほかのポートを指定する場合は、 1から65535の番号を使用してください。

Universal Print Server入力データストリームの最大帯域幅（Kbps）

この設定 では、各印刷ジョブからUniversal Print ServerにCGPで配信される 印刷データの転送速度の上限をキロビット/秒単位で指定 します。このポリシー設定を構成したポリシーは、仮想デスクトップまたはアプリケーションの ホストサーバーを含んでいる組織単位に割り当てます。

デフォルトでは、 上限なし（0）が指定されています。

Universal Print Server Webサービス（HTTP/SOAP）ポート

この設定では、Universal Print ServerのWebサービス（HTTP/SOAP）リスナーで使用されるTCPポート番号を指定します。Universal Print Serverはオプションコンポーネントで、ネットワークプリンターでのCitrixユニバーサルプリントドライバーの使用を有効にします。Universal Print Serverが使用されると、印刷コマンドがSOAP over HTTP上のSOAPを経由してXenAppおよびXenDesktopホストからUniversal Print Serverに送信されます。この設定は、Universal Print ServerがHTTP/SOAP要求を受信するためリスンするデフォルトのTCPポートを変更します。

ホストおよびプリントサーバーのHTTPポートの両方を等しく構成する必要があります。ポートを同じように構成しないと、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ホストソフトウェアがUniversal Print Serverに接続しません。この設定は、XenAppおよびXenDesktop上のVDAを変更します。また、Universal Print Serverのデフォルトのポートを変更する必要があります。

デフォルトのポート番号は、8080に設定されています。

ほかのポートを指定する場合は、0から65535の番号を使用してください。

負荷分散のためのユニバーサルプリントサーバー

この設定には、Citrixのほかの印刷ポリシー設定を評価した後、セッション起動時に確立されるプリンター接続の負荷分散に使用するUniversal Print Serverの一覧が表示されます。プリンターの作成時間を最適化するには、すべてのプリントサーバーに同じ共有プリンターを設定することをお勧めします。負荷分散のために追加できるプリントサーバーの数に上限はありません。

この設定により、プリントサーバーのフェールオーバー検出とプリンター接続復旧も実装できます。プリントサーバーは定期的に可用性を確認されます。サーバー障害が検出されると、そのサーバーは負荷分散スキーマから削除され、そのサーバーのプリンター接続は他の利用可能なプリントサーバーに再分配されます。障害が発生していたプリントサーバーが復旧すると、負荷分散スキーマに戻されます。

各サーバーがプリントサーバーであるかや、すべてのサーバーに同じ共有プリンターがインストールされていることを確認するには、**[サーバーの検証]**をクリックします。この操作にはしばらく時間がかかる可能性があります。

Universal Print Serverのサービス停止のしきい値

この設定では、ロードバランサーが、反応しないプリントサーバーの復旧を待機する時間を指定します。タイムアウト後、ロードバランサーはそのサーバーが永続的にオフラインであると判定し、そのロードを他の利用可能なプリントサーバーに再配信します。

デフォルトでは、このしきい値は180秒に設定されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユニバーサル印刷のポリシー設定

Dec 05, 2017

ユニバーサル印刷セクションには、ユニバーサル印刷の管理に関するポリシー設定が含まれています。

ユニバーサル 印刷EMF処理モード

この設定では、Windowsユーザー デバイス上でのEMFスプールファイルの処理方法を 制御します。

デフォルトでは、EMF スプールファイルがクライアント上のスプールキューに直接挿入されます。

この 設定では、次のオプションを選択します。

- ［EMFスプールファイルを再処理する］ を有効にすると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステム経由で送信されます。 通常、EMF再処理を必要とする ドライバーは 自動的に検出され、適切な印刷経路が使用されますが、セッションで正しく検出されない場合があります。そのような場合にこのオプションを選択します。
- Citrixユニバーサルプリンタードライバーで［EMFスプールファイルを直接挿入する］ を有効にすると、EMFレコードがホスト上でスプールされ、そのEMFスプールファイルがユーザーデバイス側に送信され処理されます。 通常、このEMFスプールファイルはクライアント上のスプール キューに直接挿入されます。EMF形式を処理できるプリンターおよびドライバーでは、この方法により印刷を高速に実行できます。

ユニバーサル 印刷イメージ圧縮制限

この設定では、Citrixユニバーサルプリンタードライバーでの イメージ印刷で使用できる品質レベルの上限を 指定します。

デフォルトでは、 イメージ品質の上限が ［最高 品質（無損失圧縮）］に設定されています。

［非 圧縮］を選択すると、EMF印刷では圧縮が無効になります。

この 設定では、次のオプションを選択します。

- 非圧縮
- 最高品質（無損失 圧縮）
- 高品質
- 標準品質
- 低品質（最大 圧縮）

この 設定項目を［ユニバーサル印刷最適化デフォルト］ と同じポリシーに追加する場合は、次の点に注意してください。

- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベル が ［ユニバーサル印刷最適化デフォルト］での設定よりも 低い場合は、 ［ユニバーサル印刷イメージ圧縮制限］の圧縮 レベルが適用されます。
- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、 ［ユニバーサル印刷最適化デフォルト］の ［必要なイメージ品質］および ［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル 印刷最適化デフォルト

この設定では、セッションで作成されるユニバーサルプリンター ドライバーのデフォルトの印刷最適化オプションを 指定します。

- ［必要なイメージ 品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。 デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを 印刷できます。
- ［ヘビーウェイト圧縮を有効にする］ では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに ［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。 デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- ［イメージおよびフォントのキャッシュ］ では、印刷ストリームで使用されているイメージやフォントをキャッシュする

© 1999-2017 Citrix Systems, Inc. All rights reserved.

かどうかを指定します。キャッシュを有効にすると、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。 デフォルトでは、埋め込みイメージおよびフォントが キャッシュされます。これらの設定は、ユーザーデバイスで その機能をサポートしている場合にのみ適用されます。
- ［非管理者によるこれらの設定の変更を許可する］ では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。 デフォルトでは、 禁止されています。

注： これらのすべての オプションは、EMF印刷に対してのみ適用されます。XPS印刷では、 ［必要な イメージ品質］オプションのみがサポートされます。
この 設定項目を［ユニバーサル印刷イメージ圧縮 制限］と同じポリシーに追加する場合は、次の点に注意してください。
- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベル が ［ユニバーサル印刷最適化デフォルト］での設定よりも 低い場合は、 ［ユニバーサル印刷イメージ圧縮制限］の圧縮 レベルが適用されます。
- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、 ［ユニバーサル印刷最適化デフォルト］の ［必要なイメージ品質］ および ［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル 印刷プレビューの設定

この設定では、自動作成プリンターまたは 汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを 指定します。

デフォルトでは、自動作成プリンターまたは汎用ユニバーサルプリンターの印刷 プレビューは使用できません。

この 設定では、次のオプションを選択します。
- 自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューを使用しない
- 自動作成プリンターの印刷プレビューのみを使用する
- 汎用ユニバーサルプリンターの印刷プレビューのみを使用する
- 自動作成プリンターおよび汎用ユニバーサルプリンターの印刷プレビューを使用する

ユニバーサル 印刷品質制限

この設定では、セッションでの印刷 出力で使用できる最大DPI値（インチあたりのドット数）を 指定します。

デフォルトでは ［制限なし］ が選択されており、ユーザーは接続しているプリンターで許可されている最高印刷 品質を選択できます。

そのほかの値を 選択すると、ユーザーが使用できる 出力解像度が制限されます。この設定では、印刷品質 自体と、ユーザーが接続するプリンターの印刷能力の両方が制限されます。 たとえば、 ［中 解像度（600dpi）］を選択した場合、ユーザーの印刷出力の 最高品質は600DPIに制限され、 ユニバーサルプリンターの［詳細設定］タブの印刷品質設定には、 中品質（600DPI）を超える解像度オプションが表示されなくなります。

この 設定では、次のオプションを選択します。
- ドラフト（150dpi）
- 低解像度（300dpi）
- 中解像度（600dpi）
- 高解像度（1200dpi）
- 制限なし

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セキュリティのポリシー設定

Nov 27, 2017

セキュリティセクションには、セッションの暗号化とログオンデータの暗号化の構成に関するポリシー設定が含まれています。

SecureICAの最低暗号化レベル

この設定では、サーバーとユーザーデバイスの間で送信するセッションデータの暗号化に必要な最低限の暗号化レベルを指定します。

重要： Virtual Delivery Agent 7.xの場合、この設定をRC5 128ビット暗号化によるログオンデータの暗号化を有効にするためだけに使用できます。ほかの暗号化レベルは、以前のバージョンのXenAppやXenDesktopとの互換性を保持する場合に使用します。

VDA 7.xの場合、セッションデータの暗号化はVDAのデリバリーグループの基本設定を使って設定されます。デリバリーグループに対して［Secure ICAを有効にする］がオンになっている場合、セッションデータはRC5（128ビット）暗号化で暗号化されます。デリバリーグループに対して［Secure ICAを有効にする］がオフになっている場合、セッションデータは基本レベルの暗号化で暗号化されます。

この設定では、次のオプションを選択します。

- ［基本］では、非RC5のアルゴリズムを使ってクライアント接続を暗号化します。この暗号化レベルでは、データストリームが直接読み取られることはありませんが、解読される恐れがあります。デフォルトでは、クライアントとサーバーの間のトラフィックには基本レベルの暗号化が使用されます。
- ［RC5（128ビット、ログオンのみ）］では、RC5 128ビット暗号化を使ってログオンデータを暗号化し、基本レベルの暗号化を使ってクライアント接続を暗号化します。
- ［RC5（40ビット）］では、RC5 40ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（56ビット）］では、RC5 56ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（128ビット）］では、RC5 128ビット暗号化を使ってクライアント接続を暗号化します。

クライアントとサーバー間の実際の通信では、Citrix製品やWindowsオペレーティングシステムでの暗号化設定も考慮されます。サーバーやユーザーデバイスでより高い暗号化レベルが設定されている場合は、その設定が優先されます。

機密データを使用するユーザーなど、特定のユーザーの通信データを保護してメッセージの整合性を保証するために、より高度な暗号化レベルを設定することもできます。ポリシーでより高度な暗号化レベルを指定すると、そのレベルよりも低い暗号化機能を使用するCitrix Receiverは、サーバーに接続できなくなります。

SecureICAでは認証の実行またはデータの整合性のチェックはされません。エンドツーエンドの暗号化を提供するには、SecureICAをTLSと共に使用します。

SecureICAではFIPS準拠のアルゴリズムは使用されません。このことが問題になる場合は、SecureICAを使用しないようにサーバーとCitrix Receiverを設定します。

SecureICAは、秘密保持のためにRFC 2040で説明されているようにRC5ブロック暗号を使用します。ブロックサイズは、64ビット（32ビットワード単位の倍数）です。キーの長さは、128ビットです。ラウンド数は、12です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

サーバーの制限のポリシー設定

Dec 05, 2017

［サーバーの制限］カテゴリには、アイドル状態の接続の制御に関する設定項目が含まれています。

サーバーのアイドルタイマーの間隔

この設定では、アイドル状態のセッション（ユーザーからの入力がない連続セッション）を自動的に切断するまでの時間をミリ秒単位で指定します。

デフォルトでは、アイドル状態の接続は切断されません。つまり、サーバーのアイドルタイマーの間隔は0です。この値を60000ミリ秒（60秒）以上に設定することをお勧めします。

> ### 注意
>
> このポリシー設定が使用される場合、セッションが指定した時間アイドル状態になると、「アイドル タイマーが切れました」ということを示すダイアログボックスがユーザーに表示されることがあります。このメッセージはMicrosoftのダイアログボックスで、Citrixポリシー設定によって制御されるものではありません。詳しくは、http://support.citrix.com/article/CTX118618を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの制限のポリシー設定

Dec 05, 2017

［セッションの制限］カテゴリには、セッションに接続してから強制的にログオフさせられるまでの時間を制御するための設定項目が含まれています。これらの設定は、Windows Server VDAには適用されません。

切断セッションタイマー

この設定項目では、切断状態でロックされたデスクトップセッションを一定期間後に自動的にログオフする機能を有効または無効にします。

デフォルトでは、切断状態のセッションはログオフされません。

切断セッションタイマーの間隔

この設定項目では、切断状態でロックされたデスクトップセッションを自動的にログオフするまでの時間を分単位で指定します。

デフォルトでは、1440分（24時間）に設定されています。

セッション接続タイマー

この設定項目では、ユーザーデバイスとデスクトップ間の連続セッションを一定期間後に自動的にログオフする機能を有効または無効にします。

デフォルトでは、無効になっています。

セッション接続タイマーの間隔

この設定項目では、ユーザーデバイスとデスクトップ間の連続セッションを自動的にログオフするまでの時間を分単位で指定します。

デフォルトでは、1440分（24時間）に設定されています。

セッションアイドルタイマー

この設定項目では、ユーザーからの入力がないユーザーデバイスとデスクトップ間の連続セッションを一定期間後に自動的にログオフする機能を有効または無効にします。

デフォルトでは、有効になっています。

セッションアイドルタイマーの間隔

この設定項目では、ユーザーからの入力がないユーザーデバイスとデスクトップ間の連続セッションを自動的にログオフするまでの時間を分単位で指定します。

デフォルトでは、1440分（24時間）に設定されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッション画面の保持のポリシー設定

Dec 05, 2017

セッション画面の保持セクションには、セッション画面の保持の管理に関するポリシー設定が含まれています。

セッション画面の保持

この設定では、セッション画面の保持機能を許可または禁止します。セッション画面の保持およびクライアントの自動再接続によって、ネットワークの中断からの回復後、ユーザーはCitrix Receiverセッションに自動的に再接続できます。

Citrix Receiver for Windows 4.7以降のセッション画面の保持では、Citrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、サーバーからクライアントにセッション画面の保持が同期されます。以前のバージョンのCitrix Receiver for Windowsを使用してセッション画面の保持を構成するのには、Studioポリシーを使用してレジストリまたはdefault.icaファイルを変更します。

注： Citrix Receiverグループポリシーオブジェクト管理テンプレートまたはCitrix Studioポリシーで**[セッション画面の保持を有効にする]** オプションを **[無効]** に設定すると、セッション画面の保持が無効になります。Citrix Studioのポリシーで **[セッション画面の保持を有効にする]** オプションを構成しておらず、Citrix Receiverグループポリシーオブジェクト管理でこのオプションを **[無効]** に設定すると、セッション画面の保持が有効になります。

セッション画面の保持機能は、ICAセッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。接続が失われると、ユーザーの表示は不透明になります。中断中、ユーザーにはセッションが停止しているように見えることがあり、ネットワーク接続が回復するとアプリケーションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

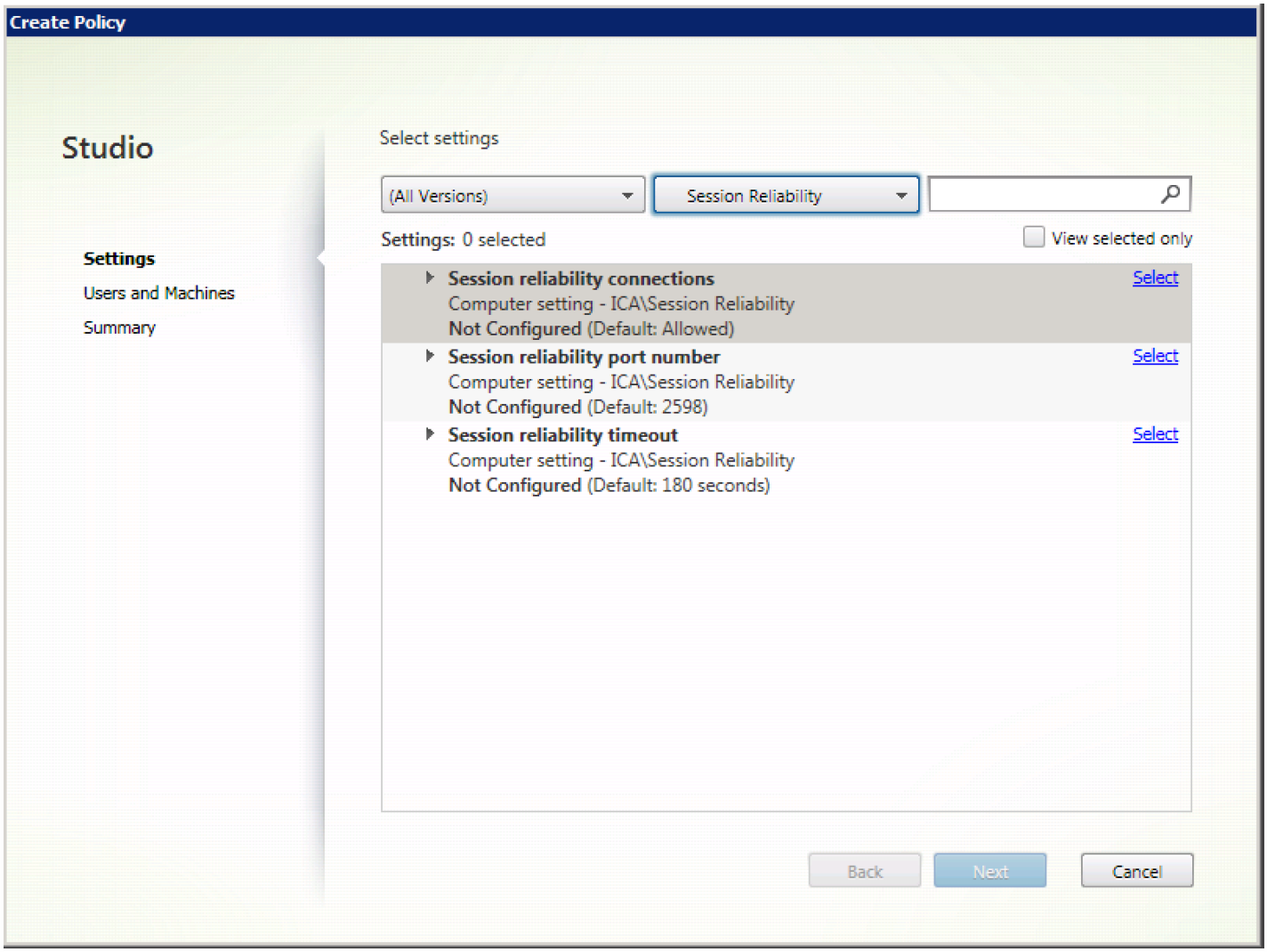
セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後でクライアントの自動再接続のポリシー設定により、切断セッションへの再接続が行われます。

デフォルトでは、セッション画面の保持が許可されます。

セッション画面の保持を無効にするには

1. Citrix Studioを開始します。
2. **［セッション画面の保持］** ポリシーを開きます。
3. ポリシーを **［禁止］** に設定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



セッション画面の保持のポート番号

この設定では、セッション画面の保持機能で使用される、受信TCPポートを指定します。

デフォルトでは、ポート番号は、2598に設定されます。

セッション画面の保持のポート番号を変更するには

1. Citrix Studioを開始します。
2. **[セッション画面の保持のポート番号]** ポリシーを開きます。
3. ポート番号を編集します。
4. **[OK]** をクリックします。

セッション画面の保持のタイムアウト

この設定では、セッション画面の保持機能でセッションをアクティブのままサーバー上に保持する時間を秒単位で指定します。ここで指定した時間が経過しても再接続されないセッションは、「切断セッション」として処理されます。

セッションの持続時間を長く設定することもできますが、この機能は利便性が高く、ユーザーに再認証を求めるメッセージを表示することもありません。セッションの持続時間を長くすると、ユーザーがデバイスを置き去りして承認されていないユーザーに利用される可能性が高まります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッション画面の保持のタイムアウトを変更するには

1. Citrix Studioを開始します。
2. **[セッション画面の保持のタイムアウト]** ポリシーを開きます。
3. タイムアウト値を編集します。
4. **[OK]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

タイムゾーン制御のポリシー設定

Dec 05, 2017

タイムゾーン制御セクションには、セッションでのローカルタイムの使用に関するポリシー設定が含まれています。

レガシークライアントのローカルタイムゾーンを検出する

この設定では、クライアント側のローカルタイムゾーンの検出を有効または無効にします。クライアントによっては、正確なタイムゾーン情報がサーバーに送信されない場合があります。

デフォルトでは、必要に応じてクライアント側のタイムゾーンが検出されます。

この設定は、詳しいタイムゾーン情報をサーバーに送信しない、従来のCitrix ReceiverまたはICAクライアントでの使用を前提にしています。Windowsでサポートされているバージョンの Citrix Receiverなど、サーバーに詳しいタイムゾーン情報を送信するCitrix Receiverで使用する場合、この設定は何の影響も及ぼしません。

クライアントのローカルタイムゾーンを使用する

この設定では、ユーザーセッションに適用されるタイムゾーンを 指定します。ユーザーセッションにサーバー側の タイムゾーンを適用したり、ユーザーデバイス側のタイムゾーンを適用したりできます。

デフォルトでは、ユーザーセッションの タイムゾーンが適用されます。

この機能を 使用するには、グループポリシーエディターの ［タイムゾーンリダイレクトを許可する］設定（［ユーザーの構成］ > ［管理用テンプレート］ > ［Windowsコンポーネント］ > ［リモート デスクトップサービス］ > ［リモートデスクトップセッションホスト］ > ［デバイスとリソースの リダイレクト］ ）を有効にしてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TWAINデバイスのポリシー設定

Dec 05, 2017

TWAINデバイスセクションには、デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピングと、サーバーからクライアントへのイメージ転送の最適化に関するポリシー設定が含まれています。

> **注意**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAIN デバイスリダイレクト

この設定 では、サーバー上でホストされるイメージ処理アプリケーションから、 クライアント側に接続されているデジタルカメラなどのTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは 許可されます。

関連する設定項目は以下のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスリダイレクトの 最大帯域幅（Kbps）
- TWAINデバイスリダイレクトの 最大帯域幅（%）

TWAIN 圧縮レベル

この設定 では、クライアントからサーバーに転送される画像の圧縮レベルを指定します。 画質を最高にするには［低］を、良好にするには ［中］を、低くするには ［高］を選択します。デフォルトでは、中 レベルの圧縮が選択されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

USBデバイスのポリシー設定

Dec 05, 2017

USBデバイスセクションには、USBデバイスのファイルリダイレクトの管理に関するポリシー設定が含まれています。

クライアントUSBデバイス最適化規則

クライアントUSBデバイス最適化規則をデバイスに適用して最適化を無効にしたり、最適化モードを変更したりできます。

ユーザーがUSB入力デバイスを接続すると、デバイスがUSBポリシー設定で許可されているかどうかホストがチェックします。デバイスが許可されている場合は、次にホストはデバイスの**クライアントUSBデバイス最適化規則**をチェックします。規則が指定されていない場合は、デバイスは最適化されません。 キャプチャモード（04）は署名デバイスに対する推奨モードです。長い遅延のためにパフォーマンスが低下しているその他のデバイスに対して、管理者は対話モード（02）を有効にできます。使用できるモードについては、以下の説明を参照してください。

ヒント

- Wacom署名パッドおよびタブレットを使用する場合、スクリーンセーバーを無効にすることをお勧めします。その実行方法については、このセクションの最後で説明します。
- Wacom STU署名パッドおよびタブレット製品シリーズの最適化のサポートは、XenAppおよびXenDesktopポリシーのインストールで事前構成されています。
- 署名デバイスはXenAppおよびXenDesktopで動作し、署名デバイスとして使用するためのドライバーは必要ありません。Wacomには、デバイスをよりカスタマイズするためインストールできる追加のソフトウェアがあります。http://www.wacom.com/を参照してください。
- 描画用タブレット。ある種の描画入力デバイスはPCI/ACPIバス上のHIDデバイスとされ、サポートされていません。これらのデバイスについては、クライアント上のUSBホストコントローラーで接続し、XenDesktopセッション内でリダイレクトする必要があります。

ポリシー規則は、スペースで区切ったtag=value式の形式にします。以下のタグがサポートされます。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスに対してサポートされます。サポートされるモード： 最適化なし - 値**01**。 対話モード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスにお勧めします。 キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨します。
VID	デバイス記述子のベンダーID
PID	デバイス記述子の製品ID
REL	デバイス記述子のリリースID

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	デバイス記述子のリリースID
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

例

Mode=00000004 VID=1230 PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=1230 PID=1230 class=03 #対話モードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=1230 PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=1230 PID=1230 #最適化を無効にしたデバイスのセットアップ（デフォルト）

Mode=00000200 VID=1230 PID=1230 #最適化を有効にしたデバイスのセットアップ

Wacom署名パッドデバイスのスクリーンセーバーの無効化

Wacom署名パッドおよびタブレットを使用する場合、次の手順に従ってスクリーンセーバーを無効にすることをお勧めします。

1. デバイスのリダイレクト後に**Wacom-STU-Driver**をインストールします。
2. **Wacom-STU-Display MSI**をインストールして、署名パッドコントロールパネルへのアクセスを有効にします。
3. **［コントロールパネル］**、**［Wacom STU Display］**、**［STU430］**または**［STU530］**の順に選択し、使用しているモデルのタブを選択します。
4. UACセキュリティウィンドウがポップアップ表示されたら**［Change］**をクリックしてから**［Yes］**をクリックします。
5. **［Disable slideshow］**を選択して、**［Apply］**をクリックします。

1つの署名パッドモデルに対しての設定が完了したら、それがすべてのモデルに適用されます。

クライアントUSB デバイスリダイレクト

この設定 では、USBデバイスのクライアント側へのリダイレクトおよびクライアント側からのリダイレクトを許可または禁します。

デフォルトでは、USB デバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定では、USBデバイスのリダイレクト規則を指定します。

デフォルトでは、規則は指定されていません。

ユーザーがUSBデバイスを装着すると、ホストデバイスで一覧の規則が順に検証され、マッチする最初の規則でリダイレクトが許可されているかどうかがチェックされます。最初の一致がAllow規則の場合、USBデバイスは仮想デスクトップにリモートで接続されます。最初の一致がDeny規則の場合、そのUSBデバイスはローカルデスクトップでのみ使用可能になります。一致する規則がない場合、デフォルトの規則が使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシー規則は、{Allow:|Deny:}の後に、「タグ=値」式をスペースで区切って設定します。以下のタグがサポートされます。

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

新しいポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の末尾に、#で始まる任意のコメントを追加できます。
- 空白行およびコメントのみの行は無視されます。
- タグには等号（=）を使用する必要があります（「VID=1230」など）。
- 各規則を1行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。
- USBクラスコードについては、USB Implementers Forum, Inc.のWebサイトを参照してください。

管理者定義のUSBポリシー規則の例

- ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
- DENY: Class=08 subclass=05 # Mass Storage
- すべてのUSBデバイスのリダイレクトを禁止する場合は、タグを指定せずに「DENY:」を使用します。

クライアントUSB プラグアンドプレイデバイスリダイレクト

この設定 では、カメラやPOS（Point-Of-Sale）デバイスなど、プラグアンドプレイ デバイスのセッション内での使用を許可または禁止します。

デフォルトでは、 許可されます。 ［許可］を選択すると、特定の ユーザーやグループのセッションですべてのプラグアンドプレイデバイスがリダイレクトされます。 ［禁止］を選択すると、デバイスはリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

視覚表示のポリシー設定

Dec 05, 2017

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信されるイメージの品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィック用の優先色数

このポリシー設定はVDAバージョン7.6 FP3以降で使用できます。8ビットオプションはVDAバージョン7.12以降で使用できます。

この設定により、単純なグラフィックがネットワーク経由で送信される際の色数を低下させることができます。ピクセルあたり8ビットまたは16ビットに色数を低下させると、画質をわずかに犠牲して、低帯域幅接続での応答性を潜在的に向上させることができます。［圧縮にビデオコーデックを使用する］ポリシー設定が［画面全体］に設定されている場合、8ビット色数はサポートされません。

デフォルトの優先色数は、ピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用されている場合、VDAは24ビット（デフォルト）色数にフォールバックします。

ターゲットフレーム数

この設定項目では、仮想デスクトップからユーザーデバイスに送信されるイメージの1秒あたりの最大フレーム数（fps）を指定します。

デフォルトの最大フレーム数は、30fpsです。

1秒あたりのフレーム数を高く（30など）すると、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を低く（10など）すると、ユーザーエクスペリエンスは低下しますが、サーバーのスケーラビリティが向上します。CPUが低速なユーザーデバイスに対しては、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。

サポートされている1秒あたりの最大フレームレートは60です。

表示品質

この設定では、ユーザーデバイス側に表示されるイメージの表示品質を指定します。

デフォルトでは、［中］に設定されています。

イメージの表示品質を指定するには、次のいずれかのオプションを選択します。

- **低**
- **中 -** 一般的に最良のパフォーマンスおよび帯域幅効率が提供されます。
- **高 -** 視覚的に無損失なイメージ品質が提供されます。
- 操作時は低品質 - 多くのネットワークトラフィックが発生している間は非可逆イメージが送信され、ネットワークトラフィックが減少したときに高品質な無損失イメージが送信されます。この設定により、帯域幅を制限されたネットワーク接続でのパフォーマンスが向上します。
- 常に無損失 - X線写真を表示するなど、イメージの画質が優先される場合では、［常に無損失］を選択します。これにより、イメージデータの損失を避けることができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[従来のグラフィックモード] 設定で［有効］を指定したポリシーに **[表示品質]** 設定を構成しても無視されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

動画のポリシー設定

Dec 05, 2017
動画セクションには、動画の圧縮機能を無効にしたり変更したりするためのポリシー設定が含まれています。

画質の下限 レベル

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定 では、アダプティブ表示の最低レベルの画質を指定します。圧縮率が小さい ほど、画質は高くなります。［超最高］、 ［最高］、［高］、［通常］、または［低］から選択します。

デフォルトでは、 ［通常］に設定されています。

動画圧縮

この設定では、アダプティブ表示を有効または無効にします。アダプティブ表示機能では、ビデオやスライドショーのスライド切り替え時の画質が、使用可能な帯域幅に基づいて自動的に調節します。アダプティブ表示を有効にすると、表示品質を劣化させることなくプレゼンテーションをスムーズに実行できます。
デフォルトでは、アダプティブ表示が有効になっています。

VDA 7.0～7.6では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA Version 7.6 FP1以降については、従来のグラフィックモードが有効の場合、または従来のグラフィックモードが無効でグラフィックの圧縮にビデオコーデックが使用されていない場合、この設定が適用されます。

従来のグラフィックモードが有効な場合、ポリシーの変更を適用する前にセッションを再起動する必要があります。アダプティブ表示とプログレッシブ表示は相互に排他的です。アダプティブ表示を有効にすると、プログレッシブ表示は無効になり、その逆の場合も同じです。ただし、プログレッシブ表示とアダプティブ表示の両方を同時に無効にすることは可能です。従来からの機能であるプログレッシブ表示はXenAppまたはXenDesktopにはお勧めしません。プログレッシブしきい値レベルを設定するとアダプティブ表示は無効になります。

プログレッシブ 圧縮のレベル

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定 では、最初にダウンロードされるイメージの品質を落として、初期表示のパフォーマンスを向上させる機能を制御します。

デフォルトでは、 プログレッシブ圧縮は適用されません。

プログレッシブ圧縮では、初期表示の後で、より詳細な イメージデータがダウンロード されます（そのイメージの圧縮レベルは非可逆圧縮設定で制御されます）。［最高］または［超最高］を選択すると、写真など 帯域幅に負荷のかかるグラフィックの表示パフォーマンスが向上します。

プログレッシブ 圧縮による効果を得るには、 ［非可逆 圧縮のレベル］よりも高い圧縮レベルを指定する必要があります。
注： プログレッシブ表示の圧縮レベルを 高くすると、セッションでの動的イメージの 対話操作性が向上します。この機能を有効にすると、3Dモデルを回転させる場合など、 イメージを動かしている間の表示品質は一時的に 低下します。イメージを停止させると、非可逆 圧縮のレベルで制御される画質が適用されます。
関連する設定項目は以下のとおりです。

- プログレッシブ圧縮の しきい値
- プログレッシブヘビーウェイト 圧縮

プログレッシブ 圧縮のしきい値

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。この設定 では、 プログレッシブ圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。この帯域幅に達しない クライアント接続にのみ圧縮が適用されます。

デフォルトの しきい値は、2147483647KB/秒です。

関連する設定項目は以下のとおりです。

- プログレッシブ圧縮の しきい値
- プログレッシブヘビーウェイト 圧縮

保持する最低フレーム数

この設定では、低帯域幅接続時に確保される動的イメージの最低フレーム数を、フレーム数/秒（fps）単位で指定します。デフォルトでは、10fpsに設定されています。

VDA 7.0～7.6では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA 7.6 FP1以降では、［従来のグラフィックモード］が有効であるか無効であるかにかかわらず、この設定が適用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

静止画のポリシー設定

Dec 05, 2017

静止画セクションには、静止画の圧縮機能を無効にしたり変更したりするための設定が含まれています。

エクストラ色圧縮

この設定では、狭帯域幅接続でのイメージ配信で使用されるエクストラ色圧縮機能を有効または無効にします。この機能を有効にすると、イメージ品質が低下しますが狭帯域幅接続におけるセッションの応答性が向上します。
デフォルトでは、エクストラ色圧縮は無効になっています。

エクストラ色圧縮を有効にした場合、［エクストラ色圧縮しきい値］の設定値を下回るクライアント接続でのみこの圧縮機能が適用されます。クライアント接続の帯域幅がしきい値を上回る場合、または［エクストラ色圧縮］設定で［無効］が選択されている場合、この圧縮機能は適用されません。

エクストラ色 圧縮しきい値

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、 エクストラ色圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。クライアント接続帯域幅がこの値を 下回る場合、エクストラ色圧縮が適用されます（［エクストラ色圧縮］設定で［有効］が選択されている場合）。

デフォルトの しきい値は、8192KB/秒です。

ヘビーウェイト 圧縮

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、プログレッシブ圧縮よりもさらに消費帯域幅を節約する機能を 有効または無効にします。ヘビーウェイト圧縮では、CPU要求度の高い グラフィックアルゴリズムが使用され、画質を 損なわずにイメージデータで使用される帯域幅を抑えることができます。

デフォルトでは、 ヘビーウェイト圧縮は無効になっています。

この 圧縮機能を有効にすると、すべての非可逆圧縮設定に適用されます。この機能はCitrix Receiverで サポートされ、ほかのプラグインソフトウェアでは無視されます。

関連する設定項目は以下のとおりです。

- プログレッシブ圧縮の レベル
- プログレッシブ圧縮の しきい値

非可逆 圧縮のレベル

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、狭帯域幅 接続でのイメージ配信で使用される非可逆圧縮のレベルを 指定します。狭帯域幅接続では、ICAセッション内での 非圧縮イメージの表示に時間がかかる場合があります。

デフォルトでは、中レベルの 圧縮が選択されています。

イメージ表示の パフォーマンスを改善させるには、高い圧縮レベルを使用します。逆に、X線写真を表示するなど イメージの画質が優先される場合では、 非可逆圧縮を無効にします。

関連する設定項目：非可逆圧縮のしきい値

© 1999-2017 Citrix Systems, Inc. All rights reserved.

非可逆 圧縮のしきい値

注： Virtual Delivery Agent 7.xでは、 ［従来の グラフィックモード］設定が有効な場合のみこの設定項目が適用されます。
この設定では、 非可逆圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で 指定します。

デフォルトの しきい値は、2147483647KB/秒です。

非可逆圧縮の しきい値を指定せずに ［非可逆 圧縮のレベル］設定をポリシーに追加すると、LAN環境での高精細ビットマップ（ 写真など）の表示速度が向上する場合があります。

関連する設定項目：非可逆圧縮のレベル

© 1999-2017 Citrix Systems, Inc. All rights reserved.

WebSocketのポリシー設定

Dec 05, 2017

WebSocketセクションには、Citrix Receiver for HTML5を使用した仮想デスクトップおよびホストアプリケーションへのアクセスに関するポリシー設定が含まれています。WebSocket機能により、Webブラウザーアプリケーションとサーバー間の双方向通信が有効になります。複数のHTTP接続を確立する必要がないため、セキュリティが向上し、サーバーのオーバーヘッドが軽減されます。

WebSocket 接続

この設定では、 WebSocketプロトコルによる接続を許可または禁止します。

デフォルトでは、 無効になっています。

WebSocket ポート番号

この設定では、 WebSocket接続の着信ポートの番号を指定します。

デフォルトでは、 値は8008です。

WebSocket信頼される接続元サーバー一覧

この設定では、信頼される接続元サーバー（通常Citrix Receiver for Web）のURLをコンマ区切りの一覧で指定します。この一覧に追加したサーバーからのWebSocket接続のみが受け入れられます。

デフォルトでは、ワイルドカード文字「*」が設定されています。これにより、すべてのCitrix Receiver for WebサイトURLが信頼され、アクセスが許可されます。

この設定では、URLを以下の形式で指定します。

<protocol>://<Fully qualified domain name of host>:[port]

ここで、はHTTPまたはHTTPSです。にポート番号を指定しない場合、HTTPでは80、HTTPSでは443が使用されます。

URLの一部にワイルドカード文字「*」を使用できますが、IPアドレスの一部には使用できません（「10.105.*.*」は無効です）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

負荷管理のポリシー設定

Dec 05, 2017

負荷管理セクションには、Windowsサーバーマシン間の負荷を管理するためのポリシー設定が含まれています。

負荷評価基準インデックスの計算については、CTX202150を参照してください。

同時ログオントレランス

この設定では、サーバーが許容できる同時ログオンの最大数を指定します。

デフォルトでは、「2」に設定されています。

この設定が有効になっているときは、サーバーVDA上のアクティブな同時ログオン数が指定された数を超えないように負荷分散されます。ただし、上限は厳密に制限されていません。上限を制限する（指定された数値を超える同時ログインを失敗させる）には、次のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
種類：DWORD
値：1

CPU使用率

この設定では、サーバーを「負荷限界」とみなすCPU使用率をパーセンテージで指定します。 この設定を有効にすると、デフォルトで90%になったときにそのサーバーが負荷限界として認識されます。

デフォルトでは無効になっており、CPU使用率が負荷計算から除外されます。

CPU使用率から除外するプロセスの優先順位

この設定では、特定の優先度レベル以下のプロセスをCPU使用率の負荷計算から除外できます。

デフォルトでは、［通常以下および低］に設定されています。

ディスク使用率

この設定では、サーバーを「75%の負荷状態」とみなすディスクキューの長さを指定します。 この設定を有効にすると、デフォルトでディスクキューの長さが8になったときにそのサーバーの負荷が75%であると認識されます。

デフォルトでは無効になっており、ディスク使用率が負荷計算から除外されます。

最大セッション数

この設定では、サーバーがホストできる最大セッション数を指定します。 この設定を有効にすると、デフォルトで最大250個のセッションを単一サーバーでホストできます。

デフォルトでは、 有効になっています。

メモリ使用率

この設定では、サーバーを「負荷限界」とみなすメモリ使用率をパーセンテージで指定します。 この設定を有効にすると、デフォルトで90%になったときにそのサーバーが負荷限界として認識されます。

デフォルトでは無効になっており、メモリ使用率が負荷計算から除外されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

基本メモリ使用量

この設定では、オペレーティングシステムの基本メモリ使用量をMB単位で指定します。この値を下回ると、サーバーは負荷なしとみなされます。

デフォルトでは、768MBに設定されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

プロファイル管理のポリシー設定

Dec 05, 2017

［プロファイル管理］ カテゴリには、プロファイル管理機能を有効にして、 その処理の対象として特定のグループを追加したり除外したりするための設定項目が含まれています。

これらの設定項目に対応するINIファイルの名前や、各設定項目をサポートするProfile managementのバージョン要件などの情報については、「Profile managementポリシー」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

上級設定のポリシー設定

Dec 05, 2017

上級設定セクションには、Profile managementの詳細構成に関するポリシー設定が含まれています。

自動構成を無効にする

この設定項目では、Profile managementによるグループポリシーの自動構成機能を無効にします。Profile managementは、環境の構成（Personal vDiskが存在するかどうかなど）を検査してそれに基づいてグループポリシーを自動的に構成します。 この機能では、未構成のProfile management関連の設定だけが自動構成され、カスタマイズした既存の設定は保持されます。 これにより、短時間での展開と容易な最適化が可能になります。 この自動構成機能には特別な構成は必要ありません。アップグレード（既存の設定を保持する場合）やトラブルシューティングを行うときは、自動構成機能を無効にすることができます。この自動構成機能は、XenAppやほかの環境では使用できません。

デフォルトでは、自動構成が許可されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも 構成しない場合、自動構成機能によりProfile management関連の設定が変更されることがあります（環境の構成に変更があった場合）。

問題が発生する場合にユーザーをログオフ

この設定では、Profile managementでユーザーストアを使用できないなどの問題が発生したユーザーを自動的にログオフする機能を有効または無効にします。 この設定を有効にすると、プロファイルに関する問題が発生したユーザーにエラーメッセージが表示され、強制的にログオフされます。 この設定を無効にすると、そのようなユーザーには一時プロファイルが提供されます。

この設定はデフォルトで無効になっており、問題が発生したユーザーに一時プロファイルが提供されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合は、一時プロファイルが提供されます。

ロックされたファイルにアクセスする場合の試行数

この設定では、ロックされたファイルにProfile managementがアクセスするときの試行数を指定します。

デフォルトでは、5回に設定されています。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定およびINIファイルをここで 構成しない場合、デフォルト値が使用されます。

ログオフ時のインターネットCookieファイルの処理

この設定では、ログオフ時にProfile managementでindex.datを処理して、ファイルシステムに残っているインターネットCookieを削除する機能を有効または無効にします。これにより、継続的なWebブラウズによるCookieでプロファイルが膨張することを避けることができます。 ただし、この処理によりログオフに時間がかかることがあるため、 問題が生じた場合にのこの設定を有効にしてください。

この設定はデフォルトで無効になっており、Profile managementはログオフ時にindex.datを処理しません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、Index.datの処理は実行されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

基本設定のポリシー設定

Dec 05, 2017

基本設定セクションには、Profile Managementの基本構成に関するポリシー設定が含まれています。

アクティブライト バック

この設定 では、更新されたファイルやフォルダー（レジストリ設定は除く）をセッション中、つまりユーザーがログオフする前にユーザーストアに 同期する機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、有効になります。

Profile managementの有効化

この設定 では、Profile managementによるログオンおよびログオフのプロファイル処理を有効または無効にします。

デフォルトでは、 展開を容易にするために無効になっています。

重要： Profile managementを有効にする前に、ほかのすべてのセットアップタスクを 実行し、Citrixユーザープロファイルの動作をテストする ことをお勧めします。
この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここでまたはINIファイルで 構成しない場合、Profile managementはいかなる方法でも Windowsユーザープロファイルを処理しません。

除外 グループ

この設定では、Profile managementでのプロファイル処理から除外するコンピューターのローカルグループおよびドメイングループ（ローカル、グローバル、および ユニバーサル）を 指定します。

この設定を有効にすると、指定したユーザーグループのプロファイルが Profile managementで処理されなくなります。

この 設定はデフォルトで無効になっており、すべてのユーザーグループのプロファイルが処理されます。

ドメイン グループを<DOMAIN NAME>\<GROUP NAME>形式で指定します。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、すべてのユーザーグループのメンバーが 処理されます。

オフライン プロファイルサポート

この設定 では、ネットワークから切断したときのプロファイル管理に関するオフラインプロファイルサポート機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定は、移動するデバイス（ラップトップやモバイルデバイス）のユーザーに 適しています。ネットワークの切断 が発生した場合、再起動や 休止状態後もプロファイルがラップトップコンピューターやモバイルデバイス上にそのまま保持されます。ネットワークが切断されたままユーザーが作業する場合、プロファイルはローカルで更新され、ネットワーク接続が再

© 1999-2017 Citrix Systems, Inc. All rights reserved.

確立されしだいユーザーストアと 同期されます。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、オフラインプロファイルサポート機能は 無効になります。

ユーザー ストアへのパス

この設定では、ユーザーの レジストリなどの設定や同期対象のファイルを格納するユーザーストアのパスを 指定します。

デフォルトでは、ホームドライブ上の Windowsフォルダーが使用されます。

この設定が 無効な場合、ユーザー設定はホーム フォルダーのWindowsサブフォルダーに格納されます。

以下のパスを設定できます。
- **相対パス**：ホームディレクトリ（通常Active Directoryユーザーの #homeDirectory#属性で構成される）からの相対パス です。
- **絶対UNCパス**： 通常、サーバー共有またはDFS名前空間です。
- **無効化または 未構成**：この場合、#homeDirectory#\Windowsの値が使用されます。

このポリシー設定を構成する場合、以下 の変数を使用します。
- パーセントで囲まれたシステム環境 変数（%ProfVer%など）。ただし、システム 環境変数が正しくセットアップされている必要があります。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（#sAMAccountName#など）。
- Profile management の変数。詳しくは、Profile managementのドキュメントを参照してください。

%username%や%userdomain%などのユーザー環境変数を使用したり、locationやusersなどの組織の変数を完全に定義するカスタム 属性を作成したりすることもできます。 属性では大文字と小文字が区別されます。

例：
- 「\\server\share\#sAMAccountName#」と指定した場合、 UNCパス\\server\share\JohnSmithにユーザー設定が格納されます（現在のユーザーの#sAMAccountName#属性がJohnSmith である場合）。
- 「\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS!」 と指定した場合、\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64などに格納されます。

重要： 属性や変数を使用する場合は、 NTUSER.DATがあるフォルダーの1つ上のフォルダーを指定 していることを確認してください。たとえば、NTUSER.DATが \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profileにある場合は、 ユーザーストアのパスとして「\\server\profiles$\JohnSmith.Finance\v2x64」を指定します。UPM_Profile サブフォルダーを含める必要はありません。
この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、ホーム ドライブのWindowsディレクトリが使用されます。

ローカル管理者のログオン 処理

この設定では、BUILTIN\Administratorsグループのメンバーのログオンを 処理するかどうかを 指定します。これにより、ローカルの管理者権限 があるドメインユーザー（通常、仮想デスクトップが割り当てられているユーザー）がログオン時 のプロファイル処理をバイパスして、Profile managementで問題が生じているデスクトップのトラブルシューティングを行えるようになります。

この設定が 無効または構成しない場合、 サーバーオペレーティングシステムではドメインユーザーのログオンは処理されますが、ローカル管理者のログオンは 処理されません。デスクトップオペレーティングシステムでは、ローカル管理者のログオンも 処理されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この 設定はデフォルトで無効になっており、ローカル管理者のログオンは処理されません。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、ローカル管理者のログオンは 処理されません。

処理済み グループ

この設定では、Profile managementでのプロファイル処理の対象となるコンピューターのローカルグループおよびドメイン
ループ（ローカル、グローバル、および ユニバーサル）を 指定します。

この設定を有効にすると、指定したユーザーグループのプロファイルのみが Profile managementで処理されるようになりま
す。

この 設定はデフォルトで無効になっており、すべてのユーザーグループのプロファイルが処理されます。

ドメイン グループを<DOMAIN NAME>\<GROUP NAME>形式で指定します。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、すべてのユーザーグループのメンバーが 処理されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

クロスプラットフォームのポリシー設定

Dec 05, 2017

クロスプラットフォームセクションには、Profile Managementのクロスプラットフォーム機能を構成するためのポリシー設定が含まれています。

クロスプラットフォーム設定ユーザーグループ

この設定では 、クロスプラットフォーム設定機能が有効な場合にプロファイルを処理する Windowsユーザーグループを指定します。

この設定項目は デフォルトで無効になっており、 [処理済みグループ] 設定で指定されているすべてのユーザーグループのプロファイルが処理されます。

この設定を ここで構成しない場合、INIファイルの値が使用されます。

この設定を ここおよびINIファイルで構成しない場合、すべてのユーザーグループが処理されます。

クロス プラットフォーム設定の有効化

この設定 では、複数のオペレーティングシステム上で同じアプリケーションを実行するユーザーのプロファイルの 移行および移動を可能にするクロスプラットフォーム機能を 有効または無効にします。

デフォルトでは、 無効になっています。

この設定をここで構成しない場合、INIファイルの値が使用されます。

この設定を ここおよびINIファイルで構成しない場合、クロスプラットフォーム設定は適用 されません。

クロス プラットフォーム定義へのパス

この設定では 、ダウンロードパッケージからコピーされた定義ファイルのネットワーク上の場所を UNCパスとして指定します。

注： このパスには、 ユーザーの読み取りアクセスおよび管理者の書き込みアクセスが設定されており、 SMB（Server Message Block）またはCIFS（Common Internet File System）ファイル 共有である必要があります。
デフォルトでは、 パスは指定されていません。

この設定を ここで構成しない場合、INIファイルの値が使用されます。

この設定を ここおよびINIファイルで構成しない場合、クロスプラットフォーム設定は適用 されません。

クロス プラットフォーム設定ストアへのパス

この設定では 、クロスプラットフォーム設定ストアへのパスを指定します。クロスプラットフォーム設定ストアとは、ユーザーの クロスプラットフォーム設定を格納するフォルダーを指します。パスは、UNCパスまたはホームディレクトリからの相対パスで指定します。

注： クロスプラットフォーム設定ストアには、 ユーザーの書き込みアクセスが設定されている必要があります。
この設定は デフォルトで無効になっており、Windows\PM_CPが使用されます。

この設定を ここで構成しない場合、INIファイルの値が使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定 およびINIファイルをここで構成しない場合、デフォルト値が使用されます。

クロス プラットフォーム設定を作成するためのソース

この設定項目 では、プラットフォーム組織単位（OU）のプラットフォームを「 基本プラットフォーム」として 指定します。基本プラットフォームのプロファイルのデータは、 クロスプラットフォーム設定ストアに移行されます。

各プラットフォームの プロファイルのセットは、個別のOUに格納されます。このため、管理者は どのプラットフォームのプロファイルデータをクロスプラットフォーム設定ストアに格納するかを決定する必要があります。 このプラットフォームを「基本プラットフォーム」と呼びます。

この設定を有効にすると、 クロスプラットフォーム設定ストアの定義ファイルにデータがない場合、 またはキャッシュされた単一プラットフォームプロファイルのデータがストア内の定義 データよりも新しい場合に、 Profile managementが単一プラットフォームプロファイルのデータをストアに移行します。

重要： この設定項目を複数のOUやユーザー /マシンオブジェクトで有効にすると、最初のユーザーがログオンしたプラットフォームが 基本プラットフォームになります。
この設定はデフォルトで 無効になっており、 単一プラットフォームプロファイルのデータはストアに移行されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ファイルシステムのポリシー設定

Dec 05, 2017

［ファイルシステム］ カテゴリには、プロファイルがインストールされているシステムとユーザーストア間で同期する、ユーザープロファイル内のファイルやフォルダーの構成に関する設定項目が含まれています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

除外のポリシー設定

Dec 05, 2017

除外セクションには、ユーザープロファイル内のファイルやディレクトリを同期処理から除外するためのポリシー設定が含まれています。

除外の一覧 - ディレクトリ

この設定では、 同期処理から除外する、ユーザープロファイル内のフォルダーを 指定します。

フォルダー 名は、ユーザープロファイル（%USERPROFILE%）からの相対パスで指定します。

この 設定はデフォルトで無効になっており、ユーザープロファイル内のすべてのフォルダーが同期されます。

例： Desktopは ユーザープロファイルのDesktopフォルダーを無視する

この設定をここで 構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、ユーザープロファイル内のすべてのフォルダーが 同期されます。

除外の一覧 - ファイル

この設定では、 同期処理から除外する、ユーザープロファイル内のファイルを 指定します。

この 設定はデフォルトで無効になっており、ユーザープロファイル内のすべてのファイルが同期されます。

ファイル名は、ユーザープロファイル（%USERPROFILE%）からの相対 パスで指定します。ワイルドカード文字を 使用することもできます（再帰的に適用されます）。

例：「デスクトップ\Desktop.ini」と指定した場合、デスクトップフォルダーのDesktop.iniファイルは同期されません。

この設定をここで 構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、ユーザープロファイル内のすべてのファイルが 同期されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

同期のポリシー設定

Dec 05, 2017

同期セクションには、プロファイルがインストールされているシステムとユーザーストア間で同期する、ユーザープロファイル内のファイルやフォルダーの指定に関するポリシー設定が含まれています。

同期するディレクトリ

この設定項目では、Profile managementで同期する、除外フォルダー内のファイルを指定します。デフォルトでは、ユーザープロファイル内のすべてのファイルがProfile managementにより同期されます。ユーザープロファイルのサブフォルダーは、この一覧に含めなくても同期されます。詳しくは、「項目の包含および除外」を参照してください。

この一覧にパスを追加するときは、ユーザープロファイルからの相対パスを入力します。

例：「Desktop\exclude\include」と指定した場合、Desktop\excludeフォルダーを同期対象から除外しても、includeフォルダーは同期されます。

この設定はデフォルトで無効になっており、フォルダーは指定されていません。

この設定をここで構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、ユーザープロファイル内の非除外フォルダーのみが同期されます。

同期するファイル

この設定項目では、Profile managementで同期する、除外フォルダー内のファイルを指定します。デフォルトでは、ユーザープロファイル内のすべてのファイルがProfile managementにより同期されます。ユーザープロファイル内のファイルは、この一覧に含めなくても同期されます。詳しくは、「項目の包含および除外」を参照してください。

この一覧にパスを追加するときは、ユーザープロファイルからの相対パスを入力します。相対パスは、ユーザープロファイルの場所から相対的に解釈されます。ワイルドカード文字は、ファイル名に対してのみ使用できます。ワイルドカードは入れ子にできず、再帰的に適用されます。

例：

- 「AppData\Local\Microsoft\Office\Access.qat」と指定した場合、デフォルト構成で除外されるフォルダー内のファイルAccess.qatは同期されます。
- 「AppData\Local\MyApp*.cfg」と指定した場合、プロファイルフォルダーAppData\Local\MyAppとそのサブフォルダー内の.cfg拡張子を持つすべてのファイルが同期されます。

この設定はデフォルトで無効になっており、ファイルは指定されていません。

この設定をここで構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、ユーザープロファイル内の非除外ファイルのみが同期されます。

ミラーリングするフォルダー

この設定項目では、ミラーリングするフォルダーを、ユーザープロファイルのルートフォルダーからの相対パスで指定します。 このポリシー設定を構成することで、相互に依存するファイルが格納されたトランザクションフォルダー（参照フォルダー）に関する問題を解決できます。

フォルダーのミラーリングにより、Profile managementがトランザクションフォルダーおよびその内容を単一エンティティ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

として処理するため、プロファイルの膨張を防ぐことができます。 ただし、ミラーリングされたフォルダー内のファイルが複数のセッションで変更された場合、最後の更新によりそのファイルが上書きされ、プロファイルの変更が失われることがある点に注意してください。

たとえば、Internet ExplorerのCookieフォルダーをミラーリングして、Index.datが対象のCookieと同期されるように設定できます。

ユーザーが異なるサーバー上の2つのInternet Explorerセッションを実行して、各セッションで異なるWebサイトにアクセスする場合、それらのWebサイトからのCookieがそれぞれのサーバーに追加されます。 ユーザーが1つ目のセッションからログオフするときに（アクティブライトバック機能が有効な場合はセッションの途中でも）、2つ目のセッションからのCookieにより最初のセッションのCookieが置き換えられなければなりません。 ところが、これらのCookieはマージされてしまい、Index.datのCookieへの参照は最新ではなくなります。 新しいセッションでの以降のWebサイト閲覧ではマージが繰り返され、Cookieフォルダーのサイズが膨張します。

Cookieフォルダーをミラーリングすると、ユーザーがログオフするたびにCookieが最新セッションのもので上書きされ、Index.datが最新の状態で維持されます。

この設定はデフォルトで無効になっており、フォルダーはミラーリングされません。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

このポリシーをここでまたはINIファイルで構成しない場合、フォルダーはミラー化されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フォルダーリダイレクトのポリシー設定

Dec 05, 2017

［フォルダー リダイレクト］カテゴリには、プロファイル内の一般的な フォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

管理者 アクセスを許可

この設定項目 では、リダイレクトされたユーザーのフォルダーに管理者がアクセスすることを有効または無効にします。

この設定は デフォルトで無効になっており、リダイレクトされたフォルダーの内容に対してユーザーの排他アクセスが 付与されています。

ドメイン 名を包含

この設定 では、リダイレクトされるフォルダーのUNCパスに環境変数%userdomain%を 含めることを有効または無効にします。

この設定はデフォルトで 無効になっており、リダイレクトされるフォルダーのUNCパスに 環境変数%userdomain%は含まれません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppData（Roaming）のポリシー設定

Dec 05, 2017

AppData（Roaming）セクションには、ユーザープロファイルのAppData（Roaming）フォルダーをネットワーク上の共有フォルダーにリダイレクトするためのポリシー設定が含まれています。

AppData（Roaming）パス

この設定では、AppData（Roaming） フォルダーのリダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

AppData（Roaming）のリダイレクト設定

この設定 では、AppData（Roaming）フォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アドレス帳のポリシー設定

Dec 05, 2017

アドレス帳セクションには、ユーザープロファイルのアドレス帳フォルダーをネットワーク上の共有フォルダーにリダイレクトするためのポリシー設定が含まれています。

アドレス帳 パス

この設定 では、アドレス帳フォルダーの リダイレクト先のネットワークフォルダーを指定します。

この設定は デフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

アドレス帳の リダイレクト設定

この設定 では、アドレス帳フォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デスクトップのポリシー設定

Dec 05, 2017

デスクトップセクションには、ユーザープロファイルのデスクトップフォルダーをネットワーク上の共有フォルダーにリダイレクトするためのポリシー設定が含まれています。

デスクトップ パス

この設定項目 では、デスクトップフォルダーのリダイレクト先のネットワークフォルダーを 指定します。

この設定は デフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

デスクトップ のリダイレクト設定

この設定 では、デスクトップフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ドキュメントのポリシー設定

Dec 05, 2017

ドキュメントセクションには、ユーザープロファイルのドキュメントフォルダーをネットワーク上の共有フォルダーにリダイレクトするためのポリシー設定が含まれています。

ドキュメント パス

この設定 では、ドキュメントフォルダーのリダイレクト先のネットワークフォルダーを 指定します。

この設定は デフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

ファイルをドキュメントフォルダーにリダイレクトするだけではなく、ミュージック、ピクチャ、およびビデオフォルダーにもリダイレクトするため、 [ドキュメントパス] 設定を 有効にする必要が あります。

ドキュメント のリダイレクト設定

この設定 では、ドキュメントフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

ドキュメントフォルダーの リダイレクト方法として、以下のいずれかのオプションを 選択します。

- 次のUNC パスにリダイレクト： [ドキュメントパス] 設定で指定されたUNCパスにリダイレクトします。
- ユーザーのホーム ディレクトリにリダイレクト：ユーザーのホームディレクトリ（通常 Active Directoryでユーザーの #homeDirectory#属性として構成される）にリダイレクトします。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ダウンロードのポリシー設定

Dec 05, 2017

［ダウンロード］カテゴリには、ユーザープロファイルのダウンロードフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

ダウンロード パス

この設定 では、ダウンロードフォルダーの リダイレクト先のネットワークフォルダーを指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

ダウンロードの リダイレクト設定

この設定 では、ダウンロードフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、この フォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

お気に入りのポリシー設定

Dec 05, 2017

［お気に入り］カテゴリには、ユーザープロファイルのお気に入りフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

お気に入り パス

この設定 では、お気に入りフォルダーの リダイレクト先のネットワークフォルダーを指定します。

この設定は デフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

お気に入りの リダイレクト設定

この設定 では、お気に入りフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、この フォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リンクのポリシー設定

Dec 05, 2017

［リンク］カテゴリには、ユーザープロファイルのリンクフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

リンク パス

この設定では、リンクフォルダーの リダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

リンクのリダイレクト 設定

この設定 では、リンクフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ミュージックのポリシー設定

Dec 05, 2017

［ミュージック］カテゴリには、ユーザープロファイルのミュージックフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

ミュージック パス

この設定では、ミュージックフォルダーの リダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

ミュージックのリダイレクト 設定

この設定では、ミュージックフォルダーの内容をどのようにリダイレクトするかを 指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

ミュージックフォルダーの リダイレクト方法として、以下のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクト 。 ［ミュージック パス］設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーに相対的リダイレクト。 ドキュメントフォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツをドキュメントフォルダーに相対するフォルダーにリダイレクトするには、 ［ドキュメント パス］設定を有効にする必要があります。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ピクチャのポリシー設定

Dec 05, 2017

［ピクチャ］カテゴリには、ユーザープロファイルのピクチャフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

ピクチャパス

この設定では、ピクチャフォルダーのリダイレクト先のネットワークフォルダーを指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

ピクチャのリダイレクト設定

この設定では、ピクチャフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

ピクチャフォルダーのリダイレクト方法として、以下のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクト 。 ［ピクチャ パス］設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーに相対的リダイレクト。 ドキュメントフォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツをドキュメントフォルダーに相対するフォルダーにリダイレクトするには、 ［ドキュメント パス］設定を有効にする必要があります。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

保存したゲームのポリシー設定

Dec 05, 2017

［保存したゲーム］カテゴリには、ユーザープロファイルにある保存したゲームフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

保存したゲームのリダイレクト 設定

この設定では、保存したゲームフォルダーの内容をどのようにリダイレクトするかを 指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

保存したゲーム パス

この設定では、保存したゲームフォルダーの リダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

検索のポリシー設定

Dec 05, 2017

［検索］カテゴリには、ユーザープロファイルの検索フォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

検索のリダイレクト 設定

この設定では、検索フォルダーの内容をどのようにリダイレクトするかを 指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

検索 パス

この設定では、検索フォルダーの リダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スタートメニューのポリシー設定

Dec 05, 2017

［スタートメニュー］カテゴリには、ユーザープロファイルのスタートメニューフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

スタートメニューのリダイレクト設定

この設定では、スタートメニューフォルダーの内容をどのようにリダイレクトするかを指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

スタートメニューパス

この設定では、スタートメニューフォルダーのリダイレクト先のネットワークフォルダーを指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ビデオのポリシー設定

Dec 05, 2017

［ビデオ］カテゴリには、ユーザープロファイルのビデオフォルダーをネットワーク上の共有フォルダーにリダイレクトするための設定項目が含まれています。

ビデオのリダイレクト 設定

この設定では、ビデオフォルダーの内容をどのようにリダイレクトするかを 指定します。

デフォルトでは、 UNCパスにリダイレクトされます。

ビデオフォルダーの リダイレクト方法として、以下のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクト 。 ［ビデオパス］ ポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーに相対的リダイレクト 。 ドキュメントフォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツをドキュメントフォルダーに相対するフォルダーにリダイレクトするには、 ［ドキュメント パス］設定を有効にする必要があります。

この設定を構成しない 場合、このフォルダーはProfile managementによりリダイレクトされません。

ビデオ パス

この設定では、ビデオフォルダーの リダイレクト先のネットワークフォルダーを 指定します。

この 設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が 未構成の場合、このフォルダーはProfile managementによりリダイレクトされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログのポリシー設定

Dec 05, 2017

［ログ］カテゴリには、Profile Managementのログ機能の構成に関する設定項目が含まれています。

Active Directory操作

この設定では、 Active Directoryで実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 ［ログの 有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

一般的な 情報

この設定では、 一般的な情報についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 ［ログの 有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

一般的な 警告

この設定では、 一般的な警告についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 ［ログの 有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

ログの 有効化

この設定では、 Profile managementのデバッグモード（詳細ログモード）のログ機能を有効または無効にします。 デバッグモードでは、詳細な状態情報が %SystemRoot%\System32\Logfiles\UserProfileManagerフォルダーのログファイルに記録されます。

この設定は デフォルトで無効になっており、エラーのみがログに記録されます。

この設定は、 Profile managementのトラブルシューティング時にのみ有効にすることをお勧めします。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも 構成しない場合、エラーのみが記録されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ファイルシステム 操作

この設定項目では、 ファイルシステムで実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 [ログの 有効化] 設定で [有効] が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

ファイルシステム 通知

この設定では、 ファイルシステムで発生した通知についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 [ログの 有効化] 設定で [有効] が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

ログオフ

この設定では、 ユーザーのログオフについての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 [ログの 有効化] 設定で [有効] が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

ログオン

この設定では、 ユーザーのログオンについての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を 有効にするときは、 [ログの 有効化] 設定で [有効] が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、エラーおよび一般的な情報のみがログに 記録されます。

ログファイルの 最大サイズ

この設定では、 Profile managementで生成されるログファイルの最大サイズを バイト単位で指定します。

デフォルトでは、 1048576バイト（1MB）に設定されています。

ディスクに十分な 空き領域がある場合は、5MB以上を指定することを お勧めします。ログファイルのサイズがここで指定した値を超えると、既存のバックアップ ファイル（.bak）が削除され、そのログファイルがバックアップファイルとして保存されて新しいログファイルが 作成されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログファイルは、%SystemRoot%\System32\Logfiles\UserProfileManagerフォルダーに生成されます。

この設定をここで構成しない場合は、.iniファイルの値が使用されます。

この設定およびINIファイルをここで構成しない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定項目では、Profile managementのログファイルの保存フォルダーを指定します。

この設定項目はデフォルトで無効になっており、デフォルトのフォルダー（%SystemRoot%\System32\Logfiles\UserProfileManager）にログファイルが生成されます。

保存フォルダーのパスとして、ローカルドライブ、リモートドライブ、またはネットワークドライブ（UNCパス）を指定できます。リモートドライブは大規模な分散環境では便利ですが、大量のネットワークトラフィックが発生するためログファイルには不適切である場合があります。プロビジョニングした仮想マシンに永続的なハードドライブがある場合は、そのドライブ上のローカルパスを指定します。これにより、仮想マシンを再起動してもログファイルが保持されます。永続的なハードドライブがない仮想マシンの場合、UNCパスを指定するとログファイルを保持できますが、この仮想マシンのシステムアカウントにはそのUNCパスに対する書き込みアクセス権が必要です。オフラインプロファイル機能で管理するラップトップコンピューターの場合は、ローカルパスを使用します。

ログファイルをUNCパス上のフォルダーに保存する場合は、そのフォルダーに適切なアクセス制御リストを適用して、認証されたユーザーやコンピューターのみがログファイルにアクセスできるようすることをお勧めします。

この設定をここで構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、デフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerが使用されます。

個人用ユーザー情報

この設定では、個人用ユーザー情報についての詳細なログ機能を有効または無効にします。

デフォルトでは、無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、エラーおよび一般的な情報のみがログに記録されます。

ログオンおよびログオフ時のポリシー値

この設定では、ユーザーのログオン時およびログオフ時のポリシー設定値についての詳細なログ機能を有効または無効にします。

デフォルトでは、無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、エラーおよび一般的な情報のみがログに記録されます。

レジストリ操作

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定では、レジストリで実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、 無効になっています。

この設定を有効に するときは、 ［ログの 有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、エラーおよび一般的な情報のみがログに記録されます。

ログオフ時の レジストリ差分

この設定では、 ユーザーのログオフ時のレジストリ設定の相違についての詳細なログ機能を 有効または無効にします。

デフォルトでは、 無効になっています。

この設定を有効に するときは、 ［ログの 有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成しない場合、エラーおよび一般的な情報のみがログに記録されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

プロファイル制御のポリシー設定

Dec 05, 2017

［プロファイル制御］カテゴリには、Profile Managementでのユーザープロファイル管理機能を制御するための設定項目が含まれています。

キャッシュしたプロファイルを削除する前の待ち時間

この設定では、ローカルにキャッシュされたプロファイルをそのユーザーのログオフ後にProfile managementが削除するまでの待機時間を指定します。

0を指定すると、ログオフ処理が完了した後でプロファイルが直ちに削除されます。 Profile Managementでは、1分ごとにログオフの状態がチェックされます。このため、この設定項目で60を指定すると、ユーザーのログオフ後1～2分後にプロファイルが削除されます。 ログオフ時にファイルやレジストリハイブにアクセスするプロセスがある場合は、ここで待機時間を延長できます。 また、プロファイルのサイズが大きい場合、待機時間を延長することでログオフ時間が短縮されることがあります。

デフォルトでは0が指定されており、ローカルにキャッシュされたプロファイルがログオフ後に直ちに削除されます。

この 設定を有効にするときは、 ［ログオフ時にローカルでキャッシュしたプロファイルの 削除］設定で［有効］が選択されていることを確認してください。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも 構成しない場合、プロファイルは直ちに削除されます。

ログオフ時にローカルでキャッシュしたプロファイルの削除

この設定では、ユーザーのログオフ後にローカルにキャッシュされたプロファイルを削除するかどうかを指定します。

この設定を有効にすると、ユーザーのローカルプロファイルキャッシュがログオフ後に削除されます。 ターミナルサーバーではこの設定を有効にすることをお勧めします。

この設定はデフォルトで無効になっており、ローカルプロファイルはユーザーのログオフ後も保持されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここでも.iniファイルでも構成 しない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイル競合の制御

この設定では、ユーザーストアのプロファイルとローカルのWindowsユーザープロファイルの両方が存在する場合に、Profile Managementがどのように動作するかを指定します。

デフォルトでは、Profile ManagementはローカルのWindowsプロファイルを使用しますが、そのプロファイルを変更することはありません。

Profile Managementの動作を制御するには、次のいずれかのオプションを選択します。

- ローカル プロファイルを使用。Profile Managementはローカルのプロファイルを使用し、そのプロファイルを変更することはありません。
- ローカル プロファイルを削除。Profile Managementは、ローカルのWindowsユーザープロファイルを削除して、 ユーザーストアからCitrixユーザープロファイルをインポートします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ローカル プロファイル名を変更。Profile Managementは、ローカルのWindowsユーザープロファイルの名前を変更してバックアップ用に保持し、ユーザー ストアからCitrixユーザープロファイルをインポートします。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成 しない場合、既存のローカルプロファイルが使用されます。

既存のプロファイルの移行

この設定では、ログオンしたユーザーのプロファイルがユーザーストアに存在しない場合に、どのプロファイルをユーザーストアに移行するかを指定します。

Profile Managementでは、ユーザーストアにプロファイルが存在しないユーザーがログオンしたときに、既存のプロファイルが自動的にユーザーストアに移行されます。 移行が完了すると、現在のセッション、および同じユーザーストアのパスが構成されたすべてのセッションで、ユーザーストアのプロファイルがProfile Managementで使用されます。

デフォルトでは、ローカルプロファイルおよび移動プロファイルがログオン時にユーザーストアに移行されます。

移行されるプロファイルを指定するには、以下のいずれかのオプションを選択します。
- ローカルおよび移動 プロファイル
- ローカル
- 移動
- なし（無効）

［なし］を選択すると、通常のWindowsの動作（つまりProfile Managementがインストールされていない場合の動作）に基づいて新しいプロファイルが作成されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、既存のローカルおよび移動プロファイルが移行されます。

テンプレートプロファイルへのパス

この設定では、Profile Managementで新しいユーザープロファイルを作成するときにテンプレートとして使用するプロファイルのパスを指定します。

このパスは、NTUSER.DATレジストリファイルや、テンプレートプロファイルに必要なそのほかのフォルダーやファイルを格納しているフォルダーのものである必要があります。
注：パスに「NTUSER.DAT」を 含めないで ください。たとえば、「 \\myservername\myprofiles\template\ntuser.dat」ではなく「 \\myservername\myprofiles\template」を指定します。
UNCパスやローカルマシン上のパスなどの絶対パスを使用します。 たとえば、Citrix Provisioning Servicesイメージ上のテンプレートプロファイルを永続的に指定するにはローカルマシン上のパスを指定します。 相対パスは使用できません。

注： Active Directory属性の拡張、システム環境変数、および%USERNAME%や%USERDOMAIN%変数を使用することはできません。
この設定はデフォルトで無効になっており、最初にログオンしたデバイス上のデフォルトのユーザープロファイルを基にそのユーザーのプロファイルが作成されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定では、新しいユーザープロファイルの作成時にローカルプロファイルよりもテンプレートプロファイルを優先する機能を有効または無効にします。

デフォルトでは、ユーザーにCitrixユーザープロファイルがなく、ローカルのWindowsユーザープロファイルが存在する場合、デフォルトでローカルのプロファイルが使用され、ユーザーストアに移行されます。 このポリシー設定を有効にすると、新しいユーザープロファイルの作成時にローカルプロファイルではなくテンプレートプロファイルが使用されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定では、新しいユーザープロファイルの作成時に移動プロファイルよりもテンプレートプロファイルを優先する機能を有効または無効にします。

デフォルトでは、ユーザーにCitrixユーザープロファイルがなく、Windowsの移動ユーザープロファイルが存在する場合、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。 このポリシー設定を有効にすると、新しいユーザープロファイルの作成時に移動プロファイルではなくテンプレートプロファイルが使用されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、テンプレートは使用されません。

すべてのログオンでCitrix固定プロファイルとして使用されるテンプレートプロファイル

この設定では、Profile Managementで新しいユーザープロファイルを作成するときに、テンプレートプロファイルをデフォルトのプロファイルとして使用するかどうかを指定します。

この設定はデフォルトで無効になっており、最初にログオンしたデバイス上のデフォルトのユーザープロファイルを基にそのユーザーのプロファイルが作成されます。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで構成しない場合、テンプレートは使用されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レジストリのポリシー設定

Dec 05, 2017

［レジストリ］カテゴリには、特定のレジストリキーをProfile managementの処理対象として指定したり除外したりするための設定項目が含まれています。

除外の 一覧

この設定では、ユーザーのログオフ時にProfile managementの処理対象から除外するHKEY_CURRENT_USERハイブのレジストリキーを 指定します。

この設定を有効にすると、一覧に 追加したレジストリキーがユーザーのログオフ時にProfile managementで処理されなくなります。

この 設定はデフォルトで無効になっており、HKEY_CURRENT_USERハイブのすべてのレジストリキーが ユーザーのログオフ時に処理されます。

この設定をここで 構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、HKEY_CURRENT_USERハイブのすべてのレジストリキーがユーザーのログオフ時に 処理されます。

包含の 一覧

この設定では、ユーザーのログオフ時にProfile managementの処理対象にするHKEY_CURRENT_USERハイブのレジストリキーを 指定します。

この設定を有効にすると、一覧に追加したレジストリ キーのみがユーザーのログオフ時にProfile managementで処理されます。

この 設定はデフォルトで無効になっており、HKEY_CURRENT_USERハイブのすべてのレジストリキーが ユーザーのログオフ時に処理されます。

この設定をここで 構成しない場合、INIファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、HKEY_CURRENT_USERハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ストリーム配信ユーザープロファイルのポリシー設定

Dec 05, 2017

［ストリーム配信ユーザープロファイル］カテゴリには、Profile managementでのストリーム配信ユーザープロファイル管理機能を制御するための設定項目が含まれています。

常時キャッシュ

この設定では、ユーザーのログオン後にストリーム配信されたファイルをキャッシュするかどうかを指定します。 ファイルをキャッシュするとネットワークの 帯域幅消費が減少し、ユーザーエクスペリエンスが向上します。

この設定項目は、 ［プロファイル ストリーム配信］設定と一緒に使用します。

この設定はデフォルトで無効になっており、ユーザーのログオン後にストリーム配信されたファイルはキャッシュされません。

この設定をここで 構成しない場合は、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、無効になります。

常時キャッシュサイズ

この設定では、ストリーム配信されるファイルの最小サイズをメガバイト（MB）単位で指定します。 Profile managementては、ここで指定した値以上のサイズのファイルがユーザーのログオン後にキャッシュされます。

デフォルトでは0が 指定されており、プロファイル全体がキャッシュされます。 この場合、ユーザーのログオン後、バックグラウンドタスクとしてユーザーストアのプロファイルの内容すべてがProfile managementによりキャッシュされます。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、無効になります。

プロファイル ストリーム配信

この設定では、Profile managementによるユーザープロファイルのストリーム配信機能を有効または無効にします。 この設定を有効にすると、プロファイルに含まれる ファイルやフォルダーが、ログオンしたユーザーがアクセスした時点でユーザーストアから ローカルコンピューターに取得されます。 待機領域内のレジストリエントリやファイルは、直ちに取得されます。

デフォルトでは、無効になっています。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、無効になります。

ストリーム配信ユーザー プロファイルグループ

この設定では、ストリーム配信する組織単位のユーザープロファイルをWindowsユーザーグループで指定します。

この設定を有効にすると、指定したユーザーグループの ユーザープロファイルのみがストリーム配信されます。ほかのユーザー プロファイルは、通常どおりに処理されます。

この設定はデフォルトで無効になっており、組織単位のすべてのユーザープロファイルが通常どおりに処理されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定をここまたはINIファイルで 構成しない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーム配信除外機能を有効にするには

プロファイルストリーム配信除外機能を有効にすると、ユーザーがログオンしたときに、Profile Managementはログオン除外一覧に指定されたフォルダーを配信せず、すべてのフォルダーはユーザーストアからローカルコンピューターに直ちには同期されません。

詳しくは、「プロファイルストリーム配信除外機能を有効にするには」を参照してください。

待機領域のロックファイルのタイムアウト

この設定項目では、サーバーが応答不能になってユーザーストアのロックが解除されない場合に、待機領域のファイルをユーザーストアに同期するまでの日数を指定します。 これにより、待機領域が膨張することを防いで、ユーザーストアに常に最新のファイルが同期されるようになります。

デフォルトでは、1日に設定されています。

この設定をここで 構成しない場合、.iniファイルの値が使用されます。

この設定 およびINIファイルをここで構成しない場合、デフォルト値が使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiverのポリシー設定

Dec 05, 2017

注：特に明記されていない限り、「Receiver」はCitrix Receiverを指します。

［Receiver］カテゴリには、仮想デスクトップ上のCitrix Receiver for Windowsで使用されるStoreFrontアドレスの一覧を指定するための設定項目が含まれています。

StoreFrontアカウント一覧

この設定では、仮想デスクトップ上で実行されるCitrix Receiver for Windowsに設定するStoreFrontストアの一覧を指定します。デリバリーグループを作成するときに、管理者はこの一覧からストアを選択して、そのデリバリーグループの仮想デスクトップ上で動作するCitrix Receiver for Windowsに適用できます。

デフォルトでは、ストアは指定されていません。

一覧にストアを追加するときは、以下の情報をセミコロンで区切って入力します。

- ストア名：ユーザーに表示されるストア名です。
- ストアURL：ストアのURLです。
- ストアの有効/無効：そのストアをユーザーが使用できるかどうかを「On」または「Off」で指定します。
- ストアの説明：ユーザーに表示される説明です。

たとえば、「Sales Store;https://sales.mycompany.com/Citrix/Store/discovery;On;Store for Sales staff」のように入力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agentのポリシー設定

Dec 05, 2017

［Virtual Delivery Agent設定］カテゴリには、Virtual Delivery Agent（VDA）とController間の通信を制御するための設定項目が含まれています。

重要： 重要： VDAをDelivery Controllerに登録するときに、これらの設定項目で提供される情報が必要になります （自動更新機能を使用しない場合）。これらの情報は登録に必要であるため、 グループポリシーエディターを使って以下の設定項目を構成する 必要があります（VDAのインストール時にこれらの情報を指定する場合を除く）。

- コントローラー登録の IPv6ネットマスク
- コントローラー登録 ポート
- コントローラーSID
- Controller
- IPv6コントローラー 登録のみを使用する
- サイトGUID

コントローラー 登録のIPv6ネットマスク

このポリシー 設定では、VDAで使用されるサブネット を指定できます。この場合、グローバルIPは使用されません。これにより、指定した IPv6アドレスおよびネットワークでのみVDAが登録されます。VDAは、指定されたネットマスクに最初にマッチしたアドレスで のみ登録されます。この設定項目を 使用する場合は、 ［IPv6 Controller 録のみを使用する］設定を有効にする必要があります。

デフォルトでは、 空白になっています。

コントローラー 登録ポート

この設定を使用する場合は、 ［コントローラーの自動更新を有効にする］ 設定で［禁止］が選択されていることを確認してください。

この設定項目では、 VDAのController登録をレジストリで行うときに 使用されるTCP/IPポート番号を指定します。

デフォルトの ポート番号は、80です。

コントローラー SID

この設定を使用する場合は、 ［コントローラーの自動更新を有効にする］ 設定で［禁止］が選択されていることを確認してください。

この設定項目では、 VDAのController登録をレジストリで行うときに使用されるControllerのセキュリティ識別子（SID）をスペース区切りの一覧で指定します。これはオプションの設定項目で、 ［Controller］設定と一緒に使用して、 登録に使用されるControllerの一覧を制限できます。

デフォルトでは、 空白になっています。

Controller

この設定を使用する場合は、 ［コントローラーの自動更新を有効にする］ 設定で［禁止］が選択されていることを確認してください。

この設定項目では、 VDAのController登録をレジストリで行うときに使用されるControllerの完全修飾ドメイン名 （FQDN）をスペース区切りの一覧で 指定します。これはオプションの設定項目で、 ［コントローラー SID］設定と一緒に使用すること

© 1999-2017 Citrix Systems, Inc. All rights reserved.

できます。

デフォルトでは、 空白になっています。

コントローラーの 自動更新を有効にする

この設定項目では、 インストール後のVDAをControllerに自動的に登録する機能を許可または禁止します。

VDAを Controllerに登録すると、登録先のControllerにより環境内の ControllerのFQDNおよびSIDの一覧がVDAに送信されます。この一覧の内容は、VDAにより永続的な ストレージに書き込まれます。また、各Controllerは90分ごとに サイトのデータベースにアクセスして、 Controllerの追加や削除、およびポリシーの変更内容について確認し、 登録したVDAに更新情報を送信します。VDAは、受信した最新の一覧に基づいてすべての Controllerからの接続を受け入れます。

デフォルトでは、 有効になっています。

IPv6 コントローラー登録のみを使用する

この設定項目では、 Controllerへの登録時にVDAで使用されるアドレスの形式を指定します。

- この設定項目を有効にすると、 そのマシンのIPv6アドレスを使用してVDAがControllerと登録および通信を行います。VDAが Controllerと通信するときに、グローバル IPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（ほかのIPv6 アドレスを使用できない場合のみ）の順でIPv6アドレスが選択されます。
- この設定が無効な場合、そのマシンのIPv4 アドレスを使用してVDA がControllerと登録および通信を行います。

デフォルトでは、 無効になっています。

サイト GUID

この設定を使用する場合は、 ［コントローラーの自動更新を有効にする］ 設定で［禁止］が選択されていることを確認してください。

この設定項目では、 VDAのController登録をActive Directoryベースで行うときに使用される、 サイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、 空白になっています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX 3D Proのポリシー設定

Dec 05, 2017

［HDX 3D Pro］カテゴリには、ユーザーの画質構成ツールを有効にして構成するための設定項目が含まれています。 ユーザーがこのツールを使用すると、画質と応答性間のバランスをリアルタイムで調整して、帯域幅の使用を最適化できます。

無損失を有効にする

この設定では、ユーザーが 画質構成ツールで無損失圧縮を有効にしたり無効にしたりすることを許可するかどうかを 指定します。デフォルトでは、ユーザーは 無損失圧縮を有効にできません。

ユーザーが無損失圧縮を 有効にすると、自動的に画質構成ツールで設定可能な 最高画質に設定されます。デフォルトでは、ユーザー デバイスとホストコンピューターの能力に応じて、GPU またはCPUベースの圧縮が使用されます。

HDX 3D Pro 品質レベル

この設定では、ユーザーが画質構成ツールで設定できる画質 調整範囲の最小値および最大値を 指定します。

画質は0～100の値で指定します。最大値には、 最小値を超える値を設定する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

監視のポリシー設定

Dec 05, 2017

監視セクションには、プロセスとリソースの監視、およびアプリケーション障害の監視に関するポリシー設定が含まれていま す。

これらのポリシーのスコープは、サイト、デリバリーグループ、デリバリーグループの種類、組織単位 、およびタグによって定義されます。

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントはVDAから収集され、監視データベースに格納されます。VDAからデータポイントを送信するとネットワーク帯域幅が消費され、これを保存すると監視データベースで大幅に容量が消費されます。特定のスコープ（特定のデリバリーグループや組織単位など）でリソースデータとプロセスデータのいずれか、または両方とも監視しない場合は、ポリシーを無効にすることをお勧めします。

プロセス監視の有効化

この設定を有効にすると、VDAがインストールされているマシンでのプロセスの監視が許可されます。CPUやメモリ使用量などの統計が監視サービスに送信されます。統計は、Directorでのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は無効になっています。

リソース監視の有効化

この設定を有効にすると、VDAがインストールされているマシンでのクリティカルパフォーマンスカウンターの監視が許可されます。統計（CPUやメモリ使用量、IOPS、ディスク遅延などのデータ）が監視サービスに送信されます。統計は、Directorでのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は有効になっています。

スケーラビリティ

CPUおよびメモリデータは、各VDAからデータベースに5分間隔で適用されます。プロセスデータ（有効な場合）は、データベースに10分間隔で適用されます。IOPSおよびディスク待ち時間のデータは、データベースに1時間間隔で適用されます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**に設定されています。データ保持の値は次のとおりです（Platinumライセンス）。

データの粒度	日数
5分データ	1日
10分データ	7日
時間単位のデータ	30日間

© 1999-2017 Citrix Systems, Inc. All rights reserved.

日単位のデータ	90日間

IOPSおよびディスク遅延データ

IOPSおよびディスク遅延データは、デフォルトで**有効**に設定されています。データ保持の値は次のとおりです（Platinumライセンス）。

データの粒度	日数
時間単位のデータ	3日
日単位のデータ	90日間

上記のデータ保持設定では、1つのVDAのCPU、メモリ、IOPS、およびディスク遅延のデータを1年間格納するのに約276KBの容量が必要です。

マシンの数	必要なストレージ
1	276KB
1,000	270MB
40,000	10.6GB

プロセスデータ

デフォルトでは、プロセスデータは**無効**になっています。プロセスデータは、必要に応じてマシンのサブセットで有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データの粒度	日数
10分のデータ	1日
時間単位のデータ	7日

プロセスデータがデフォルトの保持設定で有効な場合、プロセスデータは1年間でVDAあたり約1.5MB、ターミナルサービスVDA（TS VDA）あたり約3MB消費します。

マシンの数	必要なストレージ（VDA）	必要なストレージ（TS VDA）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1	1.5MB	3MB
1,000	1.5GB	3GB

> **注意**
>
> 上記の数値には、インデックス領域は含まれません。上記の計算は概算であり、展開によって異なる可能性があります。

オプションの構成

デフォルトの保持設定をニーズに合わせて変更できます。ただし、これはストレージを余分に消費します。以下の設定を有効にすると、プロセス使用データがより正確になります。有効にできる構成は次のとおりです。

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

これらの構成は、監視Powershellコマンドレットから有効にできます。Set-MonitorConfiguration

アプリケーション障害の監視ポリシー

デフォルトでは、**[アプリケーション障害]**タブは、サーバーOSのVDAからのアプリケーション障害のみが表示されます。アプリケーション障害の監視の設定は、以下の監視ポリシーによって変更できます。

アプリケーション障害の監視を有効にする

アプリケーション障害の監視を、アプリケーションのエラーまたは障害（クラッシュと未処理例外）のいずれか、または両方を監視するように構成するには、以下の設定を行ってください。
[値]を**[なし]**に設定して、アプリケーション障害の監視を無効にしてください。
デフォルトでは、この設定はアプリケーション障害のみになっています。

デスクトップ OS VDA でアプリケーション障害の監視を有効にする

デフォルトでは、サーバーOSのVDAでホストされたアプリケーションの障害のみが監視されています。デスクトップOSのVDAを監視するには、ポリシーを**[許可]**に設定します。
デフォルトでは、この設定は**禁止**になっています。

障害の監視から除外するアプリケーション一覧

障害を監視しないアプリケーションの一覧を指定します。
デフォルトでは、この一覧は空です。

ストレージ計画のヒント

グループポリシー。 リソースデータやプロセスデータを監視しない場合は、グループポリシーを使ってどちらかまたは両方

© 1999-2017 Citrix Systems, Inc. All rights reserved.

をオフにできます。詳しくは、「ポリシーの作成」の「グループポリシー」セクションを参照してください。

データのグルーミング。デフォルトのデータ保持設定を変更して、データを早くグルーミングし、ストレージ領域を開放できます。グルーミングの設定について詳しくは、「APIを使ったデータアクセス」の「データの粒度と保持」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

仮想IPのポリシー設定

Dec 05, 2017

［仮想IP］カテゴリには、 セッションの仮想ループバックアドレスの使用を制御するための設定項目が含まれています。

仮想IP ループバックサポート

この設定項目では、 各セッション固有の仮想ループバックアドレスの使用を有効にするかどうかを指定します。無効にすると、 セッション固有の仮想ループバックアドレスは使用されません。

デフォルトでは、無効になっています。

仮想IPループバックプログラム一覧

この設定項目では、 仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。一覧にプログラムを追加するときは、 実行可能ファイルの名前のみを指定します。パス全体を入力する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レジストリを使ったCOMポートおよびLPTポートリダイレクト設定の構成

Feb 19, 2018

VDAバージョン7.0～7.8では、COMポートおよびLPTポートの設定はレジストリを使用した場合にのみ構成できます。7.0より前のバージョンのVDA、およびVDAバージョン7.9以降では、これらの設定はStudioで構成できます。詳しくは、「ポートリダイレクトのポリシー設定」および「帯域幅のポリシー設定」を参照してください。

COMポートおよびLPTポートのリダイレクト設定は、VDAイメージまたはマシンのレジストリHKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\Deprecatedで構成します。

COMポートおよびLPTポートリダイレクトを有効にするには、以下のレジストリキーを追加してREG_DWORD値を設定します。
注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリ エディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

レジストリキー	説明	値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitComBw	COMポートリダイレクトチャネルの最大帯域幅	数値
LimitComBWPercent	COMポートのリダイレクトチャネルで使用可能な帯域幅のセッション全体に対する割合	0～100の数値
AutoConnectClientComPorts	ユーザーデバイス側のCOMポートへの自動接続	1（許可）または0（禁止）
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitLptBw	LPTポートリダイレクトチャネルの最大帯域幅	数値
LimitLptBwPercent	LPTポートのリダイレクトチャネルで使用可能な帯域幅のセッション全体に対する割合	0～100の数値
AutoConnectClientLptPorts	ユーザーデバイス側のLPTポートへの自動接続	1（許可）または0（禁止）

これらのレジストリを設定したら、そのマスターイメージまたは物理マシンが使用されるようにマシンカタログを変更します。ユーザーのデスクトップは、ログオフ時に新しい設定で更新されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Connector for Configuration Manager 2012のポリシー設定

Dec 05, 2017

［Connector for Configuration Manager 2012］カテゴリには、Citrix Connector 7.5エージェントを構成するための設定項目が含まれています。

重要： 警告、ログオフ、および再起動メッセージに関する設定項目は、手動管理またはProvisioning Servicesで管理するサーバーOSマシンカタログにのみ適用されます。これらのマシンカタログでは、保留中のアプリケーションのインストールまたソフトウェアのアップデートがある場合、Connectorサービスによりユーザーに警告が表示されます。
MCSで管理するカタログでは、Studioでユーザーに通知してください。手動管理のデスクトップOSカタログでは、Configuration Managerでユーザーに通知してください。Provisioning Servicesで管理するデスクトップOSカタログでは、Provisioning Servicesでユーザーに通知してください。

警告 表示間隔

この設定項目 では、警告メッセージを表示する間隔を定義 します。

間隔は、 ddd.hh:mm:ss形式で設定します。
- ddd は オプションのパラメーターで、日数を0～999で指定します。
- hh は時間で、 0～23で指定します。
- mm は分で、 0～59で指定します。
- ss は秒で、 0～59で指定します。

デフォルトでは、 01:00:00（1時間）が設定されています。

警告 メッセージの内容

この設定項目 では、予定されているソフトウェア更新、またはログオフが必要となるメンテナンスを ユーザーに通知するためのメッセージを入力します。

デフォルトでは、 「{TIMESTAMP} 作業を保存してください。 The server will go offline for maintenance in {TIMELEFT}」というメッセージが設定されています。

警告 メッセージのタイトル

この設定項目 では、警告メッセージのタイトルバーに表示される文字列を入力 します。

デフォルトでは、 「まもなくメンテナンス開始」というタイトルが設定されています。

警告 表示期間

この設定項目 では、ソフトウェアの更新またはメンテナンスについての警告 メッセージを表示する期間を定義します。

期間は、 ddd.hh:mm:ss形式で指定します。
- ddd は オプションのパラメーターで、日数を0～999で指定します。
- hh は時間で、 0～23で指定します。
- mm は分で、 0～59で指定します。
- ss は秒で、 0～59で指定します。

デフォルトでは、 16:00:00（16時間）が設定されています。これにより、 メンテナンスの約16時間前に最初の警告メッセー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

が表示されます。

最終的な強制 ログオフメッセージの内容

この設定項目 では、強制ログオフ処理が開始されたことをユーザーに通知するための メッセージを入力します。

デフォルトでは、「サーバーは現在 メンテナンスのためオフラインになっています。」というメッセージが設定されています。

最終的な強制 ログオフメッセージのタイトル

この設定項目 では、最終的な強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「IT担当からのお知らせ」というタイトルが設定されています。

強制ログオフの 猶予期間

この設定項目 では、ソフトウェアの更新またはメンテナンスのために、ユーザーにログオフを警告してから実際に 強制ログオフ処理を開始するまでの待機期間を定義します。

期間は、 ddd.hh:mm:ss形式で指定します。

- ddd は オプションのパラメーターで、日数を0～999で指定します。
- hh は時間で、 0～23で指定します。
- mm は分で、 0～59で指定します。
- ss は秒で、 0～59で指定します。

デフォルトでは、 00:05:00（5分）が設定されています。

強制ログオフ メッセージの内容

この設定項目 では、強制ログオフが開始される前に作業を保存してログオフするように ユーザーに通知するためのメッセージを入力します。

デフォルトでは、「{TIMESTAMP} 作業を保存してください。 The server will go offline for maintenance in {TIMELEFT}」というメッセージが設定されています。

強制ログオフ メッセージのタイトル

この設定項目 では、強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「IT担当からのお知らせ」というタイトルが設定されています。

イメージ管理モード

Connectorエージェントでは、Provisioning ServicesまたはMCSで管理されるマシンのクローン上で動作しているかどうかが自動的に検出されます。 これらのイメージ管理されたクローン上では、Configuration Managerによるアップデートが Connectorエージェントによってブロックされ、カタログのマスターイメージ上にアップデートが自動的にインストールされます。

マスターイメージのアップデートが完了したら、StudioでMCSカタログクローンの再起動をオーケストレーションします。 Connectorエージェントは、Configuration ManagerのメンテナンスウィンドウでPVSカタログクローンの再起動を自動的にオーケストレーションします。 この動作を無効にして、Configuration Managerによってソフトウェアがカタログクローンにインストールされるように設定するには、イメージ管理モードを［無効］に変更します。

再起動メッセージ の内容

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この設定項目 では、サーバーの再起動をユーザーに通知するための メッセージを入力します。

デフォルトでは、 「サーバーは現在 メンテナンスのためオフラインになっています。」というメッセージが設定されています。

定期的な エージェントタスクの実行間隔

この設定項目 では、Citrix Connectorエージェントタスクの実行間隔を指定します。

期間は、 ddd.hh:mm:ss形式で指定します。

- ddd は オプションのパラメーターで、日数を0～999で指定します。
- hh は時間で、 0～23で指定します。
- mm は分で、 0～59で指定します。
- ss は秒で、 0～59で指定します。

デフォルトでは、 00:05:00（5分）が設定されています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理

Dec 05, 2017

XenAppまたはXenDesktopサイトの管理では、さまざまなアイテムやタスクに対応する必要があります。

ライセンス管理

サイトを作成するときには、Citrix License Serverへの有効な接続が必要です。その後、Studioから、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理などのライセンス管理タスクを行うことができます。また、Studioからライセンス管理コンソールにアクセスすることもできます。

アプリケーション

アプリケーションは、デリバリーグループ、および必要に応じてアプリケーショングループで管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用して、エンドユーザーにより近いところにアプリケーションやデスクトップを配置し、パフォーマンスを向上させることができます。サイトをインストールおよび構成するときには、Controller、マシンカタログ、ホスト接続はすべて、プライマリゾーンにあります。その後、Studioを使って、これらのアイテムを含むサテライトゾーンを作成します。サイトに複数のゾーンを作成すると、新しく作成するマシンカタログ、ホスト接続、追加のControllerをどのゾーンに配置するか、指定できるようになります。また、ゾーン間でのアイテムの移動も可能です。

接続とリソース

ユーザーにアプリケーションやデスクトップを配信するマシンのホストに、ハイパーバイザーまたはクラウドサービスを使用している場合、サイトを作成したときに、そのハイパーバイザーまたはクラウドサービスへの最初の接続を作成します。この接続で使用されるストレージまたはネットワークの詳細は、その*リソース*を形成します。後でその接続やリソースを変更したり、新しい接続を作成したりできます。また、構成された接続を使用するマシンの管理も可能です。

ローカルホストキャッシュ

ローカルホストキャッシュを使用すると、Delivery Controllerとサイトデータベースの間の接続が失敗しても、サイト内の接続仲介操作を続行できます。XenAppおよびXenDesktopに提供される、最も包括的な高可用性機能です。

接続リース

接続リースでなく、ローカルホストキャッシュをお勧めします。ローカルホストキャッシュは、より強力な代替選択肢です。

仮想IPおよび仮想ループバック

Microsoft社の仮想IPアドレス機能により、セッションごとに動的に割り当てられるIPアドレスを公開アプリケーションで使用できます。Citrixの仮想ループバック機能を使用すると、ローカルホスト（デフォルトで127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

Delivery Controller

この記事では、Controllerをサイトに追加およびサイトから削除する場合の考慮事項と手順を説明します。また、Controllerを別のゾーンやサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

Delivery ControllerへのVDA登録

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAでアプリケーションやデスクトップの配信を支援できるようにするには、まず、Controllerに登録（接続を確立）する必要があります。Controllerのアドレスを指定するいくつかの方法については、この記事で説明します。Controllerをサイトに追加、移動、または削除すると同時に、VDAが最新情報を受け取ることが重要です。

セッション

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。中には、セッションの信頼性を最適化し、不便さやダウンタイム、生産性の損失を軽減できる機能もあります。

- セッション画面の保持
- クライアントの自動再接続
- ICA Keep-Alive
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioで、マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、柔軟な検索機能を使用します。

タグ

タグは、マシン、アプリケーション、グループ、ポリシーなどの項目を識別するために使用します。タグを使用すると、特定の操作が指定したタグの項目のみに適用されるように調整できます。

IPv4またはIPv6

XenAppおよびXenDesktopでは、IPv4のみまたはIPv6のみ（ピュアIPv4またはピュアIPv6）の環境がサポートされ、重複するIPv4とIPv6のネットワークを使用した「デュアルスタック」環境がサポートされます。ここでは、これらの展開について説明します。また、IPv4またはIPv6の使用を制御するCitrixポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDAをインストールすると、Citrix Profile managementも自動的にインストールされます。このプロファイルソリューションを使用する場合は、この記事で一般情報を確認し、完全な詳細については、Profile managementのドキュメントを参照してください。

Citrix Insight Services

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrixが提供するプラットフォームです。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ライセンス管理

Dec 05, 2017

> ## 注意
>
> StudioとDirectorでCitrixライセンスサーバーVPXがサポートされません。CitrixライセンスサーバーVPXについて詳しくは、Citrixライセンスのドキュメントを参照してください。

管理者は、Studioを使用してライセンスを管理したり監視したりできます（ライセンスサーバーがStudioと同じドメインまたは信頼されたドメインで動作する場合）。そのほかのライセンス関連のタスクについては、ライセンスのドキュメントおよびマルチタイプのライセンスを参照してください。

以下で説明するタスクを実行するには、すべての管理作業を実行できるライセンス管理者である必要があります。Studioでライセンス情報を表示するには、［ライセンスの表示］以上の管理者権限が必要です。組み込みのすべての管理権限を実行できる管理者と読み取り専用管理者の役割には、この権限が含まれています。

以下の表に、サポートされるエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
XenApp	• Platinum • エンタープライズ • 詳細設定	同時使用
XenDesktop	• Platinum • エンタープライズ • アプリ • VDI	• ユーザー/デバイス • 同時使用

ライセンス情報を表示するには、Studioのナビゲーションペインで**[構成] > [ライセンス]** の順に選択します。指定したライセンスサーバーにインストールされているすべてのライセンスの一覧と、それらのライセンスの使用状況およびサイトのライセンス設定の概要が表示されます。

Citrixからライセンスをダウンロードするには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. ［操作］ペインの **[ライセンスの割り当て]** を選択します。
3. ライセンスアクセスコードを入力します。このコードは、Citrixからメールで送信されます。
4. 製品を選択し、 **[ライセンスの割り当て]** をクリックします。その製品について使用できるすべてのライセンスが割り当てられダウンロードされます。ライセンスアクセスコードを入力してすべてのライセンスを割り当ておよびダウンロードすると、そのライセンスアクセスコードは使用できなくなります。そのコードで追加のライセンス処理が必要な場合は、My Accountにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスファイルを追加するには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. ［操作］ペインの **[ライセンスの追加]** を選択します。
3. ライセンスファイルを参照して、ライセンスサーバーに追加します。

ライセンスサーバーを変更するには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. ［操作］ペインの **[ライセンスサーバーの変更]** を選択します。
3. ライセンスサーバーのアドレスを「name:port」形式で入力します。nameはライセンスサーバーのDNS、NetBIOS、またはIPアドレスです。ポート番号（）を指定しない場合、デフォルトのポート（27000）が使用されます。

使用するライセンスの種類を選択するには、次の手順に従います。

- サイトを構成するときに、ライセンスサーバーを指定した後で、使用するライセンスの種類を選択します。サーバーにライセンスがない場合は、30日間製品を試用できるオプションが自動的に選択されます。
- サーバーに複数のライセンスがある場合はその詳細が表示されます。いずれかのライセンスを選択します。または、サーバーにライセンスファイルを追加してそれを選択します。

製品エディションおよびライセンスモデルを変更するには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. ［操作］ペインの **[製品エディションの編集]** を選択します。
3. 適切なオプションを更新します。

ライセンス管理コンソールにアクセスするには、［操作］ペインの**[ライセンス管理コンソール]** を選択します。ライセンス管理コンソールが自動的に開くか、パスワードによる保護が構成済みの場合は資格情報を入力するための画面が開きます。ニンソールの使い方について詳しくは、ライセンスのドキュメントを参照してください。

ライセンス管理者を追加するには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択します。
3. ［操作］ペインの **[ライセンス管理者の追加]** を選択します。
4. 管理者として追加するユーザーを参照して、権限を選択します。

ライセンス管理者の権限を変更するか、ライセンス管理者を削除するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択し、管理者を選択します。
3. ［操作］ペインの **[ライセンス管理者の編集]** または **[ライセンス管理者の削除]** を選択します。

ライセンス管理者グループを追加するには、次の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択します。
3. ［操作］ペインの **[ライセンス管理者グループの追加]** を選択します。
4. ライセンス管理者として追加するグループを参照して、権限を選択します。Active Directoryグループを追加すると、ライセンス管理者権限がそのグループのすべてのユーザーに設定されます。

ライセンス管理者グループの権限を変更するか、ライセンス管理者グループを削除するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[構成] > [ライセンス]** の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択し、管理者グループを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. ［操作］ペインの **[ライセンス管理者の編集]** または **[ライセンス管理者の削除]** を選択します。

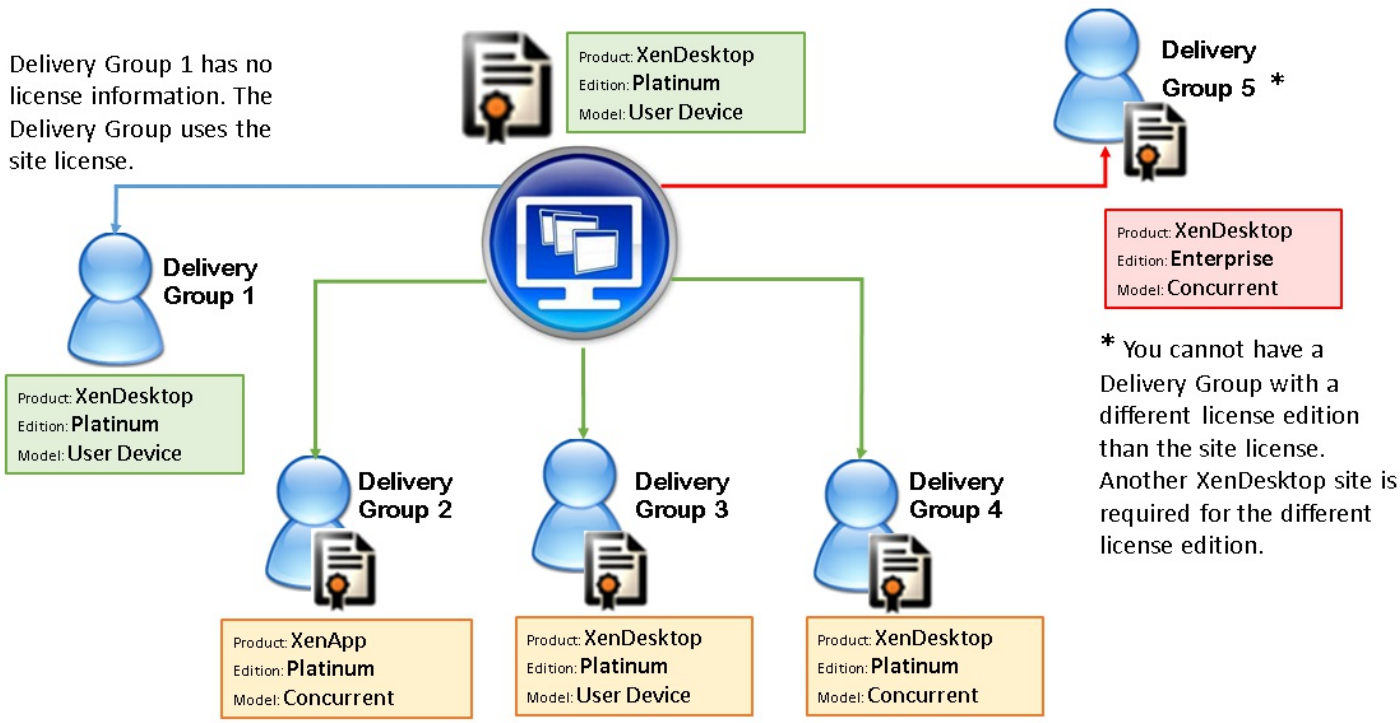
© 1999-2017 Citrix Systems, Inc. All rights reserved.

マルチタイプのライセンス

Dec 05, 2017

マルチタイプのライセンスでは、単一のXenAppまたはXenDesktopサイト上にある複数のデリバリーグループでそれぞれ異なる種類のライセンスを使用できます。**種類**とは、製品ID（XDT、MPS）とモデル（ユーザーデバイス、同時使用）の組み合わせのことです。デリバリーグループでは、サイトの製品エディションを使用する必要があります。

マルチタイプのライセンスが構成されていない場合は、完全に分割されているサイト上で構成されるときのみ異なる種類のイセンスを使用できます。デリバリーグループではサイトのライセンスが使用されます。



各種類のライセンスを使用するデリバリーグループを指定するには、次のBroker PowerShellコマンドレットを使用します。

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには次を使用します。

- Citrix Studio
- Citrix Licensing Manager
- ライセンス管理コンソール
- Citrix社のWebサイト

Subscription Advantageの有効期間は、各ライセンスファイルおよび各製品とモデルに固有です。デリバリーグループ間のSubscription Advantage有効期間は異なる場合があります。

Broker PowerShell SDK

© 1999-2017 Citrix Systems, Inc. All rights reserved.

DesktopGroupオブジェクトには次の2つのプロパティがあり、関連するNew-BrokerDesktopGroupコマンドレットおよびSet-BrokerDesktopGroupコマンドレットを使用して操作することができます。

Name	Value	Restriction
LicenseModel	グループのライセンスモデルを指定する列挙値です（ConcurrentまたはUserDevice）。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。
ProductCode	グループのライセンス製品IDを指定するテキスト文字列であり、XDT（XenDesktopの場合）またはMPS（XenAppの場合）を設定します。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。

New-BrokerDesktopGroup

デスクトップのグループの仲介を管理するデスクトップグループを作成します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループの有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

Get-BrokerDesktopGroup

指定した条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループのProductCodeプロパティとLicenseModelプロパティが含まれます。これらのプロパティがNew- BrokerDesktopGroupまたはSet-BrokerDesktopGroupにより設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/を参照してください。

例

次のPowerShellコマンドレットサンプルでは、2つの既存のデリバリーグループに対してマルチタイプのライセンスを設定し、3番目のデリバリーグループを設定する方法について説明します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 1番目のデリバリーグループをXenAppおよびConcurrentに設定します。
   Set-BrokerDesktopGroup -Name "Delivery Group for XenApp Platinum Concurrent" -ProductCode MPS -LicenseModel Concurrent
2. 2番目のデリバリーグループをXenDesktopおよびConcurrentに設定します。
   Set-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum Concurrent" -ProductCode XDT -LicenseModel Concurrent
3. 3番目のデリバリーグループを作成し、XenDesktopおよびUserDeviceに設定します。
   New-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum UserDevice" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

© 1999-2017 Citrix Systems, Inc. All rights reserved.

特殊考慮事項

マルチタイプのライセンスの機能は、通常のXenAppおよびXenDesktopのライセンスとは異なります。

DirectorまたはStudioからアラートや通知が行われることはありません。

- ライセンスの上限に近づいた場合、もしくは追加猶予期間のトリガーまたは有効期限に近づいた場合でも情報は提供されません。
- 特定のグループに問題が発生しても、通知はされません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーション

Dec 05, 2017

はじめに

デリバリーグループのみを使用する（アプリケーショングループは使用しない）環境の場合は、デリバリーグループにアプリケーションを追加します。アプリケーショングループもある場合は、通常はアプリケーショングループにアプリケーションを追加してください。このガイダンスでは、管理を簡単にする方法について説明します。アプリケーションは、常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属する必要があります。

アプリケーションの追加ウィザードで、1つまたは複数のデリバリーグループを選択するか、1つまたは複数のアプリケーショングループを選択できますが、両方は選択できません。アプリケーションのグループ関連付けは後で変更できますが（アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは複雑度が増えないようにします。アプリケーションは、どちらかの種類のグループのみに含めます。

アプリケーションを複数のデリバリーグループまたはアプリケーショングループに関連付ける場合、そのすべてのグループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。 そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションが関連付けられているグループをすべて含めるようにします。

2つのアプリケーションを（おそらくは異なるグループから）同じ名前で同じユーザーに公開する場合は、Studioで［アプリケーション名（ユーザー用）］ボックスに別の名前を入力します。これを行わないと、ユーザーのCitrix Receiverに同じ名前が2つ表示されます。

アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。アプリケーションの追加時、またはその後で、アプリケーションを配置するアプリケーションフォルダーを変更することもできます。

以下の情報を参照してください。

- デリバリーグループについて詳しくは、「デリバリーグループの作成」を参照してください。
- アプリケーショングループについて詳しくは、「アプリケーショングループの作成」を参照してください。
- アプリケーションに追加できるタグについて詳しくは、「タグ」を参照してください。

アプリケーションの追加

アプリケーションは、デリバリーグループまたはアプリケーショングループの作成時に追加できます。手順について詳しくは、「デリバリーグループの作成」と「アプリケーショングループの作成」で説明しています。次の手順で、グループ作成後にアプリケーションを追加する方法について説明します。

ヒント：

- リモートPCアクセスのデリバリーグループにアプリケーションを追加することはできません。
- デリバリーグループまたはアプリケーショングループからアプリケーションを削除するために、アプリケーションの追加ウィザードを使用することはできません。これは、別の処理になります。

1つまたは複数のアプリケーションを追加するには、以下の手順に従います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Studioのナビゲーションペインで **[アプリケーション]** を選択し、次に［操作］ペインで **[アプリケーションの追加]** を選択します。
2. アプリケーションの追加ウィザードが起動され、 **[はじめに]** ページが開きます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、［グループ］ページ、［アプリケーション］ページ、および［概要］ページの操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで **[次へ]** をクリックします。

手順1の代わりに、アプリケーションを単一のデリバリーグループまたはアプリケーショングループに追加する場合は、以下の手順に従います。

- アプリケーションを単一のデリバリーグループに追加するには、手順1で、Studioのナビゲーションペインで**[デリバリーグループ]** を選択し、中央ペインでデリバリーグループを選択してから［操作］ペインの**[アプリケーションの追加]** を選択します。ウィザードの **[グループ]** ページは表示されません。
- アプリケーションを単一のアプリケーショングループに追加するには、手順1で、Studioのナビゲーションペインで**[アプリケーション]** を選択し、中央ペインで**アプリケーショングループ**を選択してから［操作］ペインのアプリケーショングループの名前の下の **[アプリケーションの追加]** エントリを選択します。ウィザードの **[グループ]** ページは表示されません。

グループ

このページには、サイトのすべてのデリバリーグループが一覧表示されます。 アプリケーショングループも作成してある場は、このページにアプリケーショングループとデリバリーグループが一覧表示されます。 どちらかのグループから選択できすが、両方のグループからは選択できません。言い換えると、アプリケーションを同時にアプリケーショングループとデリバリーグループに追加することはできません。通常は、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加する必要があります。

すべてのアプリケーションは常に少なくとも1つのグループに関連付ける必要があるため、アプリケーションを追加するときには、少なくとも1つのデリバリーグループ（または、使用できる場合はアプリケーショングループ）の横にあるチェックボックスをオンにする必要があります。

アプリケーション

[追加] ボックスをクリックして、アプリケーションのソースを表示します。

接続元	説明
［スタート］メニューから	選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、 **［OK］** をクリックします。 このソースは、（1）デリバリーグループが関連付けられていないアプリケーショングループを選択した、（2）マシンを含まないデリバリーグループが関連付られているアプリケーショングループを選択した、（3）マシンを含まないデリバリーグループを選択した、のいずれかの場合には選択できません。
手動で定義	サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。これらの情報を入力したら、 **［OK］** をクリックします。
既存	以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、 **［OK］** をクリックします。 このソースは、サイトにアプリケーションが含まれていない場合は選択できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V	App-Vパッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページでApp-Vサーバーまたはアプリケーションライブラリを選択します。結果表示で、追加するアプリケーションのチェックボックスをオンにし、**[OK]**をクリックします。詳しくは、「App-V」を参照してください。 このソースは、サイトでApp-Vを構成していない場合は選択できません。
アプリケーショングループ	アプリケーショングループ。このソースを選択すると、新たなページが開き、アプリケーショングループが一覧表示されます。（各グループのアプリケーションの一覧も表示されますが、グループのみを選択できます。個別のアプリケーションは選択できません。）選択したグループの現在または将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスをオンにし、**[OK]**をクリックします。 このソースは、（1）アプリケーショングループがない場合、または（2）選択したデリバリーグループがアプリケーショングループをサポートしない場合（マシンが静的に割り当てられているデリバリーグループなど）は、選択できません。

表で説明したように、［追加］ボックスの一部のソースは、そのタイプの有効なソースがない場合は選択できません。互換性のないソースはボックスに含まれません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできません）。選択したグループに既に追加済みのアプリケーションは選択できません。

割り当てられたAppDiskからアプリケーションを追加するには、**[［スタート］メニューから]**を選択します。ここにアプリケーションがない場合、**[手動で定義]**を選択して詳細を入力します。フォルダーアクセスエラーが発生した場合、フォルダーを「共有」に設定して、**[手動で定義]**からアプリケーションを再度追加してください。

アプリケーションのプロパティ（設定）は、このページから、または後で変更できます。

アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。アプリケーションは、このページから、または後で変更できます。アプリケーションの追加時に、同じフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。 提案された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか別のフォルダーを選択できます。たとえば、アプリケーションフォルダーに既に「app」が存在する場合に、このフォルダーに「app」という名前の別のアプリケーションを追加しようとすると、新しい名前「app_1」が提案されます。

結果

追加するアプリケーションが10個以下の場合は、それらのアプリケーションの名前が**[追加するアプリケーション]**に一覧表示されます。追加するアプリケーションが10個より多い場合は、合計数が示されます。

概要の情報を確認し、**[完了]**をクリックします。

アプリケーションのグループ関連付けの変更

アプリケーションの追加後、アプリケーションを関連付けるデリバリーグループやアプリケーショングループを変更できます。

ドラッグアンドドロップを使用して、アプリケーションを追加のグループに関連付することができます。ドラッグアンドドロップする代わりに、［操作］ペインのコマンドを使用することもできます。

アプリケーションを複数のデリバリーグループまたは複数のアプリケーショングループに関連付けた場合、グループの優先度を使用して、アプリケーションを検索するときに複数のグループを確認する順序を指定できます。デフォルトでは、すべての

© 1999-2017 Citrix Systems, Inc. All rights reserved.

グループの優先度は0（最高）です。同じ優先度のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、（1）デリバリーグループに共有マシンが含まれていてこのグループがXenDesktop 7.x バージョンで作成されており、かつ（2）［デリバリーグループの編集］権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれるデリバリーグループを選択することもできます。［プロパティ］ダイアログボックスをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択し、中央ペインでアプリケーションを選択します。
2. ［操作］ペインの **[プロパティ]** を選択します。
3. **[グループ]** ページを選択します。
4. グループを追加するには、**[追加]** ボックスをクリックして、**[アプリケーショングループ]** または **[デリバリーグループ]** を選択します。（アプリケーショングループを作成していない場合は、［デリバリーグループ］のみが表示されます。）次に、1つまたは複数の追加可能なグループを選択します。アプリケーションと互換性のないグループや、既にそのアプリケーションが関連付られているグループは選択できません。
5. グループを削除するには、1つまたは複数のグループを選択し、**[削除]** をクリックします。グループの関連付けを削除した結果、アプリケーションがアプリケーショングループまたはデリバリーグループのいずれにも関連付けられなくなる場合は、アプリケーションが削除されることが通知されます。
6. グループの優先度を変更するには、グループを選択し **[優先度の編集]** をクリックします。優先度値を選択し、**[OK]** をクリックします。
7. 完了したら、**[適用]** をクリックして変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前変更、および削除

使用する操作：

- **複製**：アプリケーションを複製して、パラメーターまたはプロパティが異なる別のバージョンを作成することができます。アプリケーションを複製すると、一意のサフィックスを使用してアプリケーション名が自動的に変更され、元のアプリケーションに隣接して配置されます。アプリケーションを複製して、別のグループに追加することもできます。（複製後にアプリケーションを最も容易に移動する方法は、ドラッグアンドドロップです。）
- **有効化または無効化**：アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なる操作です。
- **名前変更**：同時に名前を変更できるアプリケーションは1つのみです。アプリケーションの名前を変更しようとしたときに、同じフォルダー内に同じ名前のアプリケーションが既に存在する場合、別の名前を指定するよう指示するメッセージが表示されます。
- **削除**：アプリケーションを削除すると、そのアプリケーションが関連付けられていたデリバリーグループとアプリケーショングループから削除されますが、アプリケーションの追加元として使用したソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループからアプリケーションを削除する操作とは異なる操作です。

アプリケーションを複製、有効化または無効化、名前変更、および削除するには：

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインで1つまたは複数のアプリケーションを選択し、［操作］ペインで目的のタスクを選択します。
3. 確認のメッセージが表示されたら、［はい］をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デリバリーグループからのアプリケーションの削除

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられる（属する）必要があります。アプリケーションをデリバリーグループから削除するとデリバリーグループまたはアプリケーショングループへのアプリケーションの関連付けが削除される場合、続行するとアプリケーションが削除されると通知されます。この場合、そのアプリケーションを配信する必要がある場合は、有効なソースからもう一度追加する必要があります。

1. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。
2. デリバリーグループを選択します。中央ペインの下部で **[アプリケーション]** タブを選択し、削除するアプリケーションを選択します。
3. ［操作］ペインの **[アプリケーションの削除]** を選択します。
4. 削除を確認します。

アプリケーショングループからのアプリケーションの削除

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属する必要があります。アプリケーションをアプリケーショングループから削除するとデリバリーグループまたはアプリケーショングループへのアプリケーションの関連付けが削除されてしまう場合、続行するとアプリケーションが削除されると通知されます。この場合、そのアプリケーションを配信する必要がある場合は、有効なソースからもう一度追加する必要があります。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. 中央ペインでアプリケーショングループを選択し、中央ペインで1つまたは複数のアプリケーションを選択します。
3. ［操作］ペインの **[アプリケーション グループから削除します]** を選択します。
4. 削除を確認します。

アプリケーションプロパティの変更

同時にプロパティを変更できるアプリケーションは1つのみです。

アプリケーションのプロパティを変更するには、次の手順に従います。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択します。
2. アプリケーションを選択し、［操作］ペインで **[アプリケーションプロパティの編集]** を選択します。
3. 変更するプロパティを含むページを選択します。
4. 完了したら、 **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

プロパティ	選択するページ
Receiverでアプリケーションを表示するカテゴリ/フォルダー	デリバリー
コマンドライン引数（「公開アプリケーションにパラメーターを渡す」セクションを参照）	場所

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーションを使用できるデリバリーグループおよびアプリケーショングループ	グループ
説明	識別
ファイル拡張子とファイルタイプの関連付け：アプリケーションが自動的に開く拡張子	ファイルタイプの関連付け
アイコン	デリバリー
StoreFront用のキーワード	識別
制限（「アプリケーション制限の設定」セクションを参照）	デリバリー
名前：ユーザーと管理者に表示される名前	識別
実行可能ファイルへのパス（「公開アプリケーションにパラメーターを渡す」セクションを参照）	場所
ユーザーのデスクトップにショートカットを表示するかどうか：有効化または無効化	デリバリー
表示：Citrix Receiverでアプリケーションを表示できるユーザーを制限します（非表示のアプリケーションでも開始できます。非表示にすると同時に開始できないようにするには、別のグループに追加します）	表示の制限
作業ディレクトリ	場所

使用中のアプリケーションに変更内容を反映させるには、ユーザーがそのセッションからログオフする必要があります。

アプリケーション制限の設定

アプリケーションの使用を管理するため、アプリケーション制限を設定します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理することができます。同様に、アプリケーション制限を使用して、リソースの消費量が大きいアプリケーションの同時インスタンスの数を管理することもできます。これによってサーバーパフォーマンスを維持し、サービスの質の低下を防ぐことができます。

重要： この機能により、（Citrix ReceiverやStoreFrontなどからの）Controllerを介したアプリケーション起動数が制限されます。これ以外の方法で起動されて実行されるアプリケーションの数は、制限されません。すなわち、アプリケーション制限は、同時使用を管理する管理者をサポートし、あらゆるシナリオに適用されるわけではありません。たとえば、Controllerがリース接続モードである場合は、アプリケーション制限を適用できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。以下の2つのアプリケーション制限設定があり、そのいずれかまたは両方を設定できます。

- デリバリーグループのすべてのユーザーによるアプリケーションの最大同時インスタンス数
- デリバリーグループの1人のユーザーにつき1つのアプリケーションインスタンス

制限が設定されている場合、設定された制限を超過するアプリケーションインスタンスをユーザーが起動しようとすると、エラーメッセージが生成されます。

アプリケーション制限の使用例

- **同時インスタンスの最大数の制限。**デリバリーグループで、アプリケーションAlphaの同時インスタンスの最大数を15に設定しました。その後、このデリバリーグループのユーザーが、このアプリケーションの15インスタンスを同時に実行しています。このデリバリーグループのユーザーがAlphaを起動しようとすると、エラーメッセージが生成され、Alphaは起動しません。起動すると、先に設定した、アプリケーションの同時インスタンス数の制限値（15）を超過することになるためです。
- **1ユーザーにつき1インスタンスのアプリケーション制限。**別のデリバリーグループで、1ユーザーにつき1インスタンスのオプションをアプリケーションBetaに対して有効にしました。ユーザーTonyが、アプリケーションBetaを正常に起動しました。当日のその後、このアプリケーションはTonyのセッションで引き続き実行中でしたが、TonyはBetaの別のインスタンスを起動しようとしました。しかし、起動すると1ユーザーにつき1インスタンスの制限を超過することになるため、エラーメッセージが生成され、Betaは起動しません。
- **同時インスタンスの最大数および1ユーザーにつき1インスタンスの制限。**別のデリバリーグループで、同時インスタンスの最大数を10に設定し、1ユーザーにつき1インスタンスのオプションをアプリケーションDeltaに対して有効にしました。その後、このデリバリーグループの10人のユーザーがそれぞれDeltaのインスタンスを実行している場合、このデリバリーグループの別のユーザーがDeltaを起動しようとすると、エラーメッセージが生成され、Deltaは起動しません。現在の10人のDeltaユーザーのいずれかがこのアプリケーションの2つ目のインスタンスを起動しようとしても、エラーメッセージが生成され、2つ目のインスタンスは起動しません。

アプリケーションインスタンスがControllerを介さない方法（Controllerがリース接続モードの場合など）でも起動し、設定された制限を超過している場合、アプリケーションを使用中のユーザーがインスタンスを終了し、実行中のインスタンス数が制限を超過しなくなるまで、追加のインスタンスを起動することはできません。制限を超過した分のインスタンスが強制的にシャットダウンされることはなく、ユーザーがインスタンスを終了するまで継続できます。

セッションローミングを無効にする場合、1ユーザーにつき1インスタンスのアプリケーション制限も無効にしてください。1ユーザーにつき1インスタンスのアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する2つの値は、どちらも設定しないでください。ローミングについて詳しくは、「セッション」を参照してください。

アプリケーション制限を設定するには、以下の手順に従います。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択し、アプリケーションを選択します。
2. ［操作］ペインの **[アプリケーションプロパティの編集]** を選択します。
3. **[デリバリー]** ページで、次のいずれかのオプションを選択します。 操作を終了したら、**[OK]** または **[適用]** をクリックします。 （ **[OK]** をクリックすると、変更が適用され、［アプリケーションプロパティの編集］ダイアログボックスは閉じます。 **[適用]** をクリックすると、変更が適用され、ダイアログボックスは閉じずに開いたままとなります）。

- アプリケーションの無制限使用を許可します。インスタンスの同時実行数に制限はありません。これがデフォルトの設定です。
- アプリケーションの制限を設定します。以下の2種類の制限があります。いずれかまたは両方を指定します。
  - 同時に実行できるインスタンスの最大数の指定
  - 1ユーザーにつき1アプリケーションインスタンスの制限

© 1999-2017 Citrix Systems, Inc. All rights reserved.

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの［場所］ページで、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルタイプに関連付けると、その公開アプリケーションのコマンドライン（実行可能ファイルのパス）の後に"%*"（二重引用符で囲んだパーセントとアスタリスク記号）が追加されます。これらの記号は、ユーザーデバイス側に渡されるパラメーターのプレースホルダーとして機能します。

ファイルタイプに関連付けられている公開アプリケーションが起動しない場合は、記号が正しくコマンドラインに含まれていることを確認してください。“%*”記号が追加されている場合は、ユーザーデバイスから渡されるパラメーターがデフォルトで検証されます。特殊なパラメーターを必要とする公開アプリケーションでは、コマンドラインに"%**"（二重引用符で囲んだパーセントと2個のアスタリスク記号）が追加されています。これによりコマンドライン検証が無効になります。コマンドラインにこれらの記号が含まれていない場合は、手作業で追加できます。

実行可能ファイルのパスに、「C:\Program Files」のようなスペースを使ったフォルダー名が含まれている場合は、アプリケーションのコマンドラインを二重引用符で囲み、このスペースがコマンドラインに属していることを示します。それには、パスの前後に二重引用符を追加し、%*記号の前後にもう1組の二重引用符を追加します。このとき、パスの末尾の二重引用符と、%*記号の前の二重引用符の間に、必ずスペースを1つ入力してください。

たとえば、公開アプリケーションWindows Media Playerのコマンドラインは次のようになります。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

アプリケーションフォルダーの管理

新規アプリケーションをデリバリーグループに追加すると、デフォルトでは「**アプリケーション**」という名前のフォルダー内に表示されます。 デリバリーグループの作成時、アプリケーションの追加時、またはその後で、別のフォルダーを指定することもできます。

ヒント：

- 「アプリケーション」フォルダーの名前を変更したり、「アプリケーション」フォルダーを削除したりすることはできません。ただし、「アプリケーション」フォルダー内のすべてのアプリケーションを、作成済みの別のフォルダーに移動することは可能です。
- フォルダー名は、1~64文字とすることができます。スペースを使用できます。
- フォルダーは5レベルまで入れ子にできます。
- アプリケーションを含まない空のフォルダーを使用できます。
- フォルダーは、移動したり作成時に別の場所を指定したりしない限り、Studioでアルファベット順に表示されます。
- 親フォルダーが異なる限り、同じ名前の子フォルダーを作成できます。同様に、保存先フォルダーが異なる限り、同じ名前のアプリケーションを作成できます。
- フォルダー内のアプリケーションを表示するには、［アプリケーションの表示］権限が必要です。また、フォルダー内のアプリケーションを削除したり、フォルダー内のアプリケーション名を変更したり、アプリケーションが含まれるフォルダーを削除したりするには、フォルダーに含まれるすべてのアプリケーションに対する［アプリケーションプロパティの編集］権限が必要です。
- 以下の手順の多くでは、Studioの［操作］ペインを使用した操作が求められます。また、右クリックメニューやドラッグアンドドロップも使用できます。たとえば、意図しない場所にフォルダーを作成または移動した場合は、正しい場所にド

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ラッグアンドドロップできます。

アプリケーションのフォルダーを管理するには、Studioのナビゲーションペインで**[アプリケーション]** を選択します。次の一覧を参考にしてください。

- すべてのフォルダー（サブフォルダーを除く）を表示するには、フォルダー一覧の上にある**[すべて表示]** をクリックします。
- フォルダーを最上位レベルに作成する（サブフォルダーにしない）場合は、「アプリケーション」フォルダーを選択します。「アプリケーション」フォルダー以外の既存のフォルダー内に新しいフォルダーを作成するには、その既存のフォルダーを選択します。次に、［操作］ペインの **[フォルダーの作成]** を選択します。名前を入力します。
- フォルダーを移動するには、フォルダーを選択し、［操作］ペインの **[フォルダーの移動]** を選択します。サブフォルダーを持つフォルダーを除き、一度に複数のフォルダーを移動することはできません。ヒント：フォルダーを最も容易に移動する方法は、ドラッグアンドドロップです。
- フォルダー名を変更するには、名前を変更するフォルダーを選択し、［操作］ペインの **[フォルダー名の変更]** を選択します。名前を入力します。
- フォルダーを削除するには、削除するフォルダーを選択し、［操作］ペインの **[フォルダーの削除]** を選択します。 アプリケーションやサブフォルダーを含んでいるフォルダーを削除すると、それらのアプリケーションやサブフォルダーも削除されます。アプリケーションを削除すると、そのアプリケーションの割り当てがデリバリーグループから削除されます。マシンからアンインストールされることはありません。
- アプリケーションをフォルダーに移動するには、1つまたは複数のアプリケーションを選択します。次に、［操作］ペインの **[アプリケーションの移動]** を選択します。移動先のフォルダーを選択します

デリバリーグループの作成ウィザードおよびアプリケーショングループの作成ウィザードの**[アプリケーション]** ページで、特定のフォルダー（新しいフォルダーも含む）に、追加するアプリケーションを配置することもできます。デフォルトでは、追加されたアプリケーションは、アプリケーションフォルダーに配置されます。 **[変更]** をクリックして、フォルダーを選択するか作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユニバーサルWindowsプラットフォームアプリ

Dec 05, 2017

XenAppおよびXenDesktopでは、VDAがインストールされているユニバーサルWindowsプラットフォーム（UWP）アプリのWindows 10およびWindows Server 2016マシンでの使用がサポートされます。UWPアプリについて詳しくは、以下のMicrosoft社のドキュメントを参照してください。

- ユニバーサルWindowsプラットフォーム（UWP）アプリとは
- オフラインアプリの配布
- ユニバーサルWindowsプラットフォーム（UWP）アプリのガイド

この記事全体で、UWPアプリを意味する用語として「ユニバーサルアプリ」を使用します。

要件および制限事項

ユニバーサルアプリはWindows10およびWindows Server 2016マシン上のVDAでサポートされています。

VDAのバージョンは7.11以上である必要があります。

以下のXenAppおよびXenDesktop機能は、ユニバーサルアプリの使用時にはサポートされないか、または制限されます。

- ファイルタイプの関連付けはサポートされません。
- ローカルアプリケーションアクセスはサポートされません。
- 動的プレビュー：セッションで実行中のアプリが重複している場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用されるWin32 APIは、ユニバーサルアプリではサポートされません。
- アクションセンターリモート：ユニバーサルアプリでは、アクションセンターを使用して、セッションでメッセージを表示することができます。メッセージをユーザーに表示するには、これらのメッセージをエンドポイントにリダイレクトします。

同じサーバーからのユニバーサルアプリと非ユニバーサルアプリの起動はWindows 10 VDAではサポートされません。Windows Server 2016では、ユニバーサルアプリと非ユニバーサルアプリは別のデリバリーグループまたはアプリケーショングループに属する必要があります。

マシンにインストールされるユニバーサルアプリはすべて列挙されるため、Windowsストアへのユーザーアクセスを無効にすることをお勧めします。これにより、1人のユーザーによってインストールされたユニバーサルアプリが他のユーザーによってアクセスされるのを防ぐことができます。

サイドローディングの実行中に、ユニバーサルアプリはマシンにインストールされ、他のユーザーが使用できるようになります。他のユーザーがアプリを起動すると、アプリがインストールされます。その後OSによってAppXデータベースが更新され、アプリを起動しているユーザーには「インストール時の状態」と表示されます。

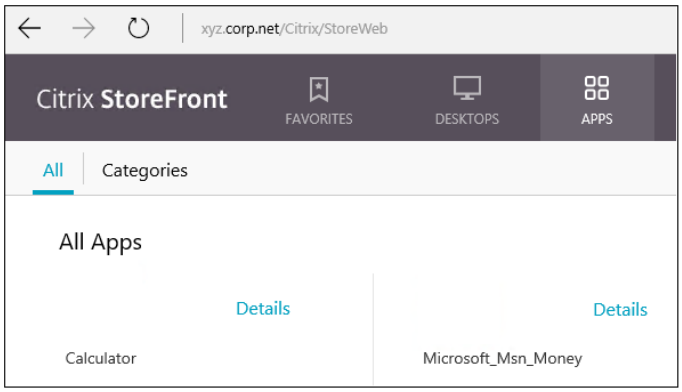
シームレスウィンドウまたは固定ウィンドウで起動された公開ユニバーサルアプリから正常にログオフすると、セッションが終了せずにユーザーがログオフしている状態になることがあります。このような場合は、セッションに残っているいくつかのプロセスが、セッションの適切な終了を阻止しています。これを解決するには、CTX891671のガイダンスに従って、セッションの修了を阻止しているプロセスを特定し、そのプロセスを「LogoffCheckSysModules」レジストリキーの値に追加します。

ユニバーサルアプリのアプリケーション表示名や説明の名前が正しくないことがあります。アプリケーションをデリバリーグループに追加するときに、これらのプロパティを編集および修正してください。

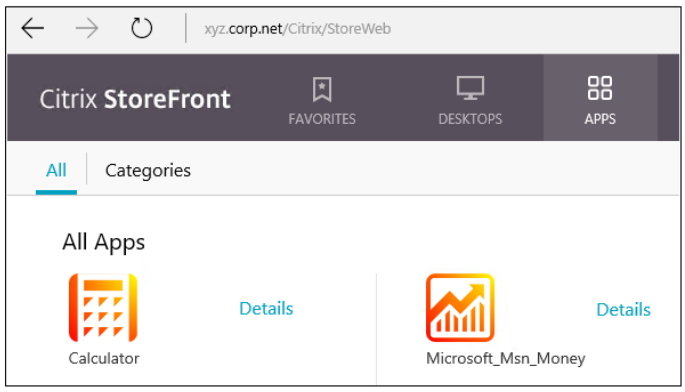
その他の問題については、「既知の問題」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

現時点では、複数のユニバーサルアプリに透過性が有効になった白いアイコンがありますが、これによってStoreFrontのディスプレイの白い背景でアイコンが見えなくなるという問題があります。これを回避するために、背景の色を変更できます。たとえば、StoreFrontマシンで、ファイルC:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.cssを編集します。このファイルの末尾に、**.storeapp-icon {background-image: radial-gradient(circle at top right, yellow, red); }**を追加します。以下の図は、この例の編集前と編集後を示しています。



Before



After

Windows Server 2016で、ユニバーサルアプリを起動するとサーバーマネージャーも起動されるという問題がありました。この問題の発生を回避するには、HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogonレジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にできます。詳しくは、https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/を参照してください。

ユニバーサルアプリのインストールと公開

ユニバーサルアプリのサポートは、デフォルトで有効になっています。

ユニバーサルアプリのVDAでの使用を無効にするには、レジストリ設定**EnableUWASeamlessSupport**をHKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggleに追加して**0**に設定します。

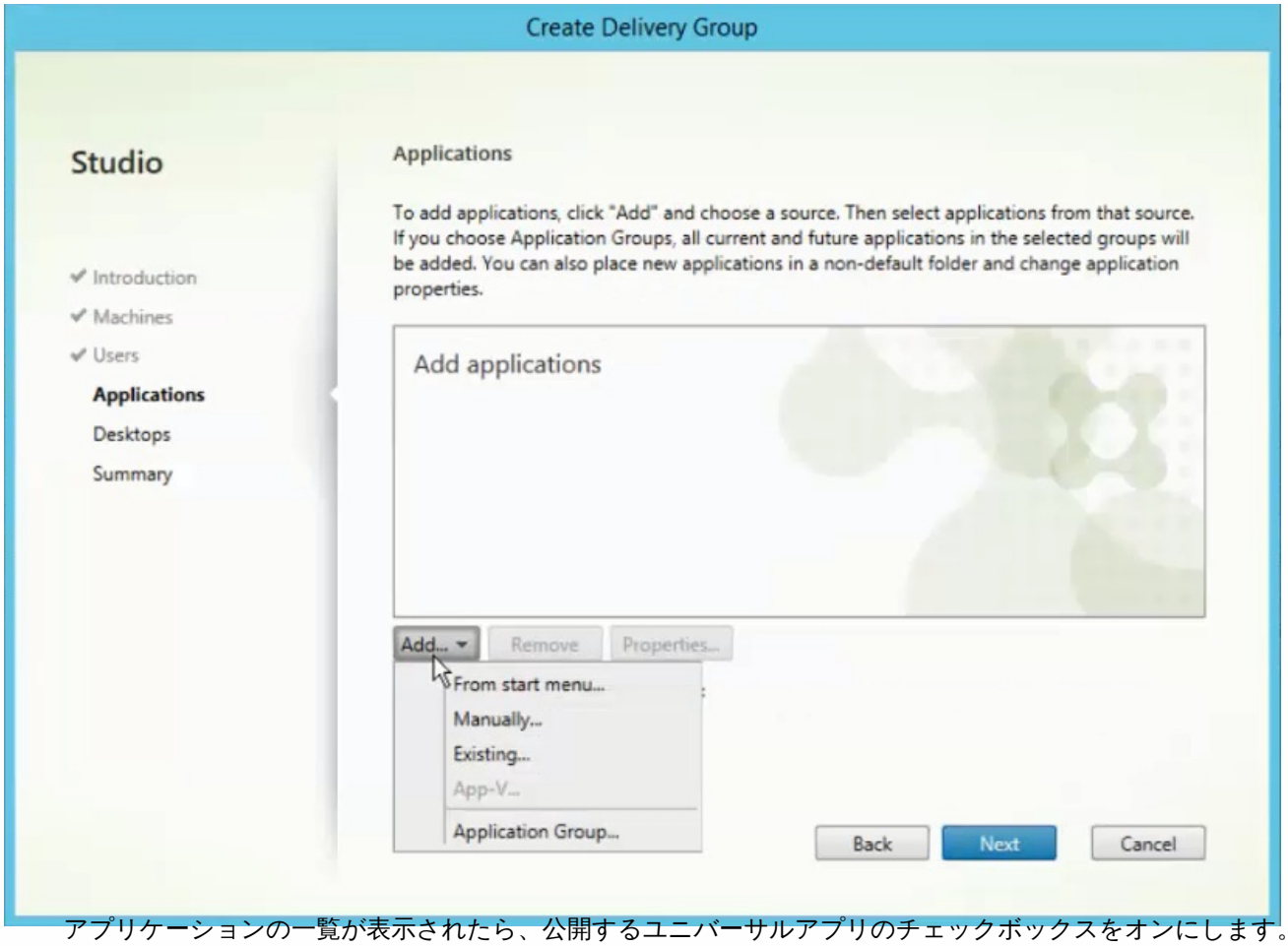
1つまたは複数のユニバーサルアプリをVDA（またはマスターイメージ）にインストールするには、以下のいずれかの方法を使用します。

- ビジネス向けWindowsストアからのオフラインインストールの完了、Deployment Image Servicing and Management（DISM）などのツールを使用した、アプリのデスクトップイメージへの展開。詳しくは、https://technet.microsoft.com/en-us/itpro/windows/manage/distribute-offline-appsを参照してください。
- アプリのサイドロード。詳しくは、https://technet.microsoft.com/en-us/itpro/windows/deploy/sideload-apps-in-windows-10を参照してください。

1つまたは複数のユニバーサルアプリををXenAppまたはXenDesktopに追加するには、以下の手順に従います。

ユニバーサルアプリがマシンにインストールされたら、ユニバーサルアプリをデリバリーグループまたはアプリケーショングループに追加します。この処理は、グループの作成時、またはその後に行うことができます。ウィザードの［アプリケーション］ページで、**［スタート］メニューから］**ソースを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



アプリケーションの一覧が表示されたら、公開するユニバーサルアプリのチェックボックスをオンにします。次に[次へ] をクリックします。

ユニバーサルアプリのアンインストール

ユニバーサルアプリをRemove-AppXPackageなどのコマンドでアンインストールする場合、アイテムは管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行する必要があります。すべてのユーザーのマシンから1つのコマンドでAppXパッケージをアンインストールすることはできません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ゾーン

Dec 12, 2017

展開がWANで接続された広範な場所に分散している場合、ネットワークの遅延と信頼性に関する問題が発生することがあります。このような問題の影響を軽減するには、次の2つの方法があります。

- それぞれに独自のSQL Serverサイトデータベースを持つ複数のサイトの展開

  このオプションは、大規模な環境で推奨されます。複数サイトは個別に管理され、各サイトに独自のSQL Serverサイトデータベースが必要です。各サイトが個別のXenApp展開です。

- 単一サイト内に複数のゾーンを構成します。

  ゾーンを構成することにより、リモートのユーザーが、WANの大規模セグメントを経由する接続を必ずしも必要とせず、リソースに接続できるようにサポートできます。ゾーンを使用することにより、単一のCitrix Studioコンソール、Citrix Director、およびサイトデータベースからの効果的なサイト管理が実現します。これにより、リモートの場所への追加サイト（個別のデータベースを含む）の展開、それに要する人員の配置、ライセンス取得、および運用のコストが削減されます。

  ゾーンは、あらゆる規模の展開で有用です。ゾーンを使用して、アプリケーションおよびデスクトップとエンドユーザーの距離を縮めることにより、パフォーマンスを改善することができます。1つのゾーンにおいて、1つまたは複数のControllerをローカルでインストールして冗長性と回復性を確保することができますが、これは必須ではありません。

  サイトで多数のControllerを構成すると、サイト自体へのControllerの新規追加など一部の操作のパフォーマンスが低下する可能性があります。こうした事態を回避するため、XenAppまたはXenDesktopサイトのゾーンの数は50以下に制限することをお勧めします。

  注：ゾーンのネットワーク待機時間が250ミリ秒（RTT）を超える場合は、ゾーンではなくサイトを複数展開することをお勧めします。

このアーティクルを通じ、「ローカル」という用語は、対象となるゾーンを指しています。たとえば、「VDAはローカルControllerに登録されます」という場合、VDAが存在するゾーンのControllerに登録されることを意味します。

このリリースでのゾーンは、XenApp Version 6.5以前と大きな違いはありませんが、同一ではありません。たとえば、このゾーン実装では、データコレクターが存在しません。サイトのすべてのControllerが、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーおよび優先ゾーンの機能が異なります。

ゾーンの種類

1つのサイトには、必ず1つのプライマリゾーンがあります。また、サイトにはオプションで1つまたは複数のサテライトゾーンを含めることもできます。サテライトゾーンは、障害回復、地理的に離れたデータセンター、支社、クラウド、またはクラウドのアベイラビリティゾーンに使用できます。

プライマリゾーン

プライマリゾーンのデフォルト名は「プライマリ」です。これには、SQL Serverサイトデータベース（および使用している場合は高可用性SQL Server）、Studio、Director、Citrix StoreFront、Citrixライセンスサーバー、およびNetScaler Gatewayが含まれます。サイトデータベースは、必ずプライマリゾーンに含まれている必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

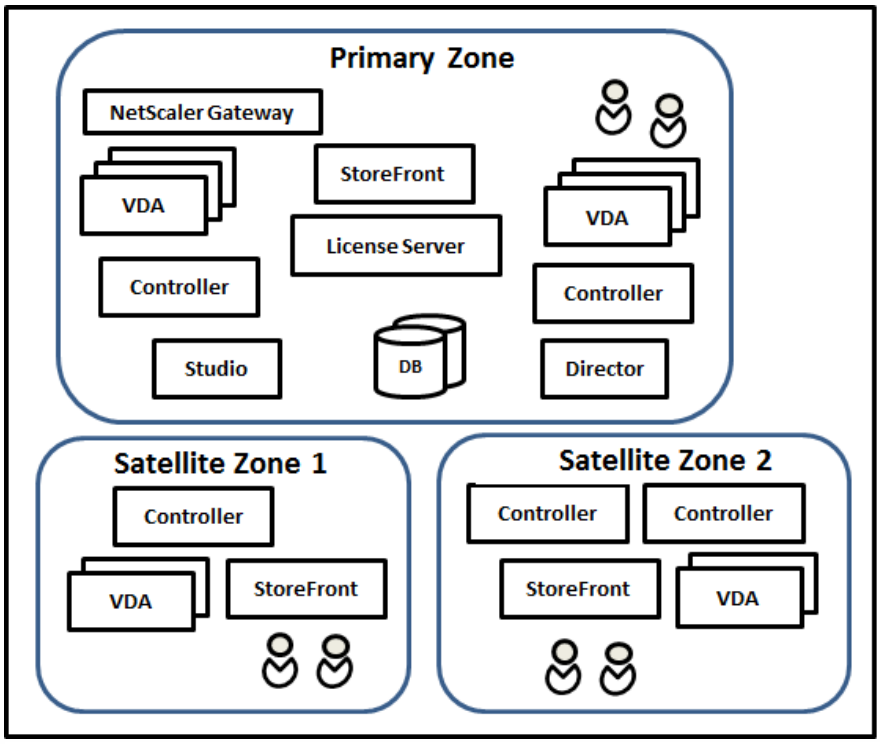
また、プライマリゾーンには、冗長性確保のために少なくとも2つのControllerが含まれている必要があります。また、データベースおよびインフラストラクチャと密結合されたアプリケーションを含む1つまたは複数のVDAが含まれる場合があります。

サテライトゾーン

サテライトゾーンには、1つまたは複数のVDAと、Controller、StoreFrontサーバー、およびNetScaler Gatewayサーバーが含まれます。通常時には、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

特に大きなサテライトゾーンには、そのゾーンのマシンのプロビジョニングまたは保存（もしくはその両方）に使用されるハイパーバイザーも含まれる場合があります。サテライトゾーンの構成時には、ハイパーバイザーまたはクラウドサービス接続をサテライトゾーンに関連付けることができます（この接続を使用するマシンカタログが同じゾーンに含まれていることを確認してください）。

ニーズと環境に応じて、1つのサイトに異なる構成のサテライトゾーンを含めることができます。次の図は、1つのプライマリゾーンと、複数のサテライトゾーンの例を示しています。



- プライマリゾーンには、2つのController、Studio、Director、StoreFront、ライセンスサーバー、サイトデータベース（および高可用性SQL Server展開）が含まれています。また、プライマリゾーンには複数のVDAおよびNetScaler Gatewayも含まれています。
- サテライトゾーン1 - VDA（Controllerあり）

  サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれています。 このサテライトゾーンのVDAは、ローカルControllerに登録されます。ローカルControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANで障害が発生した場合、接続リース機能を使用して、サテライトゾーンのControllerがそのゾーンのVDAへの接続を引き続き仲介することができます。このような展開は、オフィスを社内ネットワークに接続するWANリンクで障害が発生しても、作業者がローカルStoreFrontサイトおよびローカルControllerを使用してローカルリソースにアクセスするオ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フィスで効果的です。

- サテライトゾーン2 - VDA（冗長Controllerあり）

  サテライトゾーン2には2つのController、VDA、およびStoreFrontサーバーが含まれています。この種類のゾーンは回復性が最も高く、WANとローカルControllerの1つで同時に障害が発生しても、それに耐えることができます。

VDAの登録とControllerのフェールオーバー

プライマリゾーンとサテライトゾーンを含み、VDAのバージョンが7.7以降のサイトでは、以下のルールが適用されます。

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録されます。プライマリゾーンのVDAでは、サテライトゾーンのControllerへの登録が試行されることはありません。
- サテライトゾーンのVDAは、可能な場合はローカルControllerに登録されます（これが優先Controllerになります）。ローカルControllerを利用できない場合（ゾーンにローカルControllerがない場合、ローカルControllerで追加のVDA登録を受け入れられない場合、ローカルControllerで障害が発生している場合など）、VDAではプライマリゾーンのControllerへの登録が試行されます。この場合、サテライトゾーンのControllerが再び利用可能になっても、VDAはプライマリゾーンで登録されたままになります。サテライトゾーンのVDAでは、別のサテライトゾーンのControllerへの登録が試行されることはありません。
- ControllerのVDA検出で自動更新が有効になっており、VDAのインストール時にControllerアドレスの一覧を指定した場合、初回登録では、（Controllerが含まれるゾーンに関係なく）その一覧からランダムにControllerが選択されます。そのVDAが含まれるマシンが再起動された後、そのローカルゾーン内のControllerがVDA登録の優先Controllerになります。
- サテライトゾーンのControllerで障害が発生した場合、可能であれば別のローカルControllerへのフェールオーバーが実行されます。ローカルControllerを利用できない場合は、プライマリゾーンのControllerへのフェールオーバーが実行されます。
- Controllerをゾーン内またはゾーン外に移動し、自動更新が有効である場合、両方のゾーンのVDAに対し、ローカルのControllerとプライマリゾーンのControllerを示す更新された一覧が送信されます。これにより、登録および接続の受け入れが可能なControllerがVDAで認識されます。
- マシンカタログを別のゾーンに移動すると、そのカタログのVDAが、カタログを移動したゾーンのControllerに再登録されます（現在のゾーンに適切に接続されていないゾーンにカタログを移動する場合（遅延が大きいネットワークやまたは低帯域幅ネットワークなど）は、関連付けられているすべてのホスト接続も同じゾーンに移動してください）。
- プライマリゾーンのControllerには、すべてのゾーンの接続リース機能データが保持されます。サテライトゾーンのControllerには、そのゾーンおよびプライマリゾーンの接続リース機能データが保持されますが、ほかのサテライトゾーンのデータは保持されません。

プライマリゾーンですべてのControllerが失敗すると、以下の状態になります。

- Studioがサイトに接続できない。
- プライマリゾーンでVDAに接続できない。
- プライマリゾーンのControllerが使用できるようになるまで、サイトのパフォーマンスが低下し続ける。

Version 7.7よりも前のVDAバージョンが含まれるサイトでは、以下のルールが適用されます。

- サテライトゾーンのVDAでは、そのローカルゾーンおよびプライマリゾーンのControllerからの要求が受け入れられます（Version 7.7以降のVDAでは、ほかのセカンダリゾーンからのController要求を受け入れることができます）。
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録されます（Version 7.7以降のVDAでは、ローカルゾーンが優先されます）。

ゾーン優先度

© 1999-2017 Citrix Systems, Inc. All rights reserved.

重要： ゾーンの優先度機能を使用するには、StoreFront 3.7以上およびNetScaler Gateway 11.0-65.x以上を使用している必要があります。

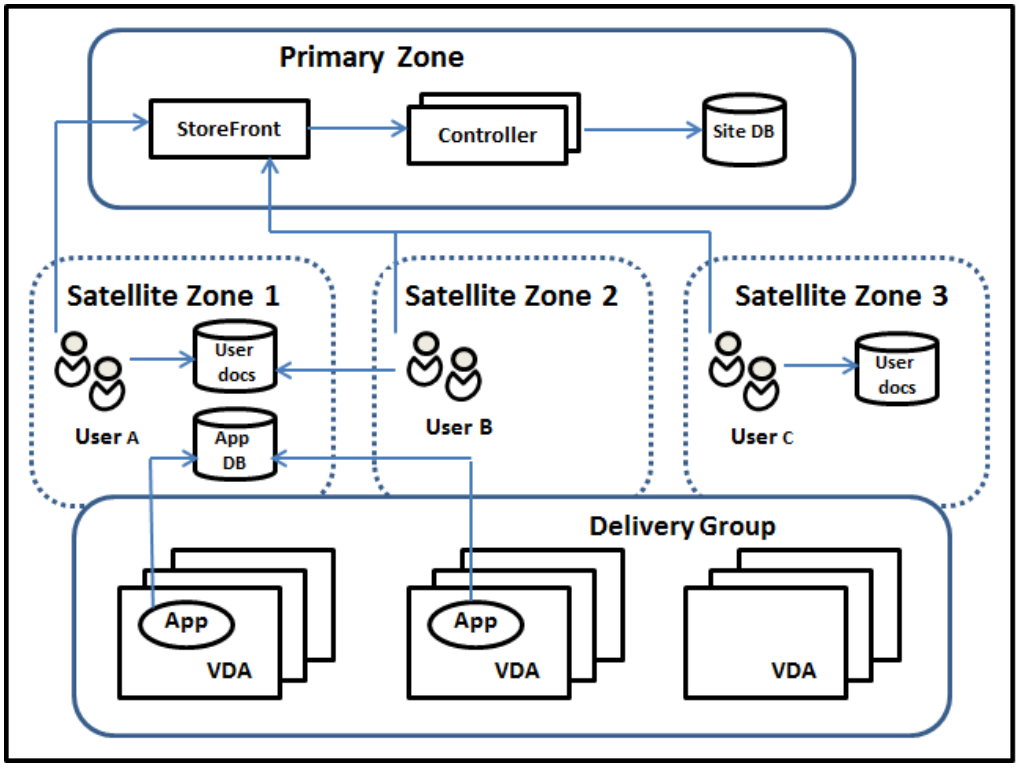
複数のゾーンがあるサイトでは、管理者は、アプリケーションやデスクトップの起動にどのVDAが使用されるかを、ゾーンの優先度機能によってより柔軟に制御できます。

ゾーンの優先度のしくみ

ゾーンの優先度には以下の3つの形式があります。以下によっては、特定のゾーンにVDAを使用するのが好ましい場合があります。

- アプリケーションのデータの保存先。これを「アプリケーションホーム」と呼びます。
- プロファイルやホームシェアなどの、ユーザーのホームデータの場所。これを「ユーザーホーム」と呼びます。
- （Citrix Receiverが実行されている）ユーザーの現在位置。これを「ユーザーの場所」と呼びます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンにまたがっていますが、同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動依頼にどのVDAを使用するかを選択できる場合があります。この例では、ユーザーがCitrix Receiveエンドポイントを実行できる場所が多数存在しています。ユーザーAはサテライトゾーン1で、Citrix Receiverでデバイスを使用しています。ユーザーBはサテライトゾーン2でデバイスを使用しています。1人のユーザーのドキュメントをさまざまな場所に格納できます。 ユーザーAとBは、サテライトゾーン1をベースに共有を使用します。ユーザーCはサテライトゾーンCからの共有を使用します。また、公開アプリケーションのいずれかによって、サテライトゾーン1にあるデータベースが使用されます。

ユーザーまたはアプリケーションにホームゾーンを構成して、ユーザーまたはアプリケーションをゾーンと関連付けることができます。すると、Delivery Controllerのブローカーがこれらの関連付けを使用して、セッションが開始されるゾーンを選択します（リソースが利用可能な場合）。 以下を行います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションに構成できるホームゾーンは1回あたり1つのみです（ユーザーについては、複数のゾーンメンバーシップがある場合は例外となることがあります。「そのほかの考慮事項」セクションを参照してください。ただし、その場合においても、ブローカーが使うホームゾーンは1つのみです）。

ユーザーおよびアプリケーションのゾーン優先度を構成できますが、ブローカーは起動する優先ゾーンを1つだけ選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム > ユーザーホーム > ユーザーの場所です（この順序は制限できます（次のセクション参照））。ユーザーがアプリケーションを起動したとき：

- アプリケーションに構成済みのゾーンの関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンとなります。
- アプリケーションには構成済みのゾーンの関連付けがなく、ユーザーには構成されたゾーンの関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンとなります。
- アプリケーションにもユーザーにも構成済みのゾーンの関連付けがない場合、優先ゾーンはユーザーがCitrix Receiverインスタンスを実行しているゾーン（ユーザーの場所）となります。このゾーンが定義されていない場合は、VDAおよびゾーンのランダム選択が使用されます。負荷分散は、優先ゾーン内のすべてのVDAに適用されます。優先ゾーンがない場合、負荷分散はデリバリーグループ内のすべてのVDAに適用されます。

ゾーン優先度の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）すると、ゾーン優先度がどのように使われるか（または使われないか）をさらに制限できます。

- **ユーザーのホームゾーンの使用必須：**デリバリーグループで、セッションがユーザーのホームゾーンで開始され、ホームゾーンでリソースが利用可能でない場合に他のゾーンにフェールオーバーしないように指定できます（ユーザーのホームゾーンがある場合）。この制限は、大きなプロファイルやデータファイルがゾーン間でコピーされないようにする必要がある場合に有用です。つまり、他のゾーンでセッションを開始するのではなく、他のゾーンではセッションが開始されないようにします。
- **アプリケーションのホームゾーンの使用必須：**同様に、アプリケーションのホームゾーンを構成すると、アプリケーションがそのゾーンでのみ起動され、アプリケーションのホームゾーンでリソースが利用可能でない場合に他のゾーンにフェールオーバーしないように指定できます。
- **アプリケーションのホームゾーンなし、および構成されたユーザーのホームゾーン無視：**アプリケーションのホームゾーンを指定しない場合、アプリケーションを起動するときに、構成済みのユーザーのゾーンが考慮されないように指定することもできます。たとえば、ユーザーの場所ゾーン優先度を使用して、ユーザーに他のホームゾーンがある場合でも、ユーザーが使用している（Citrix Receiver実行中の）マシンの近くにあるVDAで特定のアプリケーションが実行されるようにできます。

優先ゾーンによるセッション使用への影響

ユーザーがアプリケーションやデスクトップを起動すると、ブローカーは既存のセッションよりも優先ゾーンを使用しようとします。

アプリケーションまたはデスクトップを起動しているユーザーに、起動中のリソースに最適なセッション（アプリケーションのセッション共有を使用できるセッション、または起動中のリソースをすでに実行しているセッションなど）があるにもかかわらず、セッションがユーザーまたはアプリケーションの優先ゾーン以外のゾーンのVDAで実行されている場合、新しいセッションが作成されることがあります。これにより、セッションは、ユーザーのセッション要件に対して優先度の低いゾーンに再接続される前に、正しいゾーンで開始されます（そのゾーンに使用可能な容量がある場合）。

操作できなくなる孤立セッションが発生しないようにするため、優先ではないゾーンにあっても、再接続は既存の切断された

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションにのみ許可されます。

セッション開始の望ましさの順は、以下のとおりです。

1. 優先ゾーンにある既存セッションに再接続する。
2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある接続中の既存セッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

ゾーン優先度に関するそのほかの考慮事項

- ユーザーグループ（セキュリティグループなど）のホームゾーンを構成する場合、（直接または間接メンバーシップによる）そのグループのユーザーは、指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができるため、他のグループのメンバーシップで他のホームゾーンが構成されている可能性があります。そのような場合は、そのユーザーのホームゾーンの特定があいまいになる可能性があります。

  ユーザーに、グループメンバーシップで取得されなかった構成済みのホームゾーンがある場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップで取得されたゾーンの関連付けはすべて無視されます。

  ユーザーに、グループメンバーシップのみで取得された複数の異なるゾーンの関連付けがある場合、ブローカーはそれらのゾーンの中からランダムに選択します。ブローカーがゾーンを選択すると、そのゾーンはユーザーのグループメンバーシップが変更されるまで、後続のセッションの開始に使用されます。

- ユーザーの場所ゾーン優先度には、デバイスの接続を経由しているCitrix NetScaler Gatewayによるエンドポイントデバイス上のCitrix Receiverの検出が必要になります。NetScalerは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンのIDは、StoreFrontからControllerに渡される必要があります。

ゾーン優先度について詳しくは、Zone preference internalsを参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置することができます。マシンカタログでホスト接続を使用する場合は、カタログと接続の両方が同じゾーンに含まれており、遅延が少なく、高帯域幅の接続である必要があります。
- サテライトゾーンにアイテムを配置すると、これらのアイテムおよびこれらに関連する他のオブジェクトとサイトとの通信方法に影響します。
  - Controllerマシンがサテライトゾーンに配置されている場合、これらのマシンは同一のサテライトゾーンにあるハイパーバイザーおよびVDAマシンと良好に（ローカルに）接続できるものとみなされます。そのため、サテライトゾーンにあるハイパーバイザーやVDAマシンを処理する場合、プライマリゾーンのControllerではなく同じサテライトゾーンにあるControllerが使用されます。
  - ハイパーバイザー接続がサテライトゾーンに配置されている場合、このハイパーバイザー接続で管理されているすべてのハイパーバイザーも同じサテライトゾーン内に存在するものとみなされます。そのため、サテライトゾーンにあるハイパーバイザー接続を使用して通信する場合、プライマリゾーンのControllerではなく同じサテライトゾーンにあるControllerが使用されます。
  - マシンカタログがサテライトゾーンに配置されている場合、このカタログ内のすべてのマシンも同じサテライトゾーンにあるとみなされます。このため、各VDAの初回登録後にControllerリストの自動更新メカニズムが有効になると、サイトへの登録時にはプライマリゾーンのControllerではなくローカルのControllerが使用されます。
  - NetScaler Gatewayインスタンスもゾーンに関連付けることができます。この関連付けはこの記事で説明する他の要素と

© 1999-2017 Citrix Systems, Inc. All rights reserved.

同様に、XenAppまたはXenDesktopのサイト構成ではなくStoreFrontの最適なHDXルーティング構成の一環として行います。ゾーンに関連付けられたNetScaler Gatewayは、そのゾーンにあるVDAマシンへのHDX接続で優先して使用されます。

- 実稼働サイトを作成してから、最初のマシンカタログおよびデリバリーグループを作成した場合、すべてのアイテムがプライマリゾーンに含まれます。初期セットアップを完了するまで、サテライトゾーンは作成できません（空のサイトを作成した場合、プライマリゾーンには初期状態ではControllerのみが含まれています。サテライトゾーンは、マシンカタログおよびデリバリーグループの作成前または作成後に作成できます）。
- 1つまたは複数のアイテムが含まれる最初のサテライトゾーンを作成する場合、サイトのそのほかすべてのアイテムはプライマリゾーンに残ります。
- プライマリゾーンのデフォルト名は「プライマリ」です。この名前は変更できます。Studio表示ではどのゾーンがプライマリゾーンかが示されますが、プライマリゾーンには容易に特定できる名前を使用するのがベストプラクティスです。プライマリゾーンは再割り当てする（すなわち、別のゾーンをプライマリゾーンにする）ことができます。ただし、プライマリゾーンには必ずサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは、必ずプライマリゾーンに含まれている必要があります。
- ゾーンを作成した後、アイテムをゾーン間で移動できます。この柔軟性により、近くに配置することによって最適に機能する複数のアイテムを別々のゾーンに配置してしまう可能性があります。たとえば、マシンカタログを、カタログ内のマシンを作成する接続（ホスト）とは別のゾーンに移動すると、パフォーマンスが低下する場合があります。そのため、アイテムをゾーン間で移動する前に、意図しない影響が出る可能性を考慮してください。カタログとホスト接続（同じゾーンまたは適切に接続されているゾーン（遅延が少なく高帯域幅のネットワーク経由など）でカタログが使用するもの）を維持します。
- パフォーマンスを最適化するため、StudioとDirectorはプライマリゾーンのみにインストールします。サテライトゾーンに追加のStudioインスタンスが必要な場合（Controllerが含まれるサテライトゾーンが、プライマリゾーンにアクセスできなくなった場合のフェールオーバーとして使用されている場合など）、Studioをローカル公開アプリケーションとして実行します。DirectorはWebアプリケーションであるため、サテライトゾーンからもアクセスできます。
- サテライトゾーンのNetScaler Gatewayはゾーン内の接続に使用できますが、ほかのゾーンまたは外部からそのゾーンへのユーザー接続に使用するのが理想的です。
- **そのほかの注意事項：**ゾーンの優先度機能を使用するには、StoreFront 3.7以上およびNetScaler Gateway 11.0-65.x以上を使用している必要があります。
- 技術詳細およびパフォーマンスに関する考慮事項については、「ゾーンの詳細」を参照してください。

接続の質の制限

サテライトゾーンのControllerは、サイトデータベースに対してSQL操作を直接実行します。このため、サテライトゾーンと、サイトデータベースが含まれるプライマリゾーンとのリンクの質はある程度制限されます。一部の制限は、サテライトゾーンに展開されているVDAの数とこれらのVDA上のユーザーセッションの数に関係します。このため、VDAとセッションの数が少ないサテライトゾーンでは、VDAとセッションの数が多いサテライトゾーンよりもデータベースへの接続の質が低下します。

詳しくは、「遅延およびSQLブロッキングクエリの向上」を参照してください。

仲介のパフォーマンスに対する遅延時間の影響

ゾーンではリンクの遅延時間が大きくなりますが、ローカルブローカーが存在する場合、エンドユーザーのエクスペリエンスではさらに遅延が生じることになります。こうしたユーザーが行う作業のほとんどで、サテライトゾーンのControllerとサイトデータベース間での往復時間による遅れが生じます。

アプリケーションを起動する場合、セッションの仲介プロセスでセッション開始の要求を送信するのに適したVDAが見つかるまで、さらに遅れが生じます。

ゾーンの作成と管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.

すべての管理権限を実行できる管理者は、ゾーンの作成および管理に関するすべてのタスクを実行できます。ただし、ゾーンを作成、編集、または削除できるカスタムの役割を作成することもできます。アイテムをゾーン間で移動するために、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありません。ただし、移動するアイテムの編集権限は必要になります。たとえば、マシンカタログをゾーン間で移動するには、そのマシンカタログの編集権限が必要です。詳しくは、「委任管理」を参照してください。

Provisioning Servicesを使用する場合： このリリースで提供されるProvisioning Servicesコンソールではゾーンが認識されないため、Studioを使用して、サテライトゾーンに配置するマシンカタログを作成することをお勧めします。Studioウィザードを使用してカタログを作成し、適切なサテライトゾーンを指定します。その後、Provisioning Servicesコンソールを使用して、そのカタログのマシンをプロビジョニングします（Provisioning Servicesウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でサテライトゾーンに移動するにはStudioを使用する必要があります）。

ゾーンの作成

1. Studioのナビゲーションペインで **[構成] > [ゾーン]** の順に選択します。
2. ［操作］ペインの **[ゾーンの作成]** を選択します。
3. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意にする必要があります。
4. 新しいゾーンに配置するアイテムを選択します。選択できるアイテムの一覧では、フィルターまたは検索を実行できます。また、アイテムを選択せずに空のゾーンを作成することもできます。
5. **[保存]** をクリックします。

もう1つの方法として、Studioで1つまたは複数のアイテムを選択してから、［操作］ペインの**[ゾーンの作成]** を選択することもできます。

ゾーンの名前または説明の変更

1. Studioのナビゲーションペインで **[構成] > [ゾーン]** の順に選択します。
2. 中央ペインでゾーンを選択し、［操作］ペインで **[ゾーンの編集]** を選択します。
3. ゾーンの名前または説明（もしくはその両方）を変更します。プライマリゾーンの名前を変更する場合、そのゾーンをプライマリゾーンとして容易に特定できるようにしてください。
4. **[OK]** または **[適用]** をクリックします。

アイテムのゾーン間移動

1. Studioのナビゲーションペインで **[構成] > [ゾーン]** の順に選択します。
2. 中央ペインでゾーンを選択し、1つまたは複数のアイテムを選択します。
3. アイテムを移動先ゾーンにドラッグするか、または［操作］ペインで**[アイテムを移動]** を選択してから移動先ゾーンを指定します。

選択したアイテムが確認メッセージで一覧にされ、それらすべてのアイテムを移動するかどうかが確認されます。

そのほかの注意事項： マシンカタログでハイパーバイザーまたはクラウドサービスへのホスト接続が使用される場合、カタログと接続の両方が同じゾーンに含まれている必要があります。 同じゾーンに含まれていない場合、パフォーマンスが低下する可能性があります。どちらかのアイテムを移動したら、もう1つのアイテムも移動してください。

ゾーンの削除

ゾーンは、削除する前に空にする必要があります。プライマリゾーンは削除できません。

1. Studioのナビゲーションペインで **[構成] > [ゾーン]** の順に選択します。
2. 中央ペインでゾーンを選択します。
3. ［操作］ペインの **[ゾーンの削除]** を選択します。ゾーンが空ではない（アイテムが含まれている）場合、それらのアイテ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ムの移動先ゾーンを選択するよう指示するメッセージが表示されます。
4. 削除を確認します。

ユーザーのホームゾーンの追加

ユーザーにホームゾーンを構成することは、*ゾーンへのユーザーの追加*とも言います。

1. Studioのナビゲーションペインで **[構成]** > **[ゾーン]** の順に選択し、中央ペインでゾーンを選択します。
2. ［操作］ペインの **[ゾーンへのユーザーの追加]** を選択します。
3. **[ゾーンへのユーザーの追加]** ダイアログボックスで、**[追加]** をクリックしてからゾーンに追加するユーザーおよびユーザーグループを選択します。すでにホームゾーンがあるユーザーを指定すると、2つの選択肢を提供するメッセージが表示されます。 **[はい]** は、指定したユーザーのうち、ホームゾーンのないユーザーのみが追加されます。**[いいえ]** は、ユーザー選択ダイアログに戻ります。
4. **[OK]** をクリックします。

構成済みのホームゾーンがあるユーザーについては、ユーザーのホームゾーンからのセッション開始のみ要求できます。

1. デリバリーグループの作成または編集
2. **[ユーザー]** ページで、**[セッションはユーザーのホームゾーンで開始（構成済みの場合）]** チェックボックスを選択します。

   そのデリバリーグループ内のユーザーによって開始されたすべてのセッションは、そのユーザーのホームゾーンから開始される必要があります。 そのデリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は有効になりません。

ユーザーのホームゾーンの削除

この手順は、ゾーンからのユーザーの削除とも言います。

1. Studioのナビゲーションペインで **[構成]** > **[ゾーン]** の順に選択し、中央ペインでゾーンを選択します。
2. ［操作］ペインで **[ユーザーをゾーンから削除]** を選択します。
3. **[ゾーンへのユーザーの追加]** ダイアログボックスで、**[削除]** をクリックしてからゾーンから削除するユーザーおよびクループを選択します。このアクションにより、ユーザーがゾーンからのみ削除されます。これらのユーザーは、属してい
   デリバリーグループおよびアプリケーショングループには残ったままとなります。
4. 確認のメッセージが表示されたら、削除を確定します。

アプリケーションのホームゾーンの管理

アプリケーションにホームゾーンを構成することは、ゾーンへのアプリケーションの追加とも言います。デフォルトで、マルチゾーン環境では、アプリケーションにはホームゾーンがありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、またはその後に、Studioでアプリケーションを選択して、そのプロパティを編集することによって構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、またはアプリケーションを既存のグループに追加するときに、ウィザードの **[アプリケーション]** ページで **[プロパティ]** を選択します。
- アプリケーションを追加したあとにアプリケーションのプロパティを変更するには、Studioのナビゲーションペインで**[アプリケーション]** を選択します。アプリケーションを選択し、［操作］ペインで **[アプリケーションプロパティの編集]** を選択します。

アプリケーションのプロパティまたは設定の **[ゾーン]** ページで以下の処理を行います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- アプリケーションにホームゾーンを追加する場合は、
  - **[選択したゾーンを決定に使用]** ラジオボタンを選択し、ドロップダウンからゾーンを選択します。
  - アプリケーションを選択したゾーンからのみ起動する（他のゾーンからは起動しないようにする）には、ゾーン選択の下にあるチェックボックスを選択します。
- アプリケーションにホームゾーンを設定しない場合は、
  - **[ホームゾーンを構成しない]** ラジオボタンを選択します。
  - このアプリケーションを起動するときに、ブローカーによって構成済みのユーザーのゾーンが考慮されないようにするには、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションのホームゾーンまたはユーザーのホームゾーンがこのアプリケーションを起動する場所の決定に使用されることはありません。

ゾーンの指定が含まれるそのほかの操作

サテライトゾーンを少なくとも1つ既に作成している場合、ホストの接続時またはマシンカタログの作成時（サイト作成時を除く）に、アイテムの割り当て先ゾーンを指定できます。

ほとんどの場合、プライマリゾーンがデフォルトで指定されます。Machine Creation Servicesを使用してマシンカタログを作成する場合、ホスト接続に対して構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合は、プライマリゾーンとして処理され、ゾーン選択ボックスは表示されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

接続とリソース

Dec 05, 2017

ここでは次のことについて説明します。

- はじめに
- 接続の種類に関する情報の参照先
- ホスト ストレージ
- 接続とリソースの作成
- 接続の設定の編集
- 接続のメンテナンスモードのオン/オフの切り替え
- 接続の削除
- 接続の名前変更またはテスト
- 接続上のマシンの詳細の表示
- 接続上のマシンの管理
- ストレージの編集
- リソースの削除、名前変更、またはテスト
- XenServer接続でのIntelliCacheの使用
- 接続タイマー

はじめに

管理者は、サイトを作成するときに、オプションでホストリソースへの最初の接続を作成できます。後でその接続を変更したり、別の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーまたはクラウドサービスからの接続の種類の選択が含まれます。選択したストレージとネットワークが、その接続のリソースになります。

読み取り専用管理者は接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、すべての管理権限を実行できる管理者である必要があります。詳しくは、「委任管理」を参照してください。

接続の種類に関する情報の参照先

管理者は、サポートされている仮想化プラットフォームを使用してXenAppやXenDesktopの環境をホストおよび管理できます。サポートされる種類については、「システム要件」を参照してください。 サポートされたクラウド展開ソリューションを使用して、製品コンポーネントをホストしたり仮想マシンをプロビジョニングしたりすることができます。これらのソリューションでは、コンピューティングリソースをプールしてパブリック、プライベート、およびハイブリッドのIaaS（Infrastructure as a Service）クラウドを構築できます。

詳しくは、以下の情報ソースを参照してください。

Microsoft Hyper-V

- 「Microsoft System Center Virtual Machine Manager仮想化環境」
- Microsoft社のドキュメント

Microsoft Azure

- 「Microsoft Azure仮想化環境」
- Microsoft社のドキュメント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Azure Resource Manager

- 「Microsoft Azure Resource Manager仮想化環境」
- Microsoft社のドキュメント

Amazon Web Services（AWS）

- 「Citrix XenDesktop on AWS」
- AWSのドキュメント
- Studioでの接続の作成時には、APIキーおよび秘密キーの値を入力する必要があります。AWSでこれらの値を含んでいるキーファイルをエクスポートしてから、値をインポートすることができます。また、リージョン、アベイラビリティゾーン、仮想プライベートクラウド名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も必要になります。
- AWSコンソールから取得するルートAWSアカウント用の資格情報ファイルでは、標準的なAWSユーザーのものとは異なる形式が使用されています。このため、このファイルをStudioで使用してAPIキーと秘密キーの情報を入力することはできません。AWS IAM形式の資格情報ファイルを使用してください。

CloudPlatform

- CloudPlatformのドキュメント
- Studioでの接続の作成時には、APIキーおよび秘密キーの値を入力する必要があります。CloudPlatformでこれらの値を含んでいるキーファイルをエクスポートしてから、値をStudioにインポートすることができます。

Citrix XenServer

- Citrix XenServerのドキュメント
- 接続の作成時には、VMパワー管理者以上の権限を持つアカウントの資格情報を指定する必要があります。
- XenServerとの通信をHTTPSで保護することをお勧めします。HTTPSを使用するには、XenServerにインストールされたデフォルトのSSL証明書を置き換える必要があります。詳しくは、CTX128656を参照してください。
- 高可用性機能で使用されるハイパーバイザーを選択することもできます（XenServerの高可用性が有効な場合）。プールマスターに障害が生じてもXenServerとの通信が中断されないように、（［Edit High Availability］から）プール内のすべてのサーバーを選択することをお勧めします。
- XenServerでvGPUがサポートされる場合は、GPUの種類およびグループ、またはGPUパススルーを選択することができます。選択した項目で専用のGPUリソースが使用可能かどうか画面に表示されます。

Nutanix Acropolis

- 「Nutanix仮想化環境」
- Nutanixのドキュメント

VMware

- 「VMware仮想化環境」
- VMware製品ドキュメント：

ホスト ストレージ

マシンのプロビジョニング時、データは種類別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- MCSでプロビジョニングされたマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータを含む一時データ。このデータは、マシンの再起動のたびに破棄されます。
- Personal vDiskに保存された個人データ。

データの種類ごとに個別のストレージを用意することにより、各ストレージデバイスの負荷が軽減されてIOPSパフォーマンスが向上し、ホストで使用可能なリソースを最大限に活用できます。さらに、他のデータに比べて永続性と復元性がより重要なデータなど、データの種類に応じて適切なストレージを使用できるようになります。

ストレージは共有（中央に配置し、すべてのホストから分離して、すべてのホストで使用）することも、ハイパーバイザーのローカルに配置することもできます。中央共有ストレージの例には、1つまたは複数のWindows Server 2012クラスターストレージボリューム（接続されたストレージありまたはなし）、ストレージベンダーからのアプライアンスなどがあります。中央ストレージには、ハイパーバイザーのストレージ制御パスやパートナープラグインからの直接アクセスなど、独自の最適化が備わっていることもあります。

一時データをローカルに保存することにより、共有ストレージへのアクセスでネットワークを経由する必要がなくなります。さらに、共有ストレージデバイスの負荷（IOPS）も軽減されます。共有ストレージは費用が高いため、ローカルにデータを保存することによってコストを抑えられます。こうした利点は、ハイパーバイザーサーバー上で十分なストレージを使用できることよりも重要になるでしょう。

接続の作成時、ストレージをハイパーバイザー間で共有するか、またはストレージをハイパーバイザーのローカルに配置する2つのストレージ管理方法からいずれかを選択してください。

注： 一時のデータ記憶として1つ以上のXenServerホスト上のローカルストレージを使用する場合、プール内の各ストレージの場所が一意の名を持っていることを確認してください。（XenCenterで名前を変更するには、ストレージを右クリックして名前のプロパティを編集します）。

ハイパーバイザー間で共有されるストレージ

ハイパーバイザー間でストレージを共有する方法では、長期間保持する必要のあるデータが保存され、バックアップおよび管理を一元的に行うことができます。このストレージでは、OSディスクおよびPersonal vDiskが保持されます。

この方法を選択する場合、永続性を必要としない一時マシンデータや、共有ストレージ内のデータほど復元性を必要としない一時マシンデータに（同じハイパーバイザープール内のサーバー上の）ローカルストレージを使用するかどうかを選択できます。これは*一時データキャ*と呼ばれます。ローカルディスクを使用することにより、メインOSストレージへのトラフィックが軽減されます。このディスクは、マシンの再起動のたびにクリアされます。ディスクは、ライトスルーメモリーキャッシュを介してアクセスされます。一時データにローカルストレージを使用すると、プロビジョニングされたVDAは特定のハイパーバイザーホストに関連付けられることに注意してください。このホストで障害が生じると、VMを起動することができなくなります。

例外： クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージでの一時データキャッシュディスクの作成を許可しません。

接続を作成するときに一時データをローカルに保存するオプションを有効にすると、この接続を使用するマシンカタログを作成する際に、各VMのキャッシュディスクサイズおよびメモリサイズにデフォルト以外の値を有効にして構成することができます。ただし、デフォルト値は接続の種類に適切な値に設定されており、ほとんどの場合はデフォルト値で十分です。詳しくは、「マシンカタログの作成」を参照してください。

また、ハイパーバイザーはディスクイメージのローカルな読み込みキャッシュによる最適化テクノロジを提供します（例：XenServerのIntelliCache）。これも、中央ストレージへのネットワークトラフィックを軽減します。

ハイパーバイザーのローカルに配置するストレージ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ストレージをハイパーバイザーのローカルに配置する方法では、データはハイパーバイザー上にローカルで保存されます。この方法を使用する場合、最初のマシン作成時およびその後のイメージ更新時に、マスターイメージおよびほかのOSデータはサイトで使用されるすべてのハイパーバイザーに転送されます。これにより、管理ネットワークでかなりのトラフィックが生じます。イメージ転送も時間がかかる処理であり、各ホストでイメージを利用できるようになるタイミングも異なります。

この方法を選択した場合、バックアップおよび障害回復システムに復元性とサポートを提供するためにPersonal vDiskの共有ストレージを使用するかどうかを選択することができます。

接続とリソースの作成

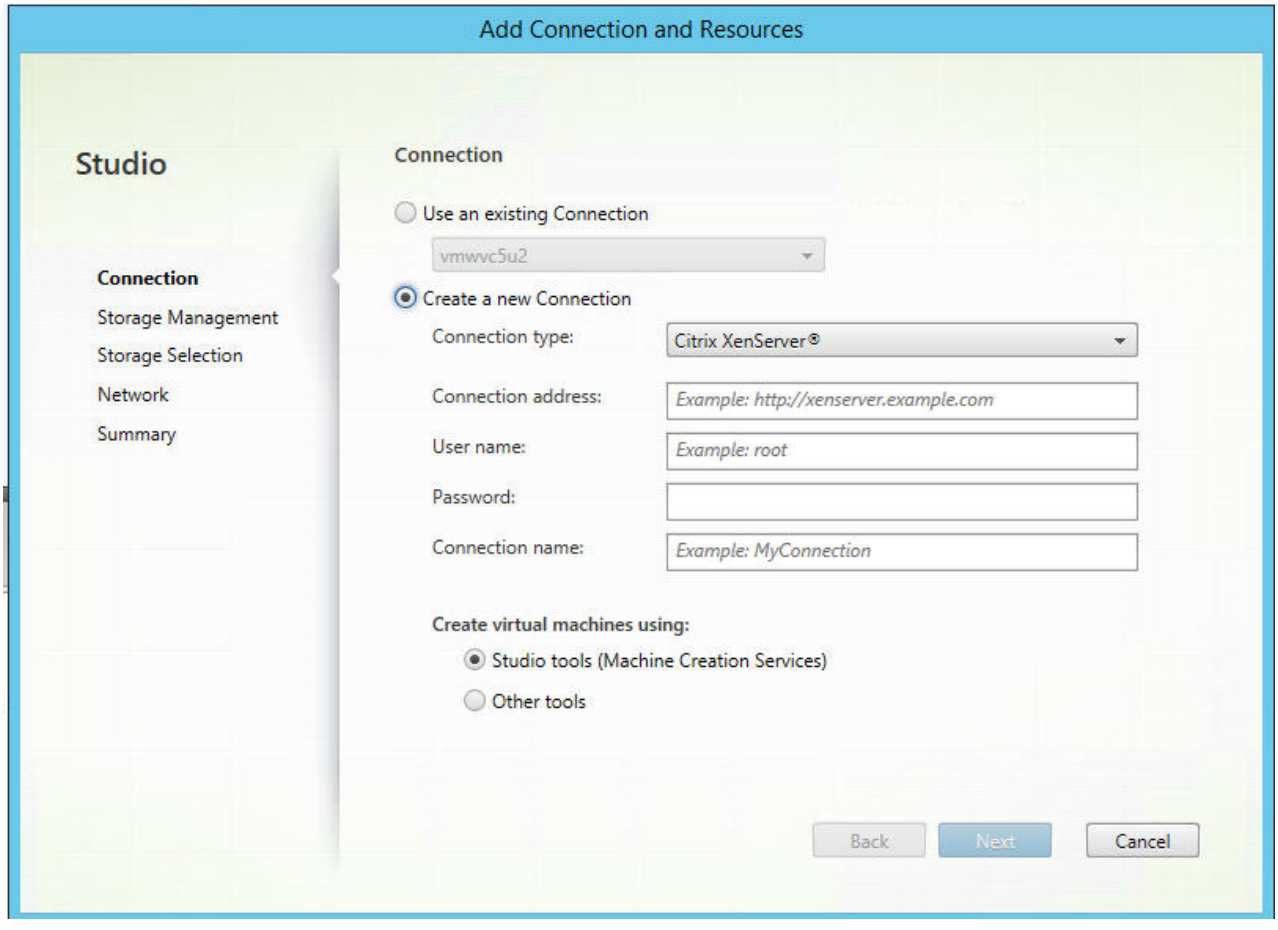
管理者は、サイトを作成するときに、オプションで最初の接続を作成できます。サイト作成ウィザードには、［接続］、［ストレージの管理］、［ストレージの選択］、［ネットワーク］といった接続関連のページがあります。

サイトの作成後に接続を作成する場合は、次の手順1から開始してください。

重要： 接続を作成する前に、ホストリソース（ストレージとネットワーク）が使用可能になっている必要があります。

- Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
- ［操作］ペインの **[接続およびリソースの追加]** を選択します。
- ウィザードの指示に従って、以下のページの操作を行います（具体的なページ内容は、選択した接続の種類に応じて異なります）。各ページの操作を終えたら、 **[概要]** ページに到達するまで **[次へ]** をクリックします。

コネクション



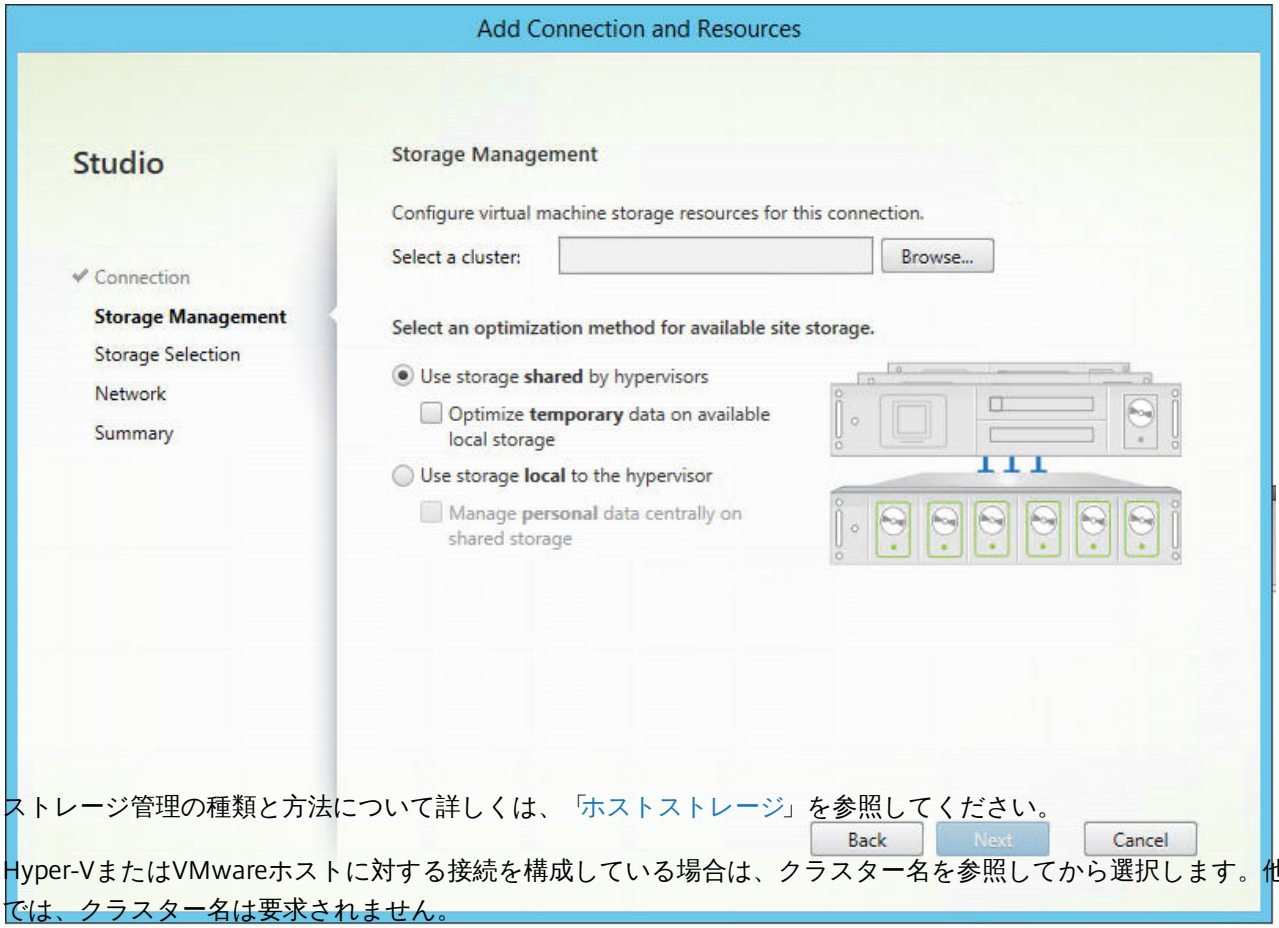
© 1999-2017 Citrix Systems, Inc. All rights reserved.

[接続] ページで、以下の操作を行います。

- 新しい接続を作成するには、**[新しい接続を作成する]** をクリックします。既存の接続と同じホスト構成に基づいて接続を作成する場合は、**[既存の接続を使用する]** を選択してから該当の接続を選択します。
- **[接続の種類]** フィールドで、使用しているハイパーバイザーまたはクラウドサービスを選択します。
- 接続のアドレスおよび資格情報は、選択した接続の種類に応じて異なります。要求された情報を入力します。
- 接続名を入力します。この接続名はStudioで表示されます。
- 仮想マシンの作成に使用するツールを、Studioツール（Machine Creation ServicesやProvisioning Servicesなど）またはその他のツールから選択します。

ストレージ管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

Hyper-VまたはVMwareホストに対する接続を構成している場合は、クラスター名を参照してから選択します。他の接続の種類では、クラスター名は要求されません。

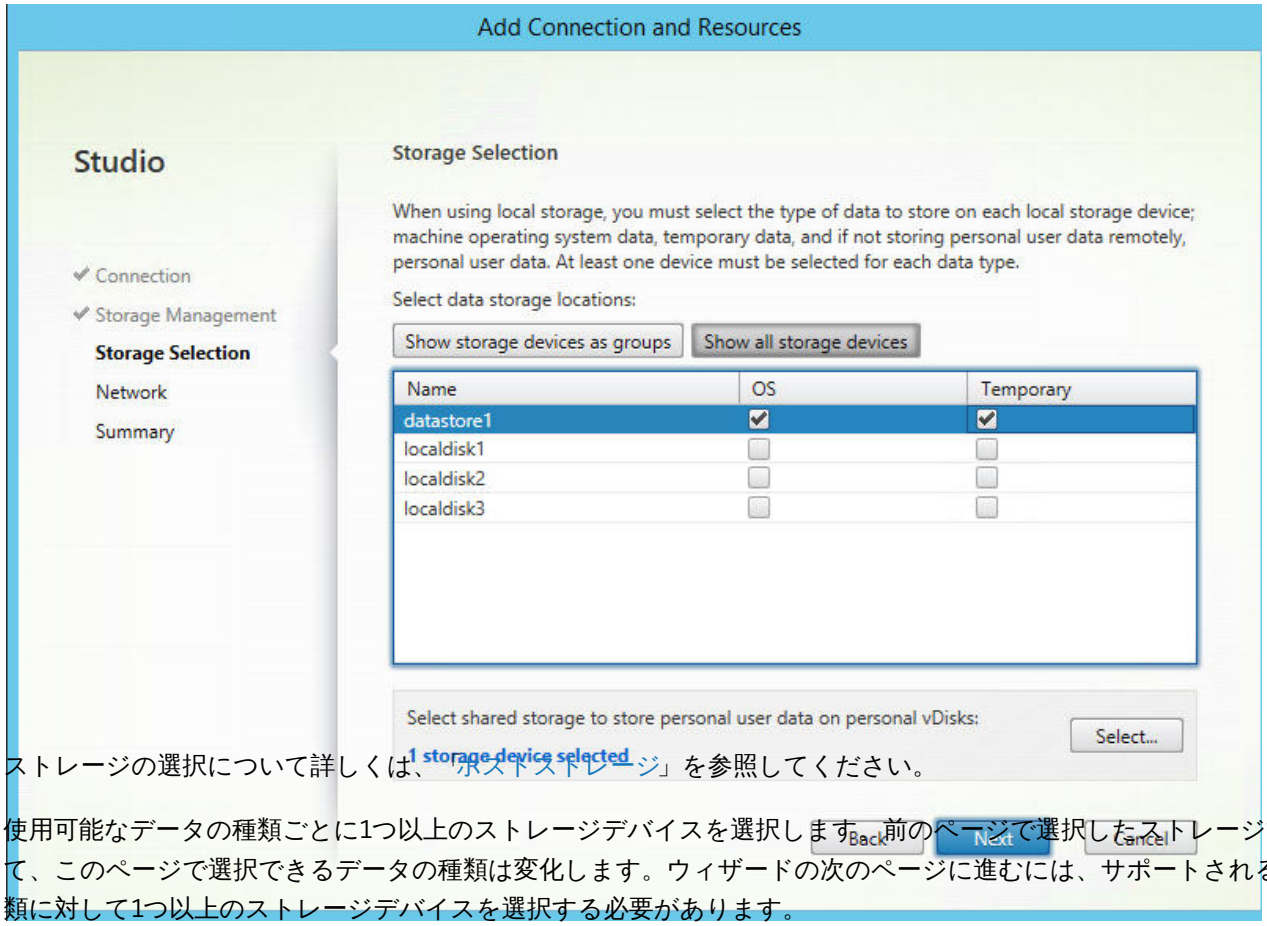
ストレージ管理方法（ハイパーバイザー間で共有されるストレージまたはハイパーバイザーのローカルに配置するストレージ）を選択します。

- ハイパーバイザー間で共有されるストレージを選択する場合、一時データを使用可能なローカルストレージで保持するかどうかを指定します（この接続を使用するマシンカタログで、デフォルトではない一時ストレージのサイズを指定できます）。**例外：** クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージでの一時データキャッシュディスクの作成を許可しないため、Studioでこのストレージ管理を設定するとエラーが発生します。
- ハイパーバイザーのローカルに配置するストレージを選択する場合は、個人データ（Personal vDisk）を共有ストレージで管理するかどうかを指定します。

XenServerハイパーバイザー上で共有ストレージを使用する場合は、IntelliCacheを使用して共有ストレージデバイスにかかる負荷を減らすかどうかを指定します。「XenServer接続でのIntelliCacheの使用」を参照してください。

ストレージの選択

© 1999-2017 Citrix Systems, Inc. All rights reserved.



ストレージの選択について詳しくは、「ホストストレージ」を参照してください。

使用可能なデータの種類ごとに1つ以上のストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータの種類は変化します。ウィザードの次のページに進むには、サポートされる各データの種類に対して1つ以上のストレージデバイスを選択する必要があります。

前のページで以下のいずれかを選択した場合、**[ストレージの選択]** ページ下部には追加の設定オプションが含まれます。

- ハイパーバイザー間で共有されるストレージを選択し、**[利用可能なローカルストレージ上で一時データを最適化します]** チェックボックスをオンにしている場合、（同じハイパーバイザープールで）一時データに使用するローカルストレージデバイスを選択できます。
- ハイパーバイザーのローカルに配置するストレージを選択し、**[共有ストレージ上でパーソナルデータを一元的に管理します]** チェックボックスをオンにしている場合、個人（PvD）データに使用する共有デバイスを選択できます。

現在選択中のストレージデバイスの数が表示されます（上図では「1個のストレージデバイスが選択されました」）。このエントリの上にマウスを合わせると、選択したデバイスの名前が表示されます（構成されたデバイスがある場合のみ）。

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

ネットワーク

リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別できるように、Studioに表示されます。

仮想マシンで使用するネットワークを1つまたは複数選択します。

結果

選択内容を確認します。変更を行う場合は、［戻る］を使って前のウィザードページに戻ります。確認が完了したら、**[完了]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

そのほかの注意事項：一時データをローカルに保存することを選択した場合、この接続を使用するマシンを含むマシンカタログを作成するときに、一時データストレージにデフォルトでない値を設定できます。「マシンカタログの作成」を参照してください。

接続の設定の編集

接続の名前の変更または新しい接続の作成のために、この手順を使用しないでください。これらの操作とは異なります。アドレスの変更は、現在のホストマシンに新しいアドレスがある場合にのみ行ってください。異なるマシンへのアドレスを入力すると、接続のマシンカタログが破損します。

接続のGPU設定を変更することはできません。これは、そのリソースにアクセスするマシンカタログで、GPU固有のマスターイメージを使用する必要があるためです。新しい接続を作成します。

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択し、［操作］ペインの **[接続の編集]** を選択します。
3. 接続の編集時に可能な設定については、以下の手順に従います。
4. 完了したら、**[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

[接続のプロパティ] ページ

- 接続アドレスおよび資格情報を変更するには、**[設定の編集]** をクリックし、新しい情報を入力します。
- XenServer接続に対して高可用性サーバーを指定する場合は、**[HAサーバーの編集]** を選択します。プールマスターに障害が生じてもXenServerとの通信が中断されないように、プール内のすべてのサーバーを選択することをお勧めします。

[詳細設定] ページ：

接続の種類が、リモートPCアクセスで使用されるMicrosoft System Center Configuration Manager（ConfMgr）のWake On LAN接続の場合は、ConfMgrのウェイクアッププロキシ、マジックパケット、およびパケットの転送情報を入力します。

制限しきい値設定を使用して、接続に対して許可される電源操作の最大数を指定することができます。電源管理設定で同時に起動するマシンの数が多すぎたり少なすぎたりする場合に、この設定を行います。 接続の種類のそれぞれに、多くのケースで適切な、通常は変更しない固有のデフォルト値があります。

[同時操作（すべての種類）] と **[Personal vDiskストレージインベントリの同時更新]** 設定について、この接続で同時に実行できる操作の最大数を絶対値、およびこの接続を使用するすべてのマシンの数に対する最大パーセンテージで指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際にはより高い制限（より低い値）の設定が適用されます。

たとえば、**[同時操作（すべての種類）]** の絶対値が10、パーセンテージ値が10、この接続の総仮想マシン数が34の場合、同時に実行される操作の上限値は3（34個のマシンのうちの10%）になります。

[1分あたりの最大新規操作] は、絶対値です。パーセンテージ値はありません。

注： **[接続オプション]** ボックスへの情報の入力は、Citrixサポート担当者からの指示があった場合のみ行ってください。

接続のメンテナンスモードのオン/オフの切り替え

接続のメンテナンスモードをオンにすると、その接続（ホスト）上に格納されているマシンに新規の電源操作が適用されるのを防ぐことができます。ユーザーは、メンテナンスモードになっているマシンには接続できません。ユーザーが既に接続して

© 1999-2017 Citrix Systems, Inc. All rights reserved.

いる場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります。

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択します。メンテナンスモードをオンにするには、［操作］ペインの**[メンテナンスモードをオンにする]** を選択します。メンテナンスモードをオフにするには、 **[メンテナンスモードをオフにする]** を選択します。

個々のマシンのメンテナンスモードをオンまたはオフにすることもできます。マシンカタログ内またはデリバリーグループ内のマシンに対し、メンテナンスモードをオンまたはオフにすることもできます。

接続の削除

注意： 接続の削除は、多くのマシンおよびそのデータの損失が発生する可能性のある操作です。削除されるマシン上に重要なユーザーデータがないかどうかを確認し、重要なデータがある場合はバックアップを作成しておいてください。

接続を削除する前に、以下の点について確認してください。

- 接続上に格納されているマシンからすべてのユーザーがログオフしていること。
- 実行したまま切断されたユーザーセッションがないこと。
- プールおよび専用のマシンの場合は、メンテナンスモードになっていること。
- 接続で使用されている、マシンカタログ内のすべてのマシンの電源がオフになっていること。

マシンカタログで指定されている接続を削除すると、そのカタログを使用できなくなります。削除する接続がマシンカタログにより参照されている場合は、同時にそのカタログを削除することもできます。ただし、そのマシンカタログがほかの接続で使用されていないことを確認してから削除してください。

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択し、［操作］ペインの **[接続の削除]** を選択します。
3. この接続上にマシンが格納されている場合、マシンを削除するかどうかを確認するメッセージが表示されます。削除する場合は、それらのマシンのActive Directoryコンピューターアカウントに対する操作を指定します。

接続の名前変更またはテスト

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択し、［操作］ペインの **[接続名の変更]** または **[テスト接続]** を選択します。

接続上のマシンの詳細の表示

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択し、［操作］ペインの **[マシンの表示]** を選択します。

上ペインにその接続でアクセスするマシンの一覧が表示されます。マシンを選択すると、その詳細が下ペインに表示されます。実行中のセッションがある場合は、そのセッションの詳細も表示されます。

検索機能を使うと、マシンをすばやく見つけることができます。ウィンドウ上部の一覧から保存済みの検索を選択するか、または新しい検索を作成します。マシン名の一部または全体を入力して検索したり、詳細な検索式を作成したりできます。検索式を作成するには、**展開**ボタンをクリックして、ドロップダウンの一覧からプロパティや演算子を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

接続上のマシンの管理

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. 接続を選択し、［操作］ペインの **[マシンの表示]** を選択します。
3. ［操作］ペインで、以下の管理タスクを選択します。マシンの状態や接続ホストの種類によっては、一部の操作を選択できない場合があります。

- **起動：** 電源がオフまたは一時停止状態のマシンを起動します。
- **一時停止：** マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
- **シャットダウン：** オペレーティングシステムにシャットダウンを要求します。
- **強制シャットダウン：** マシンの電源を強制的に切って、マシン一覧を更新します。
- **再起動：** オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、デスクトップの状態は変更されません。
- **メンテナンスモードを有効化：** マシンへの接続を一時的に停止します。この状態のマシンにユーザーが接続することはできません。ユーザーが既に接続している場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります。（前述のとおり、接続上のすべてのマシンのメンテナンスモードをオンまたはオフにすることもできます。）
- **デリバリー グループから削除：** デリバリーグループからマシンを削除しても、そのデリバリーグループで使用するマシンカタログからは削除されません。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。
- **削除：** マシンを削除すると、ユーザーはそのマシンにアクセスできなくなります。また、そのマシンはマシンカタログから削除されます。マシンを削除する前に、必要なユーザーデータをすべてバックアップしておいてください。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。

マシンのシャットダウンを伴う操作でマシンが10分以内にシャットダウンしない場合、電源が切れ、強制的にシャットダウンされます。シャットダウン中にWindowsが更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

ストレージの編集

接続を使用する仮想マシンのオペレーティングシステムデータ、一時データ、および個人（PvD）データの保存に使用されているサーバーの状態を表示できます。データの種類それぞれの保存に使用するサーバーを指定することもできます。

1. Studioのナビゲーションペインで［構成］>［ホスト］の順に選択します。
2. 接続を選択し、［操作］ペインの［ストレージの編集］を選択します。
3. 左ペインでデータの種類（オペレーティングシステムデータ、Personal vDiskデータ、一時データ）を選択します。
4. 選択したデータの種類に対し、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
5. ［OK］をクリックします。

一覧の各ストレージデバイスには、デバイス名とストレージの状態が表示されます。有効なストレージの状態の値は次のとおりです。

- **使用中**： ストレージは新しいマシンの作成に使用されています。
- **一時停止**： ストレージは既存のマシンにのみ使用されています。このストレージに新しいマシンは追加されません。
- **使用中でない**： ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、ステータスが**一時停止**に変更されます。既存のマシンは引き続き

© 1999-2017 Citrix Systems, Inc. All rights reserved.

そのストレージデバイスを使用し、そのデバイスにデータを書き込むことができます。そのため、新しいマシンの作成に使用されなくなっても、ストレージの空き領域が足りなくなる場合があります。

リソースの削除、名前変更、またはテスト

1. Studioのナビゲーションペインで **[構成] > [ホスト]** の順に選択します。
2. リソースを選択し、［操作］ペインで目的のエントリを選択します。**[リソースの削除]**、**[リソース名の変更]**、または **[リソースのテスト]**。

XenServer接続でのIntelliCacheの使用

IntelliCacheを使用すると、共有ストレージとローカルストレージを組み合わせて使用できるようになり、VDI展開のコスト効率が向上します。これによってパフォーマンスが向上し、ネットワークトラフィックが減少します。この機能では、共有ストレージ上のマスターイメージがローカルストレージにキャッシュされ、共有ストレージでのデータ読み取りが減少します。共有デスクトップの場合、差分ディスクへの書き込みはホスト上のローカルストレージに書き込まれ、共有ストレージには書き込まれません。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- パフォーマンスを向上させるため、高パフォーマンスのローカルストレージデバイスを使用することをお勧めします。

IntelliCacheを使用するには、XenServerとStudioの両方でこの機能を有効にする必要があります。

- XenServerのインストール時に **[Enable thin provisioning (Optimized storage for XenDesktop)]** を選択します。IntelliCacheが有効なサーバーと無効なサーバーを同一プールで混在させることはサポートされません。詳しくは、XenServerのドキュメントを参照してください。
- XenAppおよびXenDesktopでは、IntelliCacheはデフォルトで無効になっています。この機能はXenServer接続の作成時にのみ有効にでき、これを後で無効にすることはできません。StudioでXenServer接続を追加するときに、以下の手順に従います。
  - ストレージの種類として、**[共有]** を選択します。
  - **[IntelliCacheを使用して共有ストレージデバイス上の負荷を軽減させる]** チェックボックスをオンにします。

接続タイマー

ポリシー設定を使用すると、以下の3つの接続タイマーを構成できます。

- **最長接続タイマー：** ユーザーデバイスと仮想デスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの **[セッション接続タイマー]** 設定および **[セッション接続タイマー間隔]** 設定を使用します。
- **接続アイドルタイマー：** ユーザーからの入力がないユーザーデバイスと仮想デスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの **[セッションアイドルタイマー]** 設定および **[セッションアイドルタイマーの間隔]** 設定を使用します。
- **切断タイマー：** このタイマーでは、切断状態でロックされた仮想デスクトップを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの **[切断セッションタイマー]** 設定および **[切断セッションタイマーの間隔]** 設定を使用します。

これらの設定項目を変更する場合は、環境全体で設定が一貫していることを確認してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

詳しくは、ポリシー設定のドキュメントを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ローカルホストキャッシュ

Mar 12, 2018

XenAppおよびXenDesktopサイトデータベースを常に使用可能状態にするために、Microsoft社の高可用性ベストプラクティスに従って耐障害性の高いSQL Server展開から開始することをお勧めします（「システム要件」の「データベース」にXenAppおよびXenDesktopでサポートされているSQL Serverの高可用性機能が一覧にされています）。 ただし、ネットワークの問題および中断によってユーザーがアプリケーションやデスクトップに接続できなくなる場合があります。

ローカルホストキャッシュ（LHC）機能を使用すると、停止状態が発生しても、XenAppまたはXenDesktopサイトの接続仲介操作を続行できます。Delivery Controllerとサイト構成データベースとの間の接続が失敗すると、停止状態が発生します。ローカルホストキャッシュは、サイトデータベースに90秒間アクセスできない場合に使用されます。

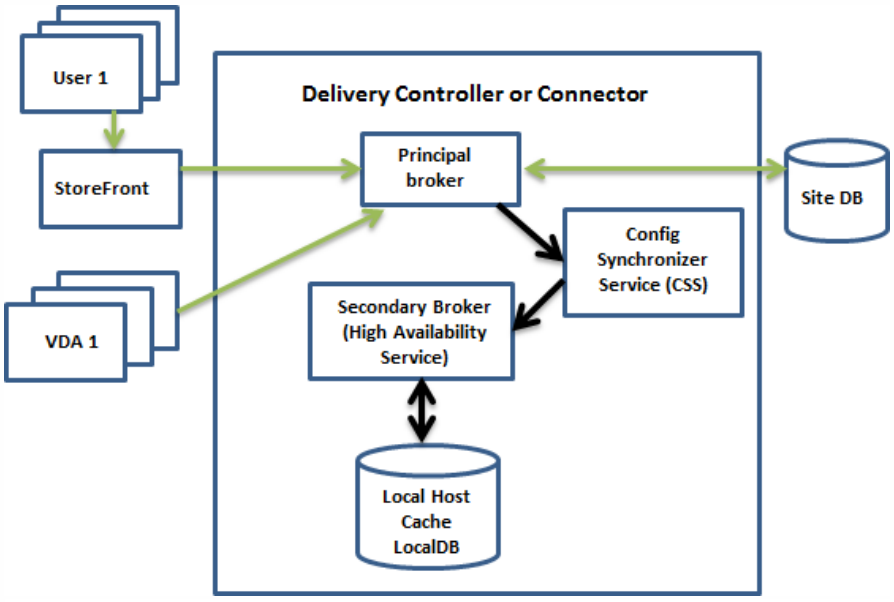
ローカルホストキャッシュは、XenAppおよびXenDesktopの最も包括的な高可用性機能です。XenApp 7.6で導入された接続リース機能のより強力な代替選択肢です。

注：バージョン7.15 LTSRでは接続リース機能はサポートされていますが、それ以降のリリースでは削除される予定です。

このローカルホストキャッシュ実装は、XenApp 6.x以前のXenAppリリースのローカルホストキャッシュ機能の名前を共有しますが、大幅に改善されています。この実装は、破損に対してより頑強で耐性もあります。定期的にdsmaintコマンドを実行する必要がないなど、メンテナンス要件が最小になります。このローカルホストキャッシュは技術的にはまったく異なる実装です。以下、その仕組みについて説明します。

仕組み

次の図は、通常の操作中のローカルホストキャッシュコンポーネントと通信経路を示しています。



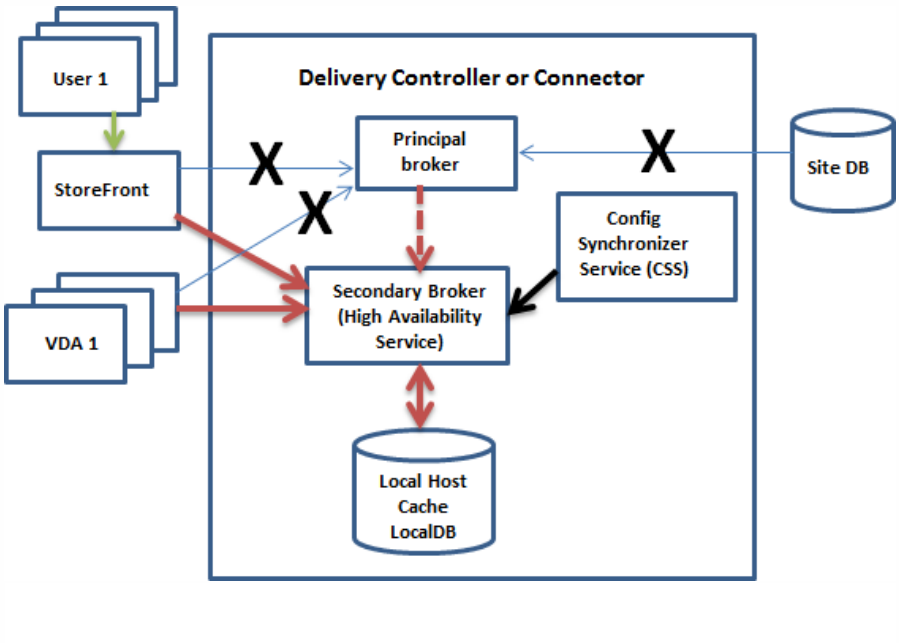
通常の操作中：

- Controller上の*プリンシパルブローカー*（Citrix Broker Service）は、StoreFrontからの接続要求を受け取り、サイトデータベースと通信して、Controllerに登録されたVDAにユーザーを接続します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 2分おきにチェックして、プリンシパルブローカーの構成が変更されたかどうか判断します。この変更は、PowerShell/Studioの操作（デリバリーグループプロパティの変更など）によっても、システム操作（マシン割り当てなど）によっても開始できます。
- 最後のチェック以降に変更されると、プリンシパルブローカーは、Citrix Config Synchronizer Service（CSS）を使用してController上の*セカンダリブローカー*（Citrix High Availability Service）に情報を同期（コピー）します。前回のチェック以降に変更された項目だけでなく、すべてのブローカー構成データがコピーされます。セカンダリブローカーは、Controller上のMicrosoft SQL Server Express LocalDBデータベースにデータをインポートします。CSSにより、セカンダリブローカーのLocalDBデータベースの情報がサイトデータベースの情報に一致することが保証されます。LocalDBデータベースは、同期が発生するたびに再作成されます。
- 最後のチェック以降に変更が発生しなかった場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合の通信径路の変更を示しています（停止状態の開始）。



停止状態が始まると：

- プリンシパルブローカーはサイトデータベースと通信できなくなり、StoreFrontおよびVDA情報（図中のX印）のリスニングを停止します。次に、プリンシパルブローカーは、接続要求（図中の赤い点線）のリスニングと処理を開始するように、セカンダリブローカー（High Availability Service）に指示します。
- 停止状態の開始時に、セカンダリブローカーにはその時点のVDA登録データがありませんが、VDAとの通信が始まるとすぐに再登録処理がトリガーされます。その処理中、セカンダリブローカーは、そのVDAに関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理する間、プリンシパルブローカーはサイトデータベースへの接続の監視を続行します。接続が回復すると、プリンシパルブローカーはセカンダリブローカーに接続情報のリスニングを停止するように指示し、プリンシパルブローカーが操作の仲介を再開します。再登録処理は、VDAがプリンシパルブローカーと次に通信するときにトリガーされます。セカンダリブローカーは、前回の停止状態以降に残ったVDA登録があれば削除して、CSSから受け取った構成変更によるLocalDBデータベースの更新を再開します。

同期中に停止状態が開始されるという可能性の低い事象では、その時点のインポートは破棄され、最新の既知の構成が使用されます。

イベントログには、同期および停止に関する情報が含まれます。詳しくは、下の「モニター」セクションを参照してくださ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

い。

また、停止状態を意図的にトリガーすることもできます。理由と方法について詳しくは「停止状態の強制」セクションを参照してください。

複数のControllerがあるサイト

CSSは、他のタスク同様、ゾーン内のすべてのControllerに関する情報を日常作業としてセカンダリブローカーに提供します（展開に複数のゾーンがない場合、この操作はサイト内のすべてのControllerに影響します）。その情報により、各セカンダリブローカーは、同じ立場にあるすべてのセカンダリブローカーを認識します。

セカンダリブローカーは独立したチャネルで相互に通信します。実行しているマシンのFQDN名のアルファベット順の一覧を使用して、停止状態が発生したときにどのセカンダリブローカーがゾーン内の仲介操作を担当するかを決定（選出）します。停止状態中、すべてのVDAが、選出されたセカンダリブローカーに再登録します。選出されていないゾーン内のセカンダリブローカーは、着信接続とVDA登録要求を能動的に拒否します。

停止状態中に、選出されたセカンダリブローカーに障害が発生した場合、別のセカンダリブローカーが選出されて引き継ぎ、VDAは選出されたセカンダリブローカーに新しく再登録します。

停止状態中にControllerを再起動した場合：

- このControllerをプライマリブローカーに選出していない場合は、再起動しても影響はありません。
- このControllerをプライマリブローカーに選出している場合は、別のControllerが選出されてVDAはそちらに再登録します。再起動したControllerの電源がオンになると、このControllerが自動的にブローカーを引き継ぐため、VDAはもう一度再登録します。このシナリオでは、再登録中にパフォーマンスが影響を受けることがあります。

プライマリブローカーに選出したControllerを、通常の操作中に電源を切ってから停止状態中に電源を入れると、ローカルホストキャッシュをこのController上で使用することはできません。

イベントログには、選出に関する情報が含まれます。後述の「モニター」セクションを参照してください。

設計に関する考慮事項および要件

ローカルホストキャッシュは、サーバーでホストされるアプリケーションおよびデスクトップと静的な（割り当て済み）デスクトップでサポートされます。プール型のVDIデスクトップ（MCSやPVSで作成）ではサポートされません。

停止モードでの操作に時間制限は適用されませんが、可能な限り速やかにサイトを通常操作に復元するようにします。

停止状態中にできなくなることと変更されること

- 管理者はStudioやPowerShellコマンドレットを使用できません。
- ハイパーバイザー資格情報をホストサービスから取得できません。すべてのマシンの電力状態が不明で、電源操作を発行できません。ただし、電源が入っているホスト上のVMを接続要求のために使用することができます。
- 割り当てられたマシンは、通常の操作中に割り当てが発生した場合のみ使用できます。停止状態中は新しい割り当てはできません。
- リモートPCアクセスマシンの自動登録と構成はできません。ただし、通常の操作中に登録、構成されたマシンは使用できます。
- サーバーでホストされるアプリケーションとデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。
- ユーザーは、現在アクティブ/選択されている（セカンダリ）ブローカーを含むゾーン内の登録済みVDAからのみ、アプリ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ケーションとデスクトップを起動できます。停止中は、ゾーン間での起動（あるゾーンのブローカーから別のゾーンのVDAへ）はサポートされません。

デフォルトでは、停止状態が発生した場合、「ShutdownDesktopsAfterUse」プロパティが有効になっているデリバリーグループにプールされた、電源管理されたデスクトップVDAは保守モードになります。このデフォルトの設定を変更して、停止状態中にこれらのデスクトップを使用できるようにすることができます。ただし、停止状態中は電源管理が機能しないことがあります。（通常の操作を開始すると電源管理が始まります）。また、これらのデスクトップは再起動していないため、前のユーザーのデータが含まれている可能性があります。

デフォルトの動作を上書きするには、サイト全体で、影響を受けるデリバリーグループごとに、これを有効にする必要があります。次のPowerShellコマンドレットを実行します。

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
Set-BrokerDesktopGroup -Name "<名前>" -ReuseMachinesWithoutShutdownInOutage $true
```

この機能をサイトでデリバリーグループごとに有効にしても、構成された「ShutdownDesktopsAfterUse」プロパティの、通常操作時の動作には影響がありません。

RAMサイズ

LocalDBサービスは、約1.2GBのRAM（データベースキャッシュ用に最大1GB、SQL Server Express LocalDBの実行用にさらに200MB）を使用できます。High Availability Serviceは、停止状態が長時間続き、多数のログオンが発生した場合（たとえば12時間でユーザー数1万人）、最大1GBのRAMを使用できます。これらのメモリ要件はControllerの通常のRAM要件とは別なので、RAMの総容量を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用する場合、サーバーに2つのsqlserver.exeプロセスを持つ点に注意してください。

CPUコアとソケットの構成

ControllerのCPU構成、特にSQL Server Express LocalDBが利用できるコア数は、メモリ割り当て以上に、ローカルホストキャッシュのパフォーマンスに直接影響を及ぼします。このCPUオーバーヘッドが発生するのは、データベースとの接続が失われ、High Availability Serviceがアクティブである停止状態の間だけです。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットだけに制限されます。ソケットを追加しても（たとえば、4つのソケットにそれぞれ1つのコア）、パフォーマンスは向上しません。それよりも複数のコアを持つ複数のソケットの使用をお勧めします。Citrixのテストでは、2x3（2つのソケット、3つのコア）の構成が、4x1および6x1の構成より良好なパフォーマンスを示しました。

ストレージ

ユーザーが停止状態の間にリソースにアクセスすると、LocalDBは増大します。たとえば、1秒に10回ログオンするログオン/ログオフテスト実行では、データベースは2～3分に1MB増大しました。通常の操作が再開すると、ローカルデータベースが再作成され、容量は元に戻ります。ただし、停止状態中のデータベース増大を考慮に入れて、LocalDBがインストールされるドライブ上のブローカーは十分な容量を持つ必要があります。ローカルホストキャッシュを使用すると、停止状態中に追加のI/Oが生じます（数十万の読み取りで、1秒あたり約3MBの書き込み）。

性能は、

停止状態中は1つのブローカーがすべての接続を処理するため、通常の操作時に複数のControllerに負荷を分散するサイト（あるいは、ゾーン）では、停止状態中に、選出されたブローカーが普通よりはるかに多くの要求を処理する必要があることがあります。このため、CPUへの要求が高くなります。選出されたブローカーが停止状態中に変更される可能性があるため、サイ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ト（ゾーン）内のすべてのブローカーが、LocalDBと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。

VDIの制限事項：

- 単一ゾーンにVDIを展開する場合、停止状態時には最大10,000のVDAを効果的に処理できます。
- 複数ゾーンにVDIを展開する場合、停止状態時には各ゾーンで最大10,000のVDA、サイト全体では最大40,000のVDAを効果的に処理できます。たとえば次のそれぞれのサイトが、停止状態時に効果的に処理されます。
  - 4つのゾーンそれぞれに10,000のVDAが含まれるサイト。
  - 1つのゾーンには10,000のVDAが含まれ、残り6つのゾーンにはそれぞれ5,000のVDAが含まれる、合計7つのゾーンからなるサイト。

停止状態中に、サイト内の負荷管理が影響を受ける可能性があります。負荷評価基準（特にセッション数規則）を超過する可能性があります。

すべてのVDAがブローカーに再登録する間、そのブローカーには現在のセッションについての完全な情報がないことがあります。このため、その間の接続要求により、既存のセッションへの再接続が可能であっても、新しいセッションが起動される可能性があります。こうした時間（「新しい」ブローカーが再登録時にすべてのVDAからセッション情報を取得する時間）が発生するのは避けられません。停止状態の開始時に接続していたセッションは移行期間に影響は受けませんが、新しいセッションおよびセッション再接続は影響を受ける可能性がある点に注意してください。

この期間は、VDAが異なるブローカーに再登録する必要があるときは常に発生します。

- 停止状態の開始：プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止状態中のブローカー障害：障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの回復：通常の操作が再開し、プリンシパルブローカーが制御を再開したとき。

Citrix Broker ProtocolのHeartbeatPeriodMsレジストリ値（デフォルト = 600000ms（10分））を小さくすることによって期間を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが発生します。

たとえば、ハートビートを5分（300000ms）に変更するには、次のコマンドを実行します。このようにすると、pingは2.5分ごとに発生します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs
-PropertyType DWORD –Value 300000
```

VDAの登録をどんなに早くしても、間隔を完全になくすことはできません。

ブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数により増加します。たとえば、5000のVDAの同期を完了するには、10分以上かかる可能性があります。イベントログの同期エントリについて詳しくは、後述の「モニター」セクションを参照してください。

ローカルホストキャッシュの管理

SQL Server Express LocalDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBは、Controllerをインストールするか、Controllerを7.9以前のバージョンからアップグレードするときに、自動的にインストールされます。LocalDBを管理者がメンテナンス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

る必要はありません。セカンダリブローカーだけがこのデータベースと通信します。PowerShellコマンドレットを使用してこのデータベースに関する変更を行うことはいっさいできません。LocalDBは、Controller間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効かどうかに関係なくインストールされます。

> このインストールを防止するには、Controllerのインストールまたはアップグレード時に、XenDesktopServerSetup.exeコマンドで「/exclude "Local Host Cache Storage (LocalDB)"」オプションを使用します。ただし、ローカルホストキャッシュ機能はデータベースがないと機能しないことと、セカンダリブローカーでは異なるデータベースを使用できないことに注意してください。

注： このLocalDBデータベースのインストールは、サイトデータベースとして使うためにSQL Server Expressをインストールするかどうかには影響しません。

XenAppまたはXenDesktopのインストールとアップグレード後のデフォルト設定

XenAppおよびXenDesktopの新規インストール時に、ローカルホストキャッシュはデフォルトで有効になっています。（接続リース機能は、デフォルトで無効になっています。）

アップグレード後、ローカルホストキャッシュ設定は変更されません。たとえば、ローカルホストキャッシュが以前のバージョンで有効にされていると、アップグレードされたバージョンでも引き続き有効になっています。以前のバージョンで無効な場合、またはサポートされていなかった場合、アップグレードされたバージョンでも無効のままです。

ローカルホストキャッシュの有効化と無効化

ローカルホストキャッシュを有効化するには、次のように入力します。

```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled $false
```

このコマンドレットは、接続リース機能も無効化します。ローカルホストキャッシュと接続リースの両方を有効化しないでください。

ローカルホストキャッシュが有効かどうかを判断するには、次のように入力します。

```
Get-BrokerSite
```

LocalHostCacheEnabledプロパティがTrueで、ConnectionLeasingEnabledプロパティがFalseであることを確認します。

ローカルホストキャッシュを無効化（および接続リースを有効化）するには、次のように入力します。

```
Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled $true
```

停止状態の強制

データベースの停止状態を意図的に強制することもできます。

- ネットワークが稼動と停止を繰り返している場合。ネットワークの問題が解決するまで停止状態を強制することにより、通常モードと停止状態モードの移行が繰り返されるのを防げます。
- 障害回復プランをテストするには：
- サイトデータベースサーバーの交換または修理中。

停止状態を強制するには、Delivery Controllerを含む各サーバーのレジストリを編集します。

- HKLM\Software\Citrix\DesktopServer\LHCで、OutageModeForcedを1に設定します。この指示により、ブローカーは

© 1999-2017 Citrix Systems, Inc. All rights reserved.

データベースの状態に関係なく停止状態モードに入ります （値を0に設定すると、サーバーの停止状態モードが終了します）
- Citrix Cloudのシナリオでは、コントロールプレーンやプライマリゾーンへの接続の状態に関係なく、コネクタが停止状態モードに入ります。

監視

イベントログに、同期および停止状態が発生した時刻が示されます。

Config Synchronizer Service

通常の操作中に、CSSがブローカー構成をコピーおよびエクスポートして、High Availability Service（セカンダリブローカー）を使用してそれをLocalDBにインポートするとき、次のイベントが発生することがあります。

- 503： プリンシパルブローカー構成に変更が見つかり、インポートが開始されます。
- 504：ブローカー構成がコピーおよびエクスポートされて、LocalDBに正常にインポートされました。
- 505：LocalDBへのインポートが失敗しました。詳しくは下記を参照してください。

高可用性サービス

- 3502：停止状態が発生し、セカンダリブローカー（High Availability Service）が操作の仲介を実行しています。
- 3503：停止状態が解決され、通常の操作が再開しました。
- 3504：どのセカンダリブローカーが選出されたかと、選出に関わった他のブローカーを示します。

トラブルシューティング

LocalDBへの同期インポートが失敗し、505イベントがポストされた場合、いくつかのトラブルシューティングツールを利用できます。

CDFトレーシング：ConfigSyncServerおよびBrokerLHCモジュールのオプションを含んでいます。それらのオプションと他のブローカーモジュールの組み合わせで問題を識別できるはずです。

レポート：障害ポイントを詳しく説明したレポートを生成して提供できます。このレポート機能は同期速度に影響するため、使用しないときは無効にしておくことをお勧めします。

CSSトレースレポートを有効化および作成するには、次のように入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは、C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htmlにポストされます。

レポートが生成されたら、レポート機能を無効にします。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート：デバッグのために正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File < file-pathname>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

例：Export-BrokerConfiguration | Out-File C:\BrokerConfig.xml

© 1999-2017 Citrix Systems, Inc. All rights reserved.

接続リース

Dec 05, 2017

重要： ローカルホストキャッシュ（LHC）は、接続リースよりも望ましいXenAppおよびXenDesktop高可用性ソリューションです。詳しくは、「ローカルホストキャッシュ」を参照してください。

- このリリースでは、XenAppとXenDesktopの新規インストールの間に、接続リース機能はデフォルトで無効になります。
- XenAppとXenDesktop 7.15 Long Term Service Releaseに続く最新のリリースでは、接続リース機能は提供されなくなる予定です。

サイトデータベースを常に使用可能状態にするために、Microsoft社の高可用性ベストプラクティスに従って耐障害性の高いSQL Server展開から開始することをお勧めします。ただし、ネットワークの問題および中断によってDelivery Controllerがデータベースにアクセスできなくなり、その結果、ユーザーがアプリケーションやデスクトップに接続できなくなる場合があります。

SQL Server高可用性ベストプラクティスを補完する接続リース機能を使用すると、サイトデータベースが使用不可の場合でも、ユーザーが直近で使用したアプリケーションやデスクトップに接続および再接続できるようになります。

通常、多くの公開リソースを使用できるユーザーでも、定期的に使用するのはその一部のみです。接続リース機能を有効にすると、通常時（データベースが使用可能なとき）に、最近使用されたアプリケーションやデスクトップのユーザー接続が各Controllerでキャッシュされます。

各Controller上でリースが生成され、それがサイトデータベースにアップロードされてほかのControllerと定期的に同期されます。各Controllerのキャッシュには、リースのほかにアプリケーション、デスクトップ、アイコン、ワーカーなどの情報が格納されます。リースとその関連情報は、各Controllerのローカルディスクに保存されます。データベースを使用できなくなると、Controllerはリース接続モードになります。この場合、ユーザーがStoreFrontから最近使用したアプリケーションやデスクトップへの接続を試みると、キャッシュされている操作が「再生」されます。

接続は、2週間の「リース期間」をキャッシュされます。そのため、ユーザーが直前の2週間に起動したデスクトップとアプリケーションは、データベースが使用不可になった場合でも引き続きStoreFront経由でアクセスできます。ただし、直前の2週間に起動しなかったデスクトップとアプリケーションは、データベースが使用不可になった場合にはアクセスできなくなります。たとえば、あるアプリケーションを最後に起動したのが3週間前である場合、そのアプリケーションのリース期限が切れているため、現時点でデータベースが使用不可になると起動できなくなります。長時間実行されているアプリケーションまたはデスクトップのアクティブセッションまたは切断セッションのリースは、期限切れにならないように延長されます。

デフォルトでは、接続リースはサイト全体に影響します。ただし、特定のユーザーのすべてのリースを取り消すことができます。これにより、Controllerがリース接続モードのときに、そのユーザーはすべてのアプリケーションやデスクトップにアクセスできなくなります。そのほかのいくつかのレジストリ設定はController単位で適用されます。

考慮事項と制限事項

接続リースを使用すると接続の回復性やユーザーの生産性を向上させることができますが、そのほかの機能のパフォーマンス、可用性、および操作に関連する注意事項があります。

接続リースは、サーバーでホストされるアプリケーションおよびデスクトップと静的な（割り当て済み）デスクトップでサポートされます。プール型のVDIデスクトップや、データベースが利用できなくなった時点でデスクトップが割り当てられていないユーザーはサポートされません。

リース接続モードのControllerでは、以下の制限事項があります。

- 管理者はStudio、Director、またはPowerShellコンソールを使用できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ワークスペースコントロールは使用できません。ユーザーがCitrix Receiverにログオンしたときにセッションには自動的に再接続されません。ユーザーはアプリケーションを再度起動する必要があります。
- すべてのController間でリース情報が同期されるまでは、データベースが利用できなくなったときにユーザーがそのリソースの起動に失敗する場合があります。
- サーバーでホストされるアプリケーションとデスクトップのユーザーは、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。次に例を示します。
  - Controllerがリース接続モードになっていないときにユーザーがデバイス（NetScaler Gateway経由で外部から接続しているデバイス）からセッションを起動し、Controllerがリース接続モードになった後でLAN上の別のデバイスから接続した場合、セッションがローミングされずに新しいセッションが作成されることがあります。
  - データベースが使用できなくなる直前にアプリケーションが起動した場合、セッションの再接続に失敗することがあります。この場合、新しいセッションとアプリケーションインスタンスが起動します。
- 静的な（割り当て済み）デスクトップでは、電源管理が行われません。Controllerがリース接続モードになるときに電源がオフになったVDAは、管理者が手動で電源をオンにしない限り、データベース接続が回復するまで使用できません。
- セッションの事前起動とセッション残留が有効になっている場合、新しい事前起動セッションは開始されません。データベースが利用可能になるまでは、構成されたしきい値に従って事前起動セッションや残留セッションが自動終了することはありません。
- サイト内の負荷管理が影響を受ける可能性があります。サーバーベースの接続は直近に使用されたVDAに割り当てられます。負荷評価基準（特にセッション数規則）を超過する可能性があります。
- SQL Server Management Studioと使ってデータベースをオフラインにすると、Controllerがリース接続モードになりません。以下のTransact-SQL文を使用してください。
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name*f*> SET OFFLINE WITH ROLLBACK AFTER <seconds>

  これらのSQL文によりすべての保留中のトランザクションがキャンセルされ、Controllerとデータベースとの接続が失われます。これにより、Controllerがリース接続モードになります。

接続リースが有効になっている場合、ユーザーが接続または再接続できない短い間隔が2回あります。1回はデータベースが利用できなくなってからControllerがリース接続モードになるまでの間、もう1回はControllerがリース接続モードを終了してからデータベースが完全に回復し、VDAの再登録が終わるまでの間です。

非デフォルトのセッションローミング値を構成する場合、Controllerがリース接続モードに入ると、セッションの再接続によりデフォルト値に戻ります。詳細は、「接続リース機能とセッションローミング」を参照してください。

接続リースデータの保存場所については、「ゾーン」の記事を参照してください。

詳細は、「XenDesktop 7.6 Connection Leasing Design Considerations（リンク先は英語）」を参照してください。

構成と展開

接続リース機能を使用するには、環境を以下のように構成する必要があります。
- VDAはVersion 7.6以上である必要があります。また、これらのマシンを使用するマシンカタログとデリバリーグループもVersion 7.6以上である必要があります。
- サイトデータベースのサイズ要件が大きくなります。
- 各Controllerには、キャッシュされるリースファイル用の追加のディスクスペースが必要です。

接続リース機能の有効/無効は、PowerShell SDK、またはWindowsのレジストリで切り替えることができます。PowerShell SDKを使用する場合は、現在のリースを削除することもできます。接続リース機能を制御するPowerShellコマンドレットは以下のとおりです。詳しくは、コマンドレットのヘルプを参照してください。
- Set-BrokerSite -ConnectionLeasingEnabled $true|$false - 接続リース機能のオン/オフを切り替えます。デフォルト値：$true
- Get-BrokerServiceAddedCapability - ローカルのControllerに「ConnectionLeasing」を出力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Get-BrokerLease - 現在のリースを取得します。フィルターで指定したリースのみを取得することもできます。
- Remove-BrokerLease - 指定したリースを削除用にマーク付けします。フィルターで指定したリースのみをマーク付けすることもできます。
- Update-BrokerLocalLeaseCache - ローカルのController上の接続リースのキャッシュを更新します。データは次の同期時に再同期されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

仮想IPおよび仮想ループバック

Dec 05, 2017

注： これらの機能は、サポートされているWindowsサーバーマシンでのみ有効です。WindowsデスクトップOSマシンでは使用できません。

Microsoft社の仮想IPアドレス機能により、セッションごとに動的に割り当てられるIPアドレスを公開アプリケーションで使用できます。Citrixの仮想ループバック機能を使用すると、ローカルホスト（デフォルトで127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

CRM（Customer Relationship Management）やCTI（Computer Telephony Integration）などの特定のアプリケーションでは、アドレス割り当て、ライセンス付与、識別、またはそのほかの目的でIPアドレスが使用されるため、セッションに固有のIPアドレスまたはループバックアドレスが必要です。また、一部のアプリケーションでは静的なポートにバインドされるため、マルチユーザー環境でそのアプリケーションの追加インスタンスを起動しようとすると、そのポートが使用済みなので起動に失敗します。これらのアプリケーションがXenApp環境で正しく動作するためには、クライアントデバイスごとに異なるIPアドレスが使用される必要があります。

仮想IPと仮想ループバックは、それぞれ独立した機能です。これらの機能のいずれかまたは両方を使用できます。

使用する機能に応じて、管理者は以下の操作を行います。

- Microsoft社の仮想IP機能を使用するには、Windowsサーバー上で仮想IPを有効にして構成します。（Citrixポリシーの設定は必要ありません。）
- Citrixの仮想ループバック機能を使用するには、Citrixポリシーで2つの設定項目を構成します。

仮想 IP

Windowsサーバー上で仮想IP機能を 有効にすると、セッション内で動作する各アプリケーション で固有のアドレスが使用されるように構成できます。ユーザーは、これらの アプリケーションを、ほかの公開 アプリケーションと同じように使用することができます。以下のいずれかの動作をするプロセスでは、仮想IPアドレスを設定します。

- ハードコードされた（固定された）TCPポート番号を 使用する。
- Windowsソケットを使用し、固有のIPアドレスまたは固定されたTCPポート 番号を 使用する。

アプリケーションで仮想IPアドレスが必要かどうかを判断するには、次の手順に従います。

1. Microsoft社のWebサイトから、 TCPViewツールを入手します。このツールを使用すると、 特定のIPアドレスおよびポートを使用しているすべてのアプリケーションを一覧表示できます。
2. TCPViewの［Options］メニューで、 ［Resolve Addresses］を無効にします。これにより、一覧にホスト 名ではなくアドレスが表示されるようになります。
3. 対象となる アプリケーションを起動して、使用されているIPアドレスとポート、およびそれらのポートを開いている プロセスの名前をTCPViewで確認します。
4. サーバーのIPアドレス0.0.0.0または127.0.0.1を使用する プロセスを構成します。
5. その アプリケーションの 追加インスタンスを起動して、別のポート上で同じIPアドレスが使用されないことを確認します。

Microsoftリモート デスクトップ（RD）のIP仮想化機能のしくみ

- 仮想IP アドレスを使用するには、Windowsサーバー上でこの機能を有効にする必要があります。
  たとえば、Windows Server 2008 R2環境でサーバーマネージャーを使用し、［リモートデスクトップサービス］>［RDセッションホストの構成］の順に展開してRD IP仮想化機能を有効にします。次に、IPアドレスをDHCP（Dynamic Host Configuration Protocol：動的ホスト構成プロトコル）サーバーによりセッションごとまたはプログラムごとに動的に割り当てるように設定を行います。 手順については、Microsoft社のドキュメントを参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- この機能を 有効にすると、セッション起動時にサーバーは、DHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- RD IP 仮想化機能によって、セッションごとまたはプログラムごとに、リモートデスクトップ接続 にIPアドレスが割り当てられます。複数のプログラムにIPアドレスを割り当てる場合、 これらのプログラム間でセッションごとのIPアドレスが共有されます。
- アドレスが割り当てられたセッションでは、bind、closesocket、connect、WSAConnect、WSAAccept、getpeername、getsockname、sendto、WSASendTo、WSASocketW、gethostbyaddr、getnameinfo、 getaddrinfoの各コール に対して、システムのプライマリIPアドレスではなく仮想アドレス が使用されます。

リモートデスクトップセッションのホスト 環境で MicrosoftのIP仮想化機能を使用すると、アプリケーションとWinsockコールとの間に 「フィルター」コンポーネントを挿入することで、アプリケーションと特定のIPアドレスがバインドされます。IPアドレスがバインドされると、 アプリケーションはそのアドレスだけで要求を待ち受けるようになります。 アプリケーションのTCPリスナーまたはUDPリスナーは自動的に 仮想IPアドレス（または仮想ループバックアドレス）にバインドされ、 アプリケーションからの 接続はその仮想アドレスから開かれます。

Windows ポリシーにより制御されるGetAddrInfo()など、アドレスを 返すファンクションでローカルホストIPアドレスが要求されると、 返されたIPアドレスがそのセッションの仮想IPアドレスに変換されます。 このようなファンクションでローカルサーバーのIPアドレスを取得しようとするアプリケーションには、 セッション固有の仮想IPアドレスだけが渡されます。このようにしてアプリケーションに渡されたIPアドレスは、後続のソケットコール（bind やconnectなど）で使用されます。

アプリケーションでは、アドレス0.0.0.0で、リスナー用のポートのバインドが必要になる場合があります。 このようなアプリケーションで静的なポート番号が使用されると、競合が発生するため、 複数のインスタンスを起動できなくなります。仮想IPアドレス機能では、 0.0.0.0へのファンクションコールが特定の 仮想IPアドレスに変換されます。これにより、セッションごとに異なる アドレス上のポートが使用されるため、 同じポート番号を使用する複数のアプリケーションを実行できるようになります。このファンクションコールは、仮想 IPアドレス機能が有効なICAセッションでのみ変換されます。たとえば、すべてのインターフェイス（0.0.0.0）と 特定のポート（9000など）にバインドするアプリケーション の2つのインスタンスが、それぞれ異なるセッションで実行される場合、VIPAddress1:9000と VIPAddress2:9000にバインドされるため、競合が起きません。

仮想ループバック

Citrixポリシーで仮想IPループバック機能を有効にすると、各セッションで通信に独自のループバックアドレスが使用されるようになります。アプリケーションがWinsockコールでローカルホストのアドレス（デフォルトで127.0.0.1）を使用する場合、仮想ループバック機能により、127.0.0.1が127に置き換えられます。X.X.XX.X.Xは、セッションID＋1の表現です。たとえば、セッションIDが7の場合は127.0.0.8になります。セッションIDが4オクテットを超える場合（つまり255を超える場合）は、127.0.1.0のように次のオクテットに繰り上げられます。また、最大値は127.255.255.255です。

以下のいずれかの動作をするプロセスでは、仮想ループバックを設定します。
- Windowsソケットのループバック（localhost）アドレス127.0.0.1を使用する。
- ハードコードされた（固定された）TCPポート番号を使用する。

プロセス間通信でループバックアドレスを使用するアプリケーションでは、仮想ループバックアドレスに関するポリシー設定を使用します。追加の構成は必要ありません。仮想ループバックは仮想IPに依存しないため、Windowsサーバーの構成は不要です。
- 仮想IPループバックサポートこのポリシー設定を有効にすると、各セッション固有の仮想ループバックアドレスが使用されるようになります。このチェックボックスは、デフォルトでオフになっています。この機能は、［仮想 IP ループバックプログラム一覧］ポリシー設定で指定したアプリケーションにのみ適用されます。
- 仮想IPループバックプログラム一覧このポリシー設定では、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、［仮想 IP ループバックサポート］ポリシー設定が有効になっている場合のみ適用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

関連機能

次のレジストリ設定により、仮想ループバックが仮想IPよりも優先されるようになります（優先ループバック機能）。ただし、以下の点に注意してください。

- 優先ループバックはWindows Server 2008 R2とWindows Server 2012 R2でのみサポートされます。
- 仮想IPアドレスと仮想ループバックの両方の機能を有効にする場合にのみ、優先ループバック機能を使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

アプリケーションのホストサーバー上で、regeditを実行します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP（32ビットマシンでは HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP）
- 値の名前：PreferLoopback、種類：REG_DWORD、値のデータ：1
- 名前： PreferLoopbackProcesses。タイプ： REG_MULTI_SZ。データ： <list of processes>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controller

Dec 05, 2017

Delivery Controllerは、ユーザーアクセスの管理や接続の仲介と最適化を行うためのサーバー側のコンポーネントです。また、Controllerは、デスクトップおよびサーバーイメージを作成するMachine Creation Serviceも提供します。

サイトには、1つ以上のControllerが必要です。1つめのControllerのインストール後、サイトを作成するとき、または後日、さらにControllerを追加できます。サイトに複数のControllerがあると、以下の2つの利点がもたらされます。

- 冗長性：ベストプラクティスとしては、実務サイトでは異なる物理サーバー上に常時2つ以上のControllerが必要です。一方のControllerに障害が発生しても、他方のControllerで接続を管理し、サイトを制御できます。
- スケーラビリティ： サイトのアクティビティが増えるにつれ、Controller上のCPU使用量およびデータベースアクティビティも増えます。Controllerを追加すると、より多くのユーザーやより多くのアプリケーションやデスクトップ要求を処理できるようになり、制御処理全体を向上させることができます。

各Controllerは、サイトデータベースと直接通信を行います。複数のゾーンを持つサイトでは、各ゾーンに存在するControllerが、プライマリゾーンにあるサイトデータベースと通信します。

重要： サイトの構成後、コンピューター名やControllerのドメインメンバーシップを変更しないでください。

ControllerへのVDAの登録方法

VDAを使用するには、そのサイトのDelivery Controllerに登録（接続を確立）する必要があります。VDAの登録について詳しくは、「Delivery ControllerへのVDAの登録」を参照してください。

（XenAppおよびXenDesktop 7.xリリース以前の文書では、この文書にVDAの登録についての情報が含まれていました。この情報は増強され、現在は上記に関連した文書に含まれています）。

Controllerの追加、削除、または移動

Controllerを追加、削除、または移動するには、「*データベース*」の記事に記載されているサーバーおよびデータベースの役割権限が必要です。

注： SQLクラスター化またはSQLミラー化インストールのおけるノード上へのControllerのインストールはサポートされていません。

展開環境でデータベースのミラーリングを使用している場合は、以下の点について注意してください。

- Controllerを追加、削除、または移動する前に、プライマリデータベースとミラーデータベースの両方が実行中であることを確認してください。また、SQL Server Management Studioでスクリプトを使用している場合は、SQLCMDモードを有効にしてください。
- Controllerの追加、削除、または移動後にミラーリングを確認するには、**get-configdbconnection PowerShell**コマンドレットを実行しミラーに対する接続文字列でフェールオーバーパートナーが設定されているか確認します。

Controllerの追加、削除、または移動後の作業

- 自動更新が有効な場合は、VDAは90分以内に最新のController一覧を受信します。
- 自動更新が無効な場合は、すべてのVDAについてControllerポリシー設定またはListOfDDCsレジストリキーが更新されてい

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ることを確認してください。Controllerをほかのサイトに移動した後は、両方のサイト上でポリシー設定またはレジストリキーを更新する必要があります。

Controllerの追加

Controllerは、サイトの作成時、または後日、追加できます。以前のバージョンがインストールされたControllerをこのバージョンのサイトに追加することはできません。

1. サポートされているオペレーティングシステムが稼動しているサーバーでインストーラーを実行します。Delivery Controllerコンポーネントと、必要なコアコンポーネントをすべてインストールします。インストールウィザードを完了します。
2. サイトをまだ作成していない場合は、Studioを起動します。サイトの作成を促すメッセージが表示されます。 サイトの作成ウィザードの［データベース］ページで［選択］ボタンをクリックし、追加するControllerがインストールされているサーバーのアドレスを追加します。 **重要：** データベースの初期化スクリプトを生成する計画がある場合は、スクリプトを生成する前に、Controllerを追加してください。
3. サイトの作成がすでに済んでいる場合は、Studioで、追加のControllerをインストールしたサーバーを指定します。**[展開の変更]** をクリックし、サイトアドレスを入力します。

Controllerの削除

Controllerを削除すると、Citrixソフトウェアやそのほかのコンポーネントはアンインストールされませんが、データベースからそのControllerが削除されます。このため、このControllerでは接続の仲介やそのほかのタスクを実行できなくなります。削除したControllerを、後で元のサイトや別のサイトに追加することができます。サイトには最低1つのControllerが必要なため、Studioの一覧に表示される最後のControllerを削除することはできません。

サイトからController削除しても、データベースサーバーへのControllerログオンは削除されません。これは、同じマシン上のほかの製品のサービスで使用されるログオンが削除されるのを防ぐためです。ログオンが必要ない場合には、手動で削除する必要があります。ログオンの削除には、securityadminサーバーロール権限が必要です。

重要： サイトからControllerを削除するまでは、Active DirectoryでそのControllerを削除しないでください。

1. Controllerが動作しており、1時間以内にそのControllerがStudioにロードされることを確認してください。削除するControllerがStudioにロードされたら、メッセージに従ってControllerをシャットダウンしてください。
2. Studioのナビゲーションペインで、**［構成］＞［Controller］** の順に選択し、削除するControllerを選択します。
3. ［操作］ペインの **［Controllerの削除］** を選択します。適切なデータベースロールや権限がない場合は、Controllerを削除するためのスクリプトを生成できます。そのスクリプトの実行をデータベース管理者に依頼してください。
4. データベースサーバーからControllerのマシンアカウントを削除しなければならない場合があります。これを行う前に、ほかのサービスがそのアカウントを使用していないことを確認してください。

Studioを使ってControllerを削除した後、実行中のタスクを適切に完了させるためにそのControllerへのトラフィックがしばらく残ることがあります。Controllerを即座に削除するには、Controllerがインストールされているサーバーをシャットダウンするか、Active Directoryからそのサーバーを削除することをお勧めします。その後で、サイト内のほかのControllerを再起動します。これにより、削除されたControllerとの通信が行われなくなります。

Controllerの別のゾーンへの移動

サイトに複数のゾーンが含まれている場合、Controllerを別のゾーンに移動できます。これがVDAの登録などの操作にどのような影響を与えるかについて、詳しくは「ゾーン」の記事を参照してください。

1. Studioのナビゲーションペインで、**［構成］＞［Controller］** の順に選択し、移動するControllerを選択します。
2. ［操作］ペインの **［移動］** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Controllerの移動先ゾーンを指定します。

Controllerの別のサイトへの移動

このソフトウェアの以前のバージョンで作成されたサイトには、Controllerを移動できません。

1. StudioのナビゲーションペインでControllerの移動元サイトを開き、**[構成] > [Controller]**の順に選択し、移動するControllerを選択します。
2. ［操作］ペインの**[Controllerの削除]**を選択します。データベースに対する適切な役割や権限がない場合は、Controllerを削除するためのスクリプトを生成できます。そのスクリプトの実行をデータベース管理者など該当する権限を持つユーザーに依頼してください。サイトには最低1つのControllerが必要なため、Studioの一覧に表示される最後のControllerを削除することはできません。
3. 移動するControllerでStudioを開き、確認メッセージに応じてサービスをリセットします。さらに、**[既存のサイトへ参加]**を選択して、移動先サイトのアドレスを入力します。

VDAから別のサイトへの移動

VDAがProvisioning Servicesを使ってプロビジョニングされた場合、または既存のイメージの場合、アップグレード時、またはテストサイトで作成されたVDAイメージを実務環境サイトに移動させる場合に、VDAをほかのサイトに移動（サイト1からサイト2へ）できます。MCSはListOfDDCsの変更をサポートせずVDAはControllerへの登録をチェックするため、 Machine Creation Services（MCS）を使ってプロビジョニングされたVDAをあるサイトから別のサイトには移動できません。MCSを使ってプロビジョニングされるVDAは、作成されたサイトに割り当てられたListOfDDCsをチェックします。

VDAをほかのサイトに移動するにはインストーラーを使用するか、Citrixポリシーを使用します。

インストーラー：インストーラーを実行して、サイト2のControllerのFQDN（DNSエントリ）を指定してこのControllerを追加します。**重要：** Controllerのポリシー設定を使用しない場合にのみ、インストーラーでControllerを指定してください。

グループポリシーエディター：次の例では、複数のVDAをほかのサイトに移動します。

1. サイト1でポリシーを作成して以下のように設定し、そのポリシーをVDA移行を行うデリバリーグループに割り当てます。
   Controller — サイト2の1つまたは複数のControllerのFQDN（DNSエントリ）を指定します。
   Controllerの自動更新を有効にする — 無効に設定します。
2. デリバリーグループの各VDAは、新しいポリシーの適用後90分以内にアラートを受信します。VDAは、受信したControllerの一覧を無視して（自動更新が無効なため）、ポリシーで指定されているサイト2のいずれかのControllerを選択します。
3. VDAがサイト2のControllerへの登録に成功すると、サイト2のListOfDDCsおよびポリシー情報を受け取って、これにより自動更新が有効になります。サイト1での登録先のControllerがサイト2のControllerによって送信された一覧にはないため、サイト2の一覧のControllerのいずれかにVDAが再登録されます。これにより、VDAはサイト2からの情報に基づいて自動的に更新されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA登録

Jan 02, 2018

はじめに

VDAを使用するには、そのサイトの1つまたは複数のControllerまたはCloud Connectorに登録（接続を確立）する必要があります。（オンプレミスのXenAppおよびXenDesktop展開環境では、VDAはControllerに登録されます。XenAppおよびXenDesktop Service展開環境では、VDAはCloud Connectorに登録されます。）VDAはListofDDCsと呼ばれる一覧をチェックして、Controllerまたはコネクタを見つけます。VDAのListOfDDCsには、そのVDAをサイトのControllerまたはCloud ConnectorにポイントするDNSエントリが含まれています。負荷分散のため、VDAは一覧のすべてのControllerまたはCloud Connectorで接続を自動的に分散させます。

VDA登録が重要な理由

- セキュリティの面で見ると、登録ではControllerまたはCloud ConnectorとVDA間の接続を確立するため、デリケートな操作と言えます。このように注意が必要な操作では、不完全なものが1つでもあればその接続を拒否する必要があります。実際には、2つの個別の通信チャネル（VDAからControllerまたはCloud Connector、ControllerまたはCloud ConnectorからVDA）を確立することになります。接続ではKerberosが使用されるため、時刻の同期およびドメインへの参加に関する問題は見過ごせないものになります。Kerberosではサービスプリンシパル名（SPN）が使用されるため、負荷分散されたIPやホスト名は使用できません。
- ControllerまたはCloud Connectorの追加および削除は、VDAに正確かつ最新のControllerまたはCloud Connectorの情報が設定されていないと、未登録のControllerまたはCloud Connectorにより仲介されたセッションの起動がVDAにより拒否される場合があります。また、無効なエントリにより、仮想デスクトップシステムソフトウェアの起動に遅延が生じることがあります。VDAでは、信頼されていない不明なControllerまたはCloud Connectorからの接続は受け入れられません。

ListOfDDCsに加えて、ListOfSIDs（セキュリティID）によりListOfDDCsに記載されているどのマシンを信頼するかが指定されます。ListOfSIDsは、Active Directoryでの負荷を軽減したり、改ざんされたDNSサーバーからのセキュリティ上の脅威を防いだりするために使用できます。詳しくは、下記「*ListOfSIDs*」を参照してください。

ListOfDDCsに複数のControllerまたはCloud Connectorが指定されている場合、VDAはランダムな順序で接続を試行します。オンプレミスの展開では、ListOfDDCsにはControllerのグループを含めることもできます。VDAは、これらのグループ内の各Controllerへの接続を試行し、その後でほかのエントリを試行します。

XenAppとXenDesktopでは、VDAのインストール中に構成済みのControllerまたはCloud Connectorに対する接続が自動でテストされます。ControllerまたはCloud Connectorに接続できない場合は、エラーが表示されます。ControllerまたはCloud Connectorに接続できないことを示す警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）は、メッセージが表示されます。

ControllerまたはCloud Connectorのアドレスの構成方法

VDAの初めての登録時（初回登録と呼びます）に、管理者は使用する構成方法を選択します。初回登録中に、VDA上に永続キャッシュが作成されます。以降の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

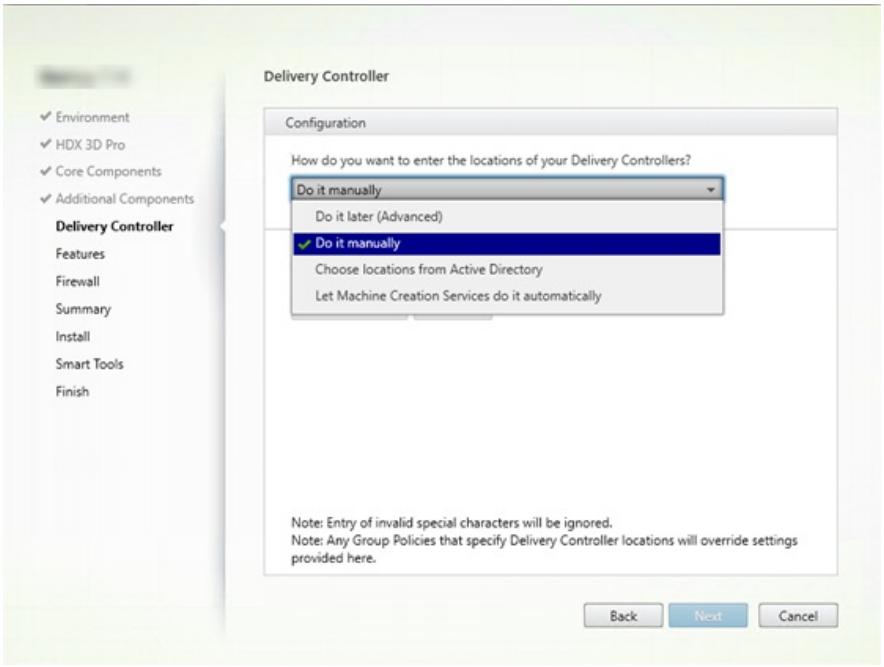
以降の登録時にこのリストを取得する一番簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳しくは、「自動更新」を参照してください。

VDAでControllerまたはCloud Connectorのアドレスを構成する方法は複数存在します。

- ポリシーベース（LGPOまたはGPO）
- レジストリベース（手動、GPP、VDAのインストール中に指定）
- Active DirectoryのOUベース（旧OU検出）
- MCSベース（personality.ini）

VDAをインストールするときに初回登録の方法を指定します（自動更新を無効にすると、初回以降の登録でもVDAのインストール時に選択した方法が使用されます）。

次の画像に、VDAインストールウィザードの［**Delivery Controller**］ページを示します。



ポリシーベース（LGPOまたはGPO）

VDAの初回登録ではGPOを使用することをお勧めします。この方法が最優先です（リスト上では自動更新が最優先となっていますが、自動更新は初回登録後にのみ使用します）。ポリシーベースの登録には、構成にグループポリシーを使用できるという集中化のメリットがあります。

この方法を指定するには、次の手順の両方を実行します。

- VDAインストールウィザードの［**Delivery Controller**］ページで、［**あとで実行（上級）**］を選択します。VDAのインストール中にControllerのアドレスの指定は行いませんが、ウィザードからこれらのアドレスを指定するように複数回促されます（これは、VDAの登録が非常に重要なためです）。
- ［Virtual Delivery Agentの設定］>［コントローラー設定］で、Citrixポリシーを使用してポリシーベースのVDA登録を有効化または無効化します（セキュリティが最優先事項である場合は、［Virtual Delivery Agent設定］>［コントローラーSID設定］を使用します）。

  この設定は、HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent（ListOfDDCs）に格納されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レジストリベース

この方法を指定するには、次の手順のいずれかを実行します。

- VDAインストールウィザードの［**Delivery Controller**］ページで、［**手動で指定する**］を選択します。次に、インストール済みのControllerのFQDNを入力し、［**追加**］をクリックします。追加のControllerをインストールした場合は、アドレスを追加します。
- コマンドラインでのVDAのインストールの場合は、/controllersオプションを使用してインストール済みのControllerまたはCloud ConnectorのFQDNを指定します。

通常、この情報は、レジストリキーHKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgentまたはHKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\VirtualDesktopAgentの下にあるレジストリ値ListOfDDCsに格納されます。

また、このレジストリキーを手動で構成するか、グループポリシーの基本設定（GPP）を使用することもできます。この方法は、ControllerまたはCloud Connector別に条件付きの処理を行う（例：コンピューター名がXDW-001-から始まる場合はXDC-001を使用する）場合などは、ポリシーベースの方法よりも適しています。

サイトのすべてのControllerまたはCloud Connectorの完全修飾ドメイン名の一覧が設定されているListOfDDCsレジストリキーを更新します。（このキーはActive Directoryサイト組織単位に相当します）。

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

レジストリ HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgentにListOfDDCsとFarmGUIDキーの両方がある場合は、ListOfDDCsがControllerまたはCloud Connectorの検出に使用されます。FarmGUIDは、VDAのインストール時にサイト組織単位を指定した場合に作成されます（このキーは古い展開環境で使用する場合があります）。

オプションで、ListOfSIDsレジストリキーを更新します（詳しくは下記「*ListOfSID*」を参照してください）。

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

注：Citrixポリシーによりポリシーベースの登録も有効化している場合は、ポリシーベースの方法の方が優先度が高いため、VDAのインストール時に指定した設定がポリシーベースの設定で上書きされます。

Active DirectoryのOUベース（旧）

この方法は主として後方互換性のためにサポートされているものであり、推奨されていません。現在もこの方法を使用している場合は、別の方法に変えることをお勧めします。

この方法を指定するには、次の手順の両方を実行します。

- VDAインストールウィザードの［**Delivery Controller**］ページで、［**Active Directoryから場所を選択する**］を選択します。
- Set-ADControllerDiscovery.ps1スクリプトを使用します（各Controller上にあります）。また、各VDA上のFarmGuidレジストリを、適切な組織単位を指すように構成します。この設定はグループポリシーを使用して行うことができます。

詳しくは、「Active Directory OU-based discovery」を参照してください。

MCSベース

VMのプロビジョニングにMCSのみを使用する予定の場合は、ControllerまたはCloud Connectorのリストを設定するようにMCSを構成することができます。この機能は自動更新と連携します。MCSは、初回プロビジョニング時（マシンカタログの作成時）にControllerまたはCloud Connectorのリストを Personality.iniファイルに書き込みます。自動更新により、このリストが最新に保たれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

大規模な環境では、この方法の使用は推奨されていません。この方法は次の場合に使用することをお勧めします。

- 環境が小規模である
- サイト間でVDAを移動させない
- VMのプロビジョニングにMCSのみを使用する
- グループポリシーを使用しない

この方法を指定するには次の手順を実行します。

- VDAインストールウィザードの［**Delivery Controller**］ページで、［**Machine Creation Services で指定する**］を選択します。

回

ベストプラクティス：

- 初回登録にはグループポリシーによる登録方法を使用します。
- 自動更新（デフォルトで有効化されています）を使用してControllerのリストを最新に保ちます。
- マルチゾーン展開（ControllerまたはCloud Connectorが2つ以上）では、初回構成にグループポリシーを使用します。各ゾーンにローカルのControllerまたはCloud Connectorに対してVDAをポイントします。自動更新を使用して、VDAを最新の状態に保ちます。自動更新により、サテライトゾーンにあるVDAのListOfDDC s が自動で最適化されます。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）は、デフォルトで有効化されています。これは、VDA登録を最新の状態に保つ最も効率的な方法です。初回登録では自動更新は使用しませんが、自動更新ソフトウェアにより、初回登録を行うときにListOfDDCsがダウンロードされ、永続キャッシュに格納されます。これはVDAごとに行われます（このキャッシュには、マシンポリシーの情報も格納されます。これにより、再起動後もポリシー設定が保持されます）。

MCSまたはPVSを使用してマシンをプロビジョニングする場合、自動更新がサポートされます。PVSサーバーのキャッシュは除外されます（自動更新キャッシュ用の永続的なストレージがないためです）。

この方法を指定するには次の手順を実行します。

- 自動更新を、［Virtual Delivery Agentの設定］>［Controllerの自動更新を有効にする］設定が含まれるCitrixポリシーを使用して有効化または無効化します。この設定は、デフォルトで有効になっています。

自動更新の仕組みは次のとおりです。

- VDAの再登録の度（マシンの再起動後など）にキャッシュが更新されます。また、各ControllerまたはCloud Connectorも90分ごとにサイトのデータベースをチェックします。最後のチェック以降にControllerまたはCloud Connectorが追加または削除されていた場合、またはVDA登録に影響するポリシー変更が行われていた場合、ControllerまたはCloud ConnectorからControllerまたはCloud Connectorに登録済みのVDAに最新のリストが送信され、キャッシュが更新されます。VDAは、最近キャッシュ化されたリストに含まれているすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが受信したリストに登録先のControllerまたはCloud Connectorが含まれていない場合（つまり、そのControllerまたはCloud Connectorがサイトから削除された場合）、ListOfDDCsのいずれかのControllerまたはCloud ConnectorにVDAが再登録されます。

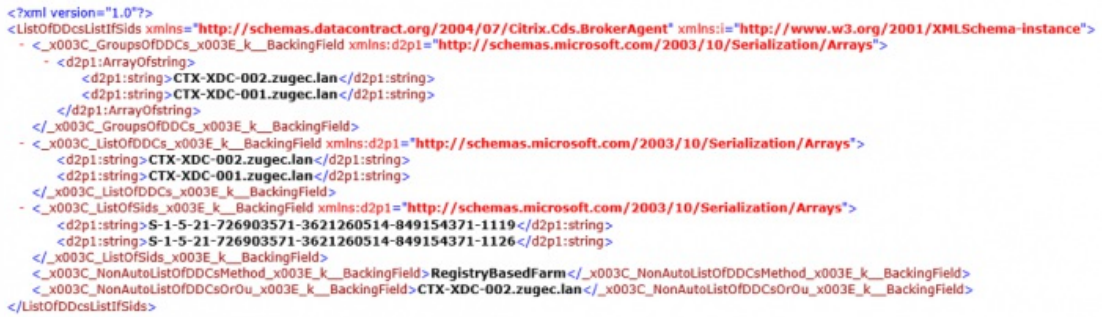
次に例を示します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 環境内に3つのController A、B、Cがあります。VDAは（VDAのインストール時に指定した）Controller Bに登録されています。
- その後、サイトに2つのController（DおよびE）を追加します。90分以内に、更新されたリストがVDAに送信されます。これにより、VDAはController A、B、C、D、Eからの接続を受け入れるようになります（VDAを再起動するまでは、すべてのController間で負荷分散は行われません）。
- さらにそのあとで、Controller Bを別のサイトに移動します。前回のチェック以降にサイトのControllerに変更があったため、元のサイトのVDAは90分以内に更新済みのリストを受信します。初めにController B（リストから削除されています）に登録されていたVDAは、現在のリストに含まれるController（A、C、D、E）のいずれかに再登録されます。

マルチゾーン展開のサテライトゾーンでは、まず自動更新によりすべてのローカルControllerがキャッシュ化されます。プライマリゾーンのControllerはすべて、バックアップグループにキャッシュ化されます。サテライトゾーンのローカルControllerを利用できない場合、プライマリゾーンのControllerへの登録が試みられます。

以下の例に示すように、キャッシュファイルにはホスト名およびセキュリティIDのリスト（ListOfSID）が含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が抑えられます。



キャッシュファイルはWMI呼び出しを使用して取得できますが、このファイルはSYSTEMアカウントのみが読み取り可能な場所に格納されています。重要：この情報は説明のみを目的として紹介しています。このファイルは変更しないでください。このファイルまたはフォルダーを変更すると、構成はサポート対象外となります。

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation”
-Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”
```

セキュリティ上の理由で（Active Directoryの負荷の抑制とは異なる理由で）ListOfSIDsを手動で構成する必要がある場合、自動更新は使用できません。詳しくは、下記「*ListOfSID*」を参照してください。

自動更新の優先度の例外

通常、自動更新はすべてのVDA登録方法の中で最も優先度が高くなっており、ほかの方法の設定を上書きしますが、例外も存在します。キャッシュのNonAutoListOfDDCs要素により、初回のVDA構成方法が指定されます。自動更新ではこの情報を監視しています。初回登録の方法が変更されると、登録プロセスでは自動更新が省略され、優先度が次に高く構成されている方法が使用されます。これは、（障害復旧時など）VDAを別のサイトに移動する場合に役立ちます。

構成に関する考慮事項

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorの指定に使用する方法にかかわらず、FQDNアドレスを使用することをお勧めします。IPアドレスはDNSレコードよりも侵害されやすいため、信頼性の高い構成とは言えません。ListOfSIDを手動で入力する

© 1999-2017 Citrix Systems, Inc. All rights reserved.

場合は、ListOfDDCsのIPを使用できます。ただし、この場合でもFQDNが推奨されています。

負荷分散

前述のとおり、VDAはListOfDDCsに含まれるすべてのControllerまたはCloud Connectorで接続を自動的に分散させます。フェイルオーバーおよび負荷分散機能は、Citrix Brokering Protocol（CBP）に組み込まれています。構成内で複数のControllerまたはCloud Connectorを指定する場合、登録では必要に応じてこれらのControllerまたはCloud Connector間で自動的にフェイルオーバーが行われます。自動更新を使用すると、すべてのVDAで自動フェイルオーバーが自動的に行われます。

セキュリティ上の理由から、NetScalerなどのネットワークロードバランサーは使用できません。VDA登録ではKerberos相互認証を使用しており、クライアント（VDA）はその身元をサービス（Controller）に対して証明する必要があります。また、ControllerまたはCloud Connectorはその身元をVDAに対して証明する必要があります。つまり、VDAとControllerまたはCloud Connectorは、サーバーであるのと同時にクライアントとしても動作するということです。本記事の初めに述べたように、通信チャネルには、VDAからController/Cloud ConnectorとController/Cloud ConnectorからVDAの2つが存在します。

このプロセスのコンポーネントはサービスプリンシパル名（SPN）と呼ばれ、Active Directoryコンピューターオブジェクトにプロパティとして格納されます。VDAは、ControllerまたはCloud Connectorに接続する場合、通信相手が「誰」かを指定する必要があります。このアドレスがSPNです。負荷分散IPを使用する場合、Kerberos相互認証では、このIPが目的のControllerまたはCloud Connectorに属していないことが適切に認識されます。

詳しくは、次のトピックを参照してください。

Kerberosの概要：https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/

Kerberosを使用した相互認証：https://msdn.microsoft.com/en-us/library/ms677600

CNAMEから自動更新への変更

自動更新機能は、バージョン7.x以前のXenAppおよびXenDesktopのCNAME（DNSエイリアス）機能に代わるものです。XenAppおよびXenDesktop 7以降では、CNAME機能は無効になっています。CNAMEの代わりに自動更新を使用してください（CNAMEを使用する必要がある場合はCTX137960を参照してください。DNSエイリアスの動作の一貫性を保つため、自動更新とCNAMEの両方を同時に使用しないでください）。

Controller/Cloud Connectorグループ

特定のシナリオでは、優先グループと、すべてのController/Cloud Connectorで障害が発生した場合のフェイルオーバーに使用する別のグループを用意して、ControllerまたはCloud Connectorをグループで処理できます。ControllerまたはCloud Connectorはリストからランダムに選択されるものであるため、グループ化すると優先的な使用を指定しやすくなります。

ControllerまたはCloud Connectorのグループを指定するにはかっこを使用します。たとえばControllerが4つ（主に使用するものが2つとバックアップ用が2つ）ある場合、次のようにグループ化します。

(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)。

この例では、最初のグループのController（001と002）が初めに処理されます。両方で障害が発生した場合、2番目のグループのController（003と004）が処理されます。

ListOfSIDs

© 1999-2017 Citrix Systems, Inc. All rights reserved.

登録時にVDAが通信可能なControllerをまとめたものがListOfDDCsです。VDAはどのControllerが信頼可能であるかも把握する必要があります。VDAは、ListOfDDCsに含まれているControllerを自動的に信頼するわけではありません。ListOfSIDs（セキュリティID）により、信頼可能なControllerが指定されます。VDAが登録を試みるのは、信頼されているControllerだけです。

ほとんどの環境では、ListOfSIDsはListOfDDCsから自動で作成されます。CDFトレースを使用してListOfSIDsを読み取ることができます。

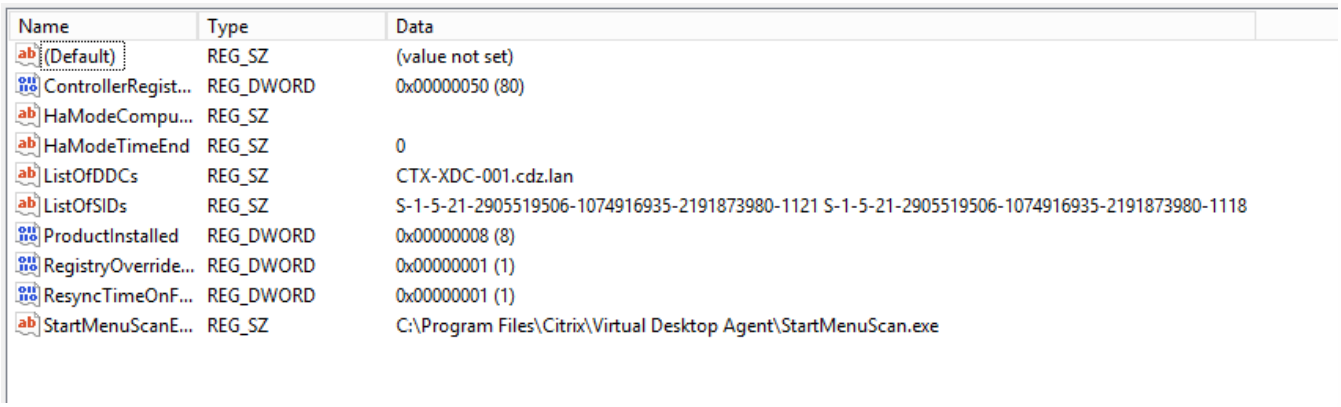
一般には、ListOfSIDsを手動で変更する必要はありません。ただし、いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが使用可能になったため有効ではなくなりました。

- **Controllerの役割の分離：**XenAppおよびXenDesktop 7.7でゾーンが導入される前は、登録にControllerのサブセットのみを使用する場合ListOfSIDsを手動で構成していました。たとえば、XDC-001とXDC-002をXMLブローカーとして使用し、XDC-003とXDC-004をVDA登録に使用する場合、ListOfSIDsにはすべてのControllerを指定し、ListOfDDCsにはXDC-003とXDC-004を指定していました。これは一般的でなく推奨される構成でもないため、新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directoryの負荷の削減：**XenAppおよびXenDesktop 7.6で自動更新機能が導入される前は、ドメインコントローラーに対する負荷を抑えるためにListOfSIDsを使用していました。ListOfSIDsを事前に指定しておくことで、DNS名からSIDへの解決を省略できていました。しかし、自動更新機能では永続キャッシュにSIDが含まれるようになったため、この作業を行う必要はなくなりました。自動更新機能は有効にしておくことをお勧めします。
- **セキュリティ：**高度なセキュリティで保護された環境では、侵害されたDNSサーバーからのセキュリティ上の脅威を防ぐために、信頼されているControllerのSIDを手動で構成していました。しかし、これを行う場合、自動更新機能を無効化する必要もあります。無効化しない場合、永続キャッシュの構成が使用されるためです。

このため、特別な理由がない限りListOfSIDsは変更しないでください。

ListOfSIDsを変更する必要がある場合は、HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgentの下にListOfSIDsという名前のレジストリキー（REG_SZ）を作成します。値には、信頼できるSIDの一覧を指定します。SIDが複数ある場合はスペースで区切って指定します。

次の例では、1つのControllerをVDAの登録に使用しますが（ListOfDDCs）、2つのControllerは仲介に使用します（ListOfSIDs）。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA登録の問題のトラブルシューティング

先に述べたように、仲介セッションを起動する場合、対象のDelivery ControllerにVDAが登録されている必要があります。VDAが登録されていないと、登録されていれば使用されるはずの資源が十分に活用されない可能性があります。VDAが登録されない場合がある理由にはさまざまなものがありますが、その多くは管理者がトラブルシューティングできます。Studioでは、カタログ作成ウィザード内で、およびカタログをデリバリーグループに登録した後に、トラブルシューティング情報が提供されます。

マシンカタログの作成時に問題を特定する：

カタログ作成ウィザードで既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージによって問題のあるマシンが特定された場合は、該当のマシンを（**[削除]** ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（Delivery Controllerで登録されたことがないなどの理由により）マシンに関する情報を取得できないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要な場合があります。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能がカタログで利用できるようになります。ただし、以前のVDAバージョンのカタログにあるマシンは登録できません。

デリバリーグループの作成後に問題を特定する：

デリバリーグループを作成すると、そのグループと関連付けられているマシンの詳細がStudioに表示されます。デリバリーグループの［詳細］ペインに、登録の必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードでないはないのに、Controllerに現在登録されていないマシンが1台または複数台存在することが考えられます。「未登録だが登録する必要がある」マシンが表示された場合は、［詳細］ペインの［トラブルシューティング］タブに、考えられる原因と推奨される修正アクションが示されます。

機能レベルについて詳しくは、「マシンカタログの作成」の「*VDAバージョンと機能レベル*」セクションを参照してください。

VDA登録に関するトラブルシューティングについて詳しくは、CTX136668を参照してください。

Citrix Health Assistantを使用して、VDA登録とセッションの開始に関するトラブルシューティングを行うことも可能です。詳しくは、CTX207624を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッション

Dec 05, 2017

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。ネットワークの信頼性が低い、通信速度が一定していない、ワイヤレスデバイスの伝送距離が制限されているなどの理由でネットワーク接続が失われると、ユーザーの労働意欲が損なわれます。ワークステーション間をすばやく移動でき、ログオンするたびに同じアプリケーションのセットにアクセスできることは、病院の医療スタッフなど多くのモバイルワーカーにとっての優先事項です。

以下の機能を使用すると、セッションの信頼性が最適化され、利便性が向上し、ダウンタイムの増加や生産性の低下を防ぐことができます。また、モバイルユーザーがデバイス間をすばやく移動できるようになります。

- セッション画面の保持
- クライアントの自動再接続
- ICA Keep Alive
- ワークスペースコントロール
- セッションローミング

「ログオン間隔」セクションでは、デフォルト設定の変更方法について説明します。

また、ユーザーのセッションからのログオフ、セッションの切断、およびセッションの事前起動と残留の構成も実行できます。「デリバリーグループの管理」を参照してください。

セッション画面の保持

セッション画面の保持機能は、ICAセッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に有用です。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、通常はセッションが切断され、セッションの画面が表示されなくなります。この場合、切断セッションに再接続されるまで、そのセッションでは何もできません。セッション画面の保持機能を有効にすると、データを損失することなくセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止し、カーソルの形が砂時計に変わるため、ユーザーにもネットワークが切断されていることがわかります。このとき、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

Citrix Receiverのユーザーには、Controller側の設定が自動的に適用されます。

セッション画面の保持機能と共に、TLS（Transport Layer Security）を使用できます。TLSはユーザーデバイスとNetScaler Gateway間で送信されるデータのみを暗号化します。

セッション画面の保持機能は、以下のポリシー設定で構成します。

- ［セッション画面の保持］設定により、セッション画面の保持を許可または禁止します。
- ［セッション画面の保持のタイムアウト］設定では、デフォルトのタイムアウト時間として180秒つまり3分が設定されています。この時間を長く設定することもできますが、この機能の本来の目的は、ネットワークから切断されたユーザーを再認証することなくセッションに再接続することにあるので注意が必要です。必要以上に長い時間を設定すると、接続の再開

© 1999-2017 Citrix Systems, Inc. All rights reserved.

を待ちきれないユーザーが席を離れてしまい、その間に不正なユーザーがセッションにアクセスしてしまう危険性があり
す。

- セッション画面の保持機能が有効な受信接続ではポート2598が使用されます。このポート番号はポリシーの［セッション画面の保持のポート番号］設定で変更できます。
- 切断したセッションに再接続するユーザーを再認証する場合は、クライアントの自動再接続機能を使用します。［クライアントの自動再接続時の認証］設定を構成して、中断されたセッションにユーザーが再接続するとき再認証を要求することができます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後でクライアントの自動再接続のポリシー設定が有効になり、切断セッションへの再接続が行われます。

クライアントの自動再接続

クライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションをCitrix Receiverが検出して、そのセッションに自動的に再接続します。この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。

アプリケーションセッションでは、Citrix Receiverは、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。

デスクトップセッションでは、Citrix Receiverは、指定された時間、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。デフォルトでは、この時間は5分です。この時間を変更するには、ユーザーデバイスで以下のレジストリを編集します。

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds、DWORD、

<*seconds*>は、セッションの再接続が試行されなくなるまでの秒数です。

クライアント自動再接続機能は、以下のポリシー設定で構成します。

- **クライアントの自動再接続**: 接続が中断した場合のCitrix Receiverによる自動再接続を有効または無効にします。
- **クライアントの自動再接続時の認証**: 自動再接続時にユーザーの認証を要求するかどうかを指定します。
- **クライアントの自動再接続のログ**: 再接続イベントのイベントログへの記録を有効または無効にします。ログ機能は、デフォルトで無効になっています。この機能を有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。再接続イベントのログは、サイト全体で記録されるのではなく、そのイベントが発生した個々のサーバーのシステムログに記録されます。

クライアントの自動再接続機能には、暗号化されたユーザー資格情報に基づく再認証メカニズムが使用されています。ユーザーが最初にログオンしたときに、サーバーにより暗号化されたユーザー資格情報がメモリに格納され、その暗号キーを含んだCookieがクライアント側に送信されます。Citrix Receiverは、再接続時にこのCookieをサーバーに送信します。サーバーは復号化した資格情報をWindowsのログオンプロセスに送信して認証を求めます。Cookieの有効期限が切れた場合、ユーザーに資格情報を再入力する必要があります。

［クライアントの自動再接続時の認証］設定を有効にする場合、Cookieは使用されません。その代わりに、切断セッションへの再接続時に、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

ユーザーの資格情報とセッションのセキュリティを最大限に保護するために、クライアントとサイトの間のすべての通信で暗号化機能を使用してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Receiver for Windowsで自動再接続機能を無効にするには、icaclient.admファイルを編集します。詳しくは、適切なバージョンのCitrix Receiver for Windowsのドキュメントを参照してください。

接続の設定も、クライアントの自動再接続機能に影響します。

- 前述のように、クライアントの自動再接続はポリシー設定のデフォルトによりサイト全体で有効になっています。ユーザーの再認証も不要です。ただし、サーバーでICA TCP接続が切断されたときにセッションをリセットするように設定すると、自動再接続は実行されません。クライアントの自動再接続は、エラーの発生またはタイムアウトによりサーバーがセッションを切断した場合にのみ実行されます。ここでのICA TCP接続とは、実際のネットワーク接続ではなく、TCP/IPネットワーク上のセッションで使用されるサーバーの仮想ポートを指します。
- サーバー上のICA TCP接続では、デフォルトでエラーやタイムアウトが発生した接続のセッションを切断するように設定されています。切断されたセッションはそのままシステムメモリに残るので、ユーザーは同じサーバーに自動的に再接続して、そのセッションでの作業を続行できます。
- エラーが生じたりタイムアウトしたりした接続のセッションについてはリセット、つまりログオフされるように構成することができます。セッションがリセットされた場合、再接続しようとすると、切断前の作業状態からセッションが復元されるのではなく、アプリケーションが再起動されて新しいセッションが開始されます。
- セッションがリセットされるようにサーバーが構成されている場合、クライアントの自動再接続により新しいセッションが開始されます。この場合、ユーザーが自分の資格情報を入力して、サーバーにログオンし直す必要があります。
- 外部からの侵入などによってクライアント側から正しくない認証情報が送信された場合、またはセッションの切断が検出されてから自動再接続までの時間が長すぎた場合は、自動再接続に失敗することがあります。

ICA Keep Alive

ICA Keep-Alive機能を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。この機能が有効な場合、セッションのアイドル状態（たとえばクロックデータの更新、マウス操作、画面更新などがない状態）が検出されたときに、リモートデスクトップサービスによりセッションが切断されることを防ぐことができます。サーバーは、定期的にKeep-Aliveパケットを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、サーバーにより「切断」状態として認識されます。

注： ICA Keep-Aliveは、セッション画面の保持機能を使用しない環境でのみ正しく動作します。セッション画面の保持機能では、ICA Keep-Aliveとは異なるメカニズムで切断セッションが管理されます。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Aliveを有効にしてください。

ここでのKeep-Alive機能の設定は、Windowsのグループポリシーによる同様の設定よりも優先されます。

ICA Keep-Alive機能は、以下のポリシー設定で構成します。

- **ICA Keep-Aliveタイムアウト**：ICA Keep-Aliveメッセージの送信間隔を1～3600秒の範囲で指定します。ただし、ネットワークの問題によるセッションの切断が少なく、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に閉じるように設定している環境では、このオプションを構成しないでください。
  デフォルト値は60秒で、サーバーからユーザーデバイスにICA Keep-Aliveパケットが60秒おきに送信されます。クライアントが60秒以内に応答しない場合、そのセッションは「切断」状態（タイムアウト）と認識されます。
- **ICA Keep-Alive**：ICA Keep-Aliveメッセージを送信するかどうかを指定します。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

上でそのデスクトップやアプリケーションでの作業を継続できます。これにより、ユーザーは自分のデスクトップや作業中のアプリケーションにどこからでもシームレスにアクセスできるようになります。たとえば、病院内の複数のワークステーション間を移動しながら、常に同じアプリケーションセットにアクセスしなければならない医療スタッフをサポートするために、この機能を利用できます。ワークスペースコントロールを構成すると、ユーザーは複数のアプリケーションを一度に切断して、その後で別のクライアントデバイスからそれらのアプリケーションに再接続できます。

ワークスペースコントロールを有効にすると、ユーザーの操作は以下のようになります。

- **ログオン：** デフォルトでは、ユーザーが移動先でログオンすると、実行されていたすべてのデスクトップおよびアプリケーションに自動的に再接続されます。デスクトップやアプリケーションを手作業で起動する必要はありません。デスクトップまたはアプリケーションのセッションがほかのクライアントデバイス上でアクティブな場合だけでなく、切断されている場合にも接続されます。ユーザーがデスクトップやアプリケーションとの接続を切断しても、サーバー上のセッションは終了しません。管理者は、ユーザーが切断したものだけが再接続されるように構成することもできます。これにより、移動先のクライアントデバイスを使ってユーザーが再ログオンしたときに、前のクライアントデバイスでアクティブデスクトップやアプリケーションには再接続されず、切断されているものだけが再接続されます。
- **再接続：** サーバーに再ログオンしたユーザーは、［再接続］をクリックすることで自分のデスクトップやアプリケーションに一度に再接続できます。デフォルトでは、切断されているデスクトップやアプリケーションと、ほかのクライアントデバイスでアクティブなデスクトップやアプリケーションが再接続されます。管理者は、切断されているデスクトップやアプリケーションだけが再接続されるように構成することもできます。
- **ログオフ：** ユーザーがStoreFront経由でデスクトップやアプリケーションにアクセスする場合に、［ログオフ］コマンドによりStoreFrontおよびすべてのアクティブセッションからログオフするのか、StoreFrontだけからログオフするのかを管理者が構成できます。
- **切断：** ユーザーは、実行中のすべてのデスクトップやアプリケーションを一度に切断できます。個々に切断する必要はありません。

ワークスペースコントロールは、Citrix ReceiverユーザーがCitrix StoreFront経由でデスクトップやアプリケーションにアクセスする場合にのみ使用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールが無効になり、ホストされたアプリケーションセッションでは有効になります。公開デスクトップ上で公開アプリケーションを実行する場合、デフォルトではこれらのセッションは共有されません。

ユーザーが別のクライアントデバイスに移動すると、ポリシー、クライアント側ドライブのマッピング、およびプリンターの設定が適切に変更されます。ポリシーとクライアント側ドライブのマッピングは、ユーザーがセッションにログオンするクライアントデバイスの条件に基づいて適用されます。たとえば、医療従事者が緊急治療室のクライアントデバイスからログオフして、レントゲン室のワークステーションにログオンして自分のワークスペースに再接続した場合は、レントゲン室でのセッションに適したポリシー、プリンターマッピング、およびクライアント側ドライブのマッピング設定がセッションの開始時に有効になります。

管理者は、ユーザーが場所を移動したときに使用可能になるプリンターをカスタマイズできます。また、ローカルプリンターでの印刷の可否やリモート接続時に使用される帯域幅などの印刷環境を制御することもできます。

ワークスペースコントロール機能を有効にして構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

デフォルトでは、ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。多くの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

このデフォルト動作には多数のメリットがありますが、すべてのケースで理想的であるわけではありません。PowerShell SDを使用して、セッションローミングを無効にすることができます。

例1：医療専門家が、2つのデバイスを使用しています。デスクトップPCでは保険用紙に入力し、タブレットでは患者情報を確認します。

- セッションローミングが有効な場合、両方のアプリケーションが両方のデバイスに表示されます（どちらかのデバイスで起動されたアプリケーションが、使用しているすべてのデバイスに表示されます）。これが、セキュリティ要件に準拠しない場合があります。
- セッションローミングを無効にすると、患者レコードはデスクトップPCには表示されず、保険用紙はタブレットには表示されません。

例2：生産管理者が、自分のオフィスにあるPCでアプリケーションを起動します。デバイスの名前と場所に基づいて、このセッションで使用できるプリンターやそのほかのリソースが決定されます。その日のうちに、生産管理者は隣の建物のオフィスに移動し、プリンターを使用する必要があるミーティングに出席します。

- セッションローミングが有効な場合、生産管理者は会議室の近くにあるプリンターを使用できない可能性があります。ミーティングより前に自分のオフィス内でアプリケーションを起動したため、オフィスの近くにあるプリンターやそのほかのリソースへの割り当てが行われているためです。
- セッションローミングが無効な場合、（同じ資格情報を使用して）別のマシンにログオンすると、新たなセッションが開始され、近くにあるプリンターやリソースを使用できるようになります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを含む以下の資格ポリシー規則コマンドレットを使用します。必要に応じて、「LeasingBehavior」プロパティも指定できます。後述の「接続リース機能およびセッションローミング」を参照してください。

デスクトップセッションの場合

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior
Allowed|Disallowed
```

アプリケーションセッションの場合

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior
Allowed|Disallowed
```

<*value*>には、次のうちいずれかを指定できます。

- **Always**：クライアントデバイスに関係なく、セッションが接続中でも、切断中でも、セッションローミングが常に実行されます。これがデフォルト値です。
- **DisconnectedOnly**： 既に切断されているセッションのみに再接続します。それ以外のセッションについては、新規セッションを開始します（最初に切断するか、ワークスペースコントロールを使用して明示的にローミングすることによって、クライアントデバイス間のセッションローミングを実行することができます）。別のクライアントデバイスからのアクティブな接続済みセッションは、使用されません。代わりに、新規セッションが開始されます。
- **SameEndpointOnly**： ユーザーが使用する各クライアントデバイスに対し、一意のセッションが割り当てられます。ローミングは、完全に無効になります。ユーザーは、セッションで過去に使用されたものと同じデバイスのみに再接続できます。

「LeasingBehavior」プロパティについては、後述の説明を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ほかの設定による影響

セッションローミングの無効化は、デリバリーグループにおけるアプリケーションのプロパティのアプリケーション制限「1ユーザーあたり1インスタンスのみ許可する」の影響を受けます。

- セッションローミングを無効にする場合、このアプリケーション制限も無効にします。
- このアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する2つの値は、どちらも設定しないでください。

接続リース機能とセッションローミング

接続リース機能に詳しくない場合は、「接続リース機能」を参照してください。

Controllerがリース接続モードに設定されると、セッション再接続がデフォルト値に戻り、ユーザーがデスクトップまたはアプリケーションのアクティブなセッションまたは切断されたセッションの1つのみに再接続されます。

デフォルト以外のセッションローミング値を設定し、複数のユーザーが複数のデバイスで同じログオン資格情報を共有している場合は、セキュリティを強化するため、そのユーザーアカウントが含まれるデリバリーグループにおいて接続リース機能を無効にすることを検討してください。

理由：このシナリオでは、1つのセッションがすべてのデバイスで共有されます。たとえば、Controllerがリース接続モードである間に、1人のユーザーが、同じ資格情報で再接続するほかのユーザーに見られることを意図していない機密情報を表示している場合、この状況は好ましくありません。

資格ポリシーで接続リース機能を無効にすることにより、この可能性が排除されます。ユーザーは、Controllerがリース接続モードであっても、同じログオン資格情報を使用する別のユーザーのセッションを表示することができなくなります。ほかの資格ポリシーは、影響を受けません。個別のユーザーアカウントで、個別の資格に基づいて接続リース機能を使用することができます。

資格ポリシーで接続リース機能を無効にするには、「LeasingBehavior Disallowed」プロパティを資格ポリシーコマンドレットに追加します。 接続リース機能を無効にする場合、既に作成され、該当する資格ポリシーに対してキャッシュされている起動リースを手動で削除する必要があります。削除しない場合、ユーザーは引き続き、データベースのダウン中に再接続できます。

ログオン間隔

デスクトップVDAがインストールされている仮想マシンが、ログオンプロセスが完了する前に終了する場合は、プロセスにより多くの時間を割り当てることができます。7.6以降のバージョンのデフォルトは180秒です（7.0～7.5は90秒です）。

マシン上（またはマシンカタログで使用されるマスターイメージ上）で、以下のレジストリキーを設定します。

キー：HKLM\SOFTWARE\Citrix\PortICA

値：AutoLogonTimeout

種類：DWORD

十進法時間（秒）を0～3600の範囲で指定します。

マスターイメージを変更する場合は、カタログを更新してください。

注： この設定は、デスクトップ（ワークステーション）のある仮想マシンにのみ適用されます。Microsoftの場合は、サー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

バーVDAのマシンでログオンタイムアウトが制御されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Studioでの検索の使用

Dec 05, 2017

検索 機能を使って、特定のマシン、セッション、マシン カタログ、アプリケーション、またはデリバリーグループに関する情報を表示します。

1. Studioのナビゲーションペインで ［検索］を選択します。
   注： ［マシン カタログ］タブや［デリバリー グループ］タブで［検索］ボックスを使用して検索できません。 ナビゲーションペインの［検索］ノードを使用してください。
   追加の検索条件を表示するには、［検索］ボックスの横にあるプラス記号をクリックします。 マイナス記号をクリックすると、その検索条件が削除されます。

2. 検索する項目の名前を入力するか、 ドロップダウンボックスの一覧からほかの 検索オプションを選択します。
3. 検索条件を保存するには、 ［名前を付けて保存］ をクリックします。保存済みの検索は、［保存済みの検索］の一覧に表示されます。

または、 矢印アイコン（二重下向き角かっこ）をクリックして検索プロパティのドロップダウン リストを表示します。このドロップダウンリストのプロパティで詳細な 検索式を作成できます。

高度な 検索を行うためのヒント：

- ［操作］ペインの ［列の選択］ を選択すると追加の検索特性を表示させることができ、その特性で検索結果を並べ替えることができます。
- マシンに接続しているユーザー デバイスを検索するには、［クライアント（IP）］および［次のもの］を指定してデバイスのIP アドレスを入力します。
- アクティブな セッションを検索するには、［セッション状態］、［次のもの］、および［接続済み］を指定します。
- 特定のデリバリーグループに含まれるすべてのマシンを一覧で表示するには、ナビゲーションペインで ［デリバリーグループ］ を選択し、グループを選択して、［操作］ペインの ［マシンの表示］ を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

タグ

Dec 05, 2017

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどといった項目を識別する文字列です。タグを作成して項目に追加すると、以下のように、特定の操作を指定されたタグのある項目のみに適用するように調整できます。

- Studioでの検索結果の表示を調整する。

  たとえば、テスターに最適化されているアプリケーションのみを表示するには、「テスト」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Studioの検索結果を「テスト」タグでフィルタリングできます。

- 選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループまたは特定のデスクトップからアプリケーションを公開する。これを*タグ制約機能*と呼びます。

  タグ制約で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制約は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。その機能は、7.xより前のリリースのXenAppワーカーグループに類似していますが、同一ではありません。

  タグ制約のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

  タグ制約の使用の詳細と例については、下記を参照してください。

- デリバリーグループ内のマシンのサブセットの定期再起動をスケジューリングする。

  マシンでタグ制約を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンのサブセットに対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」セクションの「デリバリーグループのマシンに対する再起動スケジュールの作成」を参照してください。

- デリバリーグループのマシンのサブセット、デリバリーグループの種類、指定されたタグを持つ（または持たない）OUへのCitrixポリシーの適用（割り当て）を調整する。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用するには、それらのマシンに「ハイパワー」という名前のタグを追加します。次に、ポリシーの作成ウィザードの **[ポリシーの割り当て]** ページで、そのタグを選択して **[有効化]** チェックボックスをオンにします。デリバリーグループにタグを追加し、そのデリバリーグループにCitrixポリシーを適用することもできます。 詳しくは、「ポリシーの作成」とこのブログ記事を参照してください（マシンにタグを追加するStudioインターフェイスがブログ記事の公開時から変更されていることに注意してください）。

次の項目にタグを適用できます。

- マシン
- アプリケーション
- デリバリーグループ
- アプリケーション グループ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

タグ制約は、Studioで次のものを作成または編集するときに構成できます。

- 共有デリバリーグループのデスクトップ
- アプリケーショングループ

デスクトップまたはアプリケーショングループのタグ制約

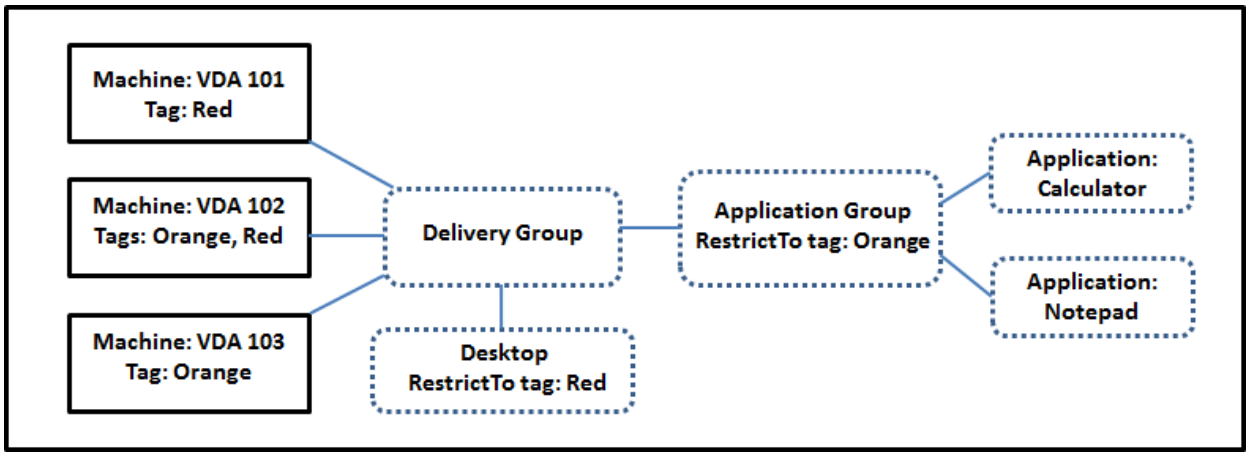
タグ制約には、いくつかの手順があります：

- タグを作成し、マシンに追加（適用）します。
- タグ制約を持つグループを作成または編集します（言い換えると、タグxを持つマシンに起動を制約します）。

タグ制約は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、関連するデリバリーグループから、アクセスポリシー、構成されたユーザーの一覧、ゾーン優先度、起動対応度、およびタグ制約（存在する場合）に従うマシンを選択します。適用では、ブローカーは優先度順に他のデリバリーグループにフォールバックし、関係する各デリバリーグループに同じマシン選択ルールを適用します。

例1

この例では、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグ制約を使用して制限する単純なレイアウトを紹介します。サイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



- 3台のマシン（VDA 101～103）それぞれにタグが追加されています。
- 共有デリバリーグループのデスクトップは「Red」という名前のタグ制約を付けて作成されているため、デリバリーグループの、「Red」という名前のタグを持つマシン（VDA 101および102）上でのみ起動できます。
- アプリケーショングループは「Orange」のタグ制約で作成されているので、各アプリケーション（計算機とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン（VDA 102および103）上でのみ起動できます。

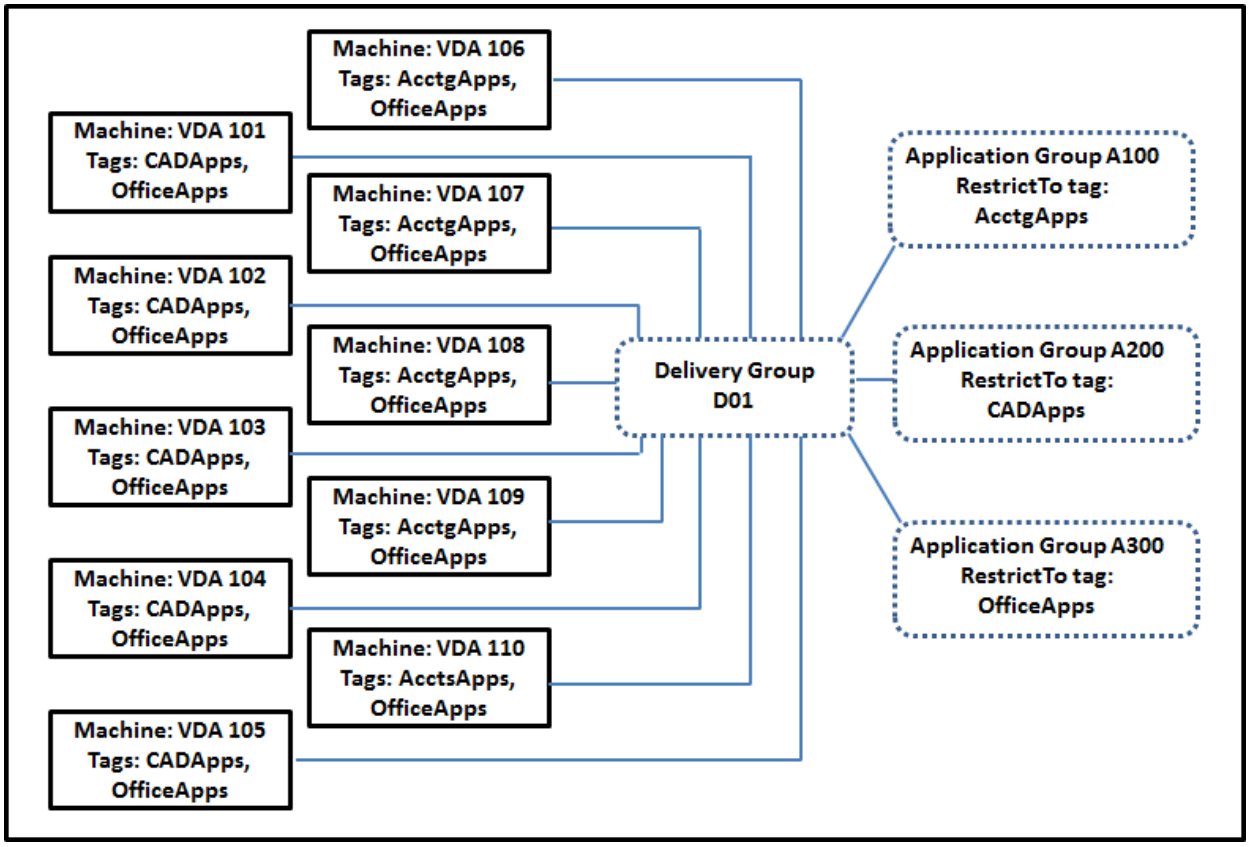
マシンVDA 102が両方のタグ（RedおよびOrange）を持っており、したがってアプリケーションとデスクトップの起動に関与できる点に注意してください。

例2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

この例には、タグ制約付きで作成された複数のアプリケーショングループが含まれます。これにより、デリバリーグループのみを使用する場合に必要な数より少ないマシンでより多くのアプリケーションを提供できます

（「例2を構成する方法」のセクションでは、タグを作成、適用し、この例のタグ制約を構成するために使用される手順を示します）。



この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各アプリケーショングループの作成時に、各マシンにタグを適用し、タグ制約を指定することにより、以下のことが可能です。

- グループ内の会計ユーザーは、5台のマシン（VDA 101～105）上で、必要なアプリにアクセスできます。
- グループ内のCADデザイナーは、5台のマシン（VDA 106～110）上で、必要なアプリにアクセスできます。
- Officeアプリケーションを必要とするグループのユーザーは、10台のマシン（VDA 101～110）上で、Officeアプリにアクセスできます。

1つのデリバリーグループで、10台のマシンのみが使用されています。1台のマシンは1つのデリバリーグループにのみ属することができるので、デリバリーグループのみを使用する場合は（アプリケーショングループ不使用時）、2倍のマシンが必要になります。

タグとタグ制約の管理

タグは、Studioの［**タグの管理**］アクションを介して、選択された項目から作成、追加（適用）、編集、および削除されます。

例外： ポリシー割り当てのために使用されるタグは、Studioの［**タグの管理**］アクションを介して作成、編集、削除さ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

れます。ただし、タグが適用される（割り当てられる）のはポリシーの作成時です。詳しくは「ポリシーの作成」を参照してください。

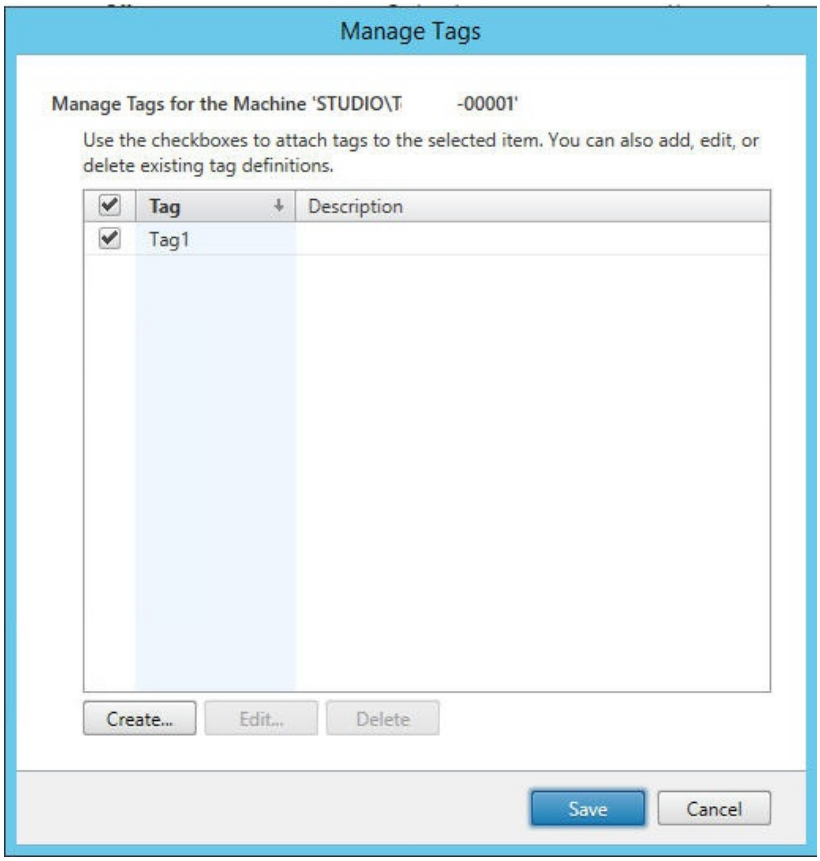
タグ制約は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。グループの作成と編集について詳しくは、次の記事を参照してください。

- デリバリーグループの作成
- デリバリーグループの管理
- アプリケーショングループの作成
- アプリケーショングループの管理

Studioでの［タグの管理］ダイアログの使用

Studioでタグを適用する項目（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、［操作］ペインの**［タグの管理］**を選択します。［タグの管理］ダイアログボックスに、選択した項目のタグだけでなく、サイトで作成されたすべてのタグが表示されます。

- チェックマークが付いているチェックボックスは、タグが選択した項目に既に追加されていることを表します（下の画面キャプチャで、選択されたマシンには「Tag1」という名前のタグが適用されています）。
- 複数の項目を選択した場合、ハイフンを含むチェックボックスは、一部の項目（すべての項目ではない）にそのタグが追加されていることを表します。



［タグの管理］ダイアログボックスでは、以下の操作を実行できます。注意のセクションを確認してください。

タグを作成するには：

［作成］をクリックします。名前と説明を入力します。タグの名前は一意でなければならず、大文字と小文字は区別さ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

れません。 **[OK]** をクリックします。（タグを作成しても、選択している項目に自動的に適用されることはありません。チェックボックスを使用してタグを適用します。）

1つまたは複数のタグを追加（適用）するには：

タグ名の隣にあるチェックボックスをオンにします。**注：** 複数の項目を選択し、タグの隣のチェックボックスにハイフンが付いている場合（選択された項目の一部（すべてではない）に、タグが既に適用されていることを示す）、それをチェックマークにすると、選択されているすべてのマシンに影響が及びます。

1つまたは複数のマシンにタグを追加しようとしていて、そのタグが現在アプリケーショングループの制約として使用されている場合、その操作により、それらのマシンが起動対象になることがあるという警告が表示されます。それが意図どおりであれば続行します。

1つまたは複数のタグを削除するには：

タグ名の隣にあるチェックボックスをオフにします。**注：** 複数の項目を選択し、タグの隣のチェックボックスにハイフンが付いている場合（選択された項目の一部（すべてではない）に、タグが既に適用されていることを示す）、チェックボックスをオフにすると、選択されているすべてのマシンからタグが削除されます。

タグを制約として使用しているマシンからそのタグを削除しようとすると、起動対象となるマシンに影響を与える場合があるという警告メッセージが表示されます。それが意図どおりであれば続行します。

タグを編集するには：

タグを選択し、 **[編集]** をクリックします。新しい名前や説明を入力します。同時に編集できるタグは1つのみです。

1つまたは複数のタグを削除するには：

タグを選択し、 **[削除]** をクリックします。 ［タグの削除］ダイアログボックスに、選択したタグを現在使用している項目の数が表示されます（「2台のマシン」など）。項目をクリックすると、詳細が表示されます。たとえば、［2台のマシン］という項目をクリックすると、そのタグを適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

Studioを使用して、制約として使用されているタグを削除することはできません。先にアプリケーショングループを編集してから、タグ制約を削除するか、異なるタグを選択する必要があります。

［タグの管理］ダイアログボックスの操作を終了したら、 **[保存]** をクリックします。

ヒント： マシンにタグが適用されているかどうかを確認するには：

ナビゲーションペインで **[デリバリーグループ]** を選択します。中央ペインでデリバリーグループを選択して、［操作］ペインの **[マシンの表示]** を選択します。中央のペインでマシンを選択し、下の［詳細］ペインで［タグ］タブを選択します。

タグ制約の管理

タグ制約の構成は複数の手順があるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制約を追加します。

タグの作成と適用：

タグを作成し、上で説明した **[タグの管理]** アクションを使用して、タグ制約の対象となるマシンに追加（適用）します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーショングループにタグ制約を追加するには：

アプリケーショングループを作成または編集します。［デリバリーグループ］ページで、**[次のタグを持つマシンに起動を制約する：]** を選択し、ドロップダウンからタグを選択します。

アプリケーショングループのタグ制約を変更または削除するには：

グループを編集します。［デリバリーグループ］ページで、異なるタグをドロップダウンから選択するか、**[次のタグを持つマシンに起動を制約する：]** をオフにして、タグ制約を完全に削除します。

デスクトップにタグ制約を追加するには：

デリバリーグループの作成または編集［デスクトップ］ページで**[追加]** または **[編集]** をクリックします。［デスクトップの追加］ダイアログボックスで、 **[次のタグを持つマシンに起動を制約する：]** を選択し、ドロップダウンからタグを選択します。

デリバリーグループのタグ制約を変更または削除するには：

グループを編集します。デスクトップのページで、**[編集]** をクリックします。ダイアログボックスで、異なるタグをドロップダウンから選択するか、 **[次のタグを持つマシンに起動を制約する：]** をオフにして、タグ制約を完全に削除します。

タグを項目に追加または削除する場合の注意事項

項目に適用されるタグはさまざまな目的に使用できるため、タグの追加や削除が意図しない結果になる可能性があることに注意してください。タグを使用してStudio検索フィールドのマシン表示を並べ替えることができます。アプリケーショングループまたはデスクトップの構成時に同じタグを制約として使用すると、そのタグが付いている指定されたデリバリーグループのマシンだけに起動対象を制限できます。

タグがデスクトップまたはアプリケーショングループのタグ制約として構成されている場合に1つまたは複数のマシンにタグを追加しようとすると、それらのマシンでその他のアプリケーションやデスクトップの起動が可能になることがあるという警告が表示されます。それが意図どおりであれば続行します。そうでない場合は、操作を取り消すこともできます。

たとえば、「Red」というタグ制約を持つアプリケーショングループを作成するとします。後から、そのアプリケーショングループによって使用される同じデリバリーグループに、他のマシンをいくつか追加します。それらのマシンに「Red」というタグを追加すると、おおむね次のようなメッセージが表示されます：「タグ「Red」は、次のアプリケーショングループ上の制約として使用されています。このタグを追加すると、選択されたマシンからこのアプリケーショングループのアプリケーションが起動可能になる可能性があります」。 次に、それらの追加のマシンへのそのタグの追加を確認またはキャンセルできます。

同様に、アプリケーショングループで起動を制限するためにタグが使用されている場合、グループを編集してタグ制約を削除するまで、そのタグを削除できないという警告が表示されます（アプリケーショングループの制約として使用されているタグの削除を許可されている場合、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動を許可することになる可能性があります）。デスクトップ起動の制約として現在タグが使用されている場合も、タグの削除は同様に不可能です。アプリケーショングループまたはデリバリーグループ内のデスクトップを編集してタグ制約を削除すれば、タグを削除できます。

すべてのマシンが同一セットのアプリケーションを持つとは限りません。1人のユーザーが、それぞれ異なるタグ制約を持ち、デリバリーグループのマシン構成が異なるか重なり合っている複数のアプリケーショングループに属する場合があります。次の表に、対象マシンがどのように決まるかを示します。

アプリケーションの追加先	選択したデリバリーグループ内で起動対象となるマシン

© 1999-2017 Citrix Systems, Inc. All rights reserved.

タグ制約を持たない1つのアプリケーショングループ	すべてのマシン
タグ制約Aを持つ1つのアプリケーショングループ	タグAが適用されているマシン
2つのアプリケーショングループ。タグ制約Aを持つグループとタグ制約Bを持つグループ	タグAとタグBを持っているマシン。存在しない場合、タグAまたはタグBを持っているマシン
2つのアプリケーショングループ。タグ制約Aを持つグループとタグ制約を持たないグループ	タグAを持つマシン。存在しない場合、すべてのマシン

マシン再起動スケジュールでタグ制約を使用している場合、タグ適用またはタグ制約に影響する変更はすべて、次のマシン再起動サイクルに影響を与えます。変更の実行中に進行している再起動サイクルには影響しません（「デリバリーグループの管理」を参照してください）。

例2を構成する方法

次の手順は、タグを作成、適用し、上の2番目の例で示したアプリケーショングループのためにタグ制約を構成する方法を示しています。

VDAとアプリケーションはマシンに既にインストール済み、デリバリーグループは作成済みです。

マシンにタグを作成し、適用します：

1. Studioでデリバリーグループ D01を選択し、［操作］ペインの **[マシンの表示]** を選択します。
2. マシンVDA 101～105を選択して、［操作］ペインの **[タグの管理]** を選択します。
3. ［タグの管理］ダイアログボックスで **[作成]** をクリックし、CADAppsという名前のタグを作成します。 **[OK]** をクリックします。
4. **[作成]** を再びクリックして、OfficeAppsという名前のタグを作成します。 **[OK]** をクリックします。
5. ［タグの管理］ダイアログボックスで、各タグ名（CADAppsおよびOfficeApps）の隣にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）し、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択して、［操作］ペインの **[マシンの表示]** を選択します。
7. マシンVDA 106～110を選択して、［操作］ペインの **[タグの管理]** を選択します。
8. ［タグの管理］ダイアログボックスで **[作成]** をクリックし、AcctgAppsという名前のタグを作成します。 **[OK]** をクリックします。
9. 各タグ名の隣にあるチェックボックスをオンにして、新しく作成したAcctgAppsタグとOfficeAppsタグを選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制約を持つアプリケーショングループを作成します。

1. Studioのナビゲーションペインで **[アプリケーション]** を選択し、次に［操作］ペインで **[アプリケーショングループの作成]** を選択します。アプリケーショングループの作成ウィザードが起動します。
2. ウィザードの **[デリバリーグループ]** ページでデリバリーグループD01を選択します。 **[次のタグを持つマシンに起動を制約する：]** を選択し、ドロップダウンからAcctgAppsタグを選択します。
3. 会計ユーザーと会計アプリケーションを指定して、ウィザードを完了します（アプリケーションを追加する場合は「［スタート］メニューから」のソースを選択すると、AcctgAppsタグの付いたマシン上のアプリケーションが検索されます）。 **[概要]** ページで、グループA100に名前を付けます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 前の手順を繰り返してアプリケーショングループA200を作成して、CADAppsタグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。
5. 手順を繰り返してアプリケーショングループA300を作成して、OfficeAppsタグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。

詳細情報の表示

ブログ記事：デスクトップを特定のサーバーに割り当てる方法（英語）。この記事には次のビデオも含まれています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IPv4/IPv6サポート

Dec 05, 2017

このリリースでは、 IPv4のみまたはIPv6のみ（ピュアIPv4またはピュアIPv6）の環境がサポートされ、重複するIPv4とIPv6の
ネットワークを使用した「デュアルスタック」環境がサポートされます。

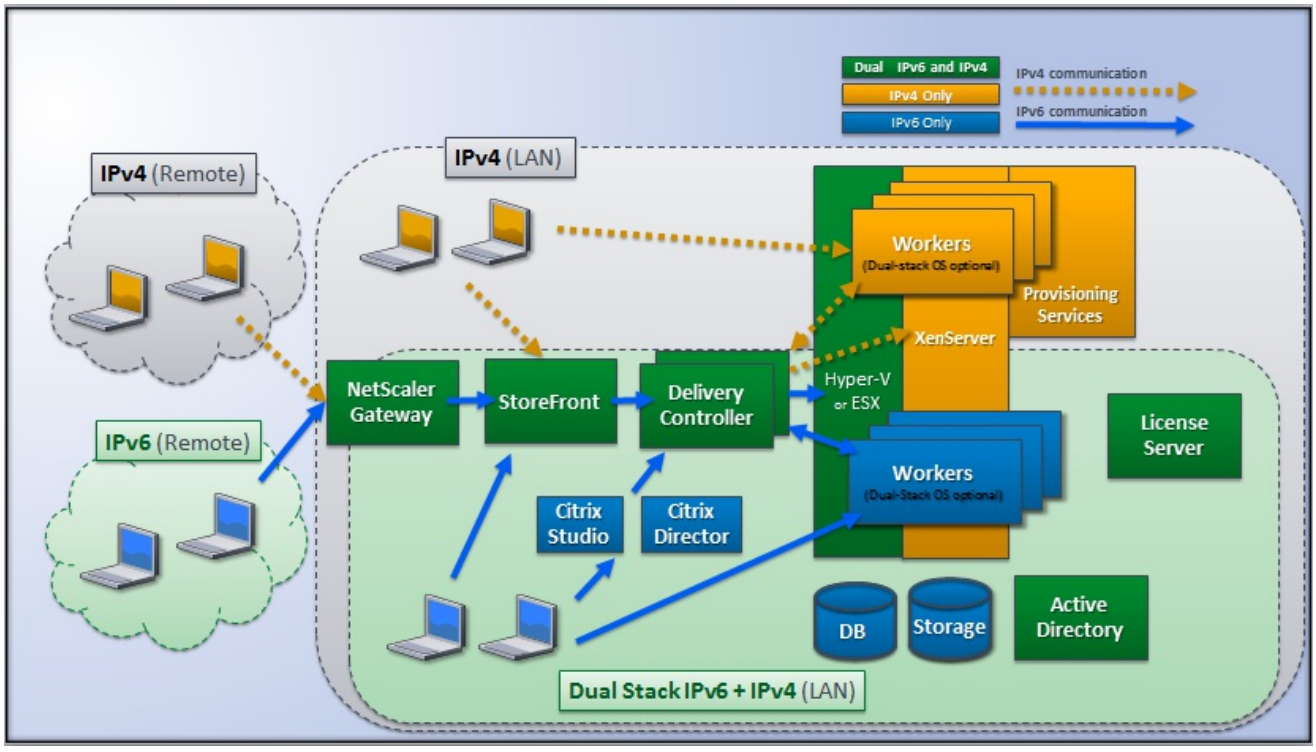
IPv6通信は、 Virtual Delivery Agent（VDA）接続関連の2つのCitrixポリシー設定で制御されます。

- IPv6を強制的に使用するプライマリ設定 ： IPv6コントローラー登録のみを使用します。
- IPv6ネットマスクを定義する従属設定： コントローラー登録のIPv6ネットマスク。

［IPv6 Controller登録のみを使用する］設定を有効にすると、VDAはIPv6アドレスで接続を受信するように Delivery Controller
に登録されます。

デュアルスタックIPv4/IPv6展開

次の図は、デュアルスタックIPv4/IPv6展開を示しています。このシナリオで、「ワーカー」とはハイパーバイザーまたは物
理システム上にインストールされたVDAを指し、主にアプリケーションやデスクトップへの接続を可能にするために使用され
ます。デュアルIPv6およびIPv4をサポートするコンポーネントは、トンネリングまたはデュアルプロトコルソフトウェアを使
用するオペレーティングシステム上で実行されます。



次のCitrix製品、コンポーネント、および機能ではIPv4のみがサポートされます。

- Provisioning Services
- XenServer 6.x
- **［IPv6 Controller登録のみを使用する］**ポリシー設定が適用されないVDA
- Version 7.5よりも古いバージョンのXenApp、Version 7よりも古いバージョンのXenDesktop、およびDirector

© 1999-2017 Citrix Systems, Inc. All rights reserved.

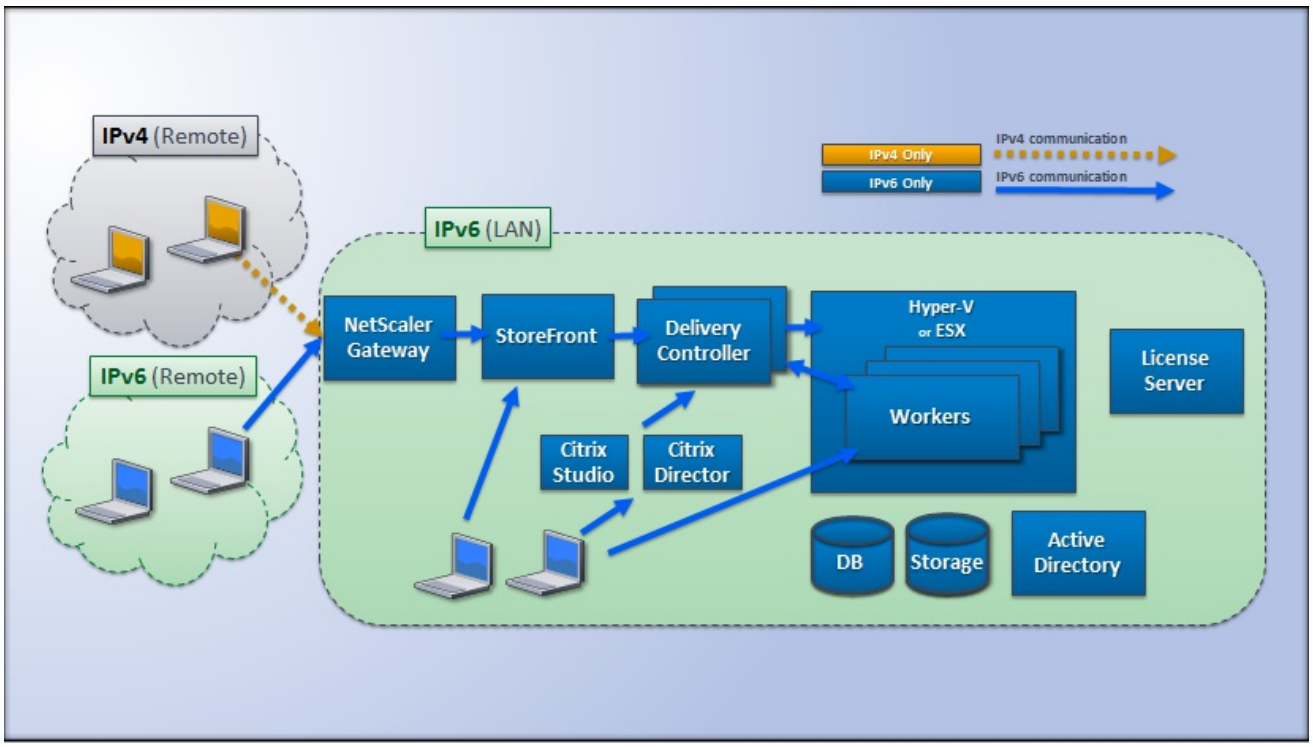
この展開は、以下のように管理されます。

- ユーザーによるIPv6ネットワークの使用頻度が高く、管理者がユーザーにIPv6トラフィックの使用を求める場合、管理者はプライマリのIPv6ポリシー設定（つまり［IPv6 Controller登録のみを使用する］）が有効な組織単位（OU）またはワーカーイメージを使用してIPv6デスクトップとアプリケーションを公開します。
- ユーザーによるIPv4ネットワークの使用頻度が高い場合、管理者はプライマリのIPv6ポリシー設定（つまり［IPv6 Controller登録のみを使用する］）が無効（デフォルト）なOUまたはワーカーイメージを使用してIPv4デスクトップとアプリケーションを公開します。

ピュアIPv6展開

次の図は、ピュアIPv6展開を示しています。このシナリオの内容は以下のとおりです。

- 各コンポーネントは、IPv6ネットワークのサポートが構成されたオペレーティングシステム上で実行されている。
- すべてのVDAに対してプライマリのIPv6ポリシー設定（［IPv6 Controller登録のみを使用する］）が有効になっている。つまり、VDAをIPv6アドレスを使ってControllerに登録する必要がある。



IPv6用のポリシー設定

Citrixポリシーには、ピュアIPv6環境やIPv4/IPv6デュアルスタック環境をサポートするための2つのポリシー設定があります。次の接続関連ポリシーを構成します。

- **IPv6コントローラー登録のみを使用する：**Delivery Controller登録でVirtual Delivery Agent（VDA）により使用されるアドレスの形式を制御します。デフォルトでは、無効に設定されています。
  - VDAがControllerと通信を行うときに、グローバルIPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（ほかのIPv6アドレスを使用できない場合のみ）の順で単一のIPv6アドレスが選択されます。
  - この設定が無効な場合、そのマシンのIPv4アドレスを使用してVDAがControllerと登録および通信を行います。
- **コントローラー登録のIPv6ネットマスク：**1つのマシンが複数のIPv6アドレスを保持することがあります。このポリシー設定では、VDAで使用されるサブネットを指定できます。この場合、グローバルIPは使用されません。これにより、VDAが登録するネットワークが、指定されたネットマスクに最初にマッチしたアドレスのみに限定されます。この設定項目を使用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

する場合は、［IPv6 Controller登録のみを使用する］設定を有効にする必要があります。デフォルトでは空文字が設定されています。

重要： これらの設定項目によってのみ、VDAで使用されるアドレスの形式（IPv4またはIPv6）が決定されます。つまり、VDでIPv6アドレスが使用されるようにするには、**［IPv6 Controller登録のみを使用する］**設定を有効にしたポリシーを適用する必要があります。

展開 に関する考慮事項

環境内に IPv4とIPv6の両方のネットワークがある場合、 IPv4のみのクライアントと IPv6ネットワークにアクセスできるクライアントに対して、別個のデリバリーグループ構成が必要です。ユーザーを区別するために、名前付け、手動Active Directoryグループ割り当て、 またはSmartAccessフィルターの使用を検討してください。

IPv6ネットワークで接続されたセッションにIPv4 アクセスのみの内部クライアントから 再接続する場合、 再接続に失敗することがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザープロファイル

Dec 05, 2017

デフォルトでは、マスターイメージ上にVirtual Delivery Agentをインストールするときに Citrix Profile managementが自動的にインストールされます。ただし、プロファイル管理ツールとしてこのコンポーネントを常に使用しなければならないということではありません。

ユーザーのニーズに応じてXenApp/XenDesktopポリシーを構成して、各デリバリーグループ内のマシンに異なるプロファイル処理を適用できます。たとえば、あるデリバリーグループではネットワーク上の特定の場所にテンプレートが格納されるCitrix固定プロファイルを使用して、別のデリバリーグループではいくつかのリダイレクトフォルダーと共に別の場所に格納されるCitrix移動プロファイルを使用するポリシーを構成できます。

- 組織内のほかの管理者がXenApp/XenDesktopポリシーを管理する場合は、すべてのデリバリーグループにプロファイル関連のポリシーが正しく適用されるように共同で作業する必要があります。
- Profile managementポリシーは、グループポリシーやProfile managementのINIファイルで設定したり、各仮想マシン上でローカルに設定したりできます。これらの設定は、以下の順に読み取られます。
  1. グループポリシー（ADMまたはADMXファイル）
  2. ［ポリシー］ノードのXenApp/XenDesktopポリシー
  3. ユーザーが接続する仮想マシン上のローカルポリシー
  4. Profile managementのINIファイル

  たとえば、グループポリシーと［ポリシー］ノードの両方で同じポリシーを構成する場合、グループポリシーのポリシー設定が適用され、XenApp/XenDesktopポリシー設定は無視されます。

いずれのプロフィル処理でも、Director管理者はユーザープロファイルの診断情報にアクセスしたりトラブルシューティングを行ったりできます。詳しくは、Directorのドキュメントを参照してください。

Personal vDisk機能を使用する場合、Citrixユーザープロファイルはデフォルトで仮想デスクトップのPersonal vDiskに格納されます。Personal vDiskにコピーが残っている間は、ユーザーストア内のプロファイルのコピーを削除しないでください。これを削除するとProfile managementでエラーが発生し、仮想デスクトップへのログオンに一時プロファイルが使用されることになります。

自動 構成

デスクトップの種類は、インストールされているVirtual Delivery Agentに基づいて 自動的に検出され、 それに応じてStudioでの構成オプションやProfile managementのデフォルトの動作が設定されます。

Profile managementで設定されるポリシーは、以下の表のとおりです。ポリシーの非デフォルトの 設定は保持され、この機能で上書きされることはありません。各ポリシーについて詳しくは、 Profile managementのドキュメントを参照してください。プロファイルを作成する マシンの種類により、調整されるポリシーが異なります。 最初の要因は、マシンの種類が固定なのかプロビジョニングなのかという点です。次の要因は、 それが複数のユーザーによって共有されるのか特定のユーザーに専用のものなのかという点です。

固定システムには ある種のローカル記憶域が備わっていて、 システムの電源がオフになってもシステムの内容を維持することができます。固定システムでは、ローカルディスク として記憶域ネットワーク（SAN）のような記憶域 テクノロジを使用できます。これと対照的に、プロビジョニングシステムは 基本ディスクとある種のIDディスクから「オンザフライ」で作成されます。通常、 RAMディスク または ネットワーク ディスクがローカル記憶域として使用され、ネットワークディスクはしばしば高速リンクのSANによって提供されます。 プロビジョニングテクノロジとは、一般的にProvisioning ServicesまたはMachine Creation Services（またはサードパーティの同等物）を指します。場合により、プロビジョニングされたシステムが Personal vDiskによって提供される 固定ローカルストレージを伴うことがあります。この場合は固定システムとして 分類されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

これらの2つの 要因により、以下の種類のマシンが定義されます。

- **固定かつ 専用** — Machine Creation Servicesで作成されるデスクトップOSマシンで、Personal vDiskを持ち静的に割り当てられるもの、VDI-in-a-Boxで作成されるデスクトップで、Personal vDiskを持つもの、物理的ワークステーション、およびラップトップコンピューターなど。
- **固定かつ共有** — Machine Creation Servicesで作成されるサーバーOSマシンなど。
- **プロビジョニングかつ 専用** — Provisioning Servicesで作成されるデスクトップOSマシンで、Personal vDiskを持たずに静的に割り当てられるものなど。
- **プロビジョニングかつ 共有** — Provisioning Servicesで作成されるデスクトップOSマシンで、ランダムに割り当てられるもの、VDI-in-a-Boxで作成されるデスクトップで、Personal vDiskを持たないものなど。

次の表は、各種類の マシンに適した Profile managementポリシー設定を示しています。通常、これらの設定は効果的ですが、 必要に応じて変更した方がよい場合もあります。

重要： ［ログオフ時にローカルでキャッシュしたプロファイルの削除］、 ［プロファイル ストリーム配信］、および ［常時キャッシュ］は自動構成機能により設定されます。 ほかのポリシー設定は、必要に応じて手作業で変更してください。

固定のマシン

ポリシー	固定かつ専用	固定かつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	有効
プロファイルストリーム配信	無効	有効
常時キャッシュ	有効（注1）	無効（注2）
アクティブライトバック	無効	無効（注3）
ローカル管理者のログオン処理	有効	無効（注4）

プロビジョニングされたマシン

ポリシー	プロビジョニングかつ専用	プロビジョニングかつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効（注5）	有効
プロファイルストリーム配信	有効	有効
常時キャッシュ	無効（注6）	無効
アクティブライトバック	有効	有効
ローカル管理者のログオン処理	有効	有効（注7）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ポリシー	プロビジョニングかつ専用	プロビジョニングかつ共有

1. このマシンの種類では ［プロファイルストリーム配信］ が無効なため、 ［常時 キャッシュ］設定は常に無視されます。
2. ［常時 キャッシュ］は無効にします。ただし、このポリシー設定を有効にして制限サイズ（MB）を指定すると、ログオン後すぐにサイズの大きなファイルが プロファイルにロードされるようになります。 制限サイズ以上のすべてのファイルは、 すぐにローカルにキャッシュされます。
3. ［アクティブ ライトバック］は無効にします。ただし、XenAppサーバー間を移動するユーザーのプロファイルの変更を保存する場合は、 このポリシー設定を有効にします。
4. ［ローカル管理者の ログオン処理］は無効にします。ただし、ホスト共有デスクトップの場合は、 このポリシー設定を有効にします。
5. ［ログオフ時に ローカルでキャッシュしたプロファイルの削除］は無効にします。これにより、ローカルにキャッシュされた プロファイルが保持されます。各マシンが 個々のユーザーに割り当てられているため、ログオフ時にマシンがリセットされても、プロファイルのキャッシュによりすばやくログオンできるようになります。
6. ［常時 キャッシュ］は無効にします。ただし、このポリシー設定を有効にして制限サイズ（MB）を指定すると、ログオン後すぐにサイズの大きなファイルが プロファイルにロードされるようになります。 制限サイズ以上のすべてのファイルは、 すぐにローカルにキャッシュされます。
7. ［ローカル管理者の ログオン処理］は有効にします。ただし、XenApp/XenDesktopサーバー間を移動するユーザーのプロファイルに対しては、 このポリシー設定を無効にします。

フォルダー リダイレクト

フォルダーリダイレクトを有効にすると、ユーザーデータをユーザー プロファイルとは異なるネットワーク共有上に 格納できます。これにより、プロファイルのサイズが小さくなるため短時間でロードされるようになりますが、 ネットワーク帯域幅が消費されます。フォルダーリダイレクト機能では、Citrixユーザー プロファイルを使用する必要はありません。管理者は独自にユーザーのプロファイルを管理して、 フォルダーをリダイレクトできます。

フォルダー リダイレクトを構成するには、StudioでCitrixポリシーを使用します。

- フォルダーのリダイレクト先の ネットワーク共有が使用可能であり、 適切なアクセス権が設定されていることを確認します。リダイレクト先のプロパティは自動的に 検証されます。
- リダイレクト先の ネットワーク共有をセットアップすると、ユーザーの次回 ログオン時にプロファイルがリダイレクトされます。

注： フォルダーリダイレクト機能は、CitrixポリシーまたはActive Directoryグループポリシー オブジェクトのいずれか一方を使用して構成してください。両方のポリシーエンジンを使用すると、 予期しない問題が発生することがあります。

詳細なフォルダー リダイレクト

複数のオペレーティングシステムが混在する展開環境では、ユーザープロファイルの一部が すべてのオペレーティングシステムで共有されるように構成できます。プロファイルの残りの部分は共有されず、 単一のオペレーティングシステムでのみ使用されます。 異なるオペレーティングシステム上で一貫したユーザーエクスペリエンスを提供するには、オペレーティングシステムごとに異なる構成が必要です。これを 詳細なフォルダー リダイレクトと呼びます。たとえば、 2つのオペレーティングシステム上で使用される異なるバージョンのアプリケーションで共通のファイルがロードされるようにするには、そのファイルをネットワーク上の単一の場所にリダイレクトします。 また、 ［スタートメニュー］フォルダーの構造が 2つのオペレーティングシステムで異なる場合は、どちらか一方のオペレーティングシステムのフォルダーのみがリダイレクトされるように設定できます。これにより、 各オペレーティングシステムでこのフォルダーおよびその内容が分離され、ユーザーに 一貫したエクスペリエンスを提供できます。

詳細なフォルダーリダイレクトを使用する場合は、 ユーザープロファイル内のデータ構造を理解して、どの部分をオペレーティングシステム間で共有できるかを確認する 必要があります。 これは、フォルダー リダイレクトによる予期せぬ問題の発生を避けるために重要です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

詳細なフォルダーリダイレクトを使用するには、 以下のタスクを行います。

- 各オペレーティングシステムで異なる デリバリーグループを使用します。
- 配信する 仮想アプリケーション（仮想デスクトップ上のものを含む）がユーザーのデータや 設定をどこに格納するか、およびそのデータ構造を確認します。
- 移動可能な共有 プロファイルデータ（異なる オペレーティングシステムでも構造が同じデータ）を含んでいるフォルダーを、各デリバリーグループでリダイレクトされるように設定します。
- 共有できない プロファイルデータについては、1つの デリバリーグループでのみリダイレクトされるように設定します。常、使用頻度の高いオペレーティングシステムやより 実用的なデータのデリバリーグループでリダイレクトを設定します。または、共有できないプロファイルデータを含んでいるフォルダーを、 オペレーティングシステムごとに異なる ネットワーク共有にリダイレクトすることもできます。

詳細な フォルダーリダイレクトの例 - この例では、Windows 8 と Windows Server 2008で異なるバージョンの Microsoft OutlookとInternet Explorerがインストールされている場合について説明します。これら2つのオペレーティングシステム用に2つの デリバリーグループをセットアップします。ユーザーがこれらのアプリケーションで共通の「アドレス帳」 と「お気に入り」にアクセスできるようにするには、詳細なフォルダーリダイレクトを以下のように構成します。
重要： ここで説明する内容は、上記のオペレーティングシステムおよび 配信環境での例であり、実際の環境ではさまざまな要因によりフォルダー構造が異なる場合があります。

- これらのデリバリーグループに適用するポリシーで、以下のフォルダーをリダイレクトします。

フォルダー	Windows 8でのリダイレクト	Windows Server 2008でのリダイレクト
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイ ミュージック	はい	はい
マイ ピクチャ	はい	はい
マイ ビデオ	はい	はい
検索	はい	いいえ
保存したゲーム	いいえ	いいえ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

フォルダー	Windows 8でのリダイレクト	Windows Server 2008でのリダイレクト
スタートメニュー	はい	いいえ

- オペレーティングシステム間で共有される フォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「アドレス帳」フォルダー と「お気に入り」フォルダーのリダイレクトを設定する前に、異なるバージョンのOutlook とInternet Explorerでユーザーデータのフォルダー構造を 確認してください。
  - 「マイドキュメント」、「マイミュージック」、「マイピクチャ」、および「マイビデオ」の各フォルダーの 構造はこれらのオペレーティングシステムで共通なので、 両方のデリバリーグループで同じネットワーク 共有にリダイレクトできます。
- オペレーティングシステム間で 共有できないフォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「デスクトップ」、「リンク」、「検索」、および「スタートメニュー」の各フォルダーの構造はこれらのオペレーティングシステムで異なるため、 Windows Server 2008用のデリバリーグループではリダイレクトされないように設定します。 これにより、これらのデータは共有されなくなります。
  - 予期せぬ問題の発生を避けるため、これらのフォルダーは Windows 8用のデリバリーグループでのみリダイレクトします。これは、通常の業務ではユーザーがWindows 8を使用することが多く、Windows Server 2008で提供されるアプリケーションには 頻繁にアクセスしないためです。 また、これらのデータは、アプリケーション環境よりも デスクトップ環境のものの方が実用的です。たとえば、 デスクトップ上のショートカットは「デスクトップ」フォルダーに格納されるため、Windows Server 2008マシンよりも Windows 8マシンのデスクトップショートカットをリダイレクトした方が便利です。
- 以下のフォルダーは、オペレーティングシステム間での共有に向いていません。
  - ユーザーが ダウンロードしたファイルがサーバー上にコピーされるのを防ぐため、「ダウンロード」フォルダーはリダイレクトしません。
  - 個々のアプリケーションのデータにより互換性やパフォーマンス上の問題が生じることがあるので、「アプリケーションデータ」フォルダーはリダイレクトしません。

フォルダーリダイレクトについて詳しくは 、 http://technet.microsoft.com/ja-jp/library/cc766489(v=ws.10).aspxを参照してください。

フォルダーリダイレクトと除外設定

Citrix Profile managementを使用する場合は、一部のユーザープロファイルフォルダーに対して除外規則を設定して、パフォーマンスを向上できます。この機能を使用する場合は、リダイレクトされるフォルダーに対して除外規則を設定しないでください。フォルダーリダイレクト機能とProfile managementの除外規則を一緒に使用する場合は、リダイレクトされるフォルダーがProfile managementの処理から除外されないようにしてください。これにより、後でリダイレクト機能を無効にしてもユーザープロファイルフォルダー構造の整合性が保持されます。 除外について詳しくは、「項目の包含および除外」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Insight Services

Dec 05, 2017

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrixが提供するプラットフォームです。この計測機能と利用統計情報機能を使用することで、技術ユーザー（顧客、パートナー、エンジニア）は自己診断を行い、問題を解決し、環境を最適化することができます。CISの詳細、最新情報、および機能について詳しくは、https://cis.citrix.comを参照してください（Citrixのアカウント資格情報が必要です）。

Citrix Insight Servicesで提供される機能は拡大と進化を続けており、今やCitrix Smart Toolsに不可欠な要素となっています。Citrix Smart Toolsでは展開タスク、ヘルスチェック、 電源管理を自動化できます。これらのテクノロジについては、Citrix Smart Toolsのドキュメントを参照してください。

Citrixにアップロードされた情報はすべて、トラブルシューティングや診断、および以下の対象となる製品の品質、信頼性、パフォーマンス向上を目的として使用されます。

- Citrix Insight Servicesポリシー（https://cis.citrix.com/legal）
- Citrixの個人情報保護ポリシー（http://www.citrix.com/about/legal/privacy.html）

このXenAppおよびXenDesktopのリリースでは、以下のツールと技術がサポートされます。

- XenAppおよびXenDesktopのインストールとアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム
- Citrix Smart Tools
- Citrix Call Home（Citrix Smart Toolsの一部）
- Citrix Scout

インストールとアップグレード分析

全製品インストーラーを使用してXenAppまたはXenDesktopコンポーネントを展開またはアップグレードする場合、インストールプロセスに関する匿名の情報が、コンポーネントをインストール/アップグレードするマシンで収集および保存されます。このデータは、インストールに関するカスタマーエクスペリエンス向上のために使用されます。詳しくは、http://more.citrix.com/XD-INSTALLERを参照してください。

この情報は、ローカルの%ProgramData%\Citrix\CTQsに保存されます。

このデータの自動アップロードは、全製品インストーラーのグラフィックおよびコマンドラインインターフェイスの両方で、デフォルトで有効です。

- デフォルト値はレジストリ設定で変更できます。インストール/アップグレードの前にレジストリ設定を変更すると、全製品インストーラーの使用時にその値が使用されます。
- コマンドラインインターフェイスを使用して、コマンドにオプションを指定してインストール/アップグレードする場合、デフォルト設定をオーバーライドできます。

インストール/アップグレード分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）：

場所： HKLM:\Software\Citrix\MetaInstall
Name： SendExperienceMetrics
Value： 0 = 無効、1 = 有効

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PowerShellを使用する場合、次のコマンドレットはインストール/アップグレード分析機能の自動アップロードを無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0
```

XenDesktopServerSetup.exeまたはXenDesktopVDASetup.exeコマンドで自動アップロードを無効にするには、/disableexperiencemetricsオプションを含めます。

XenDesktopServerSetup.exeまたはXenDesktopVDASetup.exeコマンドで自動アップロードを有効にするには、/sendexperiencemetricsオプションを含めます。

Citrixカスタマーエクスペリエンス向上プログラム（CEIP）

Citrixのカスタマーエクスペリエンス向上プログラム（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。詳しくは、http://more.citrix.com/XD-CEIPを参照してください。

サイト作成またはアップグレード時の登録

XenAppまたはXenDesktopサイトを作成するときに、自動的にCEIPに登録されます（最初のDelivery Controllerのインストール後）。サイトの作成からおよそ7日後に、初回データアップロードが行われます。サイトの作成後、このプログラムへの参加はいつでも解除できます。Studioのナビゲーションペインで**[構成]**を選択し、［製品サポート］タブに表示される手順に従ってください。

XenAppまたはXenDesktop展開をアップグレードする場合は次のようになります。

- CEIPをサポートしないバージョンからアップグレードする場合、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。
- CEIPをサポートするバージョンからアップグレードし、参加が有効になっていた場合、CEIPはアップグレードしたサイトで有効になります。
- CEIPをサポートするバージョンからアップグレードし、参加が無効になっていた場合、CEIPはアップグレードしたサイトでは無効になります。
- CEIPをサポートするバージョンからアップグレードし、参加が不明な場合、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。

収集された情報は匿名になるため、Citrix Insight Servicesへのアップグレード後は表示されません。

VDAインストール時の登録

デフォルトでは、ユーザーはWindows VDAのインストール時にCEIPに自動登録されます。このデフォルトはレジストリ設定で変更できます。VDAインストールの前にレジストリ設定を変更すると、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所： HKLM:\Software\Citrix\Telemetry\CEIP
Name： Enabled
Value： 0 = 無効、1 = 有効

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デフォルトで、「Enabled」プロパティはレジストリに表示されません。未指定のままの場合、自動アップロード機能は有効です。

PowerShellを使用する場合、次のコマンドレットはCEIPへの登録を無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0
```

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。

他の製品およびコンポーネントのインストール時の登録

CEIPへは、関連するCitrix製品、コンポーネント、テクノロジ（Provisioning Services、AppDNA、Citrix License Server、Citrix Receiver for Windows、Universal Print Server、Session Recording）のインストール時にも参加できます。インストールと参加のデフォルト値について詳しくは、該当のドキュメントを参照してください。

Citrix Smart Tools

Delivery Controllerのインストール時に、Smart Toolsのアクセスを有効にできます。

Smart Toolsのアクセス（およびまだ有効でない場合にはCall Homeへの参加）を有効にするオプションは、デフォルトで選択されています。**[接続]**をクリックします。ブラウザーウィンドウが開いて、［Smart Services］Webページに自動的に移動します。ここで、Citrix Cloudアカウントの資格情報を入力します。（Citrix Cloudアカウントをお持ちでない場合、Citrixアカウントの資格情報を入力すると、新しいCitrix Cloudアカウントが自動的に作成されます）。 認証後、Smart Tools Agentディレクトリに証明書がサイレントインストールされます。

Smart Toolsテクノロジを使用するには、Smart Toolsのドキュメントを参照してください。

Citrix Call Home

XenAppまたはXenDesktopで特定のコンポーネントおよび機能をインストールする場合、Citrix Call Homeに参加するかどうかを選択できるページが表示されます。Call Homeは診断データを収集し、その後そのデータを含む利用統計情報パッケージを、分析およびトラブルシューティングの目的で定期的にCitrix Insight Servicesに直接アップロードします（デフォルトポート443上のHTTPS経由）。

XenAppおよびXenDesktopでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。詳しくは、http://more.citrix.com/XD-CALLHOMEを参照してください。

Citrix Scoutでは、Call Homeのスケジュール機能も使用できます。詳しくは、「Citrix Scout」を参照してください。

収集される項目

Citrix Diagnostic Facility（CDF）トレースは、トラブルシューティングに役立つ情報を記録します。Call Homeは、一般的な障害（VDAの登録やアプリケーション/デスクトップの起動など）のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジは、常時トレース（AOT）と呼ばれます。Call Homeではその他のEvent Tracing for Windows（ETW）情報が収集されることはなく、収集されるように設定することもできません。

また、Call Homeでは以下の情報も収集されます。

- XenAppおよびXenDesktopによってHKEY_LOCAL_MACHINE\SOFTWARE\Citrixで作成されたレジストリ
- Citrix名前空間のWindows Management Instrumentation（WMI）情報

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 実行中のプロセス一覧
- %PROGRAM DATA%\Citrix\CDFに保存されているCitrixプロセスのクラッシュダンプ

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最長8日間、圧縮されたトレース情報を最大10MB保持します。

- データを圧縮することで、Call HomeのVDA上の占有領域を小さくできます。
- プロビジョニングされたマシンでのIOPを避けるため、トレースはメモリで保持されます。
- トレースバッファでは、循環メカニズムを使用してトレースがメモリで保持されます。

HTM

Call Homeキーデータポイント

Call Home collects these key datapoints.

サマリーの構成と管理

全製品インストールウィザードの使用時、またはそれ以降に、PowerShellコマンドレットを使用して、Call Homeに登録することができます。登録すると、デフォルトで、ローカルタイムの毎日曜日午前3時頃に診断情報が収集され、Citrixにアップロードされます。アップロードは、指定された時間の前後2時間以内に行われます。つまり、デフォルトのスケジュールの場合、アップロードは午前3時から午前5時の間に行われます。

診断情報をスケジュールベースでアップロードしない場合（またはスケジュールを変更する場合）は、PowerShellコマンドレットを使用して診断情報を手動で収集し、アップロードするかローカルに保存してください。

Call Homeのスケジュールによるアップロード登録する場合、および診断情報を手動でCitrixにアップロードする場合は、Citrixのアカウントまたは Citrix Cloudの資格情報を入力します。Citrixは、アカウント資格情報を、顧客の識別とデータのアップロードに使用されるアップロードトークンに交換します。アカウント資格情報は保存されません。

アップロードが実行されると、Citrixアカウントに関連付けられたアドレスに通知メールが送信されます。

前提条件

- PowerShell 3.0またはそれ以降が実行されている必要があります。
- Citrix Telemetry Serviceが実行されている必要があります。
- システム変数PSModulePathは、C:\Program Files\Citrix\Telemetry Service\などの、Telemetryのインストールパスに設定する必要があります。

コンポーネントインストール時のCall Homeの有効化

VDAのインストールまたはアップグレード時：全製品インストーラーのグラフィカルインターフェイスを使用してVirtual Delivery Agentをインストールまたはアップグレードする場合には、Call Home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。2つのオプションがあります。

- Call Homeに参加します。
- Call Homeに参加しません。

VDAをアップグレードしていて、Call Homeに以前参加していた場合には、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード時：グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードする場合には、Call Homeに参加するか、およびCitrix Smart Toolsに接続するかどうかを確認するメッセージが表示されます。3つのオプションがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix Smart Toolsに接続する。これには、Smart Toolsエージェントを介したCall Home機能が含まれます。これがデフォルトで、推奨されるオプションです。このオプションを選択すると、Smart Toolsエージェントが構成されます。（このオプションが選択されているかどうかに関わらず、Smart Toolsエージェントはインストールされます）。
- Call Homeに参加するのみで、Smart Toolsには接続しない。このオプションを選択すると、Smart Toolsエージェントはインストールされますが、構成されません。Call Home機能はCitrix Telemetry ServiceおよびCitrix Insight Servicesを介して提供されます。
- Smart Toolsに接続しない、またはCall Homeに参加しない。

Controllerをインストールする場合、そのサーバーがポリシー設定「サービスとしてログオン」が適用されるActive Directory GPOを持っていると、インストールウィザードでCall Homeページ上の情報を構成できません。詳しくは、CTX218094を参照してください。

Controllerをアップグレードしていて、Call Homeに以前登録していた場合、Smart Toolsに関することのみを確認するメッセージが表示されます。Call Homeに登録済みで、Smart Agentが既にインストールされている場合、ウィザードページは表示されません。

Smart Toolsについては、Smart Toolsのドキュメントを参照してください 。

PowerShellコマンドレット

各コマンドレットの説明や、上記の一般的なユースケースでは使用されないパラメーターを含む包括的な構文は、PowerShellヘルプに記載されています。

プロキシサーバーを使用してアップグレードするには、「プロキシサーバーの構成」を参照してください。

スケジュールによるアップロードの有効化

収集された診断情報は、Citrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
```

スケジュールによるアップロードが有効になっていることを確認するには「Get-CitrixCallHome」と入力します。有効な場合は、「IsEnabled=True」および「IsMasterImage=False」が返されます。

マスターイメージから作成されたマシンに対するスケジュールによるアップロードの有効化

マスターイメージでのスケジュールによるアップロードを有効にすると、マシンカタログで作成された各マシンを構成する必要がなくなります。

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

スケジュールによるアップロードが有効になっていることを確認するには「Get-CitrixCallHome」と入力します。有効な場合は、「IsEnabled=True」および「IsMasterImage=True」が返されます。

カスタムスケジュールの作成

診断情報の収集およびアップロードのスケジュールを、日次または週次で作成できます。

```
$timespan = New-TimeSpan –Hours -Minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek -UploadFrequency {Daily|Weekly}
```

スケジュールによるアップロードのキャンセル

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スケジュールによるアップロードをキャンセルしても、PowerShellコマンドレットを使用して診断データをアップロードでき
ます。

```
Disable-CitrixCallHome
```

スケジュールによるアップロードが無効になっていることを確認するには、「Get-CitrixCallHome」と入力します。無効な場合は、「IsEnabled=False」および「IsMasterImage=False」が返されます。

例

次のコマンドレットでは、毎日午後11時20分にデータを収集してアップロードするスケジュールが作成されます。Hoursパラメーターには、24時間形式を使用します。UploadFrequencyパラメーターの値がDailyの場合、DayOfWeekパラメーターは無視されます（指定されている場合）。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上述の例の場合、「StartTime=22:20:00」、「DayOfWeek=Sunday」（無視）、「Upload Frequency=Daily」が返されます。

以下のコマンドレットでは、毎週水曜日の午後11時20分にデータを収集してアップロードするスケジュールが作成されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

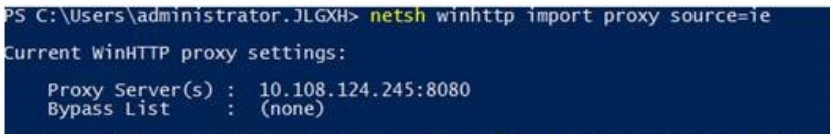
スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上述の例の場合、「StartTime=22:20:00」、「DayOfWeek=Wednesday」、「Upload Frequency=Weekly」が返されます。

Call Homeのアップロードのためにプロキシサーバーを構成

Call Homeが有効に設定されたマシンで、以下のタスクを実行します。以下の手順のサンプル図には、サーバーアドレスおよびポート10.158.139.37:3128が含まれています。お客様の情報はこれとは異なります。

手順1： ご使用のブラウザーにプロキシサーバー情報を追加します。Internet Explorerで、**[インターネット オプション] > [接続] > [LAN の設定]** を選択します。 **[LAN にプロキシ サーバーを使用する]** をオンにして、プロキシサーバーのアドレスとポート番号を入力します。

手順2： PowerShellで、**netsh winhttp import proxy source=ie**を実行します。



手順3： テキストエディターを使用して、TelemetryService.exe構成ファイルを編集します。これは、C:\Program Files\Citrix\Telemetry Serviceにあります。以下の赤いボックス内に示す情報を追加します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



手順4：Telemetry Serviceを再起動します。

PowerShellでCall Homeコマンドレットを実行します。

手動による診断情報の収集およびアップロード

CIS Webサイトを使用して、診断情報のバンドルをCISにアップロードすることができます。PowerShellコマンドレットを使って、診断情報を収集してCISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには、以下の手順に従います。

1. Citrixのアカウント資格情報を使用してCitrix Insight Servicesにログオンします。
2. **[個人用ワークスペース]** を選択します。
3. **[ヘルスチェック]** を選択し、次にデータの場所に移動します。

CISでは、データのアップロードを管理する複数のPowerShellコマンドレットがサポートされます。このドキュメントでは、つの一般的なケースにおけるコマンドレットについて説明します。

- Start-CitrixCallHomeUploadコマンドレットを使用して、診断情報のバンドルを手動で収集してCISにアップロードする（バンドルはローカルには保存されません）。
- Start-CitrixCallHomeUploadコマンドレットを使用して、手動でデータを収集し、診断情報のバンドルをローカルに保存する。これにより、データをプレビューできるようになります。その後、Send-CitrixCallHomeBundleコマンドレットを使用して、バンドルのコピーを手動でCISにアップロードします（最初に保存したデータはローカルに残ります）。

各コマンドレットの説明や、上記の一般的なユースケースでは使用されないパラメーターを含む包括的な構文は、PowerShellヘルプに記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードを確認するメッセージが表示されます。アップロードの完了前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスをチェックしてください。サービスがすでにアップロードを実行している場合は、アップロード要求が拒否されることがあります。

データの収集およびCISへのバンドルのアップロード

Start-CitrixCallHomeUpload [-Credential] [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploadHeader] [-AppendHeaders] [-Collect] []

データの収集およびローカルへの保存

Start-CitrixCallHomeUpload -OutputPath [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploaderHeader] [-AppendHeaders] [-Collect] []

パラメーター	説明

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログオン情報	アップロード先をCISに設定します。
InputPath	バンドルに含めるzipファイルの場所。これは、Citrixサポートから要求される追加ファイルである可能性があります。拡張子.zipを含めてください。
OutputPath	診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存するときに必要です。
DescriptionおよびIncidentTime	アップロードに関する自由形式の情報。
SRNumber	Citrixテクニカルサポートのインシデント番号。
名前	バンドルの識別名。
UploadHeader	CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
AppendHeaders	CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。
Collect	「{'collector':{'enabled':Boolean}}」の形で、どのデータを修正または省略するかを指定するJSON形式の文字列。Booleanはtrueまたはfalseです。 有効なcollectorの値は以下のとおりです。 • 'wmi' • 'process' • 'registry' • "crashreport' • 'trace' • 'localdata' • 'sitedata' • 'sfb' デフォルトでは、'sfb'以外のすべてのcollectorが有効です。 'sfb' collectorは、Skype for Businessの問題を診断するためにオンデマンドで使用するよう設計されています。'sfb' collectorは、'enabled'パラメーターに加えて、ターゲットユーザーを指定する'account'パラメーターと'accounts'パラメーターをサポートします。以下のいずれかの形式を使用します。 "-Collect "{'sfb':{'account':'domain\\user1'}}" -Collect "{'sfb':{'accounts':['domain\\user1', 'domain\\user2']}}"
一般的なパラメーター	PowerShellのヘルプを参照してください。

以前ローカルに保存されたデータのアップロード

```
Send-CitrixCallHomeBundle -Credential -Path []
```

Pathパラメーターにより、以前保存されたバンドルの場所を指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

例

以下のコマンドレットでは、（WMIコレクターからのデータを除く）Call HomeデータのCISへのアップロードが要求されます。このデータは、午後2時30分にCitrixサポートケース123456で記録されたPVS VDAの登録エラーに関連します。アップロードされるバンドルには、Call Homeデータに加えてファイル「c:\Diagnostics\ExtraData.zip」が含まれます。

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi': {'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下のコマンドレットでは、午前8時15分に記録されたCitrixサポートケース223344に関連するCall Homeデータが保存されます。このデータは、ネットワーク共有上のmydata.zipファイルに保存されます。保存されるバンドルには、Call Homeデータに加えてファイル「c:\Diagnostics\ExtraData.zip」が含まれます。

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344
```

以下のコマンドレットでは、以前保存したデータバンドルがアップロードされます。

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip
```

Citrix Scout

詳しくは、「Citrix Scout」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Scout

Dec 05, 2017

ここでは次のことについて説明します。

- はじめに
- 要件と考慮事項
- 診断データの収集
- トレースと再現
- 収集スケジュールの設定

はじめに

Citrix Scoutでは、XenAppおよびXenDesktop展開環境での予防的な保守に使用できる診断データを収集します。Citrixでは、Citrix Insight Servicesを通じて包括的な自動分析機能を提供しています。Scoutを使用して、お客様単独で、またはCitrix Supportの支援を受けながら問題のトラブルシューティングを行うこともできます。収集ファイルをCitrixにアップロードすると、Citrix Supportによる分析と支援を受けることができます。または、収集ファイルをローカルに保存してお客様自身でレビューを行い、その後Citrixにアップロードして分析を受けることもできます。

Scoutには3つの主要手順があります。

- **収集**：サイト内の選択したマシン上でワンタイム診断情報収集を実行します。次に、収集した情報が含まれるファイルをCitrixにアップロードするか、ローカルに保存します。
- **トレースおよび再現**：選択したマシン上で手動でトレースを開始します。次に、そのマシン上で問題を再現します。問題を再現すると、トレースは停止します。次に、Scoutはその他の診断情報を収集し、トレース情報と収集情報を含むファイルをCitrixにアップロードするか、ローカルに保存します。
- **スケジュール**：選択したマシン上で、日次または週次の指定時刻に診断情報を収集するようスケジュールを設定します。それぞれの収集情報を含むファイルは自動でCitrixにアップロードされます。

この記事で説明するグラフィカルインターフェイスは、Scoutを使用する初歩的な手段です。代わりにPowerShellインターフェイスを使用して、診断情報の収集とアップロードを1度だけまたは定期的に実行するように構成することもできます。「Call Home」を参照してください。

Scoutは次の場所で実行します。

- オンプレミスのXenAppおよびXenDesktop展開環境では、1つまたは複数のVirtual Delivery Agent（VDA）およびDelivery Controllerから診断情報を収集する場合は、Delivery ControllerからScoutを実行します。VDAからScoutを実行してローカルの診断情報を収集することもできます。
- XenAppおよびXenDesktopサービスを使用するCitrix Cloud環境では、ScoutをVDAから実行してローカルの診断情報を収集します。

収集される項目

Scoutにより収集される診断情報には、Citrix Diagnostic Facility（CDF）のトレースログファイルが含まれます。常時トレース（AOT）と呼ばれるCDFトレースファイルのサブセットも対象となります。AOTの情報は、VDAの登録やアプリケーションまたはデスクトップの起動など、よくある問題の解決に役立ちます。その他のEvent Tracing for Windows（ETW）情報が収集されることはありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

収集される情報は次のとおりです。

- XenAppおよびXenDesktopによってHKEY_LOCAL_MACHINE\SOFTWARE\Citrix以下に作成されたレジストリ
- Citrix名前空間のWindows Management Instrumentation（WMI）情報
- 実行中のプロセス
- %PROGRAM DATA%\Citrix\CDFに保存されているCitrixプロセスのクラッシュダンプ

トレース情報の概要を以下に示します。

- マシン上の占有領域を抑えるため、トレース情報は収集時に圧縮されます。
- Citrix Telemetry Serviceは、最長8日間、圧縮されたトレース情報を各マシン上に最大10MB保持します。
- プロビジョニングされたマシンでのIOPを避けるため、トレースはメモリで保持されます。
- トレースバッファでは、循環メカニズムを使用してトレースがメモリで保持されます。

Scoutで収集されるデータポイントの一覧については、「Scoutのキーデータポイント」を参照してください。

要件と考慮事項

権限

- 診断情報の収集元になる各マシンのローカル管理者およびドメインユーザーである必要があります。
- 各マシン上のLocalAppDataディレクトリに書き込む権限がある必要があります。
- Scoutの起動時には **[管理者として実行]** を使用してください。

診断情報の収集元になる各マシンには、次が必要です。

- Scoutは当該マシンと通信できる必要があります。
- ファイルとプリンターの共有は設定されている必要があります。
- PSRemotingとWinRMは有効になっている必要があります。PowerShell 3.0以降が実行されている必要もあります。
- Citrix Telemetry Serviceが実行されている必要があります。
- 診断情報の収集のスケジュールを設定するには、XenAppおよびXenDesktop 7.14以降でサポートされるバージョンで提供されるScoutのバージョンが実行されている必要があります。

Scoutでは指定したマシン上で確認テストが実行され、これらの要件が満たされているか確認されます。

確認テスト

診断情報の収集の開始前に、指定した各マシンについて自動で確認テストが実行されます。これらのテストで、上記の要件が満たされているか確認されます。あるマシンでテストが失敗した場合、Scoutには修正アクション案を含むメッセージが表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Error message	Corrective action
Scoutはこのマシンに接続できません。	以下の点を確認してください。 • マシンの電源が入れられていること。 • ネットワーク接続が正しく動作していること。（これにはファイアウォールが正しく構成されていることを含みます。） • ファイルおよびプリンターの共有が設定されていること。手順については、Microsoft社のドキュメントを参照してください。
PSRemotingとWinRMの有効化	PowerShellリモート処理とWinRMを同時に有効にすることができます。［管理者として実行］で、**Enable-PSRemoting**コマンドレットを実行します。詳しくは、Microsoftのコマンドレットのヘルプを参照してください。
Scoutには PowerShell 3.0 以降が必要です。	マシンに PowerShell 3.0（以降）をインストールして、PowerShellリモート処理を有効にします。
このマシンの LocalAppData ディレクトリにアクセスできません	マシン上のLocalAppDataディレクトリに書き込む権限がアカウントにあることを確認してください。
Citrix Telemetry Service が見つかりません	Citrix Telemetry Service がマシンにインストールされ、開始されたことを確認してください。
スケジュールを取得できません	マシンをXenAppおよびXenDesktop 7.14以上にアップグレードしてください。

バージョンの互換性

本バージョンのScout（3.x）は、XenAppおよびXenDesktop 7.14以上のControllerとVDA上での実行を想定しています。

旧バージョンのScoutは、過去のXenAppおよびXenDesktop展開で提供されています。旧バージョンについて詳しくは、CTX130147を参照してください。

バージョン7.14より前のControllerまたはVDAをバージョン7.14（以降のサポートするバージョン）にアップグレードすると、旧バージョンのScoutが最新バージョンに置き換えられます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Feature	Scout 2.23	Scout 3.0
XenAppおよびXenDesktop 7.14以上のサポート	はい	あり
XenDesktop 5.x、7.1～7.13のサポート	あり	なし
XenApp 6.x、7.5～7.13のサポート	あり	なし
製品への同梱	7.1～7.13	7.14以降
CTX記事からのダウンロード	可能	不可
CDFトレースのキャプチャ	あり	あり
常時トレース（AOT）のキャプチャ	なし	あり
診断データの収集対象	1度に10台のマシンまで（デフォルト）	無制限（リソースの可用性に依存）
Citrixへの診断データの送信	可能	可能
診断データのローカルへの保存	可能	可能
Citrix Cloud資格情報のサポート	なし	あり
Citrixの資格情報のサポート	あり	あり
アップロード用プロキシサーバーのサポート	あり	あり
スケジュールの調整	-	可能
スクリプトのサポート	コマンドライン（ローカルのControllerのみ）	Call Homeコマンドレットを使用したPowerShell（テレメトリをインストール済みのすべてのマシン）

インストール

デフォルトでは、ScoutはVDAまたはControllerのインストール時にCitrix Telemetry Serviceの一部として自動でインストールされます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDAのインストール時にCitrix Telemetry Serviceを除外した場合、またはこのサービスを後で削除した場合には、XenAppまたはXenDesktop ISOのx64\Virtual Desktop Componentsフォルダーまたはx86\Virtual Desktop Componentsフォルダーにある TelemetryServiceInstaller_xx.msiを実行します。

アップロードの認証

収集した診断情報をCitrixにアップロードする場合、CitrixまたはCitrix Cloudのアカウントが必要になります（これらのアカウントは、Citrixダウンロードまたは Citrix Cloud Control Centerへのアクセス時に使用する資格情報です）。アカウントの資格情報の検証後、トークンが発行されます。

- Citrixアカウントを使用して認証を行う場合、トークンの発行プロセスは表示されません。アカウント資格情報を入力するだけで済みます。Citrixで資格情報が検証されると、Scoutウィザードの手順を進めることができるようになります。
- Citrix Cloudアカウントを使用して認証を行う場合はリンクをクリックし、HTTPSを使用してデフォルトのブラウザーで Citrix Cloudにアクセスします。Citrix Cloud資格情報を入力すると、トークンが表示されます。このトークンをコピーして Scoutに貼り付けます。Scoutウィザードの手順を進めることができるようになります。

トークンは、Scoutが実行されているマシンにローカルに保存されます。このトークンを次回も使用するには、**[収集]** または **[トレースおよび再現]** を選択してから、 **[トークンを保存して次回以降この手順を省略する]** チェックボックスをオンにします。

Scoutの開始ページで **[スケジュール]** を選択するたびに再度認証を行う必要があります。スケジュールの作成時または変更時には、保存したトークンは使用できません。

アップロードでのプロキシの使用

プロキシサーバーを使用してCitrixへ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するようにScoutを構成するか、プロキシサーバーのIPアドレスとポート番号を指定します。

診断データの収集

収集手順では、マシンを選択し、診断情報の収集を開始してから、収集した情報が含まれるファイルをCitrixにアップロードするかローカルに保存します。

手順1：Scoutの起動

マシンの［スタート］メニューで **[Citrix] > [Citrix Scout]** の順に選択します。開始ページで **[収集]** をクリックします。

手順2：マシンの選択

［マシンの選択］ページには、サイト内にあるすべてのVDAとControllerが一覧表示されます。表示される項目をマシン名で絞り込むことができます。診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、 **[続行]** をクリックします。

選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満しているか確認されます。確認テストで不合格になると、［状態］列にメッセージが表示され該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報は収集されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

確認テストが完了したら、**[続行]**をクリックします。

手順3：マシンの診断データの収集

概要に、診断情報の収集元になるマシン（選択し、確認テストに合格したマシン）がすべて一覧表示されます。**[収集の開始]**をクリックします。

収集は以下のように進行します。

- ［状態］列には、マシンの現在の収集状態が表示されます。
- 1台のマシンで進行中の収集を停止するには、そのマシンの［操作］列の**[キャンセル]**をクリックします。
- 進行中の収集をすべて停止するには、ページの右下隅にある**[収集の停止]**をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの［操作］列で**[再試行]**をクリックします。
- すべての選択したマシンで収集が完了すると、右下隅にある**[収集の停止]**が**[続行]**に変わります。
- あるマシンの収集が正常に完了した場合にそのマシンの診断情報を再び収集するには、該当するマシンの［操作］列で**[再収集]**をクリックします。新しい収集情報によって過去の収集情報が上書きされます。
- 収集が失敗した場合は、［操作］列の**[再試行]**をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。
- すべてのマシンで収集が完了した後に、**[戻る]**をクリックしないでください。このボタンをクリックしてプロンプトで確定すると、収集した情報が失われます。

収集が完了したら、**[続行]**をクリックします。

手順4：収集情報の保存またはアップロード

収集した診断情報が含まれるファイルをCitrixにアップロードするか、ローカルのマシンに保存するかを選択します。

このファイルをすぐにアップロードすることを選択した場合は、手順5に進んでください。

このファイルをローカルに保存することを選択した場合は、次の操作を行います。

- Windowsの［保存］ダイアログボックスが開きます。保存場所を指定します。
- ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesの場合はCTX136396を、それ以外の場合は「Smart Toolsサポート」を参照してください。

[完了]をクリックしてScoutの開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

手順5：アップロードの認証とプロキシの指定（オプション）

このプロセスについて詳しくは、「アップロードの認証」を参照してください。

- 以前にScoutで認証を行ったことがない場合は、以下の手順を実行します。
- 以前にScoutで認証を行っている場合、デフォルトでは保存済みの認証トークンが使用されます。これで問題がない場合にこのオプションを選択し、**[続行]**をクリックします。今回の収集では資格情報は求められません。手順6に進んでください。
- 以前に認証を行っているものの、再度認証を行って新しいトークンを発行する場合は、**[変更/再認証]**をクリックして以下の手順を実行します。

アップロードの認証にCitrix資格情報とCitrix Cloud資格情報のどちらを使用するかを選択します。［続行］をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

［資格情報］ページで次の操作を行います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ファイルのアップロードにプロキシサーバーを使用する場合は、**[プロキシの構成]** をクリックします。プロキシサーバーを使用してCitrixへ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するようにScoutを構成するか、プロキシサーバーのIPアドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**[トークンの生成]** をクリックします。デフォルトのブラウザーでCitrix Cloudのページが開き、トークンが表示されます。このトークンをコピーしてScoutのページに貼り付けます。
- Citrixアカウントの場合はお使いの資格情報を入力します。

入力が完了したら、**[続行]** をクリックします。

手順6：アップロードに関する情報の指定

アップロードの詳細を入力します。

- ［名前］フィールドには、収集した情報が含まれるファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
- オプションとして、8桁のCitrix Supportケース番号を指定します。
- 該当する場合、オプションの［説明］フィールドに問題の詳細と発生時期を入力します。

完了したら、**[アップロードの開始]** をクリックします。

> アップロード中、ページの左下にアップロードのおおよそ何%が完了したかが表示されます。進行中のアップロードをキャンセルするには、**[アップロードの停止]** をクリックします。

アップロードが完了すると、アップロード先のURLリンクが表示されます。このCitrixのアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

[完了] をクリックしてScoutの開始ページに戻ります。

トレースと再現

トレースと再現の手順では、マシンを選択し、選択したマシンでトレースを開始して問題を再現し、診断情報の収集を開始してから、トレースと収集情報が含まれるファイルをCitrixにアップロードするかローカルに保存します。

この手順は、標準の収集手順と似ています。ただし、マシン上でトレースを開始し、問題を再現することができます。すべての収集される診断情報にはAOTトレース情報が含まれますが、この手順ではトラブルシューティングに役立つCDFトレースも追加されます。

手順1：Scoutの起動

マシンの［スタート］メニューで **[Citrix] > [Citrix Scout]** の順に選択します。開始ページで、**[トレースと再現]** をクリックします。

手順2：マシンの選択

［マシンの選択］ページには、サイト内にあるすべてのVDAとControllerが一覧表示されます。表示される項目をマシン名で絞り込むことができます。トレースと診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、**[続行]** をクリックします。

選択した各マシン上で確認テストが開始され、各マシンが「確認テスト」に記載されている基準を満しているか確認されま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報とトレースは収集されません。

確認テストが完了したら、**［続行］**をクリックします。

手順3：トレース

概要に、トレースの収集対象になるすべてのマシンが一覧表示されます。**［トレースの開始］**をクリックします。

選択した1台または複数台のマシンで、経験した問題を再現します。この間もトレースの収集は継続されています。問題の再現が完了したら、Scoutで**［続行］**をクリックします。これによりトレースが停止されます。

トレースの停止後、このトレース中に問題を再現したかどうかを指定します。

手順4：マシンの診断データの収集

［収集の開始］をクリックします。

収集は以下のように進行します。

- ［状態］列には、マシンの現在の収集状態が表示されます。
- 1台のマシンで進行中の収集を停止するには、そのマシンの［操作］列の**［キャンセル］**をクリックします。
- 進行中の収集をすべて停止するには、ページの右下隅にある**［収集の停止］**をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの［操作］列で**［再試行］**をクリックします。
- すべての選択したマシンで収集が完了すると、右下隅にある**［収集の停止］**が**［続行］**に変わります。
- あるマシンの収集が正常に完了した場合にそのマシンの診断情報を再び収集するには、該当するマシンの［操作］列で**［再収集］**をクリックします。新しい収集情報によって過去の収集情報が上書きされます。
- 収集が失敗した場合は、［操作］列の**［再試行］**をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。
- すべてのマシンで収集が完了した後に、**［戻る］**ボタンをクリックしないでください。このボタンをクリックしてプロンプトで確定すると、収集した情報が失われます。

収集が完了したら、**［続行］**をクリックします。

手順5：収集情報の保存またはアップロード

収集した診断情報が含まれるファイルをCitrixにアップロードするか、ローカルのマシンに保存するかを選択します。

このファイルをすぐにアップロードすることを選択した場合は、手順6に進んでください。

このファイルをローカルに保存することを選択した場合は、次の操作を行います。

- Windowsの［保存］ダイアログボックスが開きます。保存先を選択します。
- ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。
  注：ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesの場合はCTX136396を、それ以外の場合は「Citrix Smart Tools」を参照してください。

［完了］をクリックしてScoutの開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順6：アップロードの認証とプロキシの指定（オプション）

このプロセスについて詳しくは、「アップロードの認証」を参照してください。

- 以前にScoutで認証を行ったことがない場合は、以下の手順を実行します。
- 以前にScoutで認証を行っている場合、デフォルトでは保存済みの認証トークンが使用されます。これで問題がない場合にこのオプションを選択し、**[続行]**をクリックします。今回の収集では資格情報は求められません。手順7に進んでください。
- 以前に認証を行っているものの、再度認証を行って新しいトークンを発行する場合は、**[変更/再認証]**をクリックして以下の手順を実行します。

  アップロードの認証にCitrix資格情報とCitrix Cloud資格情報のどちらを使用するかを選択します。**[続行]**をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、**[プロキシの構成]**をクリックします。プロキシサーバーを使用してCitrixへ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するようにScoutを構成するか、プロキシサーバーのIPアドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**[トークンの生成]**をクリックします。デフォルトのブラウザーでCitrix Cloudのページが開き、トークンが表示されます。このトークンをコピーしてScoutのページに貼り付けます。
- Citrixアカウントの場合はお使いの資格情報を入力します。

入力が完了したら、**[続行]**をクリックします。

手順7：アップロードに関する情報の指定

アップロードの詳細を入力します。

- ［名前］フィールドには、収集した情報が含まれるファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
- オプションとして、8桁のCitrix Supportケース番号を指定します。
- 該当する場合、オプションの［説明］フィールドに問題の詳細と発生時期を入力します。

完了したら、**[アップロードの開始]**をクリックします。

  アップロード中、ページの左下にアップロードのおおよそ何%が完了したかが表示されます。進行中のアップロードをキャンセルするには、**[アップロードの停止]**をクリックします。

アップロードが完了すると、アップロード先のURLリンクが表示されます。このCitrixのアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

[完了]をクリックしてScoutの開始ページに戻ります。

収集スケジュールの設定

スケジュール設定手順では、マシンを選択し、スケジュールを設定またはキャンセルします。スケジュールで収集された診断情報は、Citrixに自動的にアップロードされます（PowerShellインターフェイスを使用すると、スケジュールにより収集されたデータをローカルに保存できます。「Citrix Call Home」を参照してください。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順1：Scoutの起動

マシンの［スタート］メニューで **[Citrix] > [Citrix Scout]** の順に選択します。開始ページで **[スケジュール]** をクリックします。

手順2：マシンの選択

［マシンの選択］ページには、サイト内にあるすべてのVDAとControllerが一覧表示されます。表示される項目をマシン名で絞り込むことができます。

> グラフィカルインターフェイスを使用してVDAおよびControllerをインストールした場合、Call Homeへの参加に関する情報が表示されます。詳しくは、「Citrix Call Home」を参照してください（Call HomeにはScoutと同等のスケジュール設定機能が含まれています）。デフォルトでは、Scoutにはこれらの設定が表示されます。このバージョンのScoutでは、スケジュール済みの収集を初めて開始するか、構成済みのスケジュールを変更できます。
>
> Call Homeはマシンごとに有効化または無効化しますが、Scoutのスケジュール設定でも同じコマンドを使用します。ただし、選択したマシンすべてがコマンドの影響を受けます。

診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、**[続行]** をクリックします。

選択した各マシン上で確認テストが開始され、各マシンが「確認テスト」に記載されている基準を満しているか確認されます。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報（またはトレース）は収集されません。

確認テストが完了したら、**[続行]** をクリックします。

概要ページに、スケジュールが適用されるマシンが一覧表示されます。**[続行]** をクリックします。

手順3：スケジュールの設定

診断情報を収集するタイミングを指定します。注：スケジュールは選択したマシンすべてに影響します。

- 選択したマシンについて週次のスケジュールを構成するには、**[毎週]** をクリックします。曜日を選択し、診断情報の収集を開始する時刻（24時間形式）を入力します。
- 選択したマシンについて日次のスケジュールを構成するには、**[毎日]** をクリックします。診断情報の収集を開始する時刻（24時間形式）を入力します。
- （別のスケジュールに置き換えずに）選択したマシンの既存のスケジュールをキャンセルするには、**[オフ]** をクリックします。選択したマシンで構成済みのスケジュールがすべてキャンセルされます。

[続行] をクリックします。

手順4：アップロードの認証とプロキシの指定（オプション）

このプロセスについて詳しくは、「アップロードの認証」を参照してください。注：Scoutのスケジュールを使用する場合、保存済みのトークンを使用して認証を行うことはできません。

アップロードの認証にCitrix資格情報とCitrix Cloud資格情報のどちらを使用するかを選択します。**[続行]** をクリックしま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。プロキシサーバーを使用してCitrixへ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するようにScoutを構成するか、プロキシサーバーのIPアドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**［トークンの生成］**をクリックします。デフォルトのブラウザーでCitrix Cloudのページが開き、トークンが表示されます。このトークンをコピーしてScoutのページに貼り付けます。
- Citrixアカウントの場合はお使いの資格情報を入力します。

入力が完了したら、**［続行］**をクリックします。

構成済みのスケジュールを確認します。**［完了］**をクリックしてScoutの開始ページに戻ります。

スケジュールした収集が行われるたびに、選択した各マシンのWindowsアプリケーションログに収集とアップロードの情報が書き込まれます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

監視

Dec 05, 2017

管理者およびヘルプデスク担当者は、さまざまな機能やツールを使用して、XenAppやXenDesktopのサイトをモニターできます。これらのツールを使って、モニターできるものは以下のとおりです。

- ユーザーセッションおよびセッションの利用状況
- ログオン処理のパフォーマンス
- 接続とマシン（エラーを含む）
- 負荷評価
- 履歴傾向
- インフラストラクチャ

Citrix Director

リアルタイムWebツールであるDirectorを使用して、セッションの監視、トラブルシューティングなど、エンドユーザーに対するサポートタスクを実行できます。

詳しくは、「Director」の記事を参照してください。

セッション レコーディング

Session Recordingを使用すると、接続の種類を問わず、企業ポリシーおよび既定のコンプライアンスを遵守するXenAppを実行する任意のサーバー上の任意のユーザーセッションで行われる、画面上のアクティビティを録画することができます。Session Recordingにより録画、カタログ化、およびアーカイブされるセッションを、後で取得して再生することができます。

Session Recordingでは柔軟性の高いポリシーを使用して、アプリケーションセッションの録画を自動的に起動します。IT部門ではSession Recordingを使用して、財務業務や病院での患者情報のシステムなどでエンドユーザーがアプリケーションをどのように使用するかを調査できます。内部統制をサポートすることによって、法規制の順守を徹底し、セキュリティ監視を成功に導きます。同様に、技術サポート部門でこの機能を使用すれば、問題の特定と解決までの時間を短縮することができます。

詳しくは、「Session Recording」の記事を参照してください。

構成ログ

構成ログ機能では、サイトで管理者が行った変更内容が記録されます。構成を変更した後で問題が発生した場合は、構成ログを確認して問題の内容を診断し、トラブルシューティングを施します。また、変更管理、構成の記録、および管理アクティビティのレポート生成が可能です。

ログに記録した情報に関するレポートは、Studioから表示および生成できます。ログの内容は、Directorの［傾向］ビューで確認もできます。このインターフェイスで、構成変更についての通知を提供することが可能です。これは、Studioへのアクセス権限を持たない管理者には便利な機能です。

［傾向］ビューでは、特定の期間に行われた構成変更の履歴データを表示できます。これにより、どのような変更がいつ、だれによって行われたかを確認して、問題の原因究明に役立てることができます。このビューには、構成情報が以下の3つのカテゴリに分けて表示されます。

- 接続エラー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 失敗したデスクトップOSマシン
- 失敗したサーバーOSマシン

構成ログ機能の有効化と構成方法について詳細は、「構成ログ機能」の記事を参照してください。「Director」には、このツールを使って、ログ情報を表示する方法を記載した記事があります。

イベントログ

XenAppおよびXenDesktopサービスは、発生するイベントを記録します。イベントログは、操作を監視およびトラブルシューティングするために使用できます。

詳しくは、「イベントログ」を参照してください。個別の機能に関する記事には、イベント情報も含まれることがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッション レコーディング

Dec 05, 2017

Session Recordingを使用すると、企業ポリシーおよび法規制の順守の要件に準拠して、接続の種類を問わず、VDA for Server OSまたはVDA for Desktop OSでホストされる任意のユーザーセッションで行われる、画面上のアクティビティを録画することができます。Session Recordingにより録画、カタログ化、およびアーカイブされるセッションを、後で取得して再生することができます。

Session Recordingでは柔軟性の高いポリシーを使用して、アプリケーションセッションの録画を自動的に起動します。IT部門ではSession Recordingを使用して、財務業務や病院での患者情報のシステムなどでエンドユーザーがアプリケーションをどのように使用するかを調査できます。内部統制をサポートすることによって、法規制の順守を徹底し、セキュリティ監視を成功に導きます。同様に、技術サポート部門でこの機能を使用すれば、問題の特定と解決までの時間を短縮することができます。

長所

記録と監視によるセキュリティの向上。Session Recordingにより、機密情報を取り扱うアプリケーションで、エンドユーザーの 画面上での操作を録画できます。これは、医療や 金融などの規制の厳しい業界では、特に重要な機能です。このような業界では、記録が禁止されている個人情報を取り扱っているため、 ポリシーによって選択的な録画を実行できます。

強力なアクティビティ 監視。画面の更新、 マウスのクリック、および目に見えるキーボード入力をデジタル署名されたビデオに 録画および保存し、特定のエンドユーザー、アプリケーション、および サーバーの操作を録画できます。

Session Recordingは、 法的 手続きの証拠収集用に設計、開発されてはいません。Session Recordingを使用している組織が証拠の収集を行う場合は、 一般的な動画録画とテキストベースの電子証拠開示ツールの 組み合わせなどを使用することをお勧めします。

迅速な問題 解決。再現が難しい問題についてエンドユーザーが問い合わせをしたときに、ヘルプ デスクのサポートスタッフはユーザーセッションを録画できます。問題が 再発したら、発生時刻が記録されているエラーの録画を使用して、 より迅速に問題のトラブルシューティングができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recordingの導入

Dec 05, 2017

次の工程を行うと、XenAppおよびXenDesktopセッションを録画し、検証できるようになります。

1. Session Recordingコンポーネントを理解する。
2. 環境に合う展開シナリオを選択する。
3. インストール要件を確認する。
4. Windowsの役割と機能の前提条件をインストールする。
5. Session Recordingをインストールする。
6. Session Recordingコンポーネントを構成して、録画およびセッションの表示を許可する。

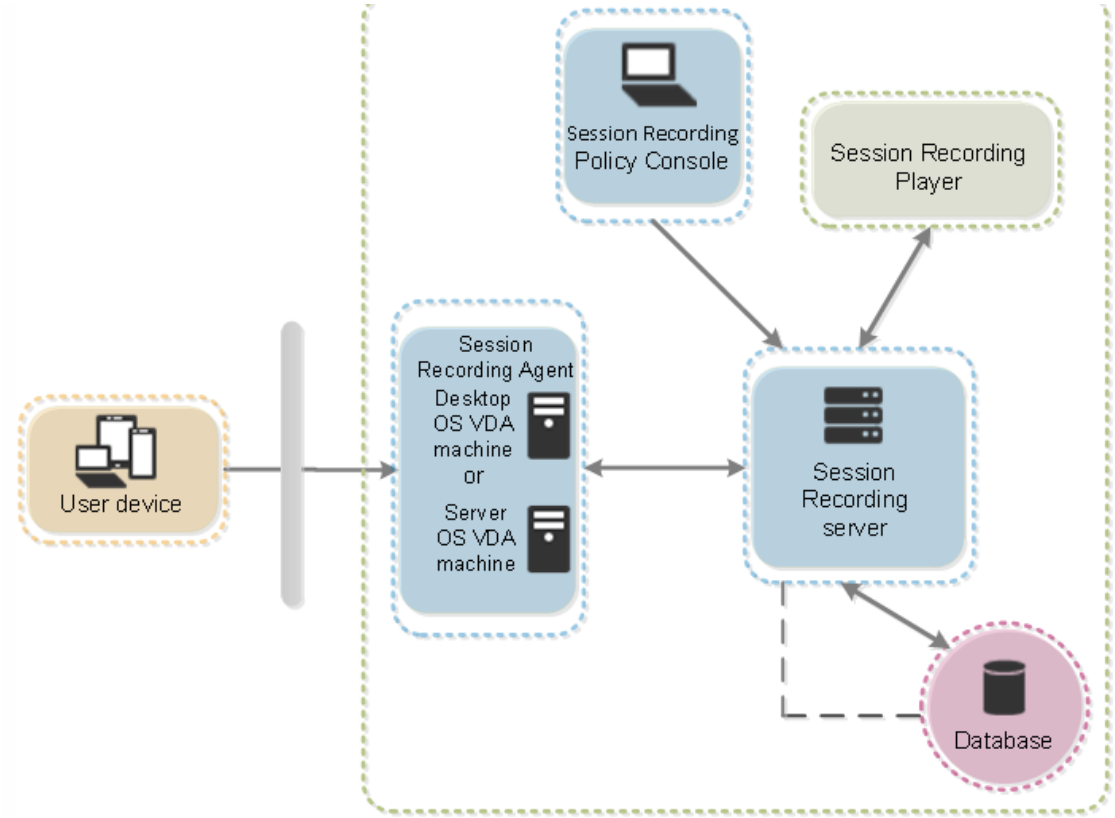
Session Recordingは5つのコンポーネントから 構成されます。

- **Session Recording Agent。**各VDA for Server OSまたはVDA for Desktop OSにインストールする、録画処理を有効にするコンポーネントです。これによりセッションデータが録画されます。
- **Session Recordingサーバー。**次のサービスをホストするサーバーです。
  - ブローカー：IIS 6.0以降によりホストされるWebアプリケーションです。これにより、Session Recording Playerからの検索クエリおよびファイルダウンロード要求と、Session Recordingポリシーコンソールからのポリシー管理要求が制御されます。また、XenAppおよびXenDesktopの各セッションの録画ポリシーが評価されます。
  - ストレージマネージャー：Windowsサービスです。これにより、XenAppとXenDesktopを実行中のSession Recordingが有効な各コンピューターから受信する、セッションの録画ファイルが管理されます。
  - Administrator Logging。 Session Recording Serverでインストールされる、管理アクティビティを記録するためのオプションのサブコンポーネントです。ログデータはすべて、**CitrixSessionRecordingLogging**という名前の個別のSQL Serverデータベースに格納されます。
- **Session Recording Player。**XenAppおよびXenDesktopセッションのファイルを調査するユーザーが、録画を再生するためにワークステーションでアクセスするユーザーインターフェイスです。
- **Session Recordingデータベース。**録画したセッションデータを格納するためのSQLデータベースを管理するコンポーネントです。このコンポーネントがインストールされていると、**CitrixSessionRecording**という名前のデータベースが作成されます。この名前は変更できません。
- **Session Recording Policy Console。** 録画するセッションを指定するポリシーを作成するコンソールです。

この図はSession Recordingコンポーネントおよび各コンポーネントの関係を 示しています。

この展開例では、Session Recording Agent、Session Recordingサーバー、Session Recordingデータベース、Session Recordingポリシーコンソール、およびSession Recording Playerのすべてが、セキュリティファイアウォールの内部に設置されています。Session Recording Agentは、VDA for Server OSまたはVDA for Desktop OSにインストールされます。第2のサーバーはSession Recordingポリシーコンソールをホストし、第3のサーバーはSession Recordingサーバーとして機能します。そして、第4のサーバーはSession Recordingデータベースをホストします。Session Recording Playerはワークステーションにインストールされます。ファイアウォール外部のクライアントデバイスは、Session Recording Agentがインストールされているを VDA for Server OSに接続します。ファイアウォール内では、Session Recording Agent、Session Recordingポリシーコンソール、Session Recording Player、およびSession Recordingデータベースはすべて Session Recordingサーバーに接続します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

導入計画

Dec 05, 2017

制限事項

Session Recordingでは、デスクトップコンポジションのリダイレクト（DCR）の表示モードはサポートされません。デフォルトでは、セッションが録画ポリシーで録画される場合にそのセッションのDCRは無効化されます。この動作は、Session Recording Agentのプロパティで設定できます。

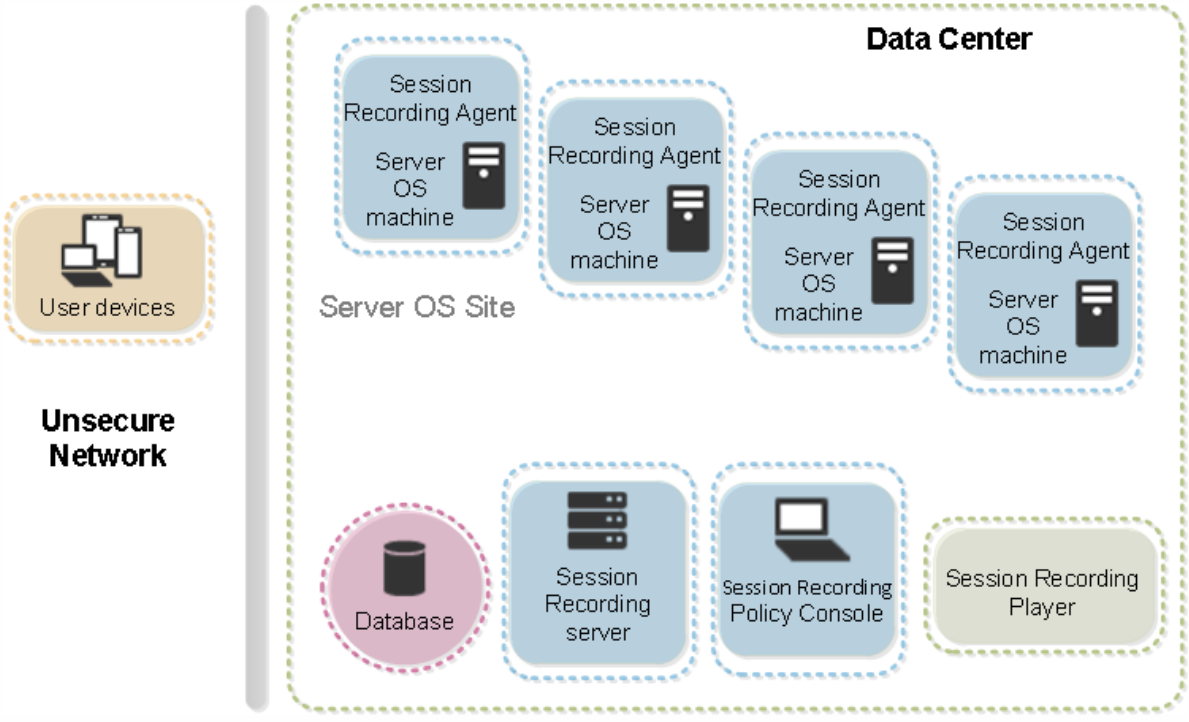
環境に応じ、異なるシナリオに基づいてSession Recordingコンポーネントを展開できます。

Session Recordingは、単一のサイトのみに限って展開する必要はありません。 Session Recording Agent以外はすべて、サーバーサイトに依存しないコンポーネントです。 例えば、複数のサイトで単一のSession Recordingサーバーを使用するように設定できます。

複数のエージェントを展開した大規模なサイトがあり、画像処理にかなりリソースを消費するアプリケーション（AutoCADなど）を数多く録画したり、多数のセッションを録画したりすることが予測される場合、Session Recording Serverに非常に負荷がかかる可能性があります。 パフォーマンスの問題を解決するために、複数のSession Recording Serverを異なるコンピューターにインストールし、Session Recording Agentがそれらのコンピューターと連携するように設定できます。 エージェントで1度に参照できるのは1つのサーバーのみであることに留意してください。

提案されたサーバーサイトの構成

1つまたは複数のサイトのセッションを録画する場合は、この構成を使用します。Session Recording Agentはサイト内の各VDA for Server OSにインストールされます。サイトはセキュリティファイアウォール内のデータセンターにあります。Session Recording Administrationコンポーネント（Session Recordingデータベース、Session Recordingサーバー、Session Recordingポリシーコンソール）を別の複数のサーバーにインストールし、Session Recording Playerはワークステーションにインストールします。これらのコンピューターはファイアウォール内ですがデータセンターの外部にあります。ワークステーション、モバイルデバイス、およびラップトップコンピューターのようなXenAppクライアントは、ファイアウォール外部の保護されていないネットワーク環境にあります。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

展開に関する重要な注意事項

- Session Recordingコンポーネントを有効にして各コンポーネント間で通信できるようにするには、同じドメイン内か、推移的な信頼関係を持つ信頼されているドメイン間にインストールします。ワークグループまたは外部の信頼関係を持つドメイン間にはインストールできません。
- 映像を処理するアプリケーションであり、サイズの大きな録画を再生するときは多くのメモリが使用されるため、Session Recording Playerを公開アプリケーションとしてインストールすることはお勧めしません。
- デフォルトでは、Session RecordingはTLS/HTTPSを使用して通信するように設定されます。Session Recording Serverに証明書をインストールし、ルート証明機関（CA）がSession Recordingコンポーネントで信頼されていることを確認します。
- Session RecordingデータベースをSQL Server 2016 Express Edition、SQL Server 2014 Express Edition、SQL Server 2012 Express Edition、またはSQL Server 2008 R2 Express Editionが動作するスタンドアロンサーバーにインストールする場合は、そのサーバーでTCP/IPプロトコルを有効にしてSQL Server Browserサービスを実行する必要があります。これらの設定はデフォルトでは無効になっていますが、Session Recording Serverとデータベースの間で通信を行うために有効にする必要があります。これらの設定の有効化について詳しくは、Microsoft社の「SQL ServerのTCP/IPネットワークプロトコルの有効化」および「SQL Server Browserサービス」を参照してください。
- Session Recordingの展開を計画するときは、セッション共有の影響を考慮します。公開アプリケーションのセッションを共有すると、Session Recordingの公開アプリケーションの録画ポリシー規則と競合する可能性があります。Session Recordingでは、アクティブなポリシーとエンドユーザーが最初に開いた公開アプリケーションを照合します。エンドユーザーが最初のアプリケーションを開いた後で、同じセッション上で次のアプリケーションを開くと、最初のアプリケーションに対して有効なポリシーが、次のアプリケーションにも適用されます。たとえば、ポリシーがMicrosoft Outlookでの操作のみを録画する設定になっている場合、エンドユーザーがOutlookを開くと録画が始まります。しかし、Microsoft Outlookの実行中に公開アプリケーションのWordをエンドユーザーが開くと、Wordでの操作も録画されます。逆に、アクティブなポリシーがWordでの操作を録画する設定になっていない場合、エンドユーザーが（ポリシーに従って操作が録画されるべき）Outlookの前にWordを開くと、Outlookでの操作が録画されません。
- Session RecordingサーバーをDelivery Controllerにインストールすることはできますが、Citrixはパフォーマンスの問題によりこの操作をお勧めしません。
- Session Recordingポリシーコンソールを Delivery Controllerにインストールできます。
- Session RecordingサーバーとSession Recordingポリシーコンソールは同じシステムにインストールできます。
- Session RecordingサーバーのNetBIOS名が15文字を超えないようにしてください（Microsoftにはホスト名長に15文字の制限があります）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セキュリティの推奨事項

Dec 05, 2017

Session Recordingは、安全なネットワーク上に展開され管理者によりアクセスされるものとして設計されており、そのことを前提にセキュリティを維持するコンポーネントです。設計上、デフォルトの構成はシンプルなシステムです。デジタル署名や暗号化などのセキュリティ機能はオプションで設定できます。

Session Recordingコンポーネント間の通信は、インターネットインフォメーションサービス（IIS）とMicrosoftメッセージキュー（MSMQ）を通じて実現されます。 IISにより、各Session Recordingコンポーネント間のWebサービスの通信リンクが提供されます。 MSMQにより、Session Recording AgentからSession Recordingサーバーへセッションの録画データを送信するための、信頼できるデータ伝送メカニズムが提供されます。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

展開計画を立てるときに、セキュリティに関する次の推奨事項について検討します。

- 社内ネットワーク、Session Recording、または個々のマシンで各種管理者の役割を適切に分離する。このようにしないと、セキュリティ上の脅威にさらされ、システム機能が影響を受けたり、システムが不正利用されたりする可能性があります。ユーザーやアカウントごとに異なる管理者の役割を割り当て、一般のセッションユーザーにVDAシステムの管理者権限を持たせないようにすることが推奨されます。
  - XenAppおよびXenDesktopの管理者は、VDAローカル管理者の役割を、公開アプリケーションまたはデスクトップのユーザーに付与しないでください。ローカル管理者の役割が必要な場合は、Windowsのメカニズムまたはサードパーティ製のソリューションを使用して、Session Recording Agentコンポーネントを保護します。
  - Session Recordingデータベース管理者とSession Recordingポリシー管理者を別々に割り当てる。
  - Citrixは、特にリモートPCアクセスを使用している場合に、VDA管理者特権を一般のセッションユーザーに割り当てないことをお勧めします。
  - Session Recordingサーバーのローカル管理者アカウントは、厳格に保護する必要があります。
  - Session Recording Playerがインストールされたマシンへのアクセスを制御します。ユーザーがSession Recording Playerの役割を許可されていない場合、そのユーザーにはどのSession Recording Playerマシンのローカル管理者の役割も付与しないようにしてください。匿名アクセスを無効にしてください。
  - Session Recordingのストレージサーバーには、物理マシンを使用することが推奨されます。
- Session Recordingでは、データの機密性にかかわらず、セッショングラフィックスアクティビティが録画されます。特定の状況においては、機密データ（ユーザーの資格情報、プライバシー情報、サードパーティの画面など。ただしこれらに限定されるものではありません）が誤って録画される場合があります。このリスクを回避するには、以下の措置を講じます。

  + 特定のトラブルシューティングの場合を除き、VDAのコアメモリダンプを無効にします。

    コアメモリダンプを無効にするには、以下の手順に従います。

    1. **[マイコンピューター]** を右クリックし、 **[プロパティ]** を選択します。
    2. **[詳細設定]** タブをクリックし、 **[起動と回復]** の **[設定]** をクリックします。
    3. **[デバッグ情報の書き込み]** で **[（なし）]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft社のhttps://support.microsoft.com/en-us/kb/307973を参照してください。

+ セッションの所有者は、デスクトップセッションが録画されている場合は、オンライン会議とMicrosoft Remote Assistanceソフトウェアが録画される可能性があることを出席者に知らせる必要があります。

+ ログオン資格情報またはセキュリティ情報が、社内で公開または使用されるすべてのローカルアプリケーションとWebアプリケーションに表示されないようにするか、またはSession Recordingで録画されないようにします。

+ ユーザーは、リモートICAセッションに切り替える前に、機密情報を公開する可能性のあるアプリケーションをすべて閉じる必要があります。

+ 公開デスクトップまたはSoftware as a Service（SaaS）アプリケーションへのアクセスには、自動認証方法（シングルサインオン、スマートカードなど）のみを推奨します。

- Session Recordingは、正常に機能し、セキュリティニーズを満たす上で、特定のハードウェアとハードウェアインフラストラクチャ（社内ネットワークデバイス、オペレーティングシステムなど）に依存しています。インフラストラクチャレベルで対策を講じることでこうしたインフラストラクチャの損傷と不正利用を防ぎ、Session Recording機能の安全性と信頼性を確保します。
  - Session Recordingをサポートするネットワークインフラストラクチャを適切に保護し、利用可能な状態を維持します。
  - サードパーティ製のセキュリティソリューションまたはWindowsのメカニズムを使用して、Session Recordingコンポーネントを保護することが推奨されます。Session Recordingコンポーネントには以下が含まれます。
    - Session Recordingサーバー上
      - プロセス：SsRecStoragemanager.exeおよびSsRecAnalyticsService.exe
      - サービス：CitrixSsRecStorageManagerおよびCitrixSsRecAnalyticsService
      - Session Recordingサーバーのインストールフォルダーにあるすべてのファイル
      - HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Serverにあるレジストリキー
    - Session Recording Agent上
      - プロセス：SsRecAgent.exe
      - サービス：CitrixSmAudAgent
      - Session Recording Agentのインストールフォルダーにあるすべてのファイル
      - HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Agentにあるレジストリキー
- Session RecordingサーバーでMessage Queuing（MSMQ）のアクセス制御リスト（ACL）を設定することで、MSMQデータをSession Recordingサーバーに送信できるVDAまたはVDIマシンを制限し、許可のないマシンがデータをSession Recordingサーバーに送信できないようにする。

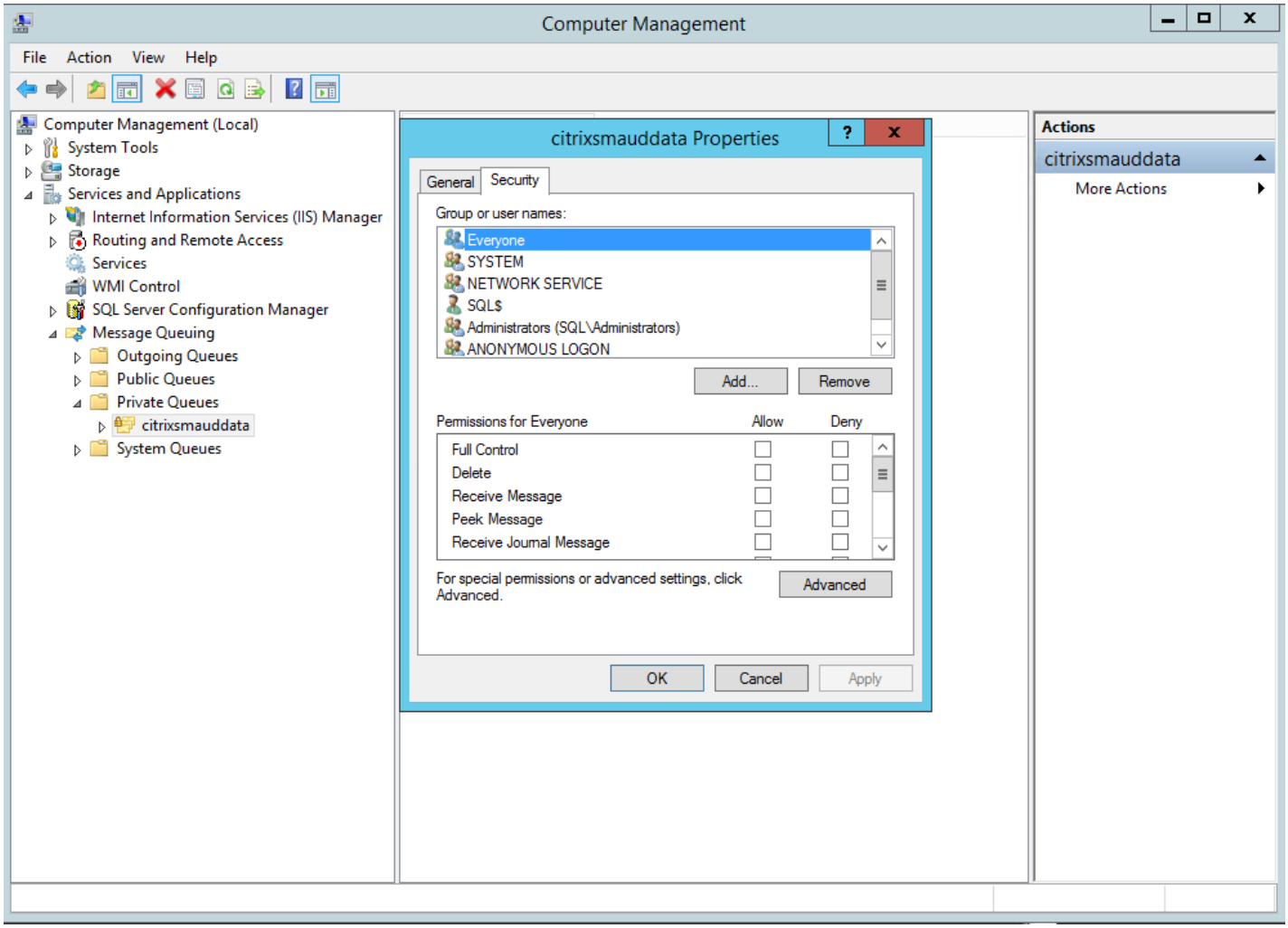
  1) 各Session Recordingサーバー、およびSession Recordingが有効になっているVDAまたはVDIマシンに、サーバー機能のDirectory Service Integrationをインストールし、次にMessage Queuingサービスを再起動します。

  2) 各Session RecordingサーバーのWindowsの **[スタート]** メニューから、 **[管理ツール]** > **[コンピューターの管理]** の順に開きます。

  3) **[サービスとアプリケーション]** > **[メッセージキュー]** > **[専用キュー]** の順に開きます。

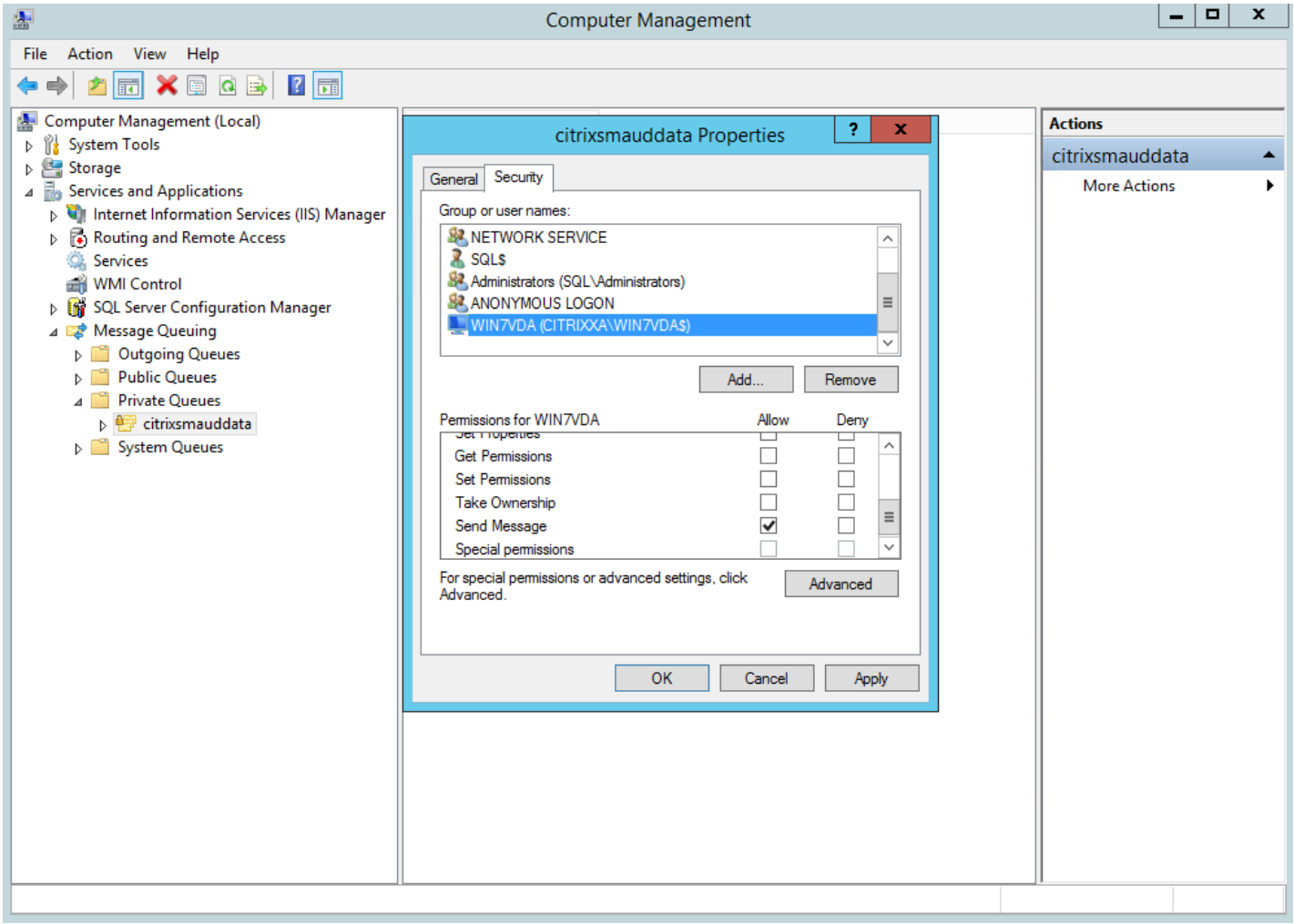
  4) **citrixsmauddata専用キューをクリックして [プロパティ] ページを開き、 [セキュリティ]** タブをクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5) MSMQデータをこのサーバーに送信するVDAのコンピューターまたはセキュリティグループを追加し、**メッセージを送信する**権限を付与します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Session RecordingサーバーとSession Recording Agentのイベントログを適切に保護する。Windowsまたはサードパーティ製のリモートログソリューションを利用してイベントログを保護するか、イベントログをリモートサーバーにリダイレクトすることが推奨されます。
- Session Recordingコンポーネントが動作するサーバーを物理的に保護する。可能であれば、権限を持つ人のみが入室できる安全なサーバー室にコンピューターを設置します。
- Session Recordingコンポーネントが動作するサーバーを別のサブネットまたはドメインに分離する。
- Session Recordingサーバーとほかのサーバーの間にファイアウォールを設置し、ほかのサーバーにアクセスするユーザーからセッションの録画データを保護する。
- Microsoftからの最新のセキュリティアップデートにより、Session Recording Admin ServerおよびSQLデータベースを最新に保ちます。
- 管理者以外の人が管理マシンにログオンできないように制限する。
- 録画ポリシーの変更およびセッションの録画ファイルの表示を行う権限を持つユーザーを厳しく制限する。
- デジタル証明書をインストールし、Session Recordingのファイル署名機能を使用し、IISでTLS通信をセットアップする。
- **[Session Recording Agent のプロパティ]** に表示されるMSMQプロトコルをHTTPSに設定して、MSMQの通信でHTTPSが使用されるようにする。詳しくは、「MSMQのトラブルシューティング」を参照してください。
- TLS 1.1またはTLS 1.2（推奨）を使いSSLv2、SSLv3、およびTLS 1.0をSession RecordingサーバーとSession Recordingデータベースで無効にします。詳しくは、Microsoftの記事http://support.microsoft.com/default.aspx?scid=kb;en-us;187498を参照してください。

Session RecordingサーバーとSession Recordingデータベースで、TLS用のRC4暗号スイートを無効にする。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Microsoftのグループポリシーエディターを使用して、**[コンピューターの構成]** > **[管理用テンプレート]** > **[ネットワーク]** > **[SSL構成設定]** に移動します。
2. 「**SSL暗号の順位**」ポリシーを **[有効]** に設定します。 デフォルトでは、このポリシーは **[未構成]** に設定されています。

3. RC4暗号スイートをすべて削除します。

- 再生データの保護機能を使用する。再生データの保護はSession Recordingの機能の1つで、これにより、Session Recording Playerにダウンロードされる前に、セッションの録画ファイルが暗号化されます。このオプションは **[Session Recording Server のプロパティ]** にあり、デフォルトで有効に設定されます。
- 暗号化キー長および暗号化アルゴリズムのNSITガイダンスに従います。
- TLS 1.2のSession Recordingサポートを構成します。
  - Session Recordingコンポーネントのエンドツーエンドセキュリティを確実にするためには、通信プロトコルとしてTLS 1.2を使用されることをお勧めします。
    TLS 1.2のSession Recordingサポートを構成するには：
  1. Session Recordingサーバーをホスティングしているコンピューターにログオンし、適切なSQL Serverクライアントコンポーネントとドライバーをインストールし、.NET Framework（バージョン4以降）に対して強固な暗号を設定します。
     a. Microsoft ODBC Driver for SQL Serverバージョン11以降をインストールします。
     b. .NETフレームワークの最新のホットフィックスロールアップを適用します。
     c. 使用している.NETフレームワークのバージョンに基づいてADO.NET - SqlClientをインストールします。詳しくは、https://support.microsoft.com/en-us/kb/3135244を参照してください。
     d. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319および HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319の下に、DWORD値SchUseStrongCrypto=1を追加します。
     e. コンピューターを再起動します。
  2. Session Recordingポリシーコンソールをホスティングしているコンピューターにログオンし、.NET Frameworkの最新のホットフィックスロールアップを適用し、.NET Framework（バージョン4以上）に対して強固な暗号を設定します。強固な暗号を設定する方法は、下位手順1-dおよび1-eと同じです。Session Recordingサーバーと同じコンピューターでSession Recordingポリシーコンソールをインストールするように選択している場合は、これらの手順を実行する必要はありません。

2016より前のバージョンのSQL Serverに対するTLS 1.2サポートを構成するには、https://support.microsoft.com/en-us/kb/3135244を参照してください。 TLS 1.2を活用するには、HTTPSを、Session Recordingコンポーネントのための通信プロトコルとして構成します。

Session Recordingセキュリティ機能の構成について詳しくは、Knowledge CenterのCTX200868を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スケーラビリティに関する注意事項

Dec 05, 2017

Session Recordingのインストールと実行のために、XenAppの実行に必要なハードウェア要件を超えて、さらにリソースを追加する必要はほとんどありません。ただし、Session Recordingを使用して数多くのセッションを録画する予定である場合、または画像処理に多くのリソースを消費するアプリケーションを録画するなど、セッションの録画ファイルのサイズが大きくなることが予測される場合は、Session Recordingの展開計画を立てるときに、使用するシステムのパフォーマンスについて検討します。

高スケーラブルなSession Recordingシステムの構築について詳しくは、CTX200869を参照してください。

ハードウェアの推奨事項

各Session Recordingサーバーに送信するデータの量と、サーバーでこのデータを処理し格納するのにかかる時間について考慮します。受信データを格納する速度がデータ入力速度より高速である必要があります。

データ入力速度を推定するには、録画対象のセッションの数をその平均サイズで乗算してから、セッションの録画期間で除算します。たとえば、5,000件のMicrosoft Outlookのセッションの平均サイズが20MBとして、毎営業日に8時間録画するとします。この場合は、データ入力速度はおよそ3.5Mbpsです （5,000セッション×20MB÷8時間÷3,600秒）。

単一のSession Recordingサーバーのパフォーマンスを最適化するか、複数のマシンにSession Recordingサーバーをインストールすることによって、パフォーマンスを向上させることができます。

ディスクとストレージ

ディスクとストレージは、Session Recordingの展開を計画するときに考慮すべき最も重要な要素です。使用するストレージソリューションの書き込み性能は特に重要です。データの書き込み速度が速いほど、システム全体のパフォーマンスが向上します。

ローカルディスクコントローラーまたは接続されたSAN（Storage Area Network：ストレージエリアネットワーク）により、RAIDアレイとしてローカルディスクのセットを制御する方法は、Session Recordingでの使用に適したストレージソリューションです。

注： Session Recordingでは、NAS（Network-Attached Storage：ネットワーク接続ストレージ）を使用しないでください。ネットワークドライブへの録画データの書き込みに関連して、パフォーマンスおよびセキュリティ上の問題が起きる可能性があります。
ローカルドライブにキャッシュメモリが組み込まれているディスクコントローラーを使用すると、パフォーマンスが向上します。キャッシュ機能付きディスクコントローラーには予備電源装置を付け、停電時にもデータの整合性を確保できるようにする必要があります。

ネットワークの性能

Session Recordingサーバーに接続するには100Mbpsのネットワークリンクが適しています。ギガビットイーサネット接続ではパフォーマンスが向上するかもしれませんが、100Mbpsのリンクの10倍のパフォーマンスが得られるわけではありません。

Session Recordingで使用するネットワークスイッチを、使用できるネットワーク帯域幅を求めて競合する可能性のあるサードパーティ製のアプリケーションと共有しないようにします。Session Recordingサーバー専用のネットワークスイッチを用意することが理想的です。

コンピューターの処理性能

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recordingサーバーをインストールするコンピューターについて、次の仕様を検討します。

- デュアルCPUまたはデュアルコアCPUをお勧めします。
- 4GBのRAMをお勧めします。

これらの仕様を超えるコンピューターを使用しても、パフォーマンスが大幅に向上することはありません。

複数のSession Recording Serverの展開

単一のSession Recording Serverではパフォーマンスのニーズを満たせない場合、複数のSession Recording Serverを異なるマシンにインストールできます。 この種の展開では、各Session Recording Serverに専用のストレージ、ネットワークスイッチ、およびデータベースを設定します。 負荷を分散するには、環境内の各Session Recording Agentで、異なるSession Recording Serverを参照するように設定します。

データベースのスケーラビリティ

Session Recordingデータベースでは、Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012、またはMicrosoft SQL Server 2008 R2が必要です。データベースにはセッション録画のメタデータのみが格納されるため、データベースに送信されるデータ量は非常に少なくなります。セッションの録画ファイル自体は別のディスクに書き込まれます。Session RecordingイベントAPIを使用してセッションに検索可能なイベントを挿入するのでなければ、セッション録画1件につきデータベースに必要な容量は通常1KBのみです。

Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012、およびMicrosoft SQL Server 2008 R2のExpress Editionでは、データベースサイズの上限は10GBです。1件のセッション録画あたり1KBのデータが書き込まれるとすれば、この制限があっても、4百万件のセッションをデータベースでカタログ化できます。Microsoft SQL Serverのほかのエディションではデータベースサイズの制限はなく、使用できるディスク容量によってのみ上限が決定されます。データベース内のセッション数が増加するにつれて、データベースのパフォーマンスと検索速度はごくわずかに低下します。

Session RecordingイベントAPIによるカスタマイズを行わない場合は、録画するセッションそれぞれについて、録画開始時に2件、ユーザーがセッションにログオンするときに1件、および録画終了時に1件の、合わせて4件のデータベーストランザクションが生成されます。Session RecordingイベントAPIを使用してセッションをカスタマイズする場合は、記録する検索可能なイベントそれぞれについて1件のトランザクションが生成されます。最も基本的な方式で展開したデータベースで、1秒あたり何百件というトランザクションを制御できるため、データベースの処理負荷が高くなる可能性はほとんどありません。影響が十分に小さいため、XenAppまたはXenDesktopのデータストアデータベースを含めたほかのデータベースと同じSQL Serverで、Session Recordingデータベースを実行できます。

Session Recordingのデータベースで何百万というセッション録画をカタログ化する必要がある場合は、SQL Serverのスケーラビリティに関するMicrosoft社のガイドラインに従います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recordingのインストール、アップグレード、およびアンインストール

Dec 05, 2017

この章では、XenAppおよびXenDesktopインストーラーを使用してSession Recordingをインストールする方法について説明します。以下のセクションがあります。

インストールチェックリスト

Session Recording Administrationコンポーネントのインストール

Directorを構成してSession Recording Serverを使用する

Session Recording Agentのインストール

Session Recording Playerのインストール

インストールの自動化

Session Recordingのアップグレード

Session Recordingのアンインストール

インストールチェックリスト

バージョン7.14以降は、XenAppおよびXenDesktopインストーラーを使用してSession Recordingのコンポーネントをインストールできます。

インストールを始める前に、以下のリストに記載されている作業を行います。

✔	作業
	Session Recordingの各コンポーネントをインストールするマシンを選択し、各コンピューターがインストールするコンポーネントのハードウェアおよびソフトウェアの要件を満たしていることを確認します。
	Citrixアカウント資格情報を使用して、XenAppおよびXenDesktopのダウンロードページにアクセスし、製品のISOファイルをダウンロードします。ISOファイルを解凍するか、ファイルのDVDを作成します。
	Session Recordingコンポーネント間の通信にTLSプロトコルを使用するには、正しい証明書を環境にインストールします。
	Session Recordingコンポーネントに必要なHotfixをインストールします。HotfixはCitrix Supportから入手できます。
	Directorを構成して、Session Recordingポリシーを作成およびアクティブ化します。詳しくは、 Directorを

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	構成してSession Recordingサーバーを使用する」を参照してください。

注：

- 公開アプリケーションのセッション共有は、同じデリバリーグループにあるとアクティブなポリシーと競合することがあるため、公開アプリケーションをSession Recordingポリシーをベースとした個別のデリバリーグループに分割することを推奨します。Session Recordingでは、アクティブなポリシーとエンドユーザーが最初に開いた公開アプリケーションを照合します。
- Machine Creation Services（MCS）またはProvisioning Servicesを使用する計画がある場合は、一意なQMIdを準備します。この手順の実行に失敗すると、録画データが損失する可能性があります。
- SQL ServerではTCP/IPを有効にする必要があり、SQL Server Browserサービスが実行中で、またWindows認証の使用が必要です。
- HTTPSを使用するには、TLS/HTTPSのサーバー証明書を構成します。
- **[ローカルユーザーとグループ]** > **[グループ]** > **[ユーザー]** のユーザーにC:\windows\Tempフォルダーに対する書き込み権限が付与されていることを確認します。

Session Recording Administrationコンポーネントのインストール

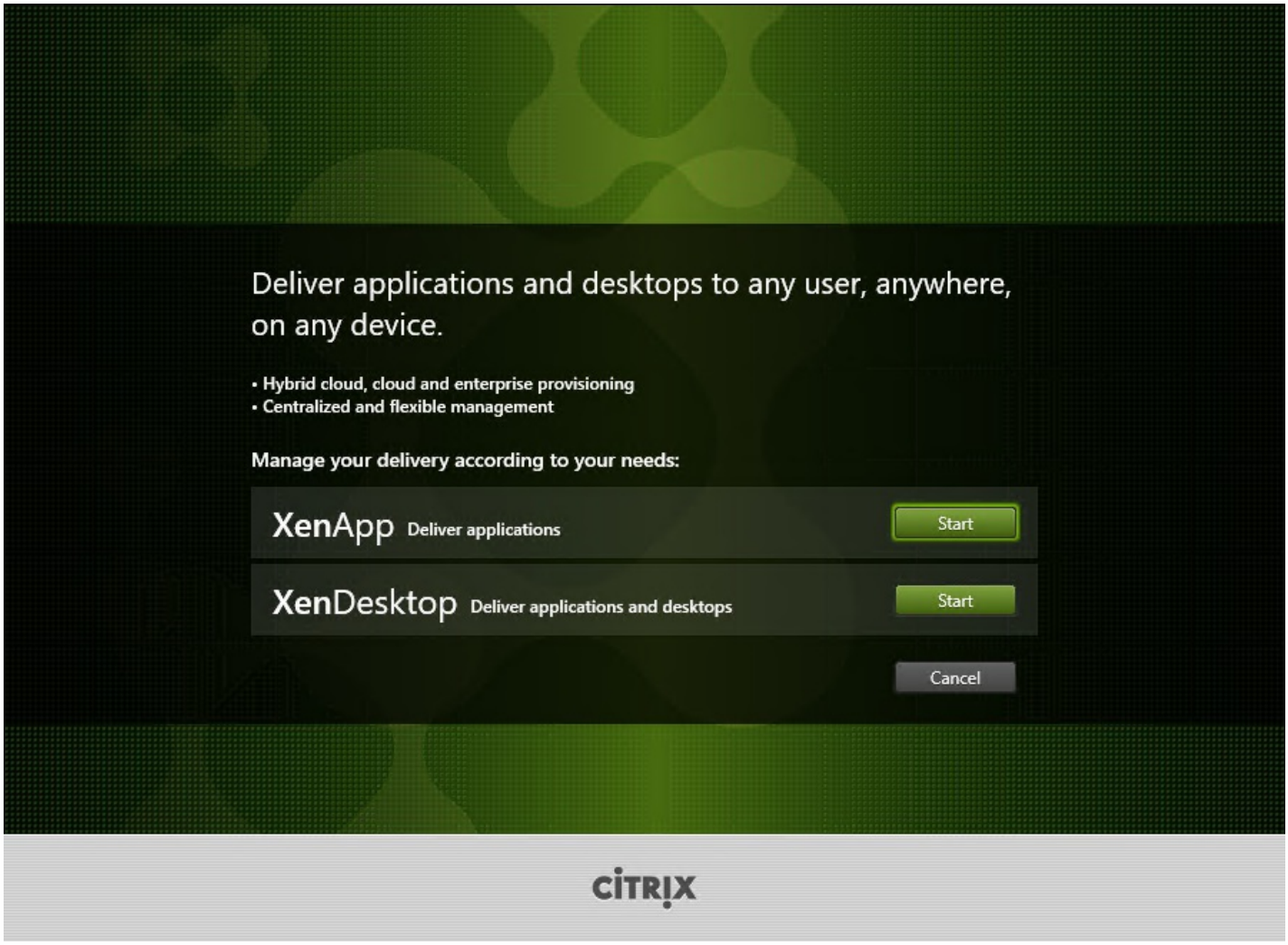
Citrixでは、Session Recording Administration、Session Recording Agent、およびSession Recording Playerの各コンポーネントを別々のサーバーにインストールすることをお勧めします。Session Recording Administrationコンポーネントは、Session Recordingデータベース、Session Recording Server、およびSession Recording Policy Consoleから構成されています。これらのコンポーネントのうち、サーバーにインストールするコンポーネントを選択できます。

手順1：製品ソフトウェアをダウンロードしてウィザードを起動する

1. XenAppおよびXenDesktopのISOのダウンロードが済んでいない場合は、Citrixアカウント資格情報を使用してXenAppおよびXenDesktopのダウンロードページにアクセスし、製品のISOファイルをダウンロードします。ISOファイルを解凍するか、ファイルのDVDを作成します。
2. ローカルの管理者アカウントを使って、Session Recording Administrationコンポーネントのインストール先マシンにログオンします。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**ファイルまたはマウントしたドライブをダブルクリックします。
   インストールウィザードが起動します。

手順2：インストールする製品を選択する

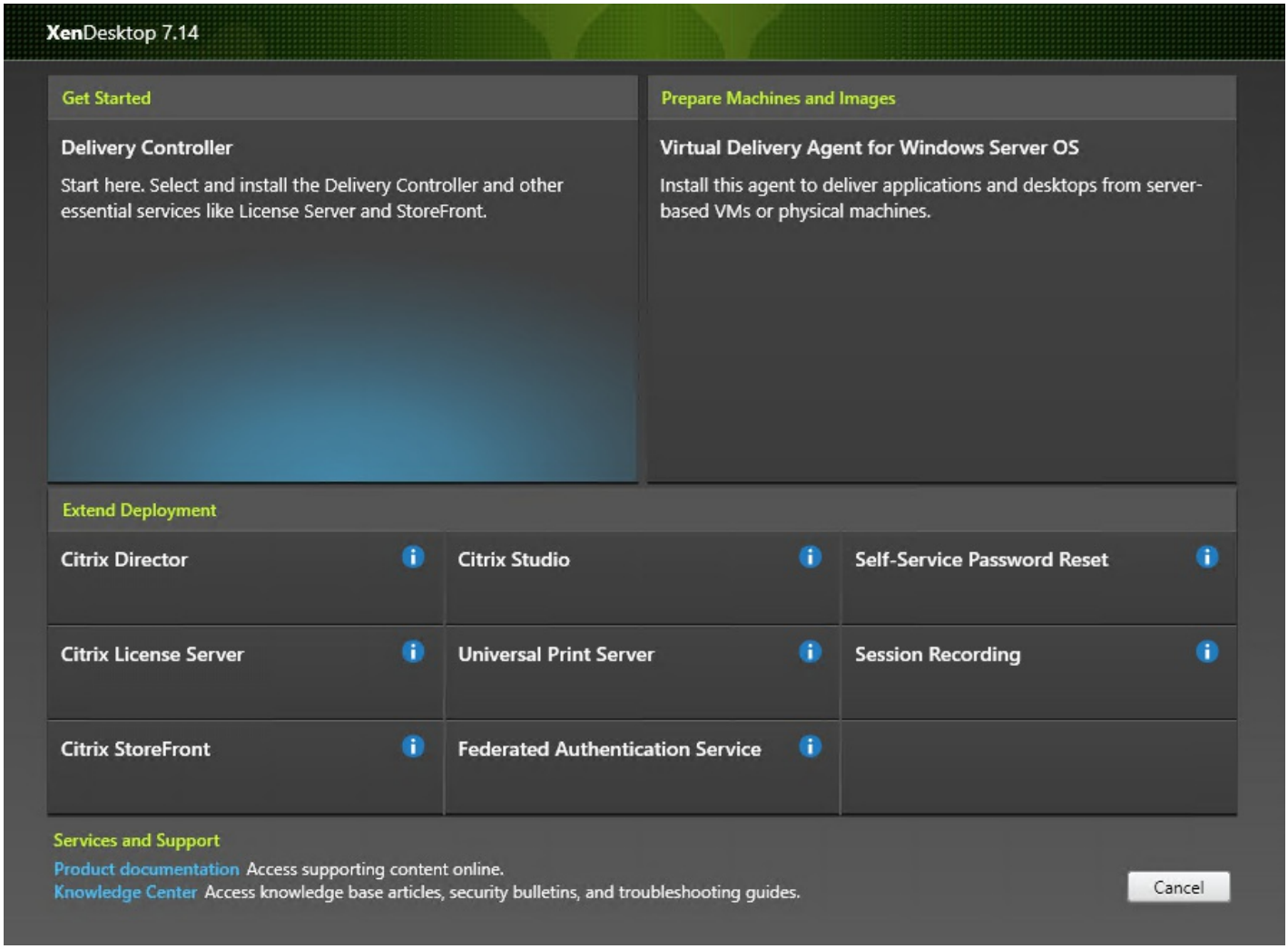
© 1999-2017 Citrix Systems, Inc. All rights reserved.



インストールする製品の隣の **[開始]** をクリックします： **XenApp**または**XenDesktop**。

手順3：Session Recordingを選択する

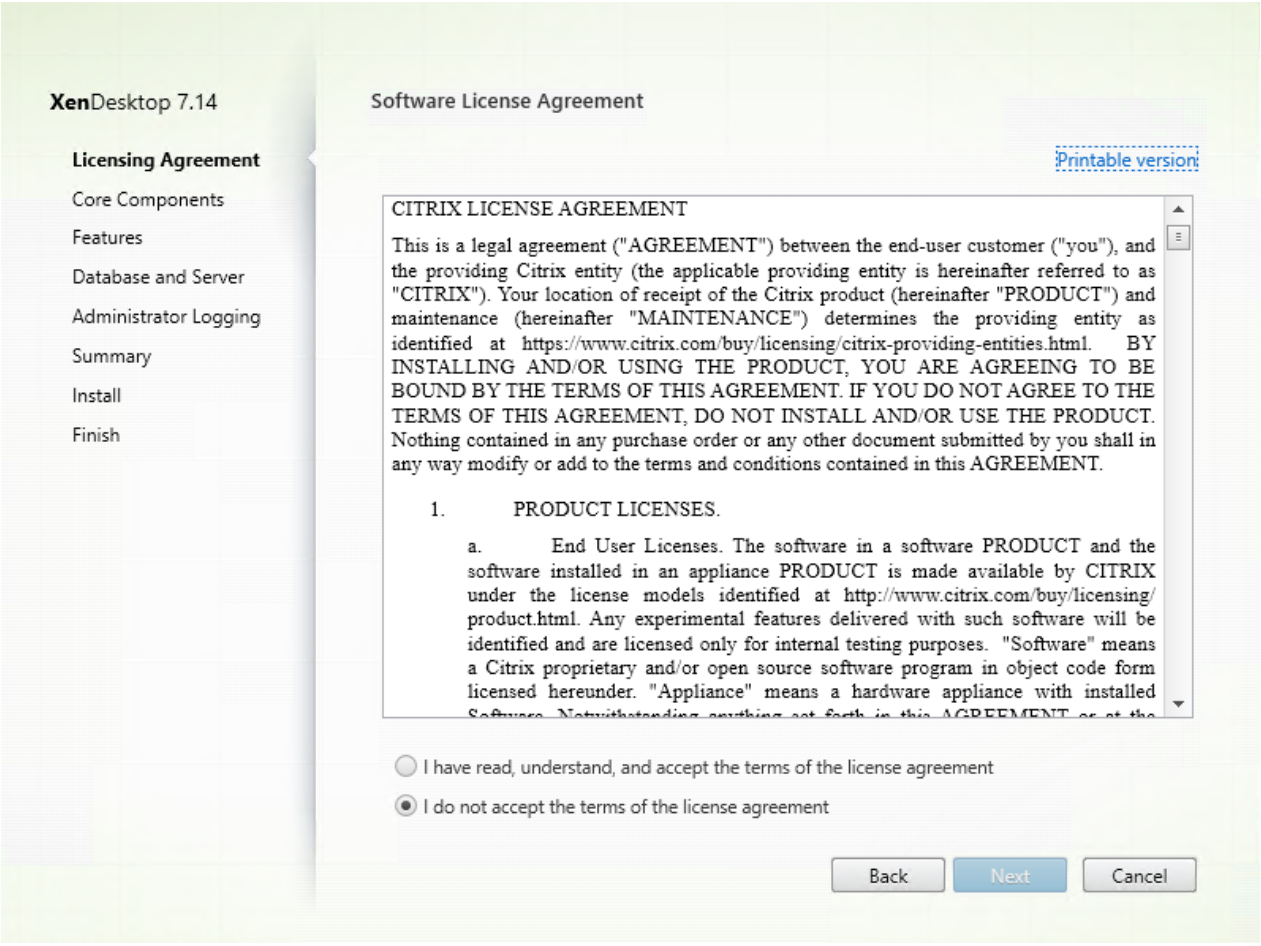
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Session Recordingエントリを選択します。

手順4：ライセンス契約書を読み、同意する

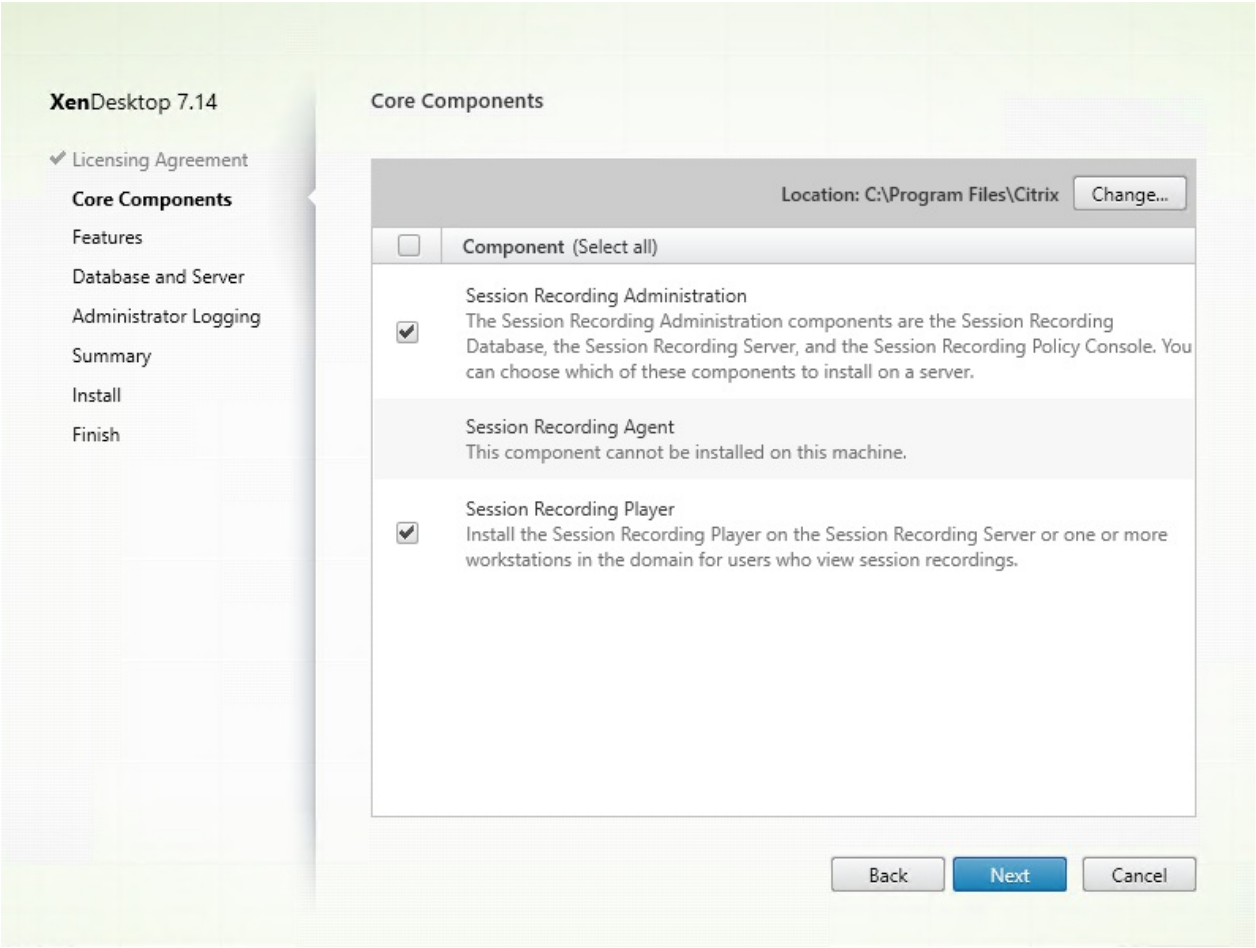
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[ソフトウェアライセンス契約] ページでライセンス契約を読み、同意して [次へ] をクリックします。

手順5：インストールするコンポーネントおよびインストール場所を選択する

© 1999-2017 Citrix Systems, Inc. All rights reserved.

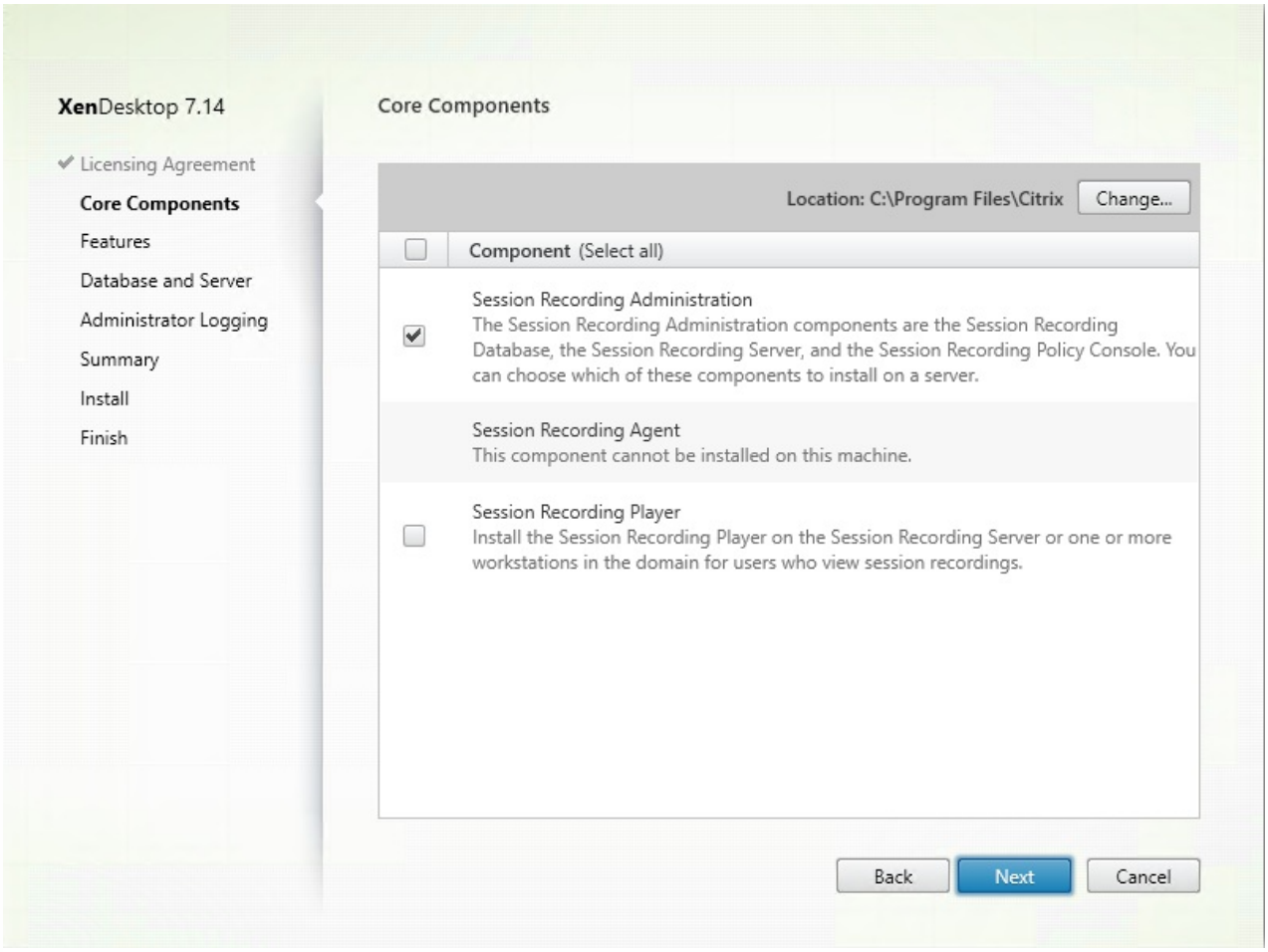


[コア コンポーネント] ページで次の作業を行います。

- **場所：** デフォルトでは、C:\Program Files\Citrixに各コンポーネントがインストールされます。ほとんどの展開ではこれで十分です。任意のインストール場所を指定することもできます。
- **コンポーネント**：デフォルトでは、インストールするコンポーネントの隣のすべてのチェックボックスがオンになっています。インストーラーは、デスクトップOSとサーバーOSのいずれの上で実行されているかを認識しています。Session Recording Administrationコンポーネントのインストールはサーバー OSのみに許可されます。また、事前にVDAがインストールされていないマシンには、Session Recording Agentのインストールは許可されません。事前にVDAがインストールされていないマシンにSession Recording Agentをインストールする場合、**Session Recording Agent**のオプションは利用できません。

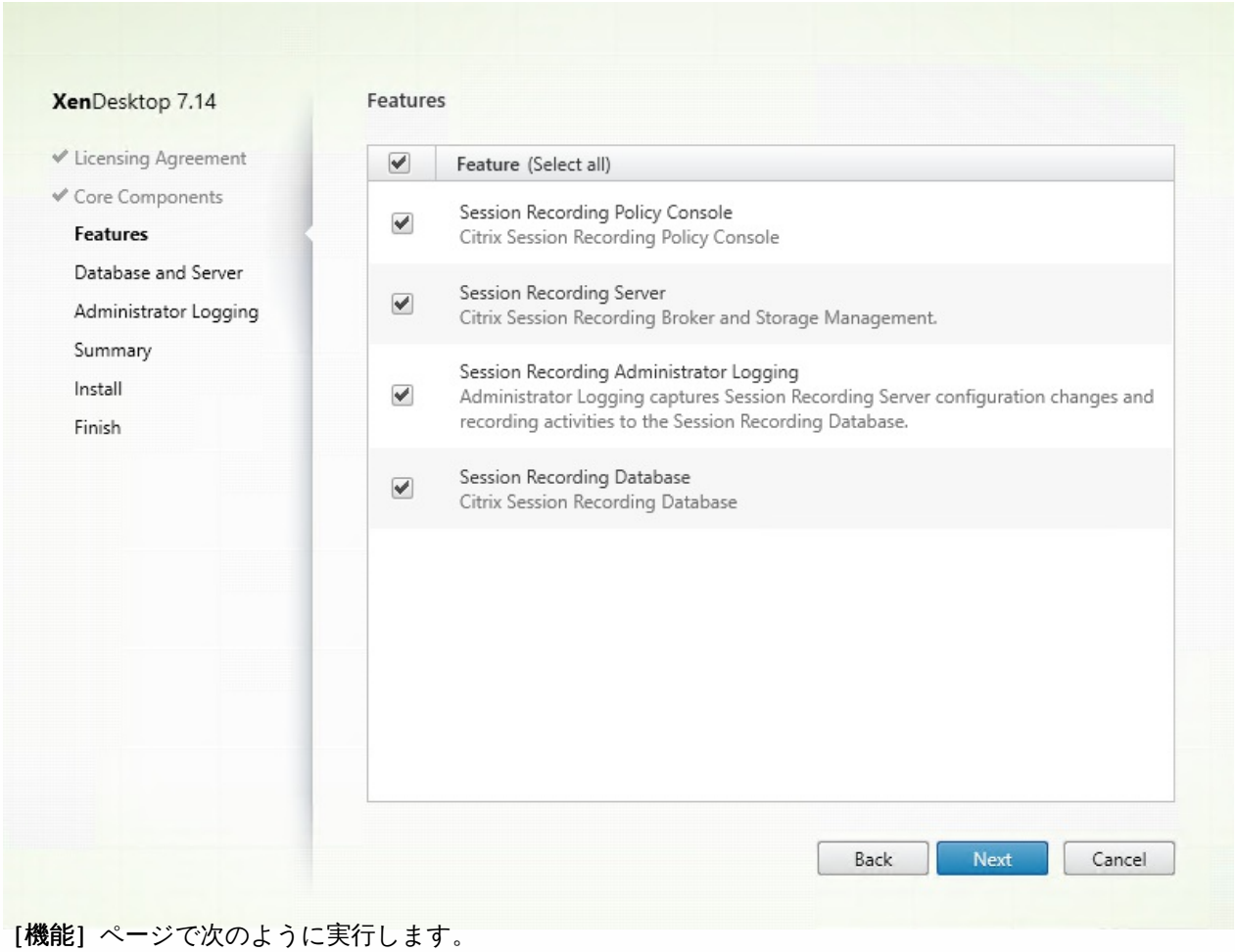
[**Session Recording Administration**] を選択して [**次へ**] をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



手順6：インストールする機能を選択する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[機能] ページで次のように実行します。

- デフォルトでは、インストールする機能の隣のすべてのチェックボックスがオンになっています。概念実証では、これらすべての機能を1つのサーバーにインストールしても構いません。ただし、大規模な実稼働環境の場合は、Citrixでは Session Recording Policy Consoleをインストールしたサーバーとは別のサーバーに、Session Recording Server、Session Recording Administrator Logging、およびSession Recordingデータベースをインストールすることをお勧めします。 Session Recording Administrator Loggingは、Session Recording Serverのオプションのサブ機能であることに注意します。 Session Recording管理者ログを選択する前に、Session Recordingサーバーを選択する必要があります。
- 機能を選択してインストールした後で同じサーバーに別の機能を追加する場合、インストーラーはもう実行できないため、msiパッケージを実行します。

インストールする機能を選択して **[次へ]** をクリックします。

手順6.1：Session Recordingデータベースのインストール

注： Session Recordingデータベースは実際のデータベースではありません。インストール中にMicrosoft SQL Serverインスタンスに必要なデータベースを作成して構成する役割のコンポーネントです。Session Recordingでは、Microsoft SQL Serverに基づくデータベースの高可用性のための3つのソリューションをサポートしています。詳しくは、「データベース高可用性をサポートするSession Recordingのインストール」を参照してください。

Session RecordingデータベースとMicrosoft SQL Serverの展開には、通常以下の3種類があります。

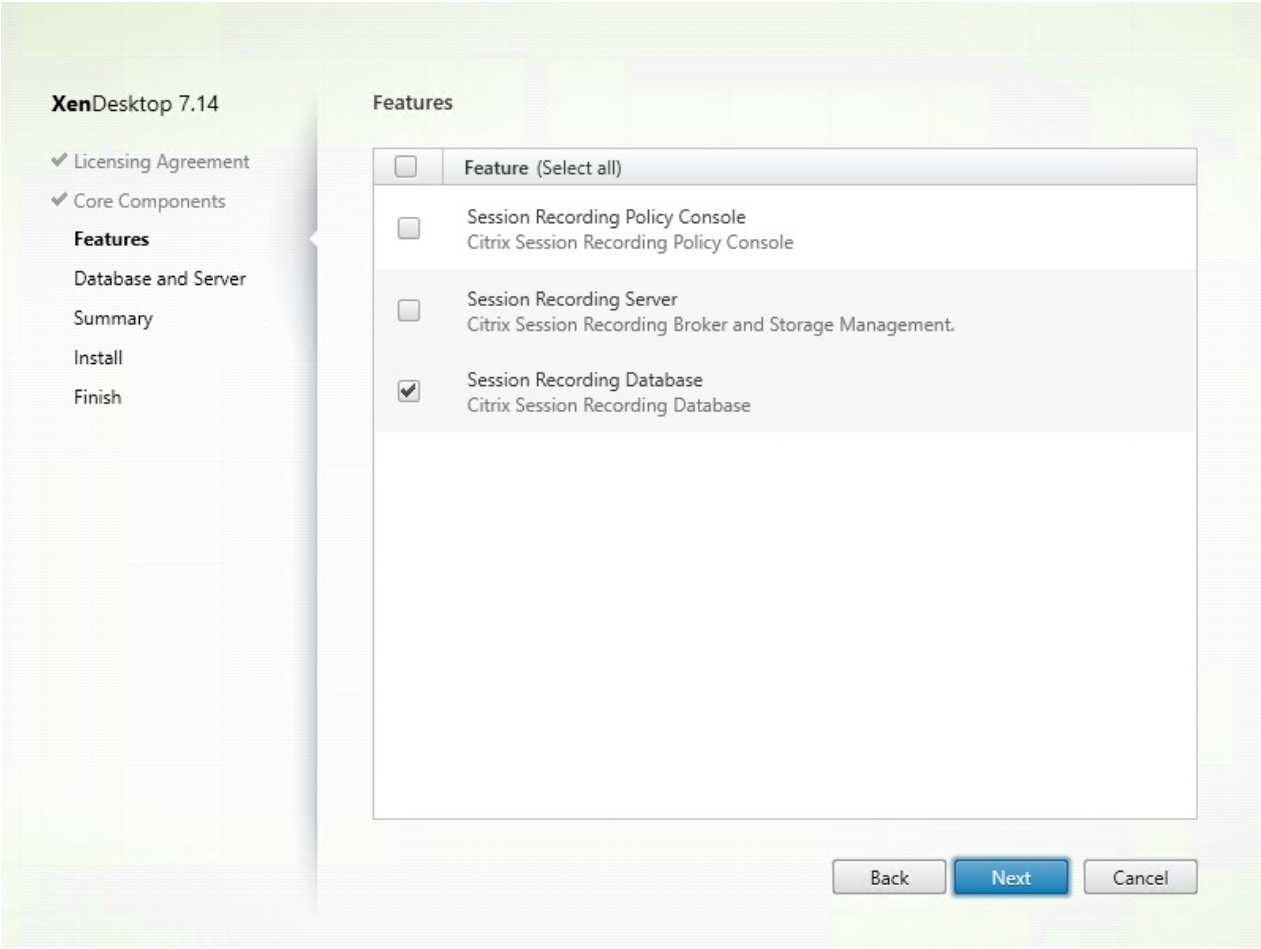
- 展開1： Session RecordingサーバーとSession Recordingデータベースを同じマシンにインストールし、Microsoft SQL Serverをリモートマシンにインストールする （**推奨**）。
- 展開2：Session Recordingサーバー、Session Recordingデータベース、およびMicrosoft SQL Serverを同じマシンにインス

© 1999-2017 Citrix Systems, Inc. All rights reserved.

トールする。

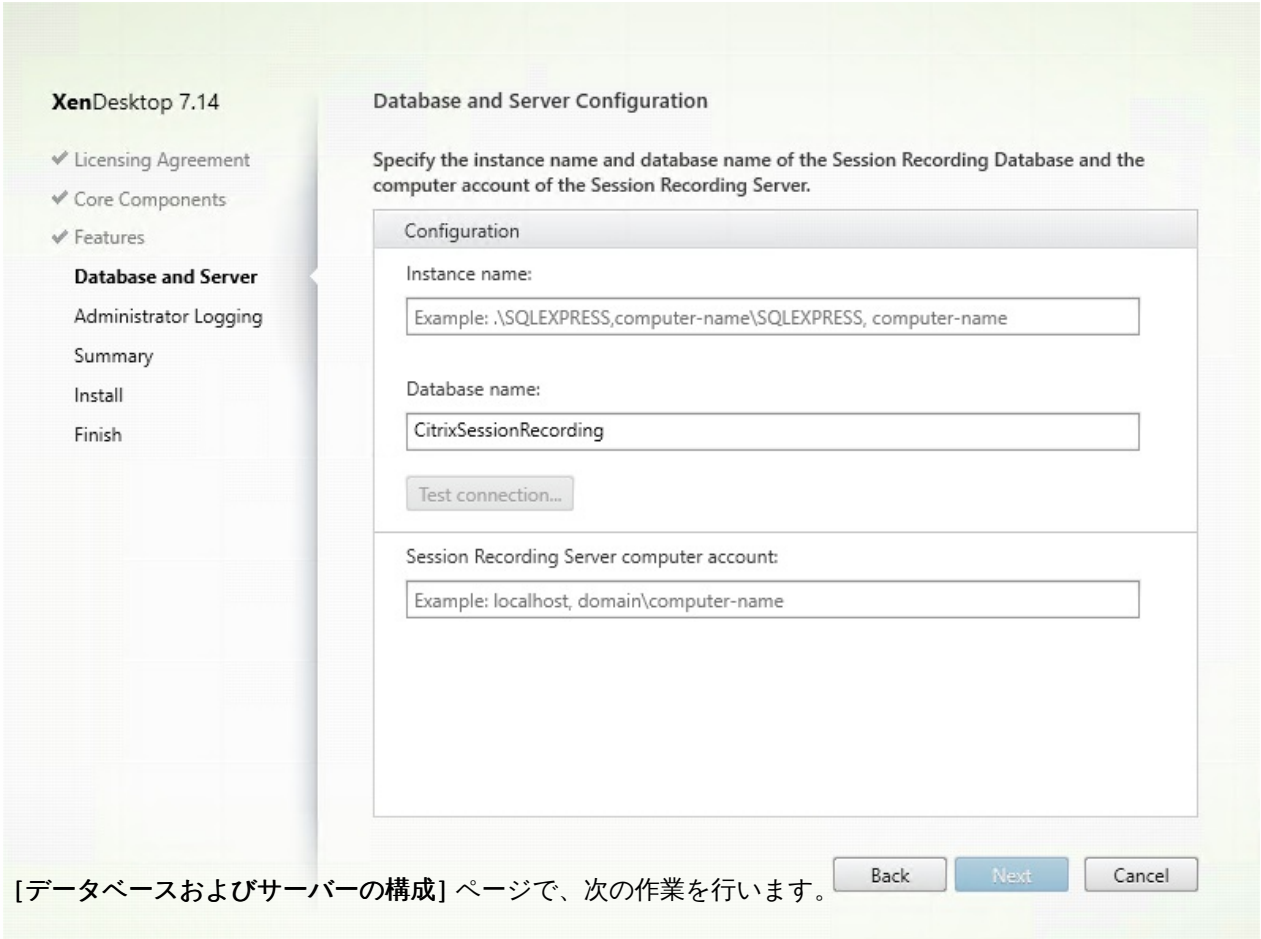
- Session Recordingデータベースのインスタンス名とデータベース名、およびSession Recordingサーバーのコンピューターアカウントを指定します。展開3：Session Recordingサーバーをあるマシンにインストールし、Session RecordingデータベースとMicrosoft SQL Serverの両方を別のマシンにインストールする（**推奨されません**）。

1. **[機能]** ページで **[Session Recordingデータベース]** を選択して **[次へ]** をクリックします。



2. **[データベースおよびサーバーの構成]** ページで、Session Recordingデータベースのインスタンス名とデータベース名、およびSession Recordingサーバーのコンピューターアカウントを指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[データベースおよびサーバーの構成] ページで、次の作業を行います。

- **インスタンス名**：データベースインスタンスが、インスタンスのセットアップ時に構成した名前付きインスタンスでない場合、SQL Serverのコンピューター名のみを使用できます。名前付きインスタンスがある場合は、データベースインスタンス名としてcomputer-name\instance-nameを使用します。使用中のサーバーインスタンス名を確認するには、SQL Serverで**select @@servername**を実行します。戻り値が正確なデータベースインスタンス名です。
- **データベース名**：**[データベース名]** テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名を使用します。 **[接続のテスト]** をクリックして、SQL Serverインスタンスへの接続とデータベース名の有効性をテストします。

> ## Important
>
> 自由なデータベース名に使用できる文字は、A～Z、a～z、0～9のみで、123文字を超えてはなりません。

- データベースの**securityadmin** および**dbcreator** サーバー役割権限が必要です。権限がない場合は、次を行います。
  - データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、**securityadmin** および**dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、SessionRecordingAdministrationx64.msiパッケージを使用します（ISOファイルを解凍すると、このmsiパッケージが...\x64\Session Recordingの下にあります）。msiのインストール中、**securityadmin**および**dbcreator**サーバー役割権限と共に、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、 **[OK]** をクリックし、インストールを続行します。

    インストールにより新しいSession Recordingデータベースが作成され、Session Recordingサーバーのマシンアカウントが**db_owner**として追加されます。

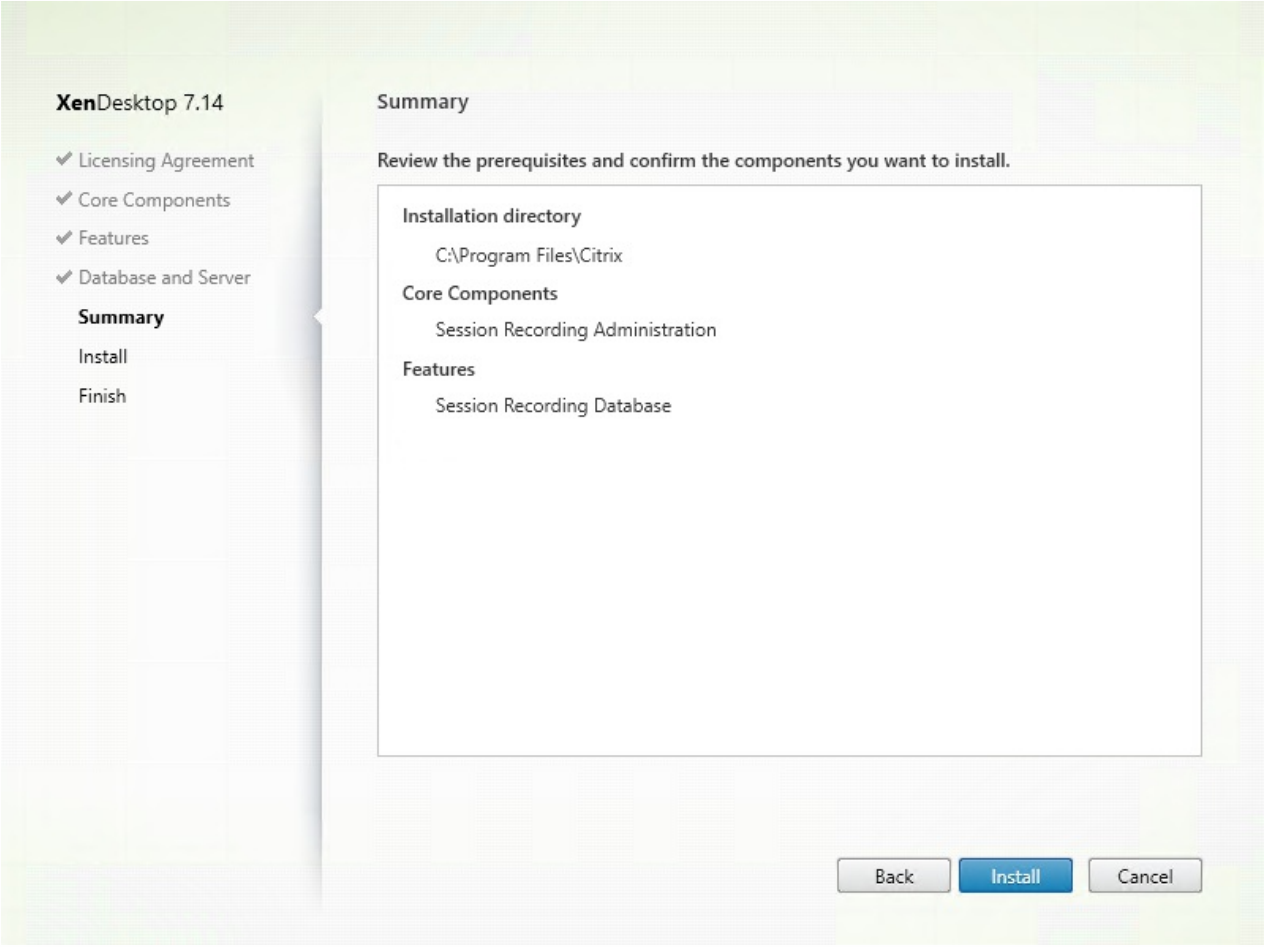
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Session Recordingサーバーコンピューターアカウント**:
  - **展開1と展開2**:**Session Recordingサーバーの［コンピューターアカウント］**フィールドで、「**localhost**」と入力します。
  - **展開3**:Session Recordingサーバーをホストするコンピューターの名前を、「ドメイン\コンピューター名」の形式で入力します。Session Recordingサーバーのコンピューターアカウントは、Session Recordingデータベースにアクセスするためのユーザーアカウントです。

    メモ:**Session Recordingサーバーの［コンピューターアカウント］**フィールドにドメイン名が設定されているときに、Session Recording Administrationコンポーネントをインストールしようとすると、エラーコード1603で失敗することがあります。回避策として、**localhost** またはNetBIOS ドメイン名\マシン名を**Session Recordingサーバーの［コンピューターアカウント］**フィールドに入力してください。

［Next］をクリックします。

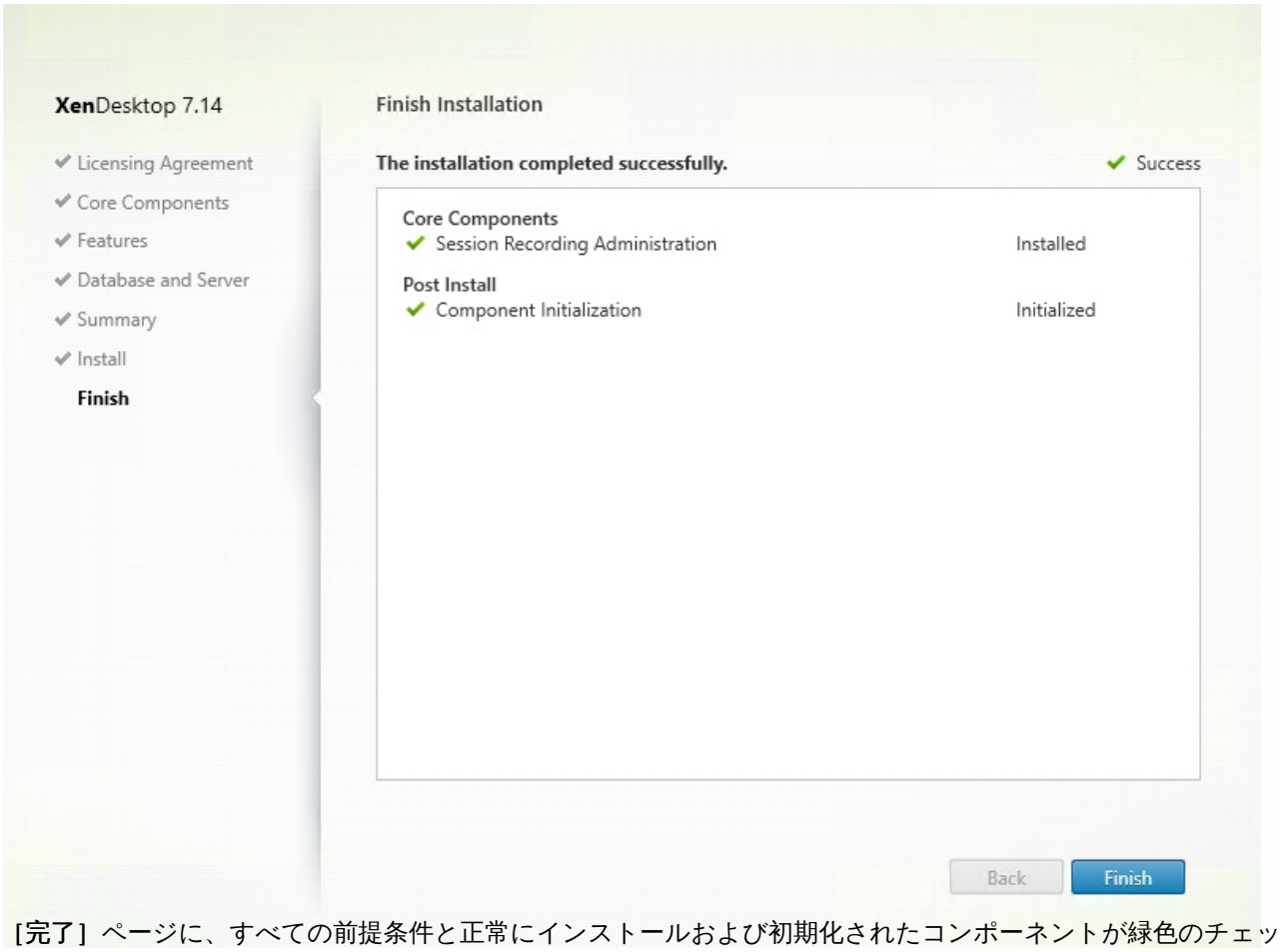
3. インストール前に前提条件を確認します。



［概要］ページにインストールの選択が表示されます。**［戻る］**をクリックして前のウィザードページに戻り、選択を変更できます。または、**［インストール］**をクリックしてインストールを開始します。

4. インストールを完了します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



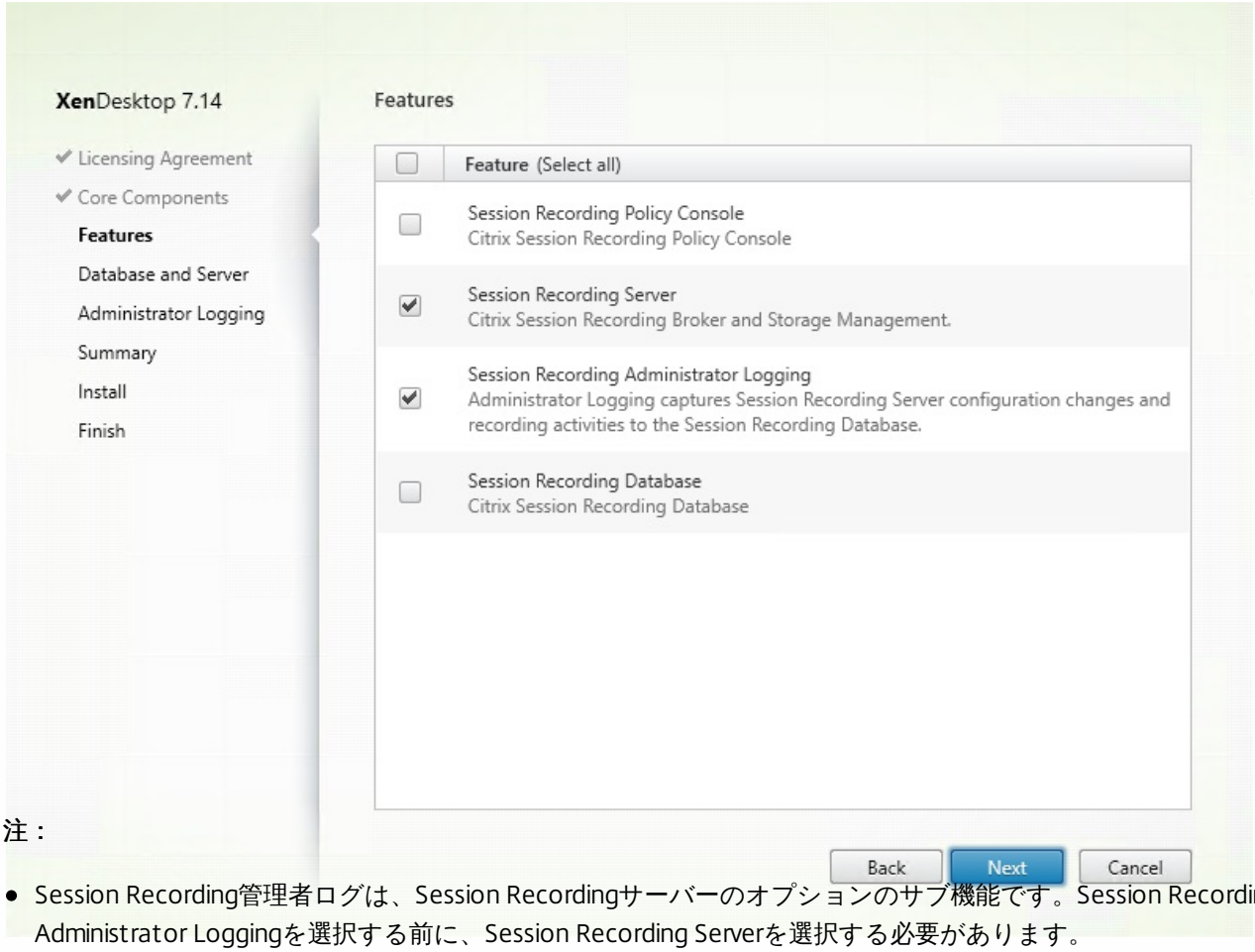
[完了]ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了]をクリックしてSession Recordingデータベースのインストールを完了します。

手順6.2：Session Recordingサーバーのインストール

1. [機能]ページで、[**Session Recording Server**]と[**Session Recording管理者ログ**]を選択します。[次へ]をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

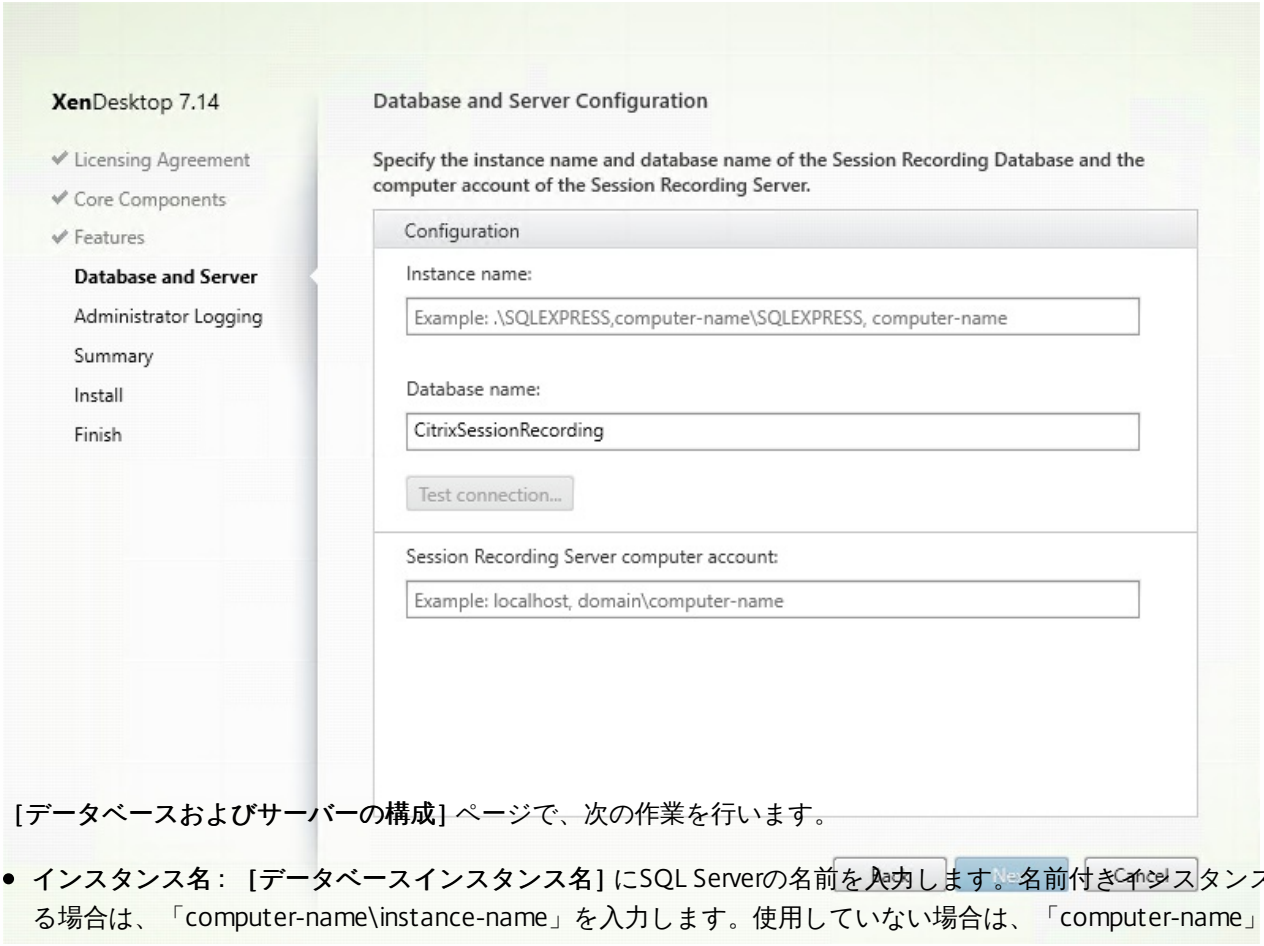


注：

- Session Recording管理者ログは、Session Recordingサーバーのオプションのサブ機能です。Session Recording Administrator Loggingを選択する前に、Session Recording Serverを選択する必要があります。
- Citrixでは、Session Recording Administrator LoggingとSession Recording Serverを同時にインストールすることをお勧めします。Administrator Logging機能を有効にしない場合は、後のページで無効にできます。ただし、最初にこの機能をインストールしない選択をし、後で追加する場合は、SessionRecordingAdministrationx64.msiパッケージを使用して手動で追加するしかありません。

2. **[データベースおよびサーバーの構成]** ページで、構成を指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

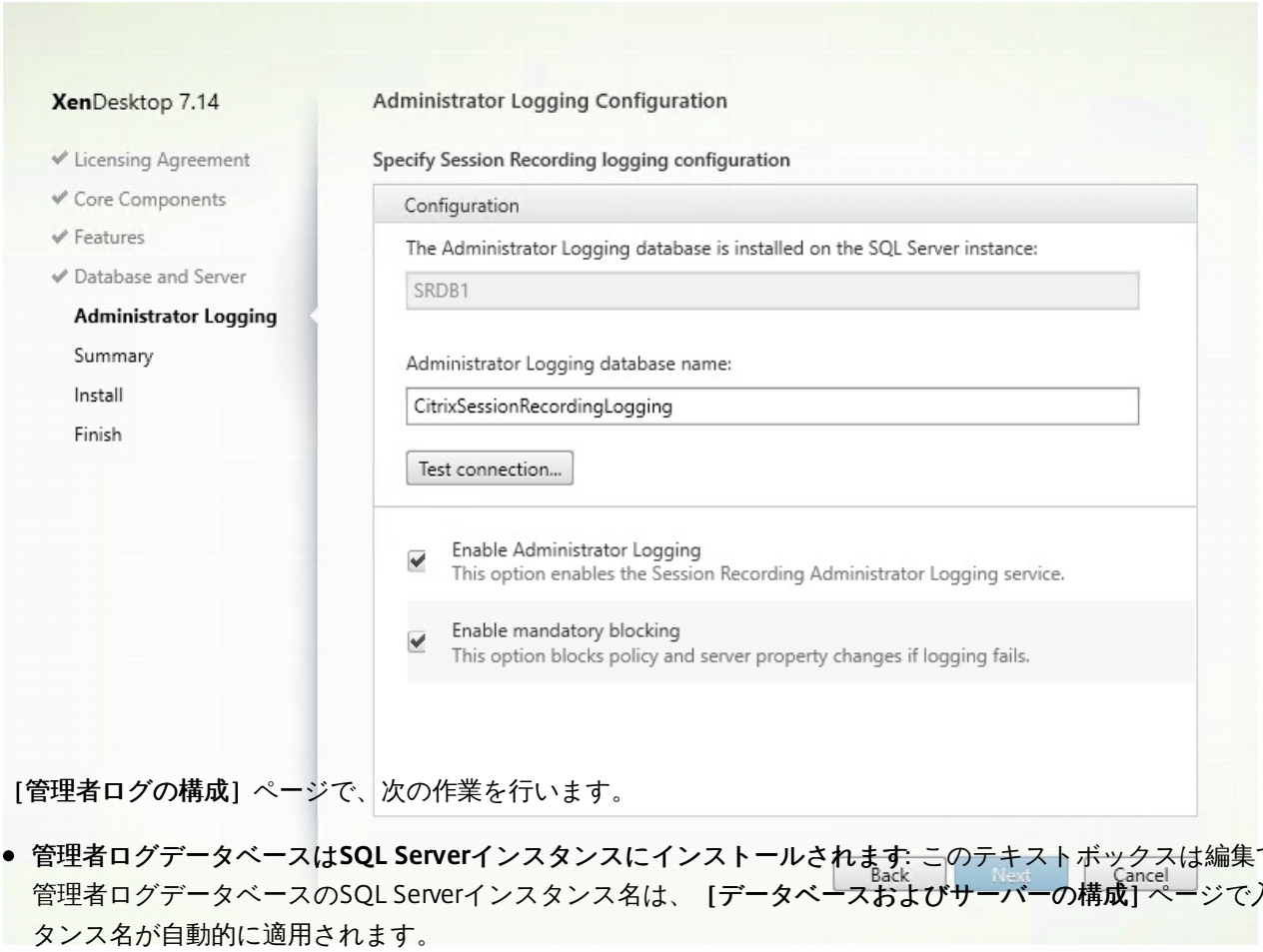


[データベースおよびサーバーの構成] ページで、次の作業を行います。

- **インスタンス名：** **[データベースインスタンス名]** にSQL Serverの名前を入力します。名前付きインスタンスを使用している場合は、「computer-name\instance-name」を入力します。使用していない場合は、「computer-name」だけを入力します。
- **データベース名：** **[データベース名]** テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名**CitrixSessionRecording**を使用します。
- データベースの**securityadmin** および**dbcreator** サーバー役割権限が必要です。権限がない場合は、次を行います。
  - データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、**securityadmin** および**dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、SessionRecordingAdministrationx64.msiパッケージを使用してSession Recordingサーバーをインストールします。msiのインストール中、**securityadmin**および**dbcreator**サーバー役割権限と共に、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、 **[OK]** をクリックし、インストールを続行します。
- 正しいインスタンス名とデータベース名を入力したら、**[接続のテスト]** をクリックしてSession Recordingデータベースへの接続をテストします。
- Session Recordingサーバーのコンピューターアカウントを入力して、**[次へ]** をクリックします。

3. **[管理者ログの構成]** ページで、管理者ログ機能の構成を指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



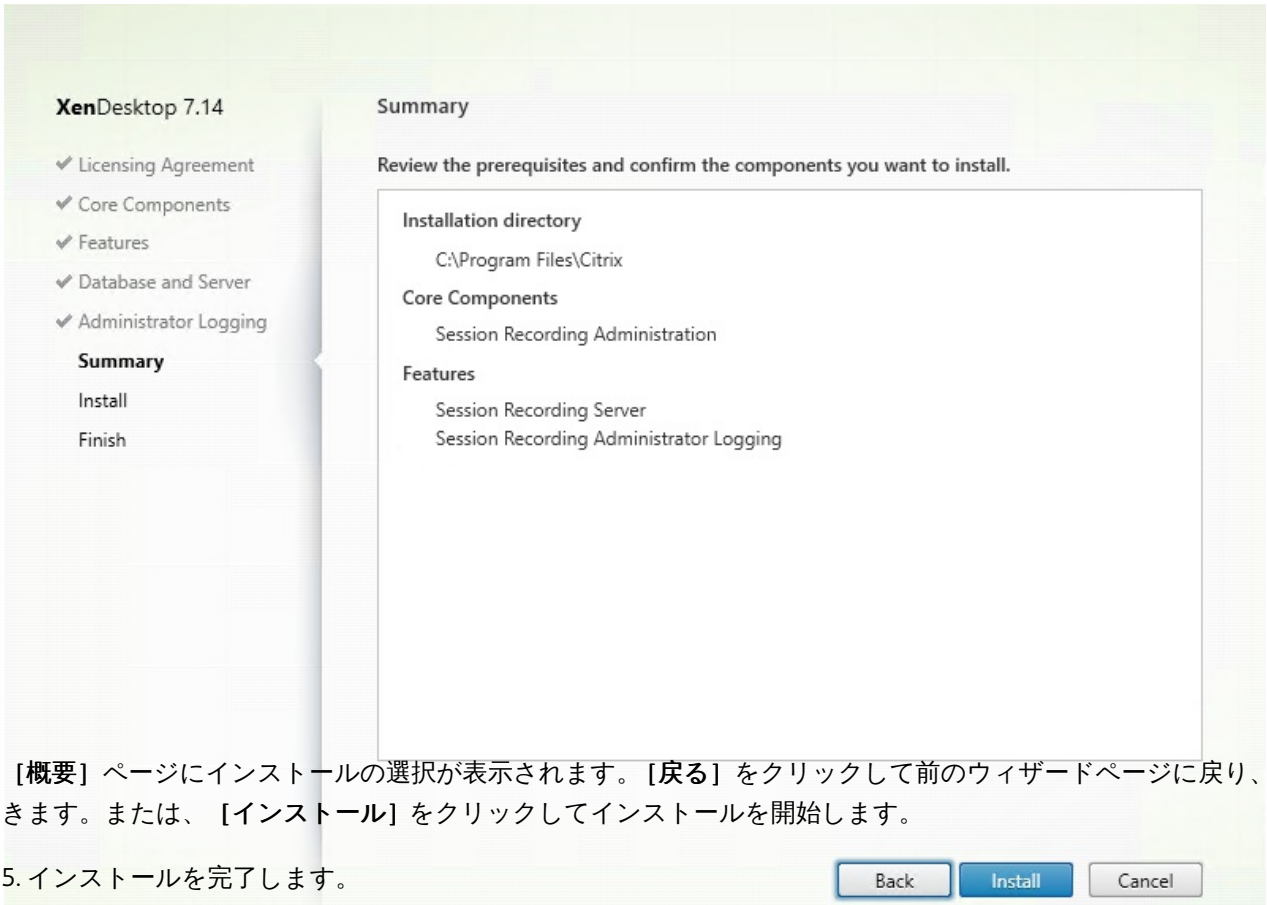
[管理者ログの構成]ページで、次の作業を行います。

- **管理者ログデータベースはSQL Serverインスタンスにインストールされます**: このテキストボックスは編集できません。管理者ログデータベースのSQL Serverインスタンス名は、[データベースおよびサーバーの構成]ページで入力したインスタンス名が自動的に適用されます。
- **管理者ログデータベース名**: Session Recording管理者ログ機能のインストールを選択した場合、このテキストボックスで管理者ログデータベースの任意のデータベース名を入力するか、またはテキストボックスに事前設定されたデフォルトのデータベース名**CitrixSessionRecordingLogging**を使用します。
  メモ：管理者ログデータベース名は、前の**データベースとサーバーの構成**ページの**データベース名**テキストボックスに設定されたSession Recordingデータベース名と異なっている必要があります。
- 管理者ログデータベース名を入力したら、[**接続**のテスト]をクリックして管理者ログデータベースへの接続をテストします。
- **管理者ログを有効にする**：デフォルトでは、管理者ログ機能は有効になっています。チェックボックスをオフにしてこの機能を無効にできます。
- **強制ブロッキングを有効にする**：デフォルトでは強制ブロッキングが有効になっているため、ログが失敗すると通常の機能がブロックされることがあります。チェックボックスをオフにして強制ブロッキングを無効にできます。

[次へ]をクリックしてインストールを続行します。

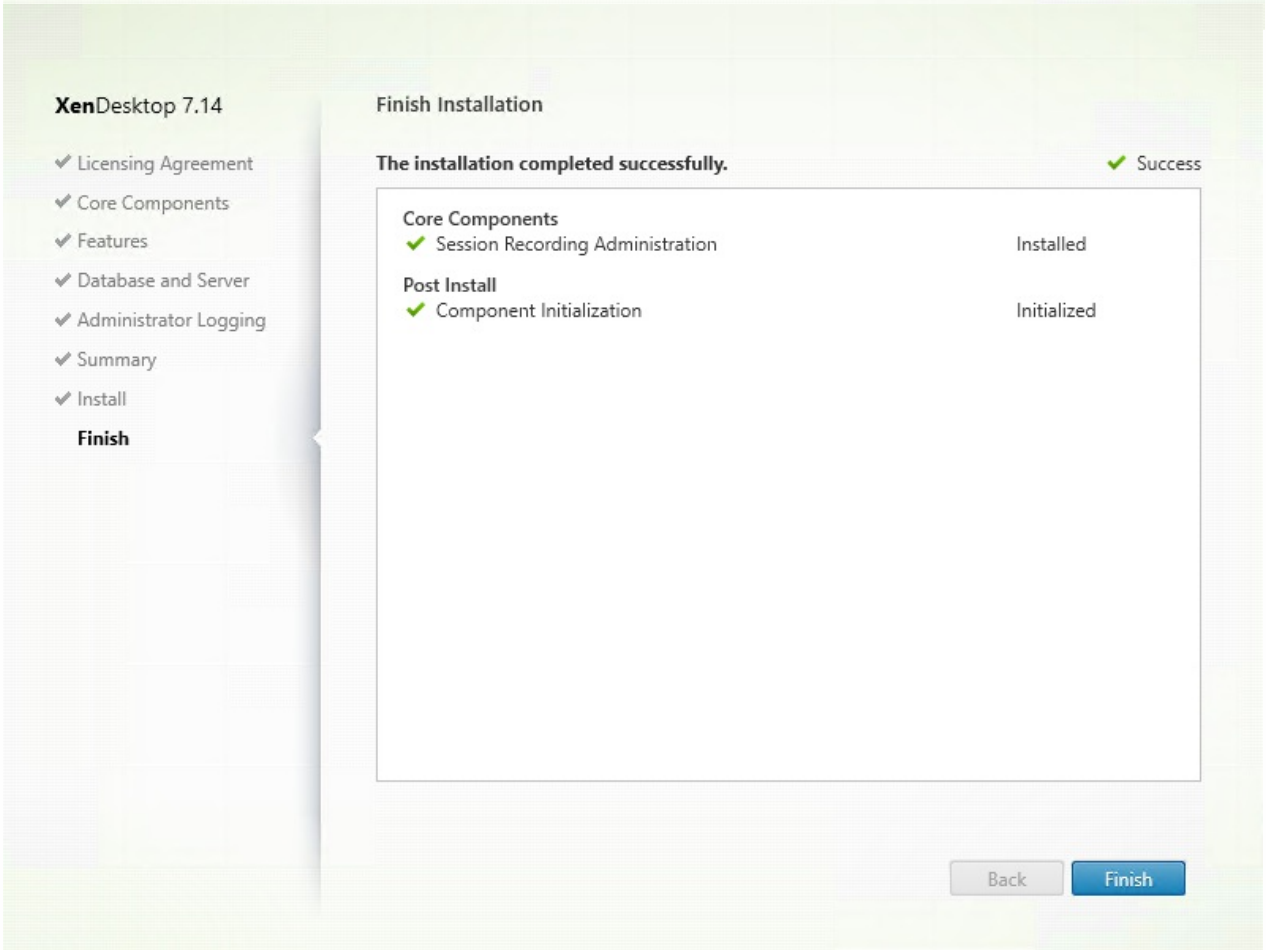
4. インストール前に前提条件を確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[**概要**] ページにインストールの選択が表示されます。[**戻る**] をクリックして前のウィザードページに戻り、選択を変更できます。または、[**インストール**] をクリックしてインストールを開始します。

5. インストールを完了します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

[完了] ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

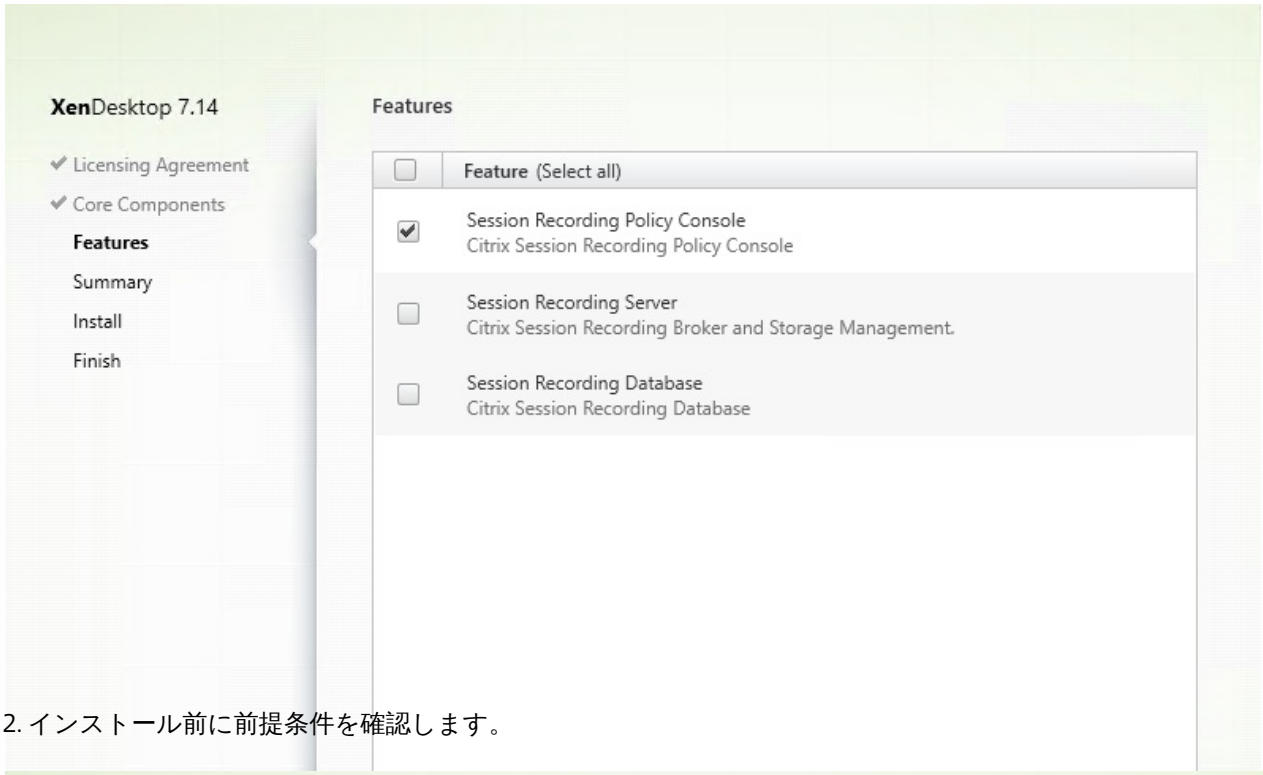
[完了] をクリックしてSession Recordingサーバーのインストールを完了します。

注：Session Recordingサーバーのデフォルトのインストールでは、通信をセキュリティで保護するためHTTPS/TLSを使用します。Session Recordingサーバーのデフォルト IISサイトでTLSが構成されていない場合は、HTTPを使用します。これを実行するには、Session Recording Brokerサイトに移動してIIS管理コンソールでSSLを選択解除し、SSL設定を開き、 **[SSLを必要とする]** ボックスをオフにします。

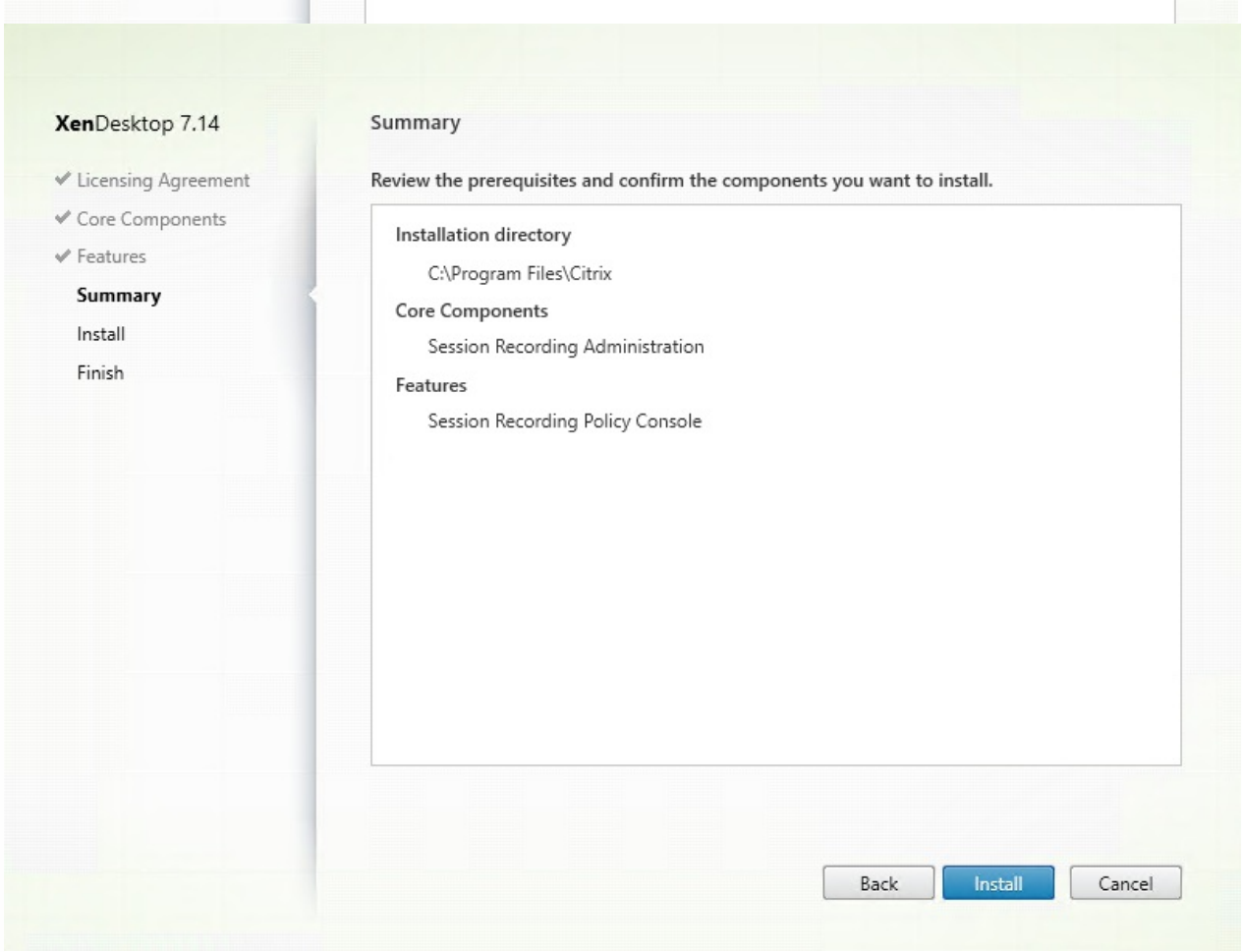
手順6.3：Session Recordingポリシーコンソールのインストール

1. **[機能]** ページで **[Session Recordingポリシーコンソール]** を選択して **[次へ]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



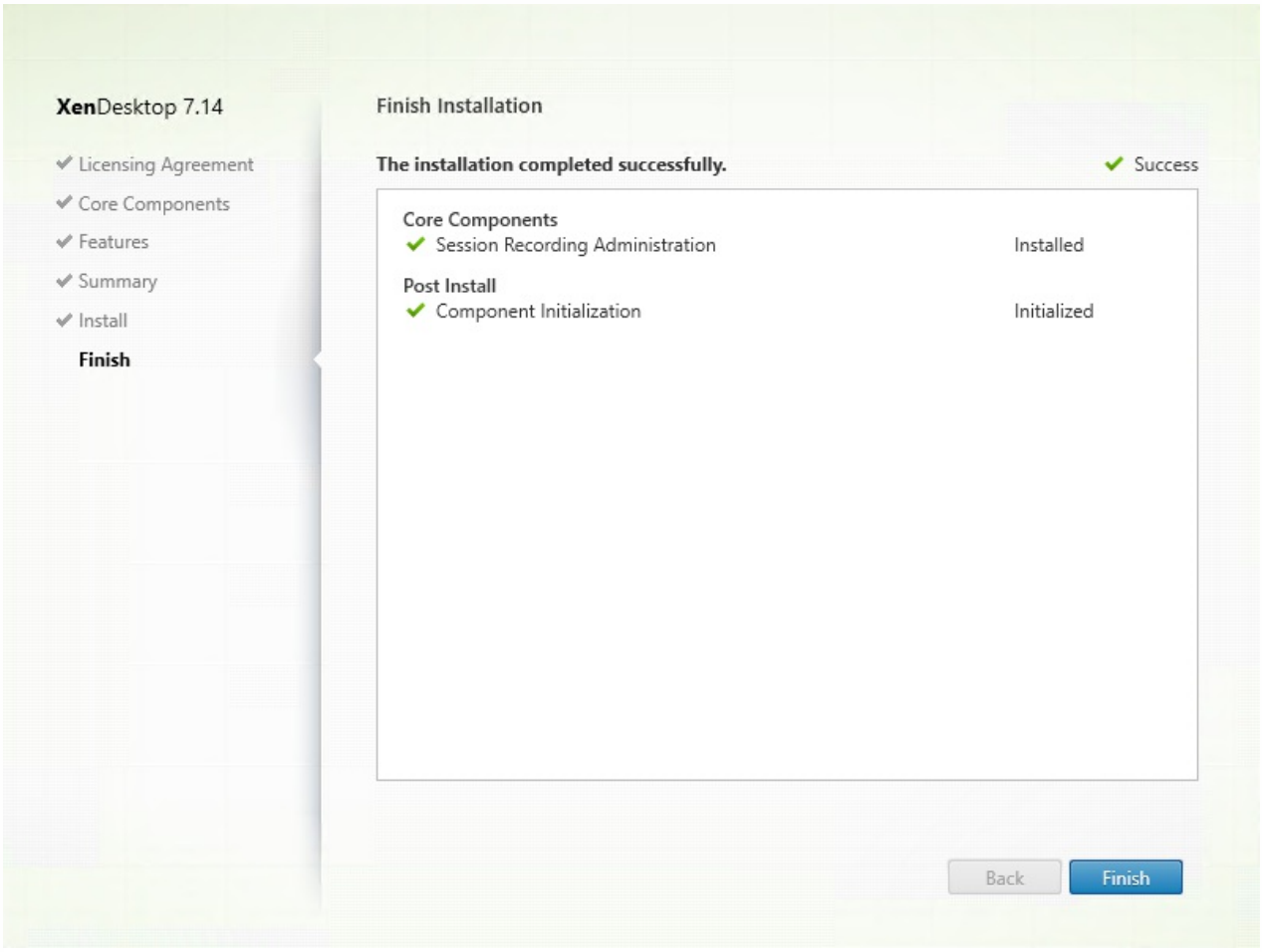
2. インストール前に前提条件を確認します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

［**概要**］ページにインストールの選択が表示されます。［**戻る**］をクリックして前のウィザードページに戻り、選択を変更できます。または、［**インストール**］をクリックしてインストールを開始します。

3. インストールを完了します。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

［完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックしてSession Recordingポリシーコンソールのインストールを完了します。

手順7：Broker_PowerShellSnapIn_x64.msiをインストールする

重要：Session Recordingポリシーコンソールを使用するには、Broker PowerShellスナップイン（Broker_PowerShellSnapIn_x64.msi）をインストールする必要があります。スナップインは、インストーラーによって自動的にインストールされません。XenAppおよびXenDesktopのISO（\layout\image-full\x64\Citrix Desktop Delivery Controllerの下にあります）でスナップインを検索し、指示に従って手動でインストールする必要があります。従わない場合、エラーが発生する可能性があります。

Directorを構成してSession Recording Serverを使用する

Directorコンソールを使用して、Session Recordingポリシーを作成およびアクティブ化できます。

1. HTTPS接続の場合は、Directorサーバーの［信頼されたルート証明書］にSession Recordingサーバーを信頼する証明書をインストールします。
2. Session Recordingサーバーを使用するようにDirectorサーバーを構成するには、**C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**コマンドを実行します。
3. Directorサーバーで、Session Recording ServerのIPアドレスまたはFQDN、ポート番号、およびSession Recording AgentがSession Recording Brokerとの接続に使用する接続の種類（HTTPまたはHTTPS）を入力します。

Session Recording Agentのインストール

Session Recording Agentは、セッションを録画するVDAまたはVDIマシンにインストールする必要があります。

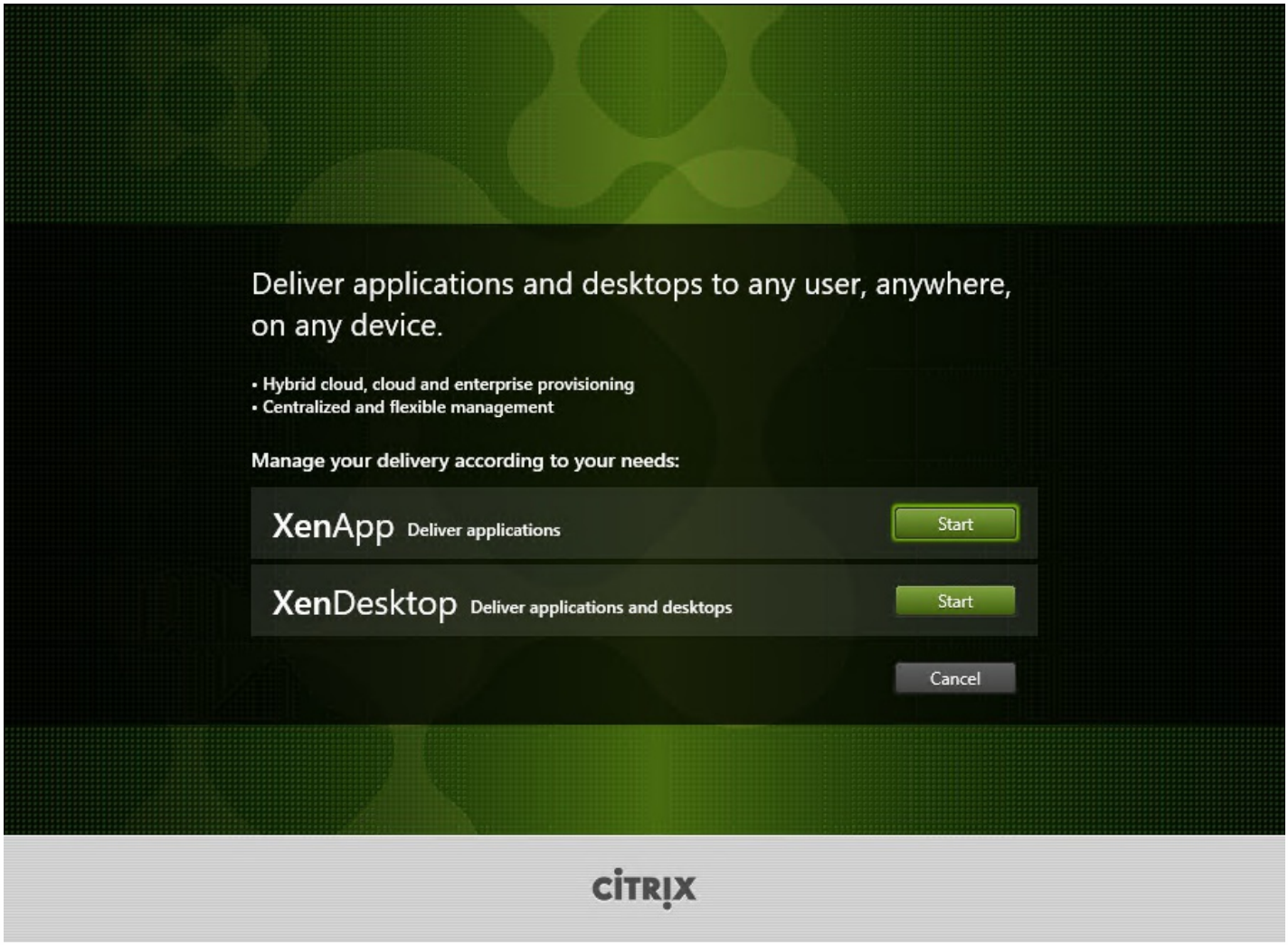
© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順1：製品ソフトウェアをダウンロードしてウィザードを起動する

ローカルの管理者アカウントを使って、Session Recording Agentコンポーネントのインストール先マシンにログオンします。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**ファイルまたはマウントしたドライブをダブルクリックします。

インストールウィザードが起動します。

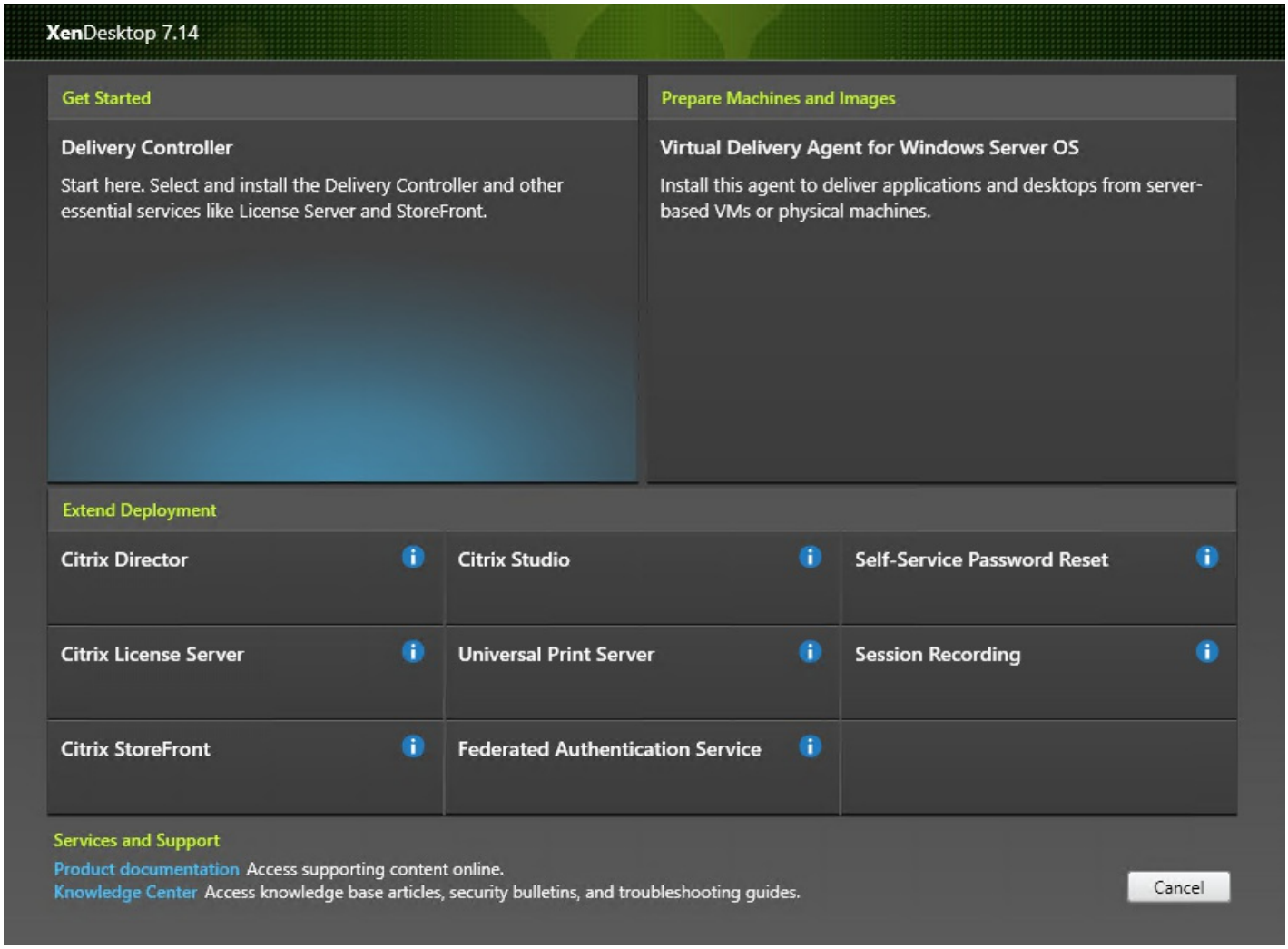
手順2：インストールする製品を選択する



インストールする製品の隣の **[開始]** をクリックします： **XenApp**または**XenDesktop**。

手順3：Session Recordingを選択する

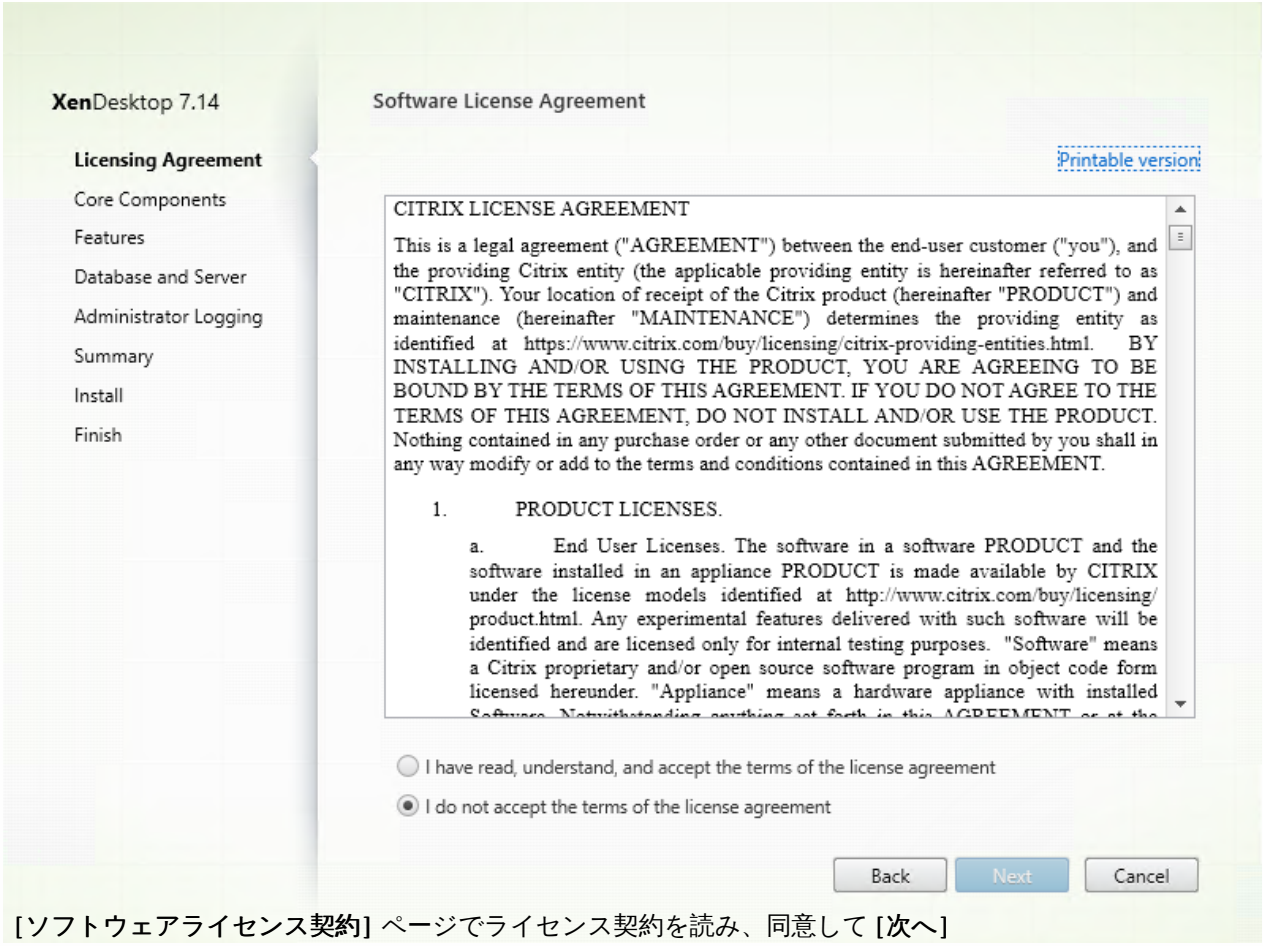
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Session Recordingエントリを選択します。

手順4：ライセンス契約書を読み、同意する

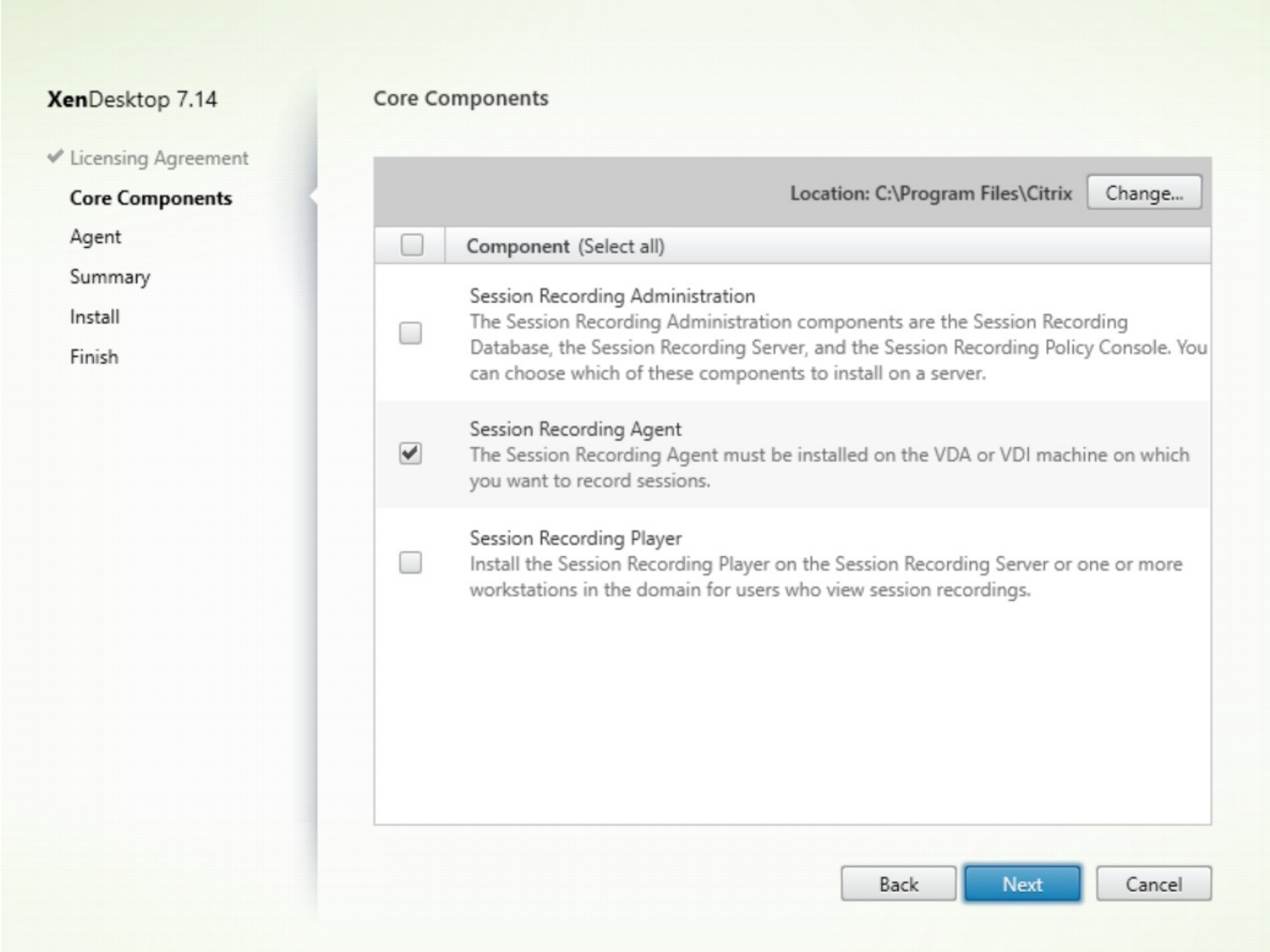
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[ソフトウェアライセンス契約] ページでライセンス契約を読み、同意して **[次へ]** をクリックします。

手順5：インストールするコンポーネントおよびインストール場所を選択する

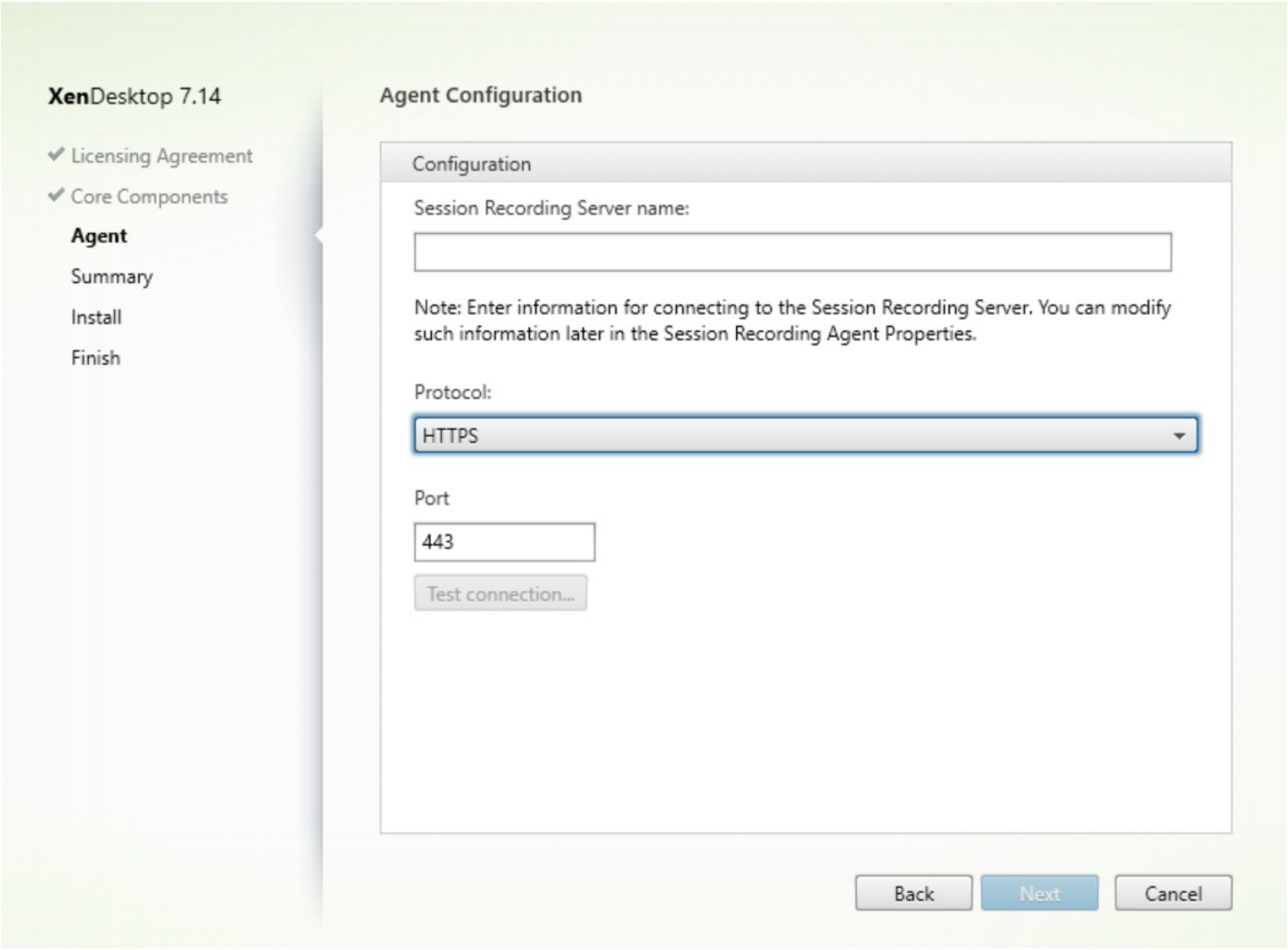
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[**Session Recording Agent**] を選択して [**次へ**] をクリックします。

手順6：Agentの構成を指定する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



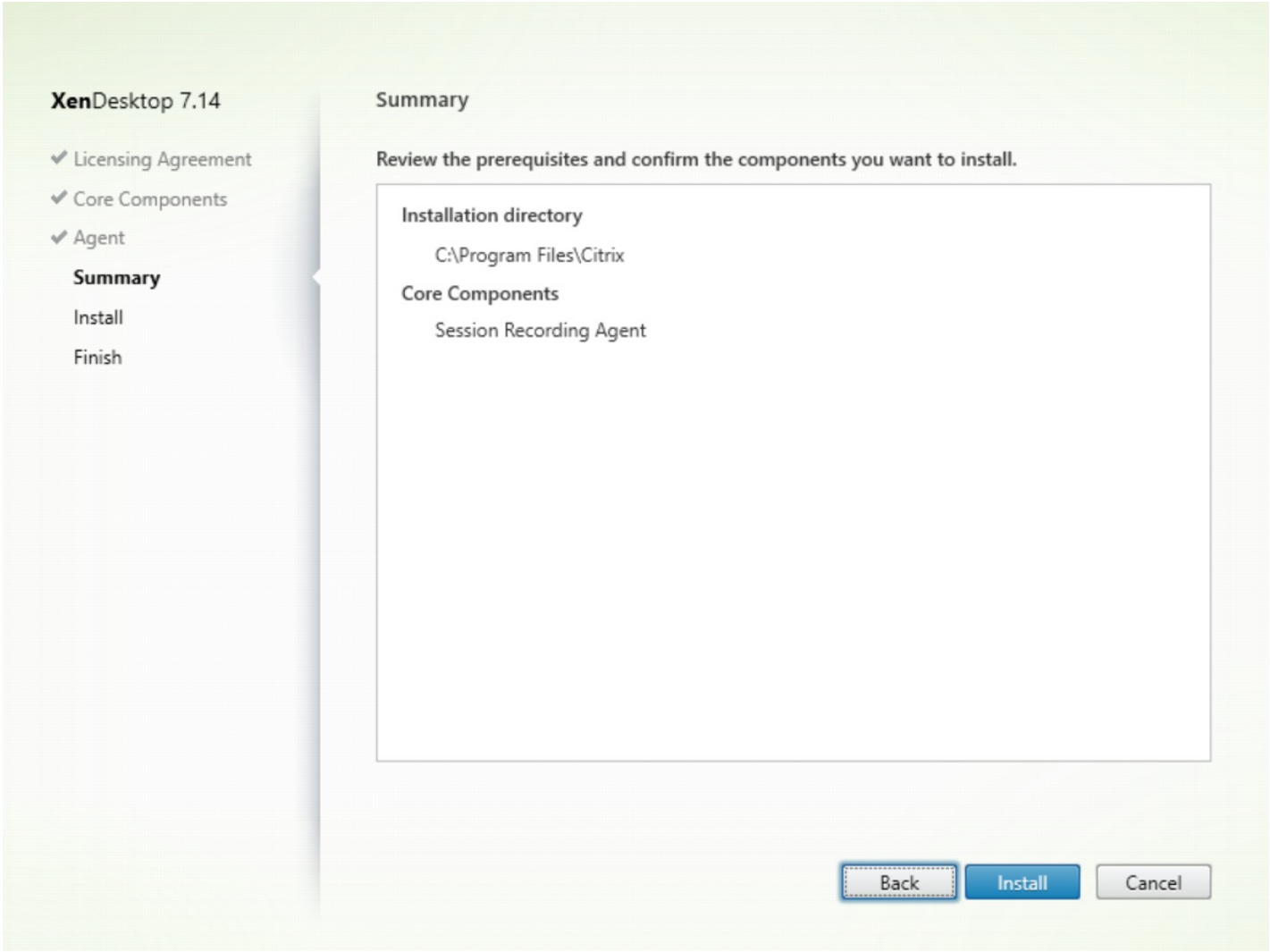
［**Agentの構成**］ページで、次の作業を行います。

- Session Recordingサーバーを事前にインストールしている場合は、Session Recordingサーバーをインストールしたコンピューターの名前と、Session Recordingサーバーとの接続のプロトコルとポート情報を入力します。Session Recordingのインストールが済んでいない場合は、後で**Session Recording Agentのプロパティ**でこれらの情報を変更できます。

注：インストーラーのテスト接続機能には限界があります。「HTTPSがTLS 1.2を必要とする」シナリオはサポートしていません。このシナリオでインストーラーを使用する場合はテスト接続に失敗しますが、失敗を無視して［**次へ**］をクリックし、インストールを続行できます。これによって通常の機能が影響を受けることはありません。

手順7：インストール前に前提条件を確認する

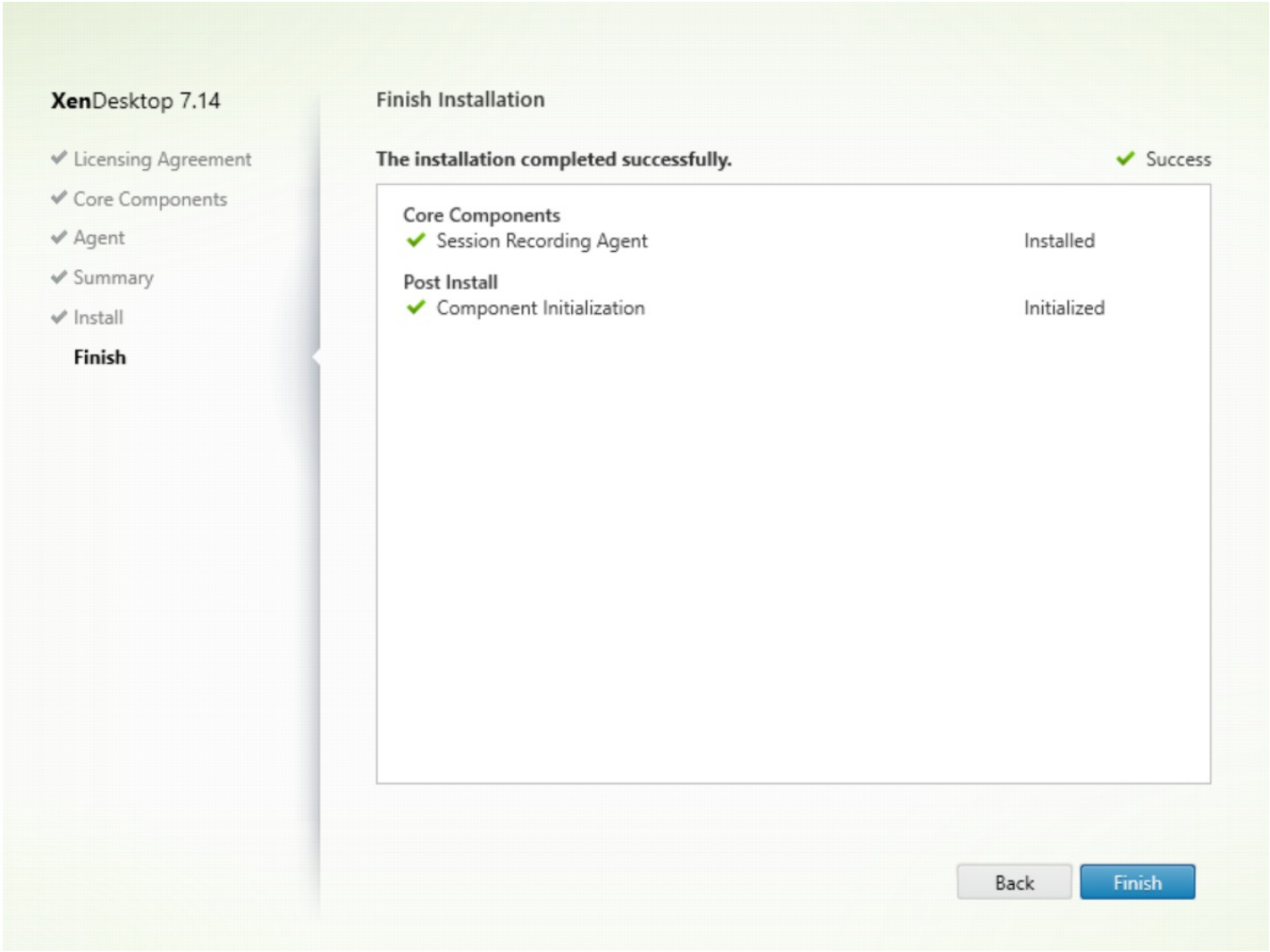
© 1999-2017 Citrix Systems, Inc. All rights reserved.



［**概要**］ページにインストールの選択が表示されます。［**戻る**］をクリックして前のウィザードページに戻り、選択を変更できます。または、［**インストール**］をクリックしてインストールを開始します。

手順8：インストールを完了する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[完了]ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了]をクリックしてSession Recording Agentのインストールを完了します。

注：Machine Creation Services（MCS）またはProvisioning Services（PVS）で、構成済みのマスターイメージとインストール済みのMicrosoft Message Queuing（MSMQ）を使用して複数のVDAを作成すると、一定の状況下において、これらのVDAのQMIdが同じになる可能性があります。これは、次のようなさまざまな問題が発生する原因となる場合があります。

- 録画契約が承認されていても、セッションが録画されない場合があります。
- セッションのログオフ信号がSession Recordingサーバーによって受信されず、セッションのステータスが常に［ライブ］になってしまう可能性があります。

解決策はVDAごとに固有のQMIdを作成することですが、方法は展開方法によって異なります。

Session Recording Agentがインストールされたデスクトップ OSのVDAを、PVS 7.7以降またはMCS 7.9以降のバージョンを使用して静的デスクトップモードで作成する場合（たとえば、すべての変更が別のPersonal vDiskまたはVDAのローカルディスクで永続的になるように構成する場合）、追加の操作は不要です。

サーバーOSのVDAがMCSまたはPVSとデスクトップOSのVDAを使用して作成され、ユーザーがログオフするとすべての変更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

が削除されるように構成されている場合は、GenRandomQMID.ps1スクリプトを使用してシステム起動時にQMIdを変更します。電源管理方法を変更して、ユーザーがログインを試行する前に十分な数のVDAが実行されているようにします。

GenRandomQMID.ps1スクリプトを使用するには、以下の手順に従ってください。

1. PowerShellの実行ポリシーが**RemoteSigned**か**Unrestricted**に設定されていることを確認します。

   次のように入力します。「Set-ExecutionPolicy RemoteSigned」

2. スケジュールされたタスクを作成し、トリガーを［システム起動時］に設定して、PVSまたはMCSマスターイメージマシンでSYSTEMアカウントを使って実行します。

3. スタートアップタスクとしてコマンドを追加します。

   powershell .exe -file C:\GenRandomQMID.ps1

GenRandomQMID.ps1スクリプトの概要：

1. レジストリから現在のQMIdを削除します。
2. HKEY_LOCAL_MACHINE\Software\Microsoft\MSMQ\ParametersにSysPrep = 1を追加します。
3. CitrixSmAudAgentやMSMQなどの関連サービスを停止します。
4. ランダムなQMIdを生成するために、先ほど停止したサービスを開始します。

GENRANDOMQMID.PS1（参照用）： コピー

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

}

}
```

Session Recording Playerのインストール

Session Recordingサーバーまたはセッションの録画を見るユーザーのドメイン内の1つ以上のワークステーションにSession Recording Playerをインストールします。

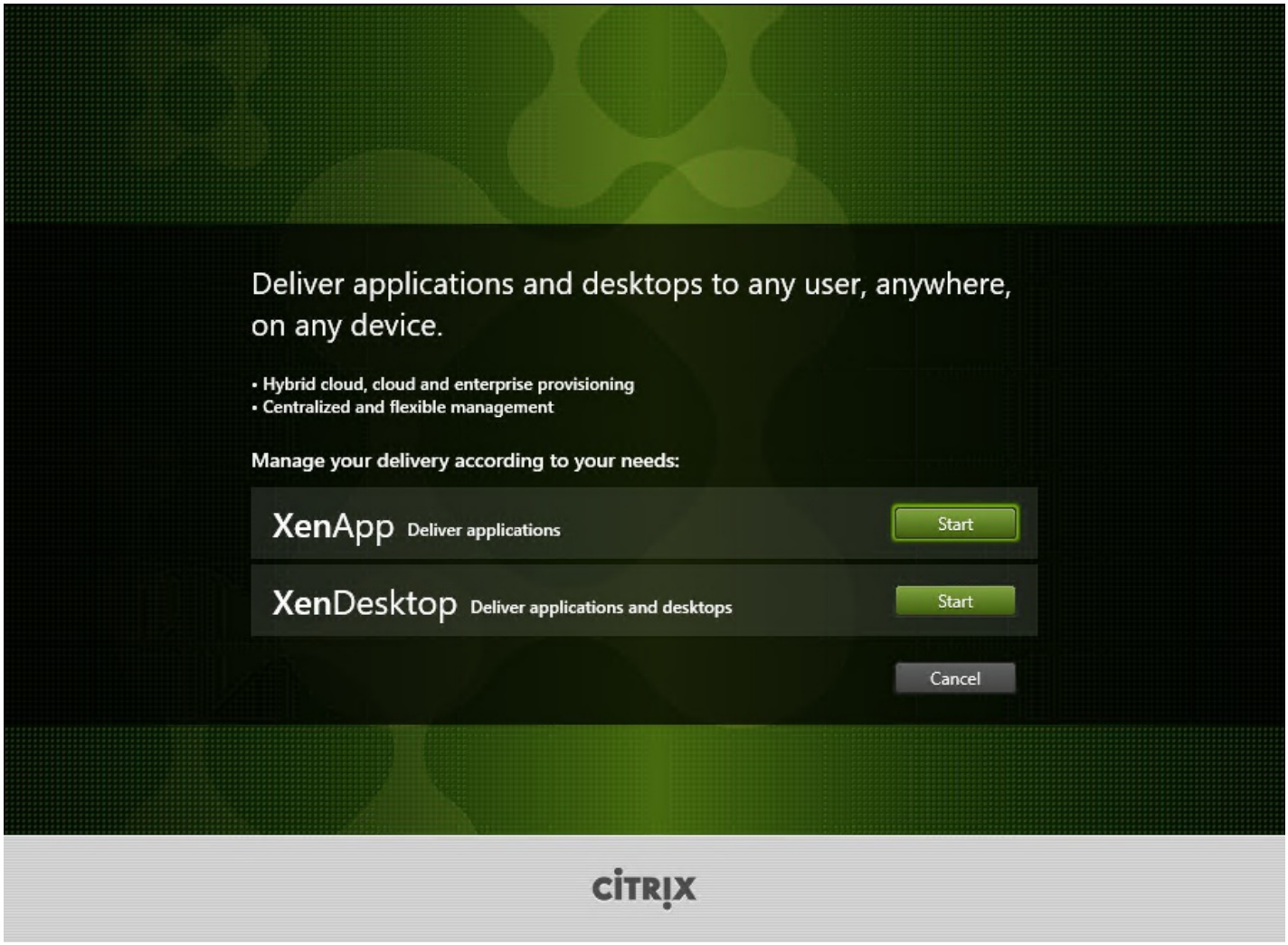
© 1999-2017 Citrix Systems, Inc. All rights reserved.

手順1：製品ソフトウェアをダウンロードしてウィザードを起動する

ローカルの管理者アカウントを使って、Session Recording Playerコンポーネントのインストール先マシンにログオンします。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**ファイルまたはマウントしたドライブをダブルクリックします。

インストールウィザードが起動します。

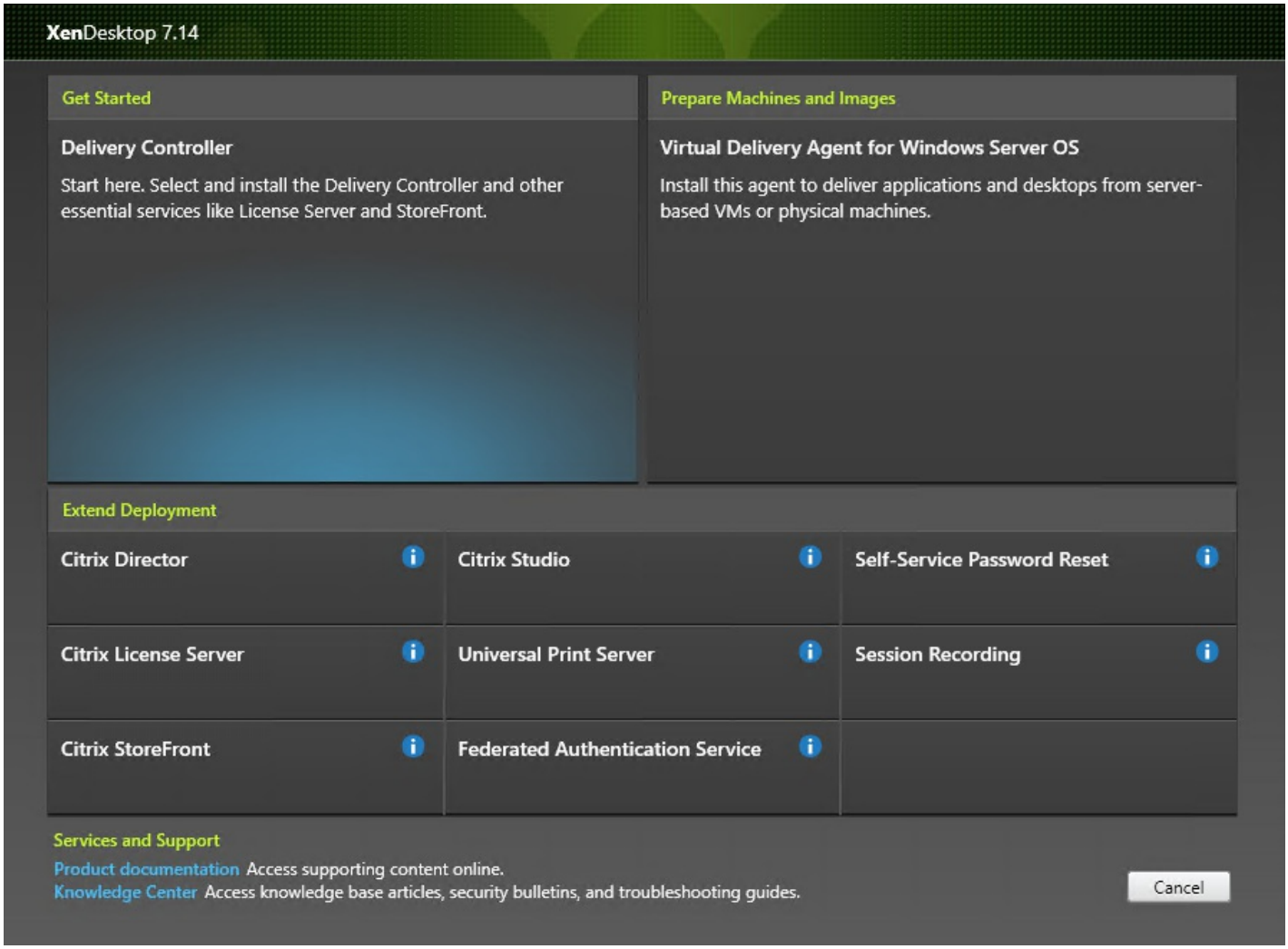
手順2：インストールする製品を選択する



インストールする製品の隣の **[開始]** をクリックします： **XenApp**または**XenDesktop**。

手順3：Session Recordingを選択する

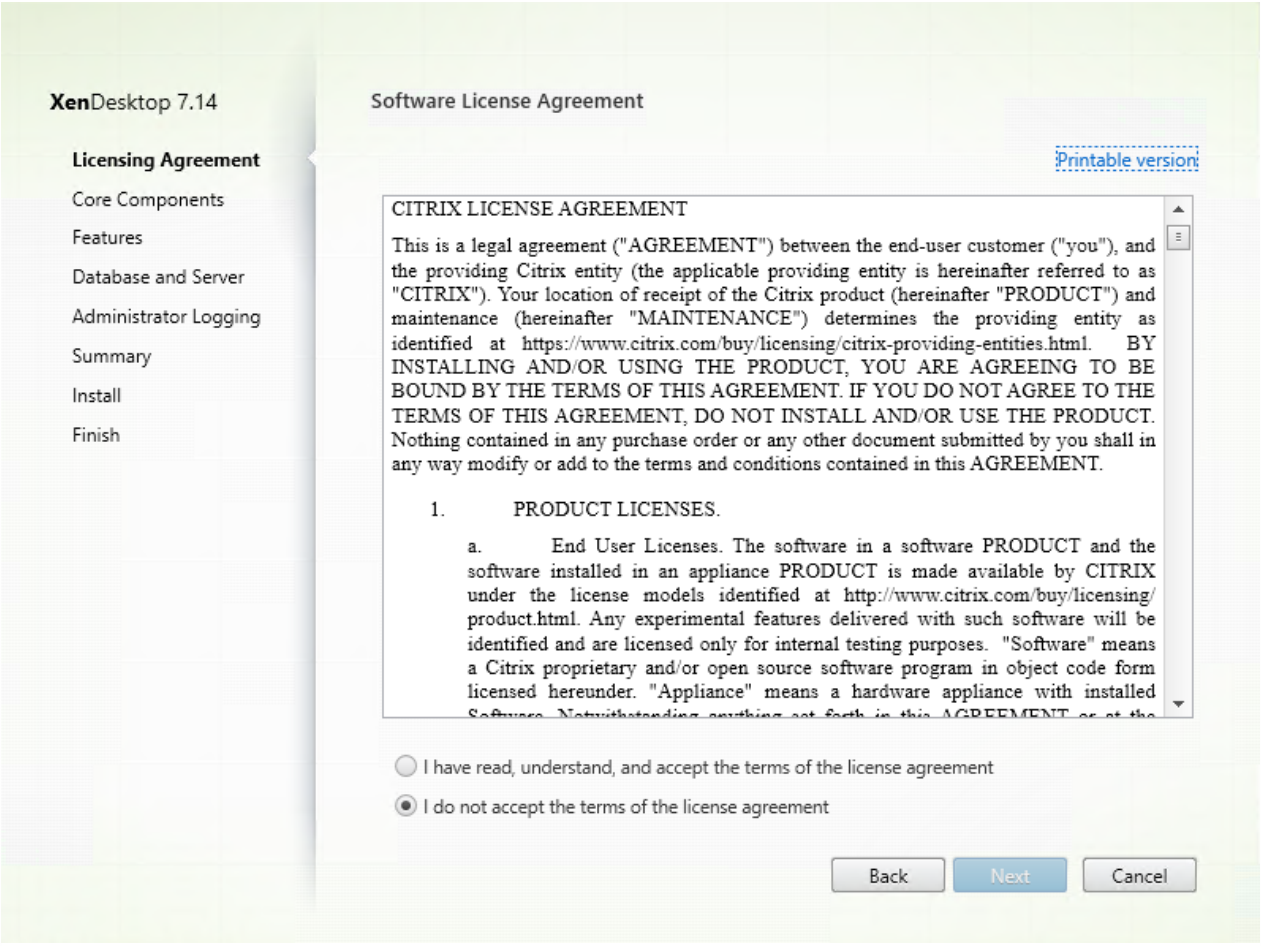
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Session Recordingエントリを選択します。

手順4：ライセンス契約書を読み、同意する

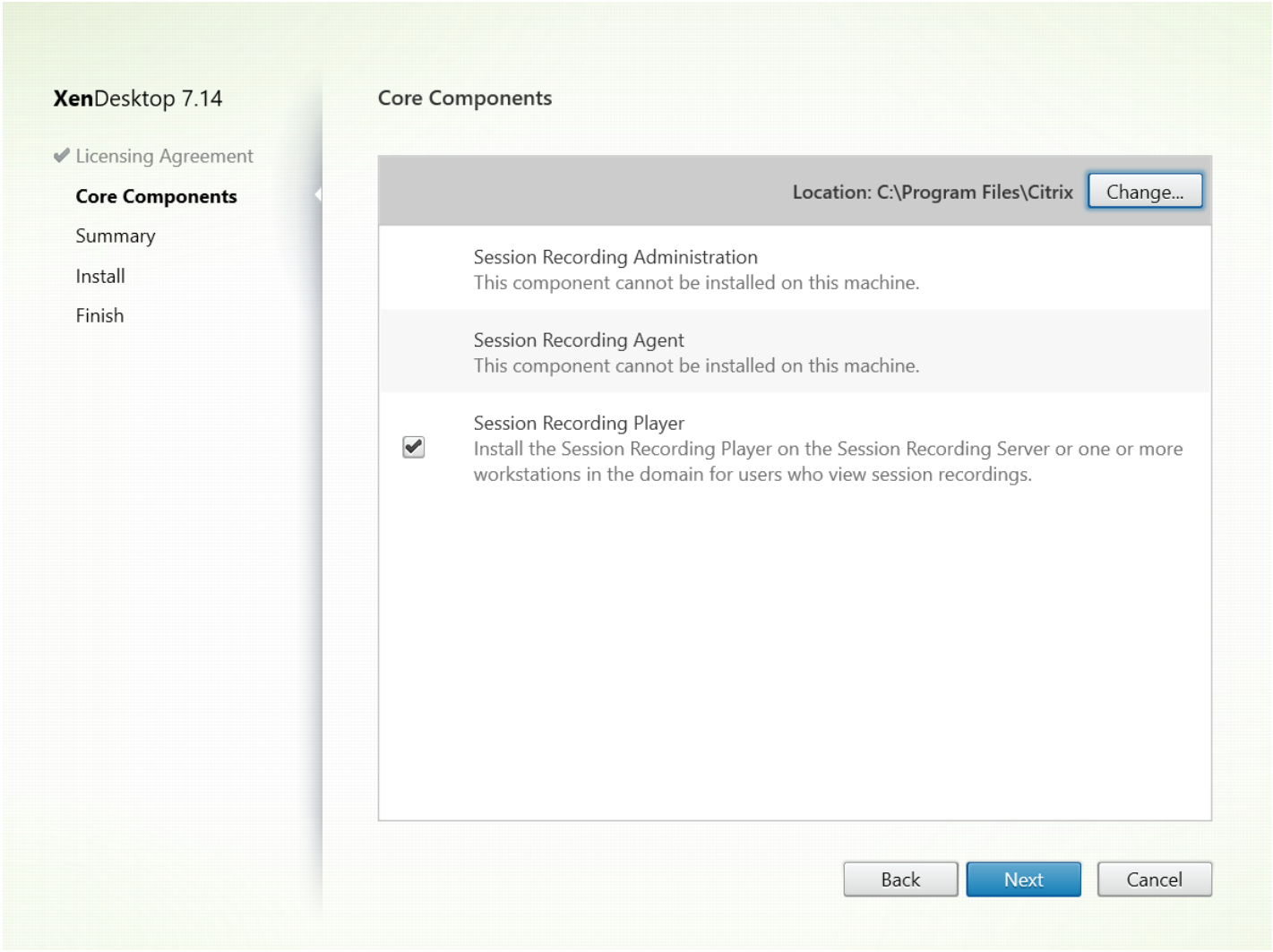
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[ソフトウェアライセンス契約] ページでライセンス契約を読み、同意して **[次へ]** をクリックします。

手順5：インストールするコンポーネントおよびインストール場所を選択する

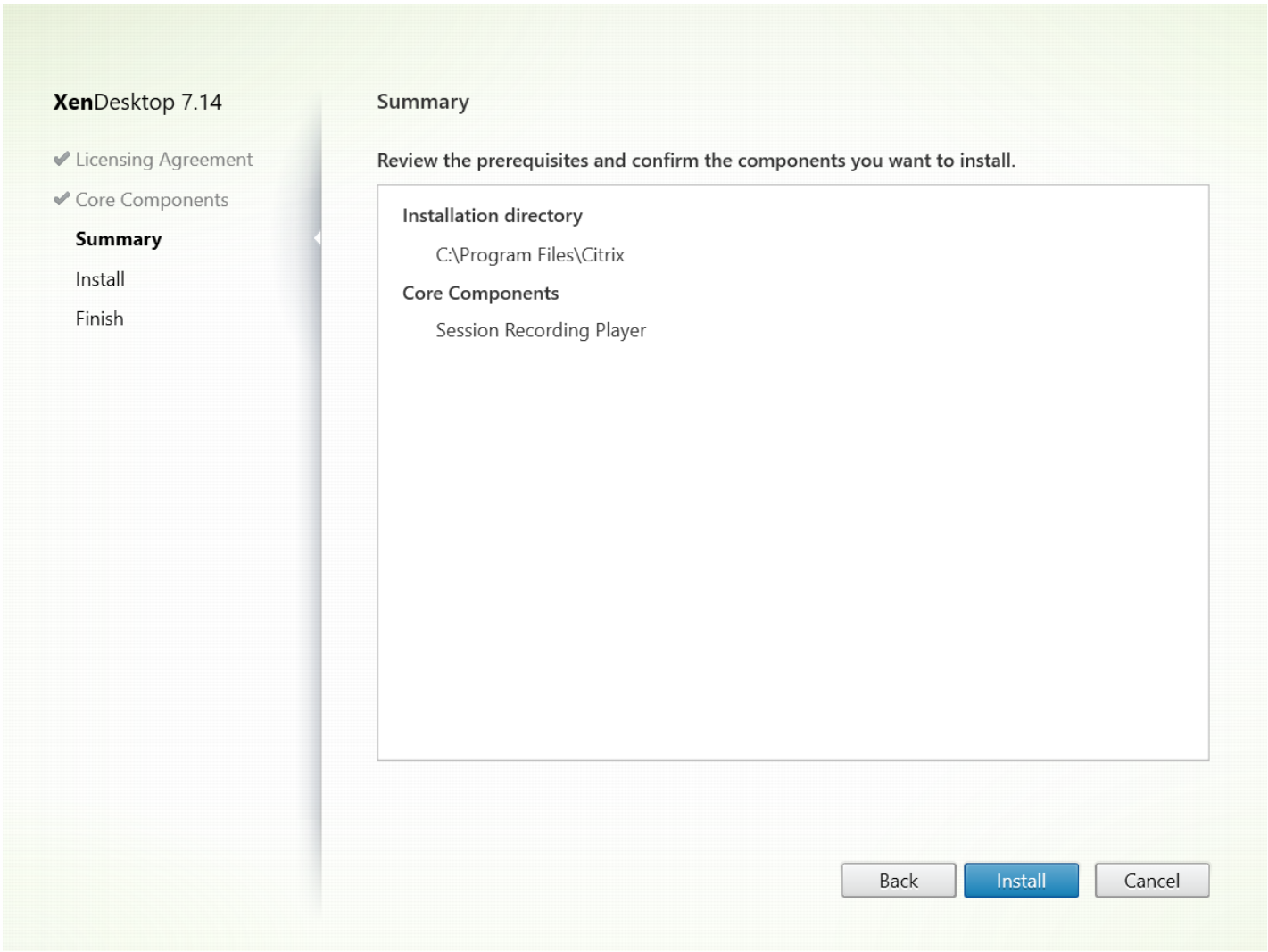
© 1999-2017 Citrix Systems, Inc. All rights reserved.



[**Session Recording Player**] を選択して [**次へ**] をクリックします。

手順6：インストール前に前提条件を確認する

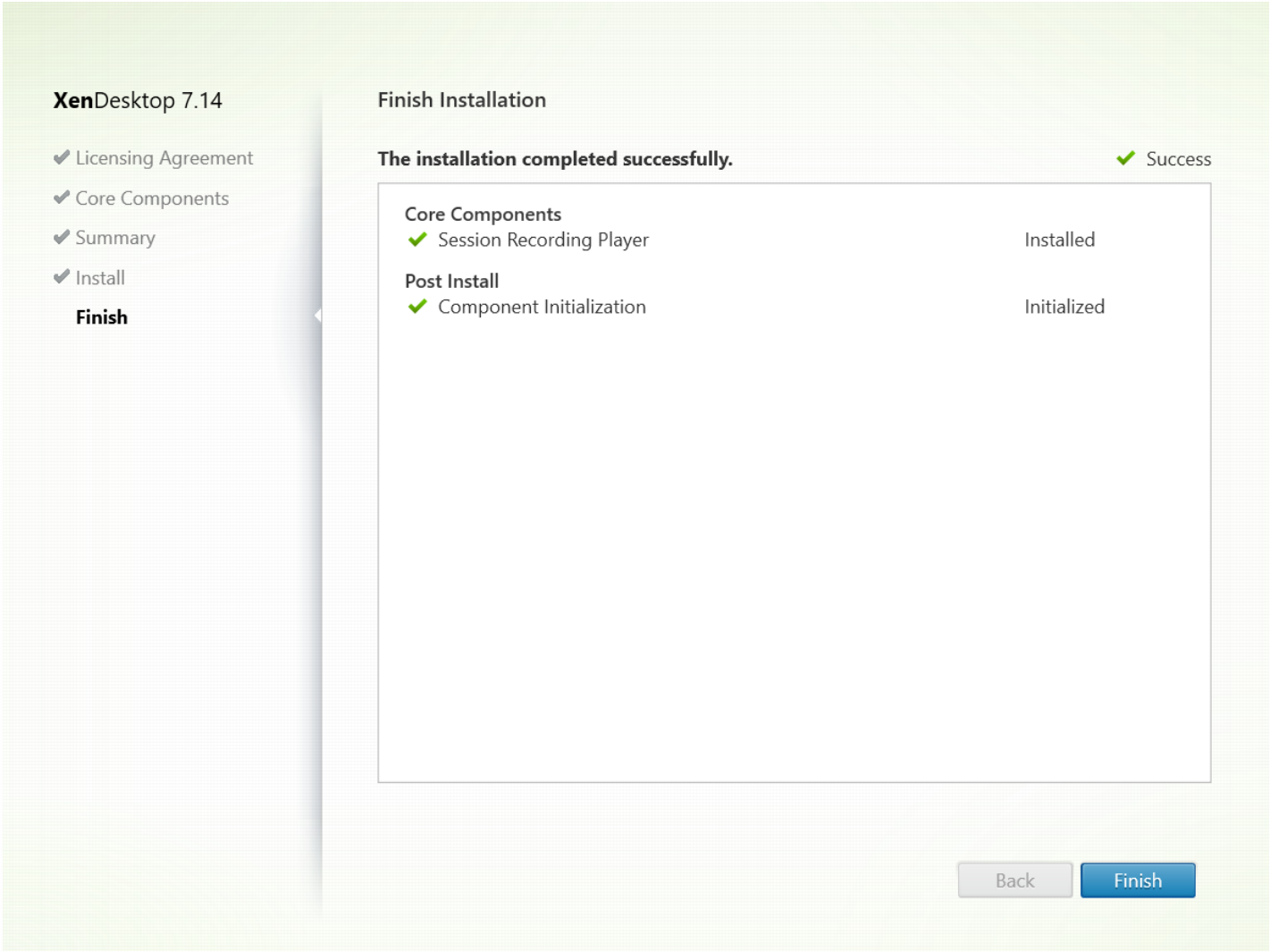
© 1999-2017 Citrix Systems, Inc. All rights reserved.



［**概要**］ページにインストールの選択が表示されます。［**戻る**］をクリックして前のウィザードページに戻り、選択を変更できます。または、［**インストール**］をクリックしてインストールを開始します。

手順7：インストールを完了する

© 1999-2017 Citrix Systems, Inc. All rights reserved.



[完了]ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了]をクリックしてSession Recording Playerのインストールを完了します。

インストールの自動化

Session Recording Agentを複数のサーバーにインストールするには、サイレントインストールを行うスクリプトを作成します。

次のコマンドラインでは、Session Recording Agentをインストールし、インストール情報を取得するためにログファイルを作成します。

64ビットシステム：

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注：XenAppおよびXenDesktop ISOのSessionRecordingAgentx64.msiファイルは、\layout\image-full\x64\Session Recording

© 1999-2017 Citrix Systems, Inc. All rights reserved.

の下にあります。

32ビットシステム：

msiexec /i SessionRecordingAgent.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注：XenAppおよびXenDesktop ISOのSessionRecordingAgent.msiファイルは、\layout\image-full\x86\Session Recordingの下にあります。

各項目の意味は次のとおりです。

yourservername は、Session Recordingサーバーをホストするコンピューターの NetBIOS名またはFQDNです。指定しない場合のデフォルト値は**localhost**です。

yourbrokerport は、Session Recording Brokerとの通信にSession Recording Agentで使用されるポートを表すHTTPまたはHTTPSです。指定しない場合のデフォルト値はHTTPSです。

yourbrokerport は、Session Recording Brokerとの通信にSession Recording Agentで使用されるポートを表す整数です。指定しない場合のデフォルト値は0で、選択したプロトコルのデフォルトのポート番号を使用するようSession Recording Agentに指示します。 具体的には、HTTPでは80、HTTPSでは443です。

/l*vスイッチにより詳細モードでログが記録されます。

yourinstallationlogは、セットアップログを作成する場所です。

/qスイッチによりサイレントモードでインストールされます。

Session Recordingのアップグレード

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。Session Recording 7.6（またはそれ以降のバージョン）を、最新リリースのSession Recordingにアップグレードすることができます。

注：

- Session Recording Administrationを7.6から7.13以降にアップグレードし、Session Recording Administrationで **[変更]** を選択して管理者ログサービス追加した場合、［**管理者ログの構成**］ページにSQL Serverインスタンスの名前が表示されません。 **[次へ]** をクリックすると次のエラーメッセージが表示されます。「データベース接続テストに失敗しました。正しいデータベースインスタンス名を入力してください。」この問題を回避するには、SmartAuditorサーバーの次のレジストリフォルダーにローカルホストのユーザーの読み取りのアクセス許可を追加します（HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server）。
- マシン上にコンポーネントをインストールしただけで、Session Recordingデータベースをアップグレードしようとした場合は、失敗することがあります。その場合は、以下のレジストリエントリが、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Databaseの下にあるかどうかを確認してください。ない場合は、アップグレードの前にエントリを手動で追加してください。

キー名	キー型	キー値
SmAudDatabaseInstance	文字列	Session Recordingデータベースのインスタンス名

© 1999-2017 Citrix Systems, Inc. All rights reserved.

DatabaseName	文字列	Session Recordingデータベースのデータベース名

要件、準備、および制限

注： Technical Previewバージョンからはアップグレードできません。

- Session Recordingコンポーネントのアップグレードは、コンポーネントをインストールしたマシンで、Session Recordingインストーラーのグラフィカルインターフェイスまたはコマンドラインインターフェイスを使用して行う必要があります。
- アップグレードを開始する前に、SQL ServerインスタンスでCitrixSessionRecordingという名前のデータベースをバックアップします。これにより、データベースのアップグレード後に問題が発生した場合に元の状態に復元することができます。
- Session Recordingコンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。
- Session Recording ServerとSession Recordingデータベースが同じサーバーにインストールされていない場合、Session Recordingデータベースをアップグレードするには、データベースの役割権限が必要です。この権限がない場合は
  - データベース管理者に頼んで、アップグレードのために**securityadmin** および**dbcreator** サーバー役割権限を割り当ててもらいます。アップグレードの完了後は、**securityadmin** および**dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、SessionRecordingAdministrationx64.msiパッケージを使用してアップグレードします。msiのアップグレード中、**securityadmin**および**dbcreator**サーバー役割権限と共に、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、［**OK**］をクリックし、アップグレードを続行します。
- 同時にすべてのSession Recording Agentをアップグレードしない場合は、Session Recording Agent 7.6.0（またはそれ以降）を、最新リリース（現行）のSession Recording Serverと共に使用できます。ただし、一部の新機能やバグ修正は反映されない可能性があります。
- Session Recording Serverのアップグレード中に起動されたセッションは録画されません。
- デスクトップコンポジションリダイレクトモードとの互換性を維持するために、新規インストールまたはアップグレード後にSession Recording Agentプロパティの［**グラフィック調整**］オプションがデフォルトで有効になります。このオプションは、新規インストールまたはアップグレード後に手動で無効にできます。
- 管理者ログ機能は、この機能を含まない以前のリリースからSession Recordingをアップグレードした後はインストールされません。この新しい機能を追加するには、アップグレード後にインストールを修正します。
- アップグレードプロセスの開始時にライブ録画セッションが実行されていた場合、録画を完了できる可能性はほとんどありません。
- サイトが停止する場合に備えて影響を軽減するために、後述のアップグレードの順序を確認してください。

アップグレードの順序

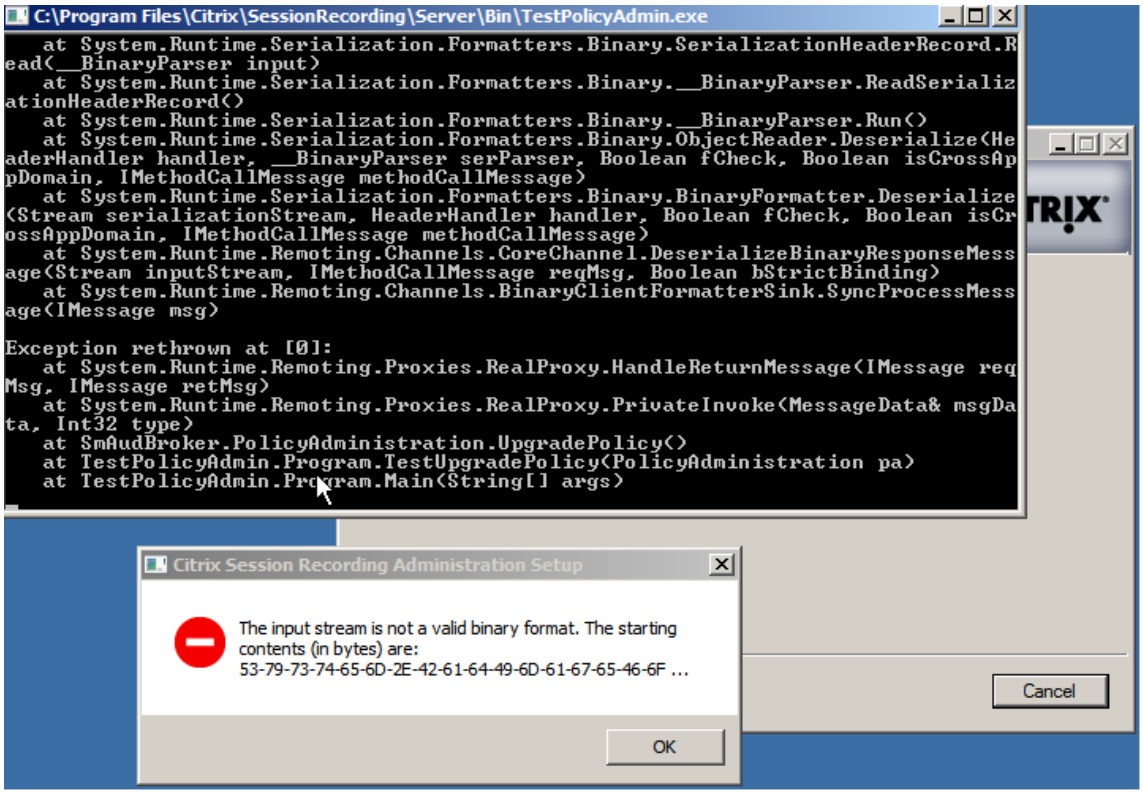
1. Session RecordingデータベースとSession Recording Serverが別々のサーバーにインストールされている場合、Session Recording ServerでSession Recordingストレージマネージャーサービスを手動で停止して、まずSession Recordingデータベースをアップグレードします。
2. Session Recording BrokerがIISサービスと共に実行されていることを確認します。Session Recording Serverをアップグレードします。Session RecordingデータベースとSession Recording Serverが同じサーバーにインストールされている場合、Session Recordingデータベースもアップグレードします。
3. Session Recording Serverのアップグレードが完了すると、Session Recordingサービスは自動的にオンラインに戻ります。
4. （マスターイメージの）Session Recording Agentをアップグレードします。
5. Session Recordingサーバーと一緒に、またはSession Recordingサーバーの後に、Session Recordingポリシーコンソールを

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アップグレードします。

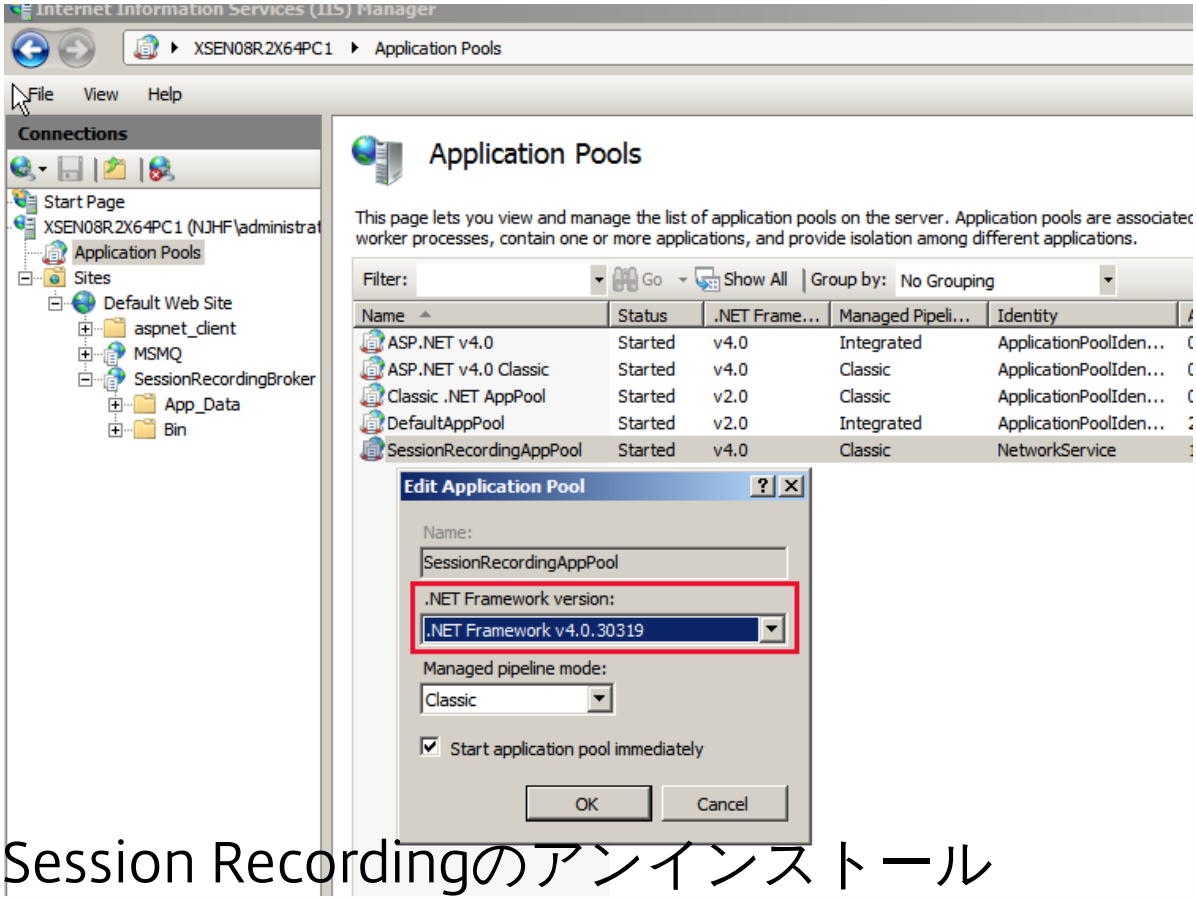
6. Session Recording Playerをアップグレードします。

注：Windows Server 2008 R2でSession Recording Administrationコンポーネントをアップグレードすると、次のエラーが発生することがあります。



この場合は、［SessionRecordingAppPool］の［.NET Frameworkのバージョン］をIISの［.NET Framework v4］に変更し、再度アップグレードしてください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Session Recordingのアンインストール

サーバーやワークステーションから**Session Recording**コンポーネントを削除するには、**Windows**のコントロールパネルの「プログラムのアンインストールまたは削除オプションを使用します。Session Recordingデータベースを削除するには、インストール時と同じSQL Serverの役割権限**securityadmin**および**dbcreator**が必要です。

セキュリティ上の理由により、コンポーネントがアンインストールされた後には管理者ログデータベースは削除されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recordingの構成

Dec 05, 2017

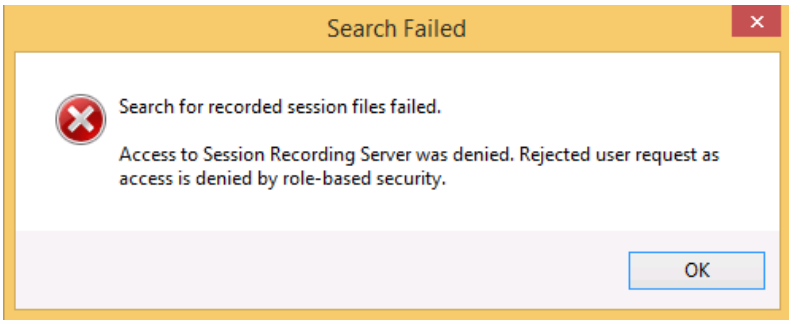
セッションの再生と録画のためのSession Recordingの構成

Session Recordingコンポーネントをインストールしたら、次の手順を実行し、Session Recordingを構成して、XenAppまたはXenDesktopセッションを録画して表示できるようにします。

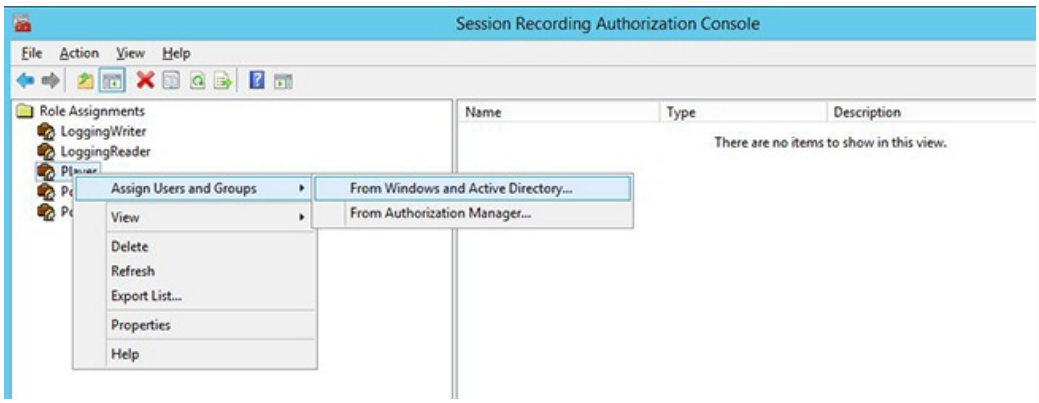
- ユーザーに録画を再生する権限を与える。
- ユーザーに録画ポリシーを管理する権限を与える。
- セッションを録画する録画ポリシーをアクティブに設定。
- カスタムポリシーの構成
- Session Recording Playerを構成してSession Recording Serverと接続する

ユーザーに録画したセッションを再生する権限を与える。

Session Recordingのデフォルト設定では、どのユーザーにも録画したセッションを再生する権限はありません。管理者も含め、各ユーザーに権限を割り当てる必要があります。録画したセッションを再生する権限がないユーザーが録画したセッションを再生しようとすると次のエラーメッセージが表示されます。



1. Session Recording Serverをホストするコンピューターに管理者としてログオンします。
2. Session Recording承認コンソールを起動します。
3. Session Recording承認コンソールで［Player］を選択します。
4. 録画したセッションを表示する権限を与えるユーザーおよびグループを追加すると、右側のペインに表示されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーに録画ポリシーを管理する権限を与える。

Session Recordingをインストールすると、ドメイン管理者から、録画ポリシーを制御する権限がデフォルトで与えられます。承認設定は変更できます。

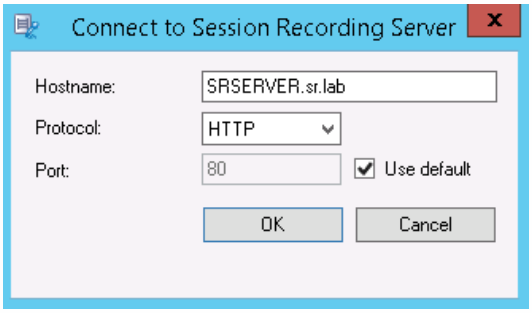
1. Session Recording Serverをホストするマシンに管理者としてログオンします。
2. Session Recording承認コンソールを起動して、PolicyAdministratorsを選択します。
3. 録画ポリシーを管理できるユーザーとグループを追加します。

セッションを録画する録画ポリシーをアクティブに設定。

アクティブな録画ポリシーにより、Session Recording AgentがインストールされておりSession Recording Serverに接続する、すべてのVDAまたはVDIでのセッションの録画処理が決定されます。Session Recordingのデフォルト設定では、アクティブな録画ポリシーは「**録画しない**」ポリシーです。アクティブな録画ポリシーを変更するまで、セッションは録画できません。

重要： ポリシーには多くの規則を含めることができますが、一度に実行できるのはアクティブなポリシー1つだけです。

1. 承認済みのポリシー管理者として、Session Recording Policy Consoleがインストールされているサーバーにログオンします。
2. Session Recording Policy Consoleを起動します。
3. **[Session Recording Serverに接続する]** ダイアログボックスが開いたら、Session Recording Serverをホストするコンピューターの名前、プロトコル、およびポート番号が正しいことを確認します。



4. Session Recording Policy Consoleで、 **[録画ポリシー]** を展開します。Session Recordingの標準の録画ポリシーが表示されます。チェックマークはアクティブなポリシーを示します。
   - **録画しない**。これがデフォルトのポリシーです。ほかのポリシーを指定しなければ、セッションは録画されません。
   - **すべてのユーザーを通知して録画する**。このポリシーを選択すると、すべてのセッションが録画されます。録画されていることを通知するウィンドウが表示されます。
   - **すべてのユーザーを通知しないで録画する**。 このポリシーを選択すると、すべてのセッションが録画されます。録画されていることを通知するウィンドウが表示されません。
5. アクティブにするポリシーを選択します。
6. メニューバーで **[操作]** 、 **[ポリシーのアクティブ化]** の順に選択します。

Session Recordingでは独自の録画ポリシーを作成できます。録画ポリシーを作成すると、Session Recording Policy Consoleの［録画ポリシー］フォルダーに表示されます。
一般的な録画ポリシーでは要件に合わないことがあります。ユーザー、VDAおよびVDIサーバー、デリバリーグループ、およびアプリケーションをベースとしてポリシーとルールを構成できます。カスタムポリシーについて詳しくは、「カスタム録ポリシーの作成」を参照してください。
注： Session RecordingのAdministrator Logging機能により、録画ポリシーの変更を記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

Session Recording Playerの構成

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording Playerでセッションを再生するには、録画されたセッションを格納するSession Recording Playerとの接続を設定する必要があります。Session Recording Playerごとに複数のSession Recordingサーバーとの接続を設定できますが、同時に複数のSession Recordingサーバーに接続することはできません。Session Recording Playerに複数のSession Recordingサーバーとの接続が構成される場合は、**[ツール]** > **[オプション]** の **[接続]** タブのチェックボックスをオンにして、接続先のSession Recordingサーバーを変更できます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. Session Recording Playerを起動します。
3. Session Recording Playerのメニューバーで **[ツール]** > **[オプション]** の順に選択します。
4. **[接続]** タブで **[追加]** をクリックします。
5. **[ホスト名]** フィールドに、Session Recordingサーバーをホストするコンピューターの名前かインターネットプロトコル（IP）アドレスを入力し、プロトコルを選択します。デフォルトでは、セキュリティで保護された通信のためHTTPS/SSLを使用するようにSession Recordingが構成されます。SSLが構成されていない場合は、HTTPを選択します。
6. Session Recording Playerが複数のSession Recordingサーバーと接続できるように構成するには、Session Recordingサーバーごとに手順4および5を繰り返します。
7. 接続するSession Recording Serverのチェックボックスがオンになっていることを確認します。

Session Recording Serverとの接続の設定

Session Recording AgentとSession Recording Serverの間の接続は、通常、Session Recording Agentをインストールするときに設定します。Session Recording Agentをインストールした後でこの接続を設定するには、［Session Recording Agentのプロパティ］を使用します。

1. Session Recording Agentがインストールされているサーバーにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Agentのプロパティ]** を選択します。
3. **[接続]** タブをクリックします。
4. **[Session Recording Server]** フィールドに、サーバーの名前かインターネットプロトコル（IP）アドレスを入力します。
5. **[Session Recordingストレージマネージャーメッセージのキュー]** で、Session Recordingストレージマネージャーが通信に使用するプロトコルを選択し、必要であればデフォルトのポート番号を変更します。
6. **[メッセージの有効期間]** フィールドで、通信エラーが発生したときにキューに各メッセージを保持する秒数として、デフォルトの7,200秒（2時間）を受け入れるか、新しい値を入力します。この期間が経過すると、メッセージは削除され、ファイルを再生できるのはデータが失われた時点までになります。
7. **[Session Recording Broker]** で、Session Recording Brokerが通信に使用するプロトコルを選択し、必要であればデフォルトのポート番号を変更します。
8. 確認メッセージが表示されるので、**Session Recording Agentサービス**を再起動して変更を受け入れます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーへのアクセス権の付与

Dec 05, 2017

> **Important**
>
> セキュリティ上の理由から、セッションの録画の表示など、特定の機能を実行するために必要な権限のみをユーザーに付与します。

Session Recording ServerをホストするコンピューターでSession Recording承認コンソールを使用して役割を割り当てることにより、Session Recordingユーザーに権限を付与します。Session Recordingユーザーには3つの役割があります。

- **Player。**録画したXenAppセッションを表示できます。デフォルトでこの役割のメンバーになるユーザーはありません。
- **PolicyQuery。**Session Recording Agentをホストするサーバーで録画ポリシーの評価を要求できます。デフォルトでは、Authenticated Usersがこの役割のメンバーです。
- **PolicyAdministrator。**録画ポリシーの表示、作成、編集、削除、および有効化を実行できます。デフォルトでは、Session Recording Serverをホストするコンピューターの管理者がこの役割のメンバーです。

Session Recordingでは、Active Directoryで定義されるユーザーおよびグループがサポートされます。

役割へのユーザーの割り当て

1. Session Recording Serverをホストするコンピューターに、管理者またはPolicyAdministratorのメンバーとしてログオンします。
2. Session Recording承認コンソールを起動します。
3. ユーザーを割り当てる役割を選択します。
4. メニューバーで、**[操作]** > **[Windowsユーザーとグループの割り当て]** の順に選択します。
5. ユーザーとグループを追加します。

管理コンソールで加えた変更は、1分間隔の更新時に有効になります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画ポリシーの作成とアクティブ化

Dec 05, 2017

Session Recordingポリシーコンソールを使用して、録画するセッションを決定するポリシーを作成しアクティブにします。

重要：Session Recordingポリシーコンソールを使用するには、Broker PowerShellスナップイン（Broker_PowerShellSnapIn_x64.msi）をインストールする必要があります。スナップインは、インストーラーによって自動的にインストールされません。XenAppおよびXenDesktopのISO（\layout\image-full\x64\Citrix Desktop Delivery Controllerの下にあります）でスナップインを検索し、指示に従って手動でインストールする必要があります。従わない場合、エラーが発生する可能性があります。

Session Recordingをインストールすると使用できるようになるシステムポリシーをアクティブにすることも、独自のカスタムポリシーを作成してアクティブにすることもできます。Session Recordingのシステムポリシーでは、すべてのユーザー、公開アプリケーション、およびサーバーに、単一の規則を適用します。カスタムポリシーでは、録画対象のユーザー、公開アプリケーション、およびサーバーを指定します。

アクティブなポリシーによって録画するセッションが決定されます。 一度にアクティブにできるポリシーは1つだけです。

システムポリシー

Session Recordingには、次の3つのシステムポリシーがあります。

- **録画しない**：これがデフォルトのポリシーです。ほかのポリシーを指定しなければ、セッションは録画されません。
- **すべてのユーザーを通知して録画する**: このポリシーを選択すると、すべてのセッションが録画されます。記録の発生を通知するポップアップウィンドウが表示されます。
- **すべてのユーザーを通知しないで録画する**: このポリシーを選択すると、すべてのセッションが録画されます。記録の発生を通知するポップアップウィンドウは表示されません。

システムポリシーは変更したり削除したりできません。

ポリシーのアクティブ化

1. Session Recordingポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recordingポリシーコンソールを起動します。
3. **［Session Recording Serverへの接続］**ポップアップウィンドウが開いたら、Session Recordingサーバーの名前、プロトコル、およびポートが正しいことを確認します。 **［OK］**をクリックします。
4. Session Recordingポリシーコンソールで、**［録画ポリシー］**を展開します。
5. アクティブにするポリシーを選択します。
6. メニューバーで**［操作］**、**［ポリシーのアクティブ化］**の順に選択します。

カスタム録画ポリシーの作成

独自のポリシーを作成するときは、規則を作成して、録画対象のユーザーおよびグループ、公開アプリケーション、およびサーバーを指定します。Session Recordingポリシーコンソールにはウィザードが用意されており、このウィザードに従って規則を作成します。公開されているアプリケーションやサーバーの一覧を取得するには、サイト管理者の読み取り権限が必要です。この権限はこのサイトのDelivery Controllerで設定します。

作成する規則ごとに録画操作および規則条件を指定します。録画操作は規則条件を満たすセッションに適用されます。

規則ごとに録画操作を1つ選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **録画しない**：（**規則**ウィザードで **[セッションを録画しない]** をクリックします） この録画操作では、規則条件を満たすセッションを録画しないことを指定します。
- **通知して録画する**：（**規則**ウィザードで **[通知してセッションを録画する]** をクリックします） この録画操作では、規則条件を満たすセッションを録画することを指定します。記録の発生を通知するポップアップウィンドウが表示されます。
- **通知しないで録画する**：（**規則**ウィザードで **[通知しないでセッションを録画する]** をクリックします） この録画操作では、規則条件を満たすセッションを録画することを指定します。エンドユーザーは録画されていることに気付きません。

規則ごとに次の項目のいずれかを少なくとも1つ選択して、規則条件を作成します。

- **ユーザーまたはグループ**。規則の録画操作を適用するユーザーまたはグループの一覧を作成します。
- **公開リソース**。 規則の録画操作を適用する公開アプリケーションまたはデスクトップの一覧を作成します。**規則**ウィザードで、アプリケーションまたはデスクトップを使用できる1つまたは複数のXenApp/XenDesktopサイトを選択します。
- **デリバリーグループまたはマシン**。規則の録画操作を適用するデリバリーグループまたはマシンの一覧を作成します。**規則**ウィザードで、デリバリーグループまたはマシンの場所を選択します。
- **IPアドレスまたはIP範囲**。規則の録画操作を適用するIPアドレスまたはIPアドレスの範囲の一覧を作成します。 **[IPアドレスとIPの範囲の選択]** 画面で、録画を有効または無効にする有効なIPアドレスまたはIP範囲を追加します。

注：Session Recordingポリシーコンソールでは、1つの規則内で複数の条件を構成できます。規則が適用される際には、「AND」と「OR」の両方の論理演算子が、最終的なアクションを計算するために使われます。一般的に、「OR」演算子は一定の条件内の項目に使われ、「AND」演算子は違った複数の条件に当てはまる項目に使われます。結果がtrueであれば、Session Recordingポリシーエンジンがその規則のアクションをとります。そうでなければ、次の規則に進み、処理を繰り返します。

録画ポリシーに複数の規則を作成する場合は、複数の規則条件に一致するセッションがある可能性があります。そのような場合は、優先順位が最も高い規則がセッションに適用されます。

規則により実行される録画操作によってその優先順位が決まります。

- **[録画しない]** 規則の優先順位が最も高くなります。
- **[通知して録画する]** 規則の優先順位が次に高くなります。
- **[通知しないで録画する]** 規則の優先順位が最も低くなります。

録画ポリシーの規則条件のいずれにも当てはまらないセッションがある可能性があります。そのようなセッションについては、フォールバック規則の録画操作が適用されます。フォールバック規則の録画操作は常に **[録画しない]** です。フォールバック規則は変更したり削除したりできません。

カスタムポリシーを構成するには、次を実行します。

1. 承認済みのポリシー管理者として、Session Recording Policy Consoleがインストールされているサーバーにログオンします。
2. Session Recordingポリシーコンソールを起動して、左側のペインの **[レコーディングポリシー]** をクリックします。メニューバーで **[操作]** > **[新しいポリシーの追加]** の順にクリックします。
3. **[新しいポリシー]** を右クリックして **[規則の追加]** をクリックします。
4. 録画オプションの選択 - **規則**ウィザードで、 **[セッションを録画しない]** 、 **[通知してセッションを録画する]** （または **[通知しないでセッションを録画する]** ）を選択し、 **[次へ]** をクリックします。
5. 規則条件の選択 - オプションの 1 つまたは任意の組み合わせを選択することができます。
   ユーザーまたはグループ
   公開リソース
   デリバリーグループまたはマシン
   IPアドレスまたはIPの範囲

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 規則条件の編集 - 編集するには、下線付きの値をクリックします。前の手順で選択した条件に基づき、値に下線が引かれます。
   注：［公開リソース］の下線付きの値を選択した場合、**［サイトアドレス］**はIPアドレス、URL、またはコントローラーがローカルネットワーク上にある場合はコンピューター名になります。**［アプリケーションの名前］**リストに表示名が表示されます。
7. ウィザードの指示に従って構成を終了します。

Active Directoryグループの使用

Active Directoryグループを使用して、Session Recordingのポリシーを作成できます。個々のユーザーではなくActive Directoryグループを使用すると、規則とポリシーを簡単に作成したり管理したりできます。たとえば、財務部門のユーザーがFinanceという名前のActive Directoryグループに含まれている場合は、規則を作成するときに**規則**ウィザードでFinanceグループを選択することで、このグループのすべてのメンバーに適用される規則を作成できます。

ユーザーのホワイトリスト化

組織内の一部のユーザーのセッションを確実に録画対象から除外する、Session Recordingポリシーを作成できます。これはユーザーの*ホワイトリスト化*と呼ばれます。個人情報を取り扱う社員や特定の階層の従業員など、セッションを録画するべきではないユーザーをホワイトリストに登録すると便利です。

すべての上級管理職がExecutiveという名前のActive Directoryグループのメンバーである場合、Executiveグループのセッション録画を無効にする規則を作成して、それらのユーザーのセッションが決して録画されないように設定できます。この規則を含むポリシーがアクティブな間は、Executiveグループのメンバーのセッションは録画されません。組織内のほかのメンバーのセッションは、アクティブなポリシーのほかの規則に基づいて録画されます。

IPアドレスまたはIPの範囲規則条件の使用

ポリシー一致の規則条件として、クライアントIPアドレスを使用できます。たとえば、特定のIPアドレスを持つか、あるIP範囲に含まれるクライアントからのセッションを記録する場合、**規則**ウィザードを使用して、それらのクライアントにのみ適用される規則を作成します。

新しいポリシーを作成する

注：規則ウィザードで、下線付きの値が表示されていないにもかかわらず「下線が引かれている値をクリックして編集できます」と表示される場合があります。このウィザードでは、適用される場合のみ下線付きの値が表示されます。下線付きの値が表示されない場合は、この手順を無視して次に進んでください。

1. Session Recording Policy Consoleがインストールされているサーバーにログオンします。
2. Session Recordingポリシーコンソールを起動します。
3. **［Session Recording Serverへの接続］**ポップアップウィンドウが開いたら、Session Recording Serverの名前、プロトコル、およびポートが正しいことを確認します。**［OK］**をクリックします。
4. Session Recordingポリシーコンソールで、**［録画ポリシー］**をクリックします。
5. メニューで**［新しいポリシーの追加］**を選択します。「**新しいポリシー**」という名前のポリシーが左ペインに表示されます。
6. 新しいポリシーを右クリックし、メニューで**［名前の変更］**をクリックします。
7. 作成したポリシーの名前を入力し、**Enter**キーを押すか新しい名前の外側の任意の場所をクリックします。
8. ポリシーを右クリックし、メニューバーで**［新しい規則の追加］**をクリックして、**規則**ウィザードを起動します。
9. 画面の指示に従ってこのポリシーの規則を作成します。

ポリシーの変更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Session Recordingポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recordingポリシーコンソールを起動します。
3. **[Session Recording Serverへの接続]**ポップアップウィンドウが開いたら、Session Recordingサーバーの名前、プロトコル、およびポートが正しいことを確認します。 **[OK]**をクリックします。
4. Session Recordingポリシーコンソールで、**[録画ポリシー]**を展開します。
5. 変更するポリシーを選択します。ポリシーの規則が右ペインに表示されます。
6. 新しい規則を追加するか、規則を変更または削除します。
   - メニューバーで**[操作]** > **[新しい規則の追加]**の順に選択します。 ポリシーがアクティブな場合はポップアップウィンドウが開き、操作の確認を促すメッセージが表示されます。**規則**ウィザードを使用して新しい規則を作成します。
   - 変更する規則を選択し、右クリックして**[プロパティ]**をクリックします。**規則**ウィザードを使用して規則を変更します。
   - 削除する規則を選択し、右クリックして**[規則の削除]**をクリックします。

ポリシーの削除

注：システムポリシーまたはアクティブなポリシーは削除できません。

1. Session Recordingポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recordingポリシーコンソールを起動します。
3. **[Session Recording Serverへの接続]**ポップアップウィンドウが開いたら、Session Recordingサーバーの名前、プロトコル、およびポートが正しいことを確認します。 **[OK]**をクリックします。
4. Session Recordingポリシーコンソールで、**[録画ポリシー]**を展開します。
5. 左ペインで削除するポリシーを選択します。ポリシーがアクティブな場合は、ほかのポリシーをアクティブにする必要があります。
6. メニューバーで**[操作]** > **[ポリシーの削除]**の順に選択します。
7. **[はい]**をクリックして操作を確定します。

注：事前起動されたアプリケーションセッションに関する制限事項

- アクティブなポリシーでアプリケーション名を照合する場合、事前起動されたセッションで起動されたアプリケーションは照合されないため、セッションが録画されません。
- アクティブなポリシーですべてのアプリケーションが録画される場合、ユーザーがCitrix Receiver for Windowsにログインすると、（事前起動されたセッションが確立されるのと同時に）録画に関する通知が表示され、事前起動された（空の）セッションと、今後そのセッションで起動されるすべてのアプリケーションが録画されます。

回避するには、録画ポリシーに従って、別のデリバリーグループのアプリケーションを公開します。録画条件にアプリケーション名を使用しないでください。こうすることで、事前起動されたセッションを録画できます。ただし、通知は表示されます。

ロールオーバーの動作

ポリシーをアクティブにするとき、それまでアクティブだったポリシーはユーザーセッションが終了するまで効力を保ちます。ただし、一部の場合、ファイルがロールオーバーされると新しいポリシーが有効になります。ロールオーバーは、ファイルサイズが上限に達すると実行されます。録画ファイルのサイズの上限について詳しくは、「録画ファイルのサイズの指定」を参照してください。

次の表で、セッションの録画中に新しいポリシーを適用してロールオーバーが起きたときに生じる現象について説明します。

以前のポリシー	新しいポリシー	ロールオーバーの後

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

録画しない。	ほかのポリシー	変更なし。エンドユーザーが新しいセッションにログオンするときのみに新しいポリシーが有効になります。
通知しないで録画する	録画しない	録画を停止します。
	通知して録画する	録画を続行し通知メッセージを表示します。
通知して録画する	録画しない	録画を停止します。
	通知しないで録画する	録画を続行します。エンドユーザーが次にログオンするときはメッセージが表示されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通知メッセージの作成

Dec 05, 2017

アクティブな録画ポリシーにより、セッションを録画するときにユーザーに通知する設定になっている場合、ユーザーが資格情報を入力した後にポップアップウィンドウが開き、通知メッセージが表示されます。デフォルトの通知メッセージは「現在開始しているプログラムでの操作が録画されています。この条件に不服である場合は、プログラムを閉じてください」です。ユーザーが **[OK]** をクリックすると、ウィンドウが閉じセッションを続行できます。

デフォルトの通知メッセージは、Session Recording Serverをホストするコンピューターのオペレーティングシステムの言語で表示されます。

選択した言語でカスタムの通知を作成できますが、言語ごとに作成できる通知メッセージは1つだけです。ユーザーには、ユーザーが選択したローカル設定の言語で通知メッセージが表示されます。

新しい通知メッセージの作成

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Serverのプロパティ]** を選択します。
3. **[Session Recording Serverのプロパティ]** で、 **[通知]** タブをクリックします。
4. **[追加]** をクリックします。
5. メッセージの言語を選択し新しいメッセージを入力します。1つの言語につき作成できるメッセージは1つです。

新しいメッセージを受け入れてアクティブにすると、[言語特有の通知メッセージ] ボックスに表示されます。
注： Session RecordingのAdministrator Logging機能により、Session Recordingのサーバーポリシー変更を記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画の無効化または有効化

Dec 05, 2017

Session Recording Agentは、セッションを録画する各VDA for Server OSにインストールします。インストール先のサーバーで録画を有効にするかどうかの設定を、Session Recording Agentで行います。録画を有効にすると、Session Recordingにより、アクティブな録画ポリシーが評価されます。このポリシーにより録画対象のセッションが決定されます。

Session Recording Agentをインストールすると、デフォルトで録画が有効になります。録画しないサーバーではSession Recordingを無効にすることをお勧めします。録画をしていないときでも、サーバーのパフォーマンスが多少影響を受けるためです。

サーバーでの録画の無効化または有効化

1. Session Recording Agentがインストールされているサーバーにログオンします。
2. **[スタート]** メニューから、 **[Session Recording Agentのプロパティ]** を選択します。
3. **[Session Recording]** で **[このXenAppサーバーでセッションを録画する]** チェックボックスをオンまたはオフにし、このサーバーでセッションを録画できるようにするかどうかを指定します。
4. 確認メッセージが表示されるので、Session Recording Agentサービスを再起動して変更を受け入れます。

注： Session Recordingをインストールしたときにアクティブになっているポリシーは **録画しない**」ポリシーです。どのサーバーのセッションも録画されません。録画を開始するには、Session Recordingポリシーコンソールを使用して別のポリシーをアクティブにします。

カスタムイベントの録画を有効にする

Session Recordingでは、サードパーティ製のアプリケーションを使用して、イベントとして知られるカスタムデータを録画されたセッションに挿入することができます。これらのイベントは、Session Recording Playerを使用してセッションを再生するときに表示されます。これらは録画されたセッションの一部であり、録画の後に変更することはできません。

たとえば、イベントに 「ユーザーがWebブラウザーを開きました」というテキストが含まれることがあります。というテキストが含まれることがあります。このテキストは、録画対象のセッションでエンドユーザーがWebブラウザーを開くたびに録画に挿入されます。Session Recording Playerを使用してセッションを再生するとき、Session Recording Playerの［イベントとブックマーク］の一覧に表示されるマーカーの数から、ユーザーがWebブラウザーを開いた回数がわかります。

サーバー上の録画にカスタムイベントを挿入するには

- **[Session Recording Agentのプロパティ]** を使用して、カスタムイベントを挿入する各サーバーで設定を有効にします。サーバーは個別に有効にする必要があります。サイト内のすべてのサーバーをまとめて有効にすることはできません。
- イベントAPIに基づくアプリケーションを開発します。このアプリケーションを各エンドユーザーのXenAppセッションで実行し、録画にデータを挿入します。

Session Recordingのインストールにはイベント記録COMアプリケーション（API）が含まれており、サードパーティ製のアプリケーションからテキストを録画に挿入することができます。Visual Basic、C++、またはC#を含む、多くのプログラミング言語でAPIを使用できます。詳しくは、CTX226844の記事を参照してください。Session RecordingイベントAPIのDLLはSession Recordingの一部としてインストールされます。APIのファイルは、%ProgramFiles%\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dllです。

サーバーでカスタムイベントの記録を有効にするには、以下の手順を実行します。

1. Session Recording Agentがインストールされているサーバーにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Agentのプロパティ]** を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. **[Session Recording Agentのプロパティ]** で、 **[録画]** タブをクリックします。
4. **[カスタムイベントの記録]** で **[このサーバーでサードパーティ製アプリケーションによるカスタムデータの記録を許可する]** チェックボックスをオンにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ライブセッションの再生と再生データの保護を有効または無効にする

Dec 05, 2017

ライブセッションの再生を有効または無効にする

Session Recording Playerを使用して、セッションの録画後または録画中にセッションを再生できます。録画中のセッションの再生は現在実行されている操作の表示と似ていますが、XenAppまたはXenDesktopサーバーからのデータ伝達で、実際には1、2秒の遅れが生じます。

録画が完了していないセッションを再生するときは、次の機能は使用できません。

- 録画が完了するまでデジタル証明書を割り当てることはできません。デジタル署名が有効な場合は、ライブセッションを再生できますが、まだ録画に署名はされていません。セッションが完了して初めて、証明書を表示できます。
- 録画が完了するまで、再生データの保護は適用できません。再生データの保護が有効な場合は、ライブセッションを再生できますが、セッションが完了するまでは暗号化されません。
- 録画が完了するまで、ファイルをキャッシュできません。

デフォルトで、ライブセッションの再生は有効になっています。

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Server のプロパティ]** を選択します。
3. **[Session Recording Server Properties]** で、 **[再生]** タブをクリックします。
4. **[ライブセッションの再生を許可する]** チェックボックスをオンまたはオフにします。

再生データの保護を有効または無効にする

セキュリティ上の安全のため、Session Recordingでは録画ファイルが自動的に暗号化されます。その後でファイルがダウンロードされ、Session Recording Playerで表示できるようになります。この再生データの保護機能により、録画ファイルをダウンロードしたユーザー以外のユーザーは、ファイルをコピーしたり表示したりできなくなります。ほかのワークステーションまたはユーザーアカウントでは、ファイルを再生できません。暗号化されたファイルは拡張子がICLEで、暗号化されていないファイルの拡張子はICLです。ファイルは、Session Recording Playerがインストールされているワークステーションのキャッシュにある間は暗号化されたままです。権限を持つユーザーがファイルを開いて初めて、暗号が解読されます。

HTTPSを使用して転送データを保護することをお勧めします。

再生データの保護は、デフォルトで有効になります。

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Serverのプロパティ]** を選択します。
3. **[Session Recording Serverのプロパティ]** で、 **[再生]** タブをクリックします。
4. **[再生のためダウンロードされるセッションの録画ファイルを暗号化する]** チェックボックスをオンまたはオフにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デジタル署名を有効および無効にする

Dec 05, 2017

Session Recordingコンポーネントがインストールされているコンピューターに証明書をインストールする場合は、デジタル署名をSession Recordingに割り当てることにより、Session Recording環境のセキュリティを強化できます。

デフォルトで、デジタル署名は無効になっています。 録画に署名する証明書を選択すると、Session RecordingからSession Recordingストレージマネージャーサービスに読み取り権限が付与されます。

デジタル署名の有効化

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Serverのプロパティ]** を選択します。
3. **[Session Recording Serverのプロパティ]** で、 **[署名]** タブをクリックします。
4. Session Recordingコンポーネントがインストールされているコンピューターの間で安全な通信を有効にする証明書を参照します。

デジタル署名の無効化

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Serverのプロパティ]** を選択します。
3. **[Session Recording Serverのプロパティ]** で、 **[署名]** タブをクリックします。
4. **[消去]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画の格納先の指定

Dec 05, 2017

［Session Recording Serverのプロパティ］を使用して、録画の格納先とアーカイブされた録画の再生時の復元先を指定します。

注： ファイルをアーカイブまたは削除されたファイルを復元するには、ICLDBコマンドを使用します。詳しくは、how to archiveand restore recordingsを参照してください。

録画を格納するフォルダーを指定する

デフォルトでは、録画はSession Recordingサーバーをホストするコンピューターのdrive:**\SessionRecordings**フォルダーに格納されます。録画を保存するフォルダーを変更したり、複数のボリューム間で負荷分散をするため、または追加の容量を活用するために、フォルダーを追加したりできます。複数のフォルダーが一覧にある場合は、録画がフォルダー間で負荷分散されていることを示します。1つのフォルダーを複数回追加できます。負荷分散は各フォルダーを循環して行われます。

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **［スタート］**ボタンをクリックし、**［Session Recording Serverのプロパティ］**を選択します。
3. **［Session Recording Serverのプロパティ］**で、**［格納場所］**タブをクリックします。
4. **［ファイル格納フォルダー］**ボックスの一覧を使用して、録画を格納するフォルダーを管理します。

フォルダーを選択すると、それらのフォルダーにフルコントロール権限のサービスが付与されます。

ローカルドライブ、SANボリューム、またはUNCネットワークパスで指定する場所にファイル格納フォルダーを作成できます。マップされたネットワークドライブのドライブ文字はサポートされません。Session Recordingでは、NAS（Network-Attached Storage：ネットワークアタッチトストレージ）を使用しないでください。ネットワークドライブへの録画データの書き込みに関連して、パフォーマンスおよびセキュリティ上の重大な問題が起きる可能性があります。

アーカイブされた録画の再生時の復元フォルダーを指定する

デフォルトでは、アーカイブされた録画はSession Recordingサーバーをホストするコンピューターのdrive:**\SessionRecordingsRestore**フォルダーに復元されます。フォルダーは変更できます。

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **［スタート］**ボタンをクリックし、**［Session Recording Serverのプロパティ］**を選択します。
3. **［Session Recording Serverのプロパティ］**で、**［格納場所］**タブをクリックします。
4. **［アーカイブ済みファイルの復元フォルダー］**ボックスにアーカイブ済み録画を復元するフォルダーを入力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画ファイルのサイズの指定

Dec 05, 2017

録画ファイルのサイズが大きくなるにつれて、ダウンロードに時間がかかり、再生中にシークスライダーを使用して再生箇所を変更するときに反応が遅くなるようになります。ファイルサイズを制御するにはファイルのしきい値を指定します。録画ファイルがこの限界に達すると、Session Recordingによってファイルが閉じられ、録画を続行するために新しいファイルが開かれます。この操作をロールオーバーと呼びます。

重要： ロールオーバーの設定は、XenDesktop 7.8およびSession Recording AgentのVDIデスクトップセッションに適用されません。この場合、各録画ファイルの最大サイズは1GBであり、この上限に到達するとアクティビティは録画されません。

ロールオーバーのため、2つのしきい値を指定できます。

- **ファイルサイズ。**ファイルがMB単位で指定された大きさに達すると、ファイルが閉じられ、新しいファイルが開かれます。デフォルトでは、ファイルが50MBに達するとロールオーバーが起こります。ただし、10MBから1GBの範囲で上限を指定できます。
- **時間。**セッションが時間単位で指定された時間録画されると、ファイルが閉じられ、新しいファイルが開かれます。デフォルトでは、12時間録画するとロールオーバーが起こります。ただし、1時間から24時間の範囲で上限を指定できます。

Session Recordingにより両方のボックスの値が確認され、ロールオーバーを実行するタイミングを決定するイベントとして、どちらのしきい値を先に超過するかが判断されます。たとえば、ファイルサイズに17MB、時間に6時間を指定し、録画ファイルのサイズが3時間で17MBに達したとします。この場合、17MBのファイルサイズに対応してロールオーバー処理が起動し、ファイルが閉じられ、新しいファイルが開かれます。

多くの小さなファイルが作成されないように、ファイルサイズに指定された値にかかわらず、少なくとも1時間（指定できる最小の値）が経過するまでロールオーバーは起こりません。この規則の例外は、ファイルサイズが1GBを超えた場合です。

録画の最大ファイルサイズの指定

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. **[スタート]** ボタンをクリックし、**[Session Recording Serverのプロパティ]** を選択します。
3. **[Session Recording Serverのプロパティ]** で、**[ロールオーバー]** タブをクリックします。
4. 10から1,024の間の整数を入力して、ファイルサイズの上限をMB単位で指定します。
5. 1から24の間の整数を入力して、録画時間の上限を時間単位で指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ログ管理アクティビティ

Dec 05, 2017

Session Recording Administrator Loggingでは以下のアクティビティが記録されます。

- Session Recording Policy ConsoleまたはCitrix Directorでの録画ポリシーへの変更。
- Session Recordingサーバーのプロパティにおける変更。
- Session Recording Playerでの録画のダウンロード。
- ポリシークエリ完了後のSession Recordingによるセッションの録画。
- 権限のない管理者ログサービスへのアクセス試行。

> **警告**
>
> レジストリエディターの編集を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

管理者ログの無効化または有効化

インストール後、Session Recordingサーバーのプロパティでsession Recording管理者ログ機能を無効または有効にできます。

1. Session Recording管理者ログがインストールされているサーバーに管理者としてログオンします。
2. **[スタート]** メニューから、 **[Session Recording Server Properties]** を選択します。
3. **[ログ]** タブをクリックします。

Session Recording管理者ログを無効にすると、新しいアクティビティは記録されません。既存のログをWebベースのUIから照会できます。

[必須ブロック] が有効な場合、ログが失敗すると以下のアクティビティがブロックされます。システムイベントもイベントID 6001で記録されます。

- Session Recording Policy ConsoleまたはCitrix Directorでの録画ポリシーへの変更。
- Session Recordingサーバーのプロパティにおける変更。

セッションの録画は必須のブロック設定による影響を受けません。

ユーザーへのアクセス権の付与

セキュリティ上の理由から、Administrator Loggingのログの照会など、特定の機能を実行するために必要な権限のみをユーザーに付与します。

Session Recording Serverをホストするコンピューターでsession Recording承認コンソールを使用して役割を割り当てることにより、ユーザーに権限を付与します。Administrator Loggingには2つの役割があります。

- **LoggingWriter**。Administrator Loggingのログを書き込む権限を付与します。デフォルトでは、ローカル管理者および

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Network Serviceがこの役割のメンバーです。

注： デフォルトの**LoggingWriter**メンバーシップを変更すると、ログの書き込みが失敗する原因となる可能性があります。

- **LoggingReader**。管理者ログを照会する権限を付与します。デフォルトでこの役割のメンバーになるユーザーはありません。

ユーザーに役割を割り当てるには

1. 管理者として、Session Recording Serverをホストするコンピューターにログオンします。
2. **Session Recording承認コンソール**を起動します。
3. ユーザーを割り当てる役割を選択します。
4. メニューバーで、**[操作]** > **[Windowsユーザーとグループの割り当て]** の順に選択します。
5. ユーザーとグループを追加してください。

管理コンソールで加えた変更は、1分間隔の更新時に有効になります。

Administrator Loggingサービスアカウントの構成

デフォルトで、管理者ログはインターネットインフォメーションサービス（IIS）のWebアプリケーションとして実行されており、IDはNetwork Serviceです。セキュリティレベルを拡張するために、このWebアプリケーションのIDをサービスアカウントまたは特定のドメインアカウントに変更できます。

1. 管理者として、Session Recordingサーバーをホストするコンピューターにログオンします。
2. IISマネージャーで、**[アプリケーションプール]をクリックします。**
3. **[アプリケーションプール]** で、**SessionRecordingLoggingAppPool**を右クリックして**[詳細設定]** を選択します。
4. 属性**ID**を、使用する特定のアカウントに変更します。
5. **db_owner**権限を、Microsoft SQL Serverのデータベース**CitrixSessionRecordingLogging**のアカウントに付与します。
6. レジストリキー**HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**の読み取り権限をアカウントに付与します。

録画アクションの記録の無効化または有効化

デフォルトで、管理者ログではポリシークエリ完了後のすべての録画アクションが記録されます。これにより、大量のログが生成される可能性があります。パフォーマンスを向上させてストレージを確保するには、レジストリでこの種類のログを無効にします。

1. 管理者として、Session Recordingサーバーをホストするコンピューターにログオンします。
2. レジストリエディターを開きます。
3. **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**を表示します。
4. **EnableRecordingActionLogging**の値として、以下を設定します。

   0録画アクションの記録の無効化

   1録画アクションの記録の有効化

Administrator Loggingデータの照会

Session Recordingでは、すべてのAdministrator Loggingを照会するためのWebベースのUIが提供されます。

Session Recording Serverをホストするコンピューターで、次の処理を行います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. **[スタート]** ボタンをクリックし、 **[Session Recording管理者ログ]** を選択します。
2. **LoggingReader**ユーザーの資格情報を入力します。

他のコンピューターで、次の処理を行います。

1. Webブラウザーを開いて、管理者ログのWebページにアクセスします。

   HTTPSで接続する場合： HTTPSで接続する場合：https://*servername*/SessionRecordingLoggingWebApplication/（ここで、*servername*はSession Recording Serverをホストするコンピューターの名前です）

   HTTPで接続する場合： http://*servername*/SessionRecordingLoggingWebApplication/（ここで、*servername*はSession Recording Serverをホストするコンピューターの名前です）

2. **LoggingReader**ユーザーの資格情報を入力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

データベースの高可用性を備えたSession Recordingのインストール

Dec 05, 2017

Session Recordingは、Microsoft SQL Serverをベースとしたデータベースの高可用性に関する次のソリューションをサポートしています。プリンシパルSQL ServerまたはプライマリSQL Serverのハードウェアまたはソフトウェアに障害が発生した場合、データベースが自動的にフェールオーバーするので、Session Recordingが想定どおりに機能し続けます。

- Always On可用性グループ

  AlwaysOn可用性グループ機能は、高可用性および障害回復ソリューションで、データベースのミラーリングに取って代わるエンタープライズレベルのサービスです。SQL Server 2012で導入されたAlwaysOn可用性グループ機能によって、エンタープライズ向けのユーザーデータベースの可用性が最大化します。AlwaysOn可用性グループ機能では、Windows Server Failover Clustering（WSFC）ノード上にSQL Serverインスタンスが存在する必要があります。詳しくは、http://msdn.microsoft.com/en-us/library/hh510230を参照してください。

- SQL Serverクラスタリング

  MicrosoftのSQLクラスタリングテクノロジーを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQL Serverデータベースミラーリングなどほかのソリューションよりも自動フェールオーバーには一般的に時間がかかります。詳しくは、https://msdn.microsoft.com/en-us/library/ms189134.aspxを参照してください。

- SQL Serverデータベースミラーリング

  データベースのミラーリングによって、アクティブなデータベースサーバーが停止しても数秒で自動的にフェールオーバーが実行されます。各データベースサーバー上に完全なSQL Serverライセンスが必要になるため、ほかの2つのソリューションよりも費用が高くつきます。SQL Server Expressエディションを使用してデータベースをミラーリングすることはできません。詳しくは、https://msdn.microsoft.com/en-us/library/ms189852.aspxを参照してください。

データベースの高可用性を備えたSession Recordingのインストール方法

データベースの高可用性を備えたSession Recordingをインストールするには、次のいずれかを実行します。

- 最初にSession Recording Serverコンポーネントをインストールし、次に作成したデータベースのデータベース高可用性を構成します。
  準備したSQL Serverインスタンスにデータベースがインストールされるよう構成して、Session Recording Administrationコンポーネントをインストールした後で、作成したデータベースのデータベース高可用性を構成できます。
  - AlwaysOn可用性グループおよびクラスタリングの場合は、SQL Serverインスタンス名を手動で、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstanceの可用性グループのリスナーの名前、またはSQL Serverネットワークの名前に変更する必要があります。
  - データベースのミラーリングの場合、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartnerおよびHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartnerにデータベースのフェイルオーバーパートナーを手動で追加する必要があります。
- 最初に空のデータベースのデータベース高可用性を構成し、次にSession Recording Administrationコンポーネントをインストールします。
  想定したプライマリSQL Serverインスタンスに、Session Recordingデータベースおよび監理者ログデータベースとして空

© 1999-2017 Citrix Systems, Inc. All rights reserved.

のデータベースを2つ作成し、高可用性を構成できます。次に、Session Recordingサーバーコンポーネントをインストールするときに、SQL Serverのインスタンス名を入力します。

- AlwaysOn可用性グループソリューションを使用するには、可用性グループのリスナーの名前を入力します。
- データベースのミラーリングソリューションを使用するには、プリンシパルSQL Serverの名前を入力します。
- クラスタリングソリューションを使用するには、SQL Serverのネットワーク名を入力します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画の表示

Dec 05, 2017

Session Recording Playerを使用して、録画したXenAppまたはXenDesktopセッションを表示、検索、およびブックマークします。

ライブセッションの再生機能を有効にしてセッションを録画する場合は、完了したセッションはもちろん、進行中のセッションも数秒遅れで表示できます。

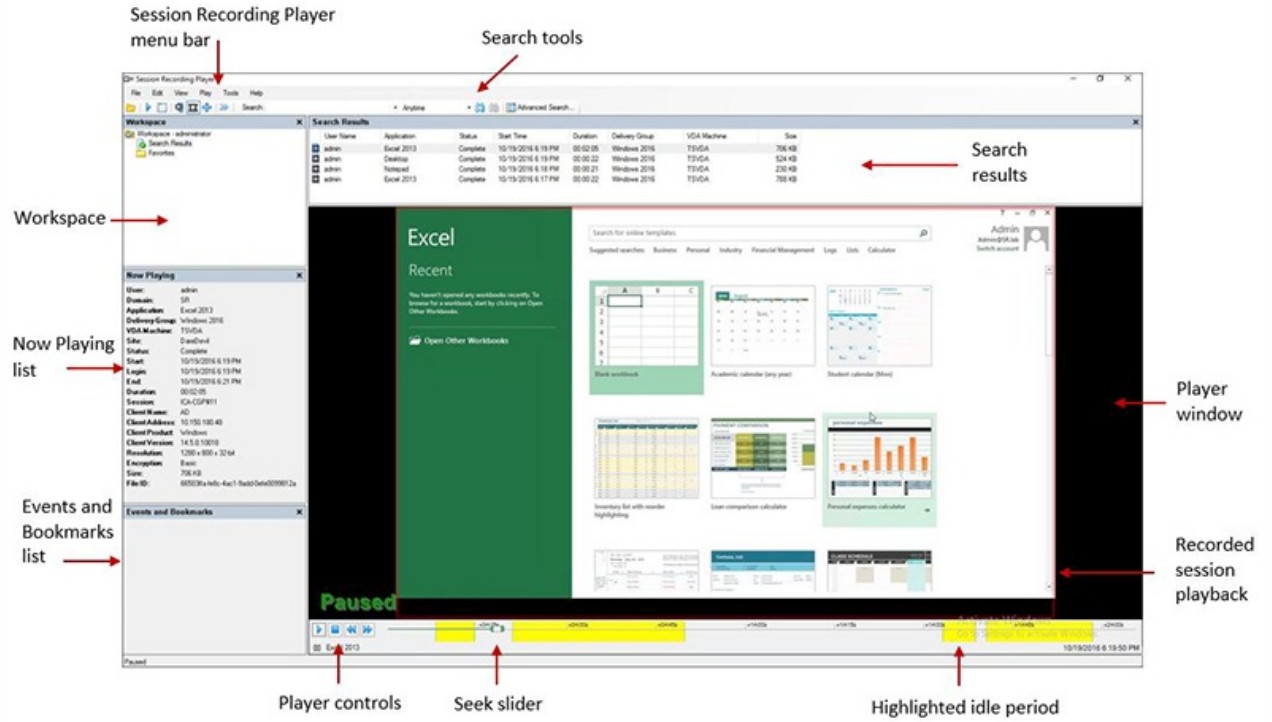
Session Recording管理者が設定する 時間やファイルサイズの上限を超えるセッションは、複数のセッションファイルに分けて表示されます。

注：Session Recording管理者が、録画されたVDA for Server OSのセッションへのアクセス権をユーザーに付与する必要があります。セッションを表示できない場合は、Session Recording管理者に連絡してください。
通常、Session Recording管理者がSession Recording Playerをインストールするとき、Session Recording PlayerとSession Recording Serverの間の接続も設定します。この接続が未設定の場合は、初めてファイルを検索するときに設定のダイアログボックスが開きます。設定に必要な情報についてはSession Recording管理者に問い合わせてください。

Session Recording Playerの起動

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **［スタート］ボタンをクリックし、［Session Recording Player］**を選択します。
   Session Recording Playerが表示されます。

この図はSession Recording Playerとその主な要素を示します。これらの要素の機能について、以下で説明します。



ウィンドウ要素の表示または非表示

Session Recording Playerには、表示するかどうかを切り替えるためのウィンドウ要素があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]ボタンをクリックし、[Session Recording Player]**を選択します。
3. **Session Recording Player**のメニューバーで、**[表示]**を選択します。
4. 表示する要素を選択します。選択するとすぐにその要素が表示されます。チェックマークはその要素が選択されていることを示します。

Session Recording Serverの変更

Session Recording管理者がSession Recording Playerから複数のSession Recording Serverに接続できるように設定した場合は、Session Recording Playerが接続するSession Recording Serverを選択できます。Session Recording Playerから同時に複数のSession Recording Serverに接続することはできません。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]ボタンをクリックし、[Session Recording Player]**を選択します。
3. **Session Recording Player**のメニューバーで、**[ツール]** > **[オプション]** > **[接続]**の順に選択します。
4. 接続するSession Recordingサーバーを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

録画の再生

Dec 05, 2017

Session Recording Playerでセッションの録画を開くには、次の3つの方法があります。

- Session Recording Playerを使用して検索を実行する。検索条件に一致するセッションの録画が、検索結果の領域に表示されます。
- ローカルディスクドライブまたは共有ドライブ上のセッションの録画ファイルに直接アクセスする。
- お気に入りフォルダーからセッションの録画ファイルにアクセスする。

デジタル署名なしで録画されたファイルを開くと、その元ファイルと整合性が検証されていないという警告が表示されます。ファイルの整合性について確信がある場合は、警告のポップアップウィンドウで **[はい]** をクリックしてファイルを開きます。

注： Session Recordingの管理者ログ機能により、Session Recording Playerの録画ダウンロードを記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

検索結果の領域にある録画を開いて再生する

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
3. 検索を実行します。
4. 検索結果の領域が表示されていない場合は、［ワークスペース］ペインの **[検索結果]** を選択します。
5. 検索結果の領域で、再生するセッションを選択します。
6. 次のいずれかを実行します。
   - セッションをダブルクリックします。
   - セッションを右クリックして **[再生]** を選択します。
   - **Session Recording Player**のメニューバーで、 **[再生]** > **[再生]** の順に選択します。

ファイルにアクセスして録画を開き再生する

セッションの録画ファイルの名前は、冒頭にi_が付く一意な英数字のファイルIDで、ファイル拡張子は.iclか.icleになります。.icl拡張子は再生データの保護機能が無効な録画を示し、.icle拡張子は有効な録画を示します。録画されたセッションのファイルは、セッションが録画された日付が組み込まれたフォルダに保存されます。たとえば、2014年12月22日に録画されたセッションのファイルは、2014\12\22というフォルダパスに保存されます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
3. 次のいずれかを実行します。
   - **Session Recording Player**のメニューバーで、 **[ファイル]** > **[開く]** の順に選択し、ファイルを参照します。
   - Windowsのエクスプローラーを使用してファイルを表示し、ファイルを**プレーヤー**ウィンドウにドラッグします。
   - Windowsのエクスプローラーを使用してファイルを表示し、ダブルクリックします。
   - ［ワークスペース］ペインにお気に入りを作成した場合は **[お気に入り]** を選択して、検索結果の領域から開く場合と同様に、お気に入りの領域からファイルを開きます。

お気に入りの使用

お気に入りフォルダーを作成して、頻繁に表示する録画にすばやくアクセスすることができます。お気に入りフォルダーによって、ワークステーションまたはネットワークドライブに格納されているセッションの録画ファイルが参照されます。こ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

れらのファイルはほかのワークステーションとの間でインポートとエクスポートをして、ほかのSession Recording Playerのユーザーと共有できます。

注： Session Recording Playerへのアクセス権を持つユーザーのみが、お気に入りフォルダーに関連付けられているセッションの録画ファイルをダウンロードできます。アクセス権については、Session Recording Player管理者に問い合わせてください。

お気に入りサブフォルダーを作成するには

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]** ボタンをクリックし、**[Session Recording Player]** を選択します。
3. **Session Recording Player**ウィンドウの［ワークスペース］ペインで **[お気に入り]** フォルダーを選択します。
4. メニューバーで **[ファイル]**、**[フォルダー]**、**[フォルダーの作成]** の順に選択します。**[お気に入り]** フォルダーの下の階層に新しいフォルダーが表示されます。
5. フォルダー名を入力し、**Enter**キーを押すか任意の場所をクリックして新しい名前を受け入れます。

[ファイル]、**[フォルダー]** の順に選択すると表示されるほかのオプションを使用して、フォルダーの削除、名前の変更、移動、コピー、インポート、およびエクスポートを行います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの録画の検索

Dec 05, 2017

Session Recording Playerでは、クイック検索を実行することも、高度な選択を実行して検索に適用するオプションを指定することもできます。検索結果はSession Recording Playerの検索結果の領域に表示されます。

注：使用可能な録画されたセッションを1回の検索で表示できるセッション数の上限まですべて表示するには、検索パラメーターを指定せずに検索を実行します。

クイック検索の実行

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
3. 次の方法で検索条件を定義します。
   - **[検索]** ボックスに検索条件を入力します。次の補助機能を使用できます。
   - **[検索]** ラベルの上にマウスポインターを移動すると、入力できるパラメーターの一覧が表示されます。
   - **[検索]** ボックス右側の矢印をクリックすると、過去に使用した検索文字列が最新の64件まで表示されます。
   - **[検索]** ボックス右側のドロップダウンリストを使用して、セッションが録画された期間を指定できます。
4. ドロップダウンリスト右側の双眼鏡のアイコンをクリックして、検索を開始します。

高度な検索の実行

ヒント：高度な検索では、結果に150,000個を超えるエンティティが含まれている場合、返されるまでに最大20秒かかる場合があります。日付範囲やユーザーなどのより厳密な検索条件を使用して、結果の数を減らすことをお勧めします。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
3. **[Session Recording Player]** ウィンドウで、ツールバーの **[高度な検索]** をクリックするか、メニューバーで **[ツール]** > **[高度な検索]** の順に選択します。
4. **[高度な検索]** ダイアログボックスのタブで検索条件を定義します。
   - **[共通]** タブでは、ドメインまたはアカウントの認証先、サイト、グループ、サーバーOSのVDA、アプリケーション、またはファイルIDを使用して検索できます。
   - **[日付/時刻]** タブでは、日付、曜日、および時刻を使用して検索できます。
   - **[イベント]** タブでは、Session Recording管理者がセッションに挿入したカスタムイベントを使用して検索できます。
   - **[そのほか]** タブでは、セッション名、クライアント名、クライアントアドレス、および録画時間を使用して検索できます。このタブでは、表示される検索結果数の上限およびアーカイブ済みのファイルを検索に含めるかどうかも指定できます。

   検索条件を指定するにつれて、作成しているクエリがダイアログボックス下部のペインに表示されます。
5. **[検索]** をクリックして検索を開始します。

ヒント：高度な検索のクエリは、保存しておいて後で取得することができます。**[高度な検索]** ダイアログボックスの **[保存]** をクリックして、現在のクエリを保存します。保存したクエリを取得するには、**[高度な検索]** ダイアログボックスの **[開く]** をクリックします。保存したクエリファイルの拡張子は.isqです。

検索オプションの設定

Session Recording Playerの検索オプションにより、表示される検索結果数の上限およびアーカイブ済みのファイルを検索に含めるかどうかも指定できます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
3. **Session Recording Player**メニューバーで、 **[ツール]** > **[オプション]** > **[検索]** の順に選択します。
4. **[検索結果の表示件数の上限]** ボックスに、表示する検索結果数を入力します。最大で500件の検索結果を表示できます。
5. アーカイブ済みのファイルを検索に含めるかどうかを設定するには、**[アーカイブ済みファイルを含める]** チェックボックスをオンまたはオフにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの録画の再生

Dec 05, 2017

Session Recording Playerでセッションの録画を開いた後は、次の方法で録画されたセッション内を移動できます。

- プレーヤーウィンドウのボタンを使用して、再生、停止、一時停止、および再生速度の変更を行います。
- シークスライダーを使用して、前後に移動します。

マーカーが録画に挿入されている場合、およびセッションの録画にカスタムイベントが含まれている場合は、マーカーおよびイベントのポイントに移動することによって、録画されたセッション内を移動することもできます。

注：

- セッションの録画の再生時に、マウスポインターが2つ表示される場合があります。この問題は、ユーザーがInternet Explorerを使用中に、Internet Explorerにより自動的に縮小表示されたイメージをユーザーがクリックすると発生します。セッション中は1つのマウスポインターしか表示されませんが、セッションの録画の再生時にのみ2つ目のマウスポインターが表示されます。
- このバージョンのSession Recordingは、XenAppのSpeedScreenマルチメディアアクセラレーション機能や［Flash品質の調整］ポリシー設定をサポートしません。この機能が有効の場合、再生画面が黒く表示されます。
- HDX RealTime Optimization Packを使用している場合、Session RecordingでLync Webカメラの映像を録画することはできません。
- 4096 x 4096以上の解像度でセッションを録画すると、録画が断片化する場合があります。
- XenDesktopサイトポリシーによって**従来のグラフィックモード**が有効になっており、Citrix Receiver for Windowsポリシーによって**ディスクベースのキャッシュ**が有効になっている場合、Windows 7デスクトップセッションを正しく録画できません。録画したものを再生すると、真っ黒の画面が表示されます。
  この問題を回避するには、Citrix Receiver for Windowsをインストールしたマシンで、グループポリシーオブジェクトを使用して**ディスクベースのキャッシュ**を無効化します。**ディスクベースのキャッシュ**を無効化する方法について詳しくは、CTX123169および「グループポリシーオブジェクト管理用テンプレート」を参照してください。
- Session Recordingでは、Franehawkの表示モードはサポートされません。このため、Framehawkの表示モードのセッションを正しく録画および再生することはできません。Framehawkの表示モードで録画されたセッションには、セッションアクティビティが含まれない可能性があります。

プレーヤーウィンドウのボタンの使用

プレーヤーウィンドウのボタンを使用するか、**Session Recording Player**メニューバーの［**再生**］の下のメニューアイテムを選択して、セッションの録画を操作します。プレーヤーウィンドウのボタンまたはメニューアイテムを使用して次の操作を実行します。

	選択したセッションファイルを再生します。
	再生を一時停止します。
	再生を停止します。［**停止**］、［**再生**］の順にクリックすると、ファイルの冒頭から再生が開始されます。
	現在の再生速度の半分に速度を変更します。最低で標準の4分の1にまで速度を下げます。
	現在の再生速度の2倍に速度を変更します。最高で標準の32倍にまで速度を上げます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

シークスライダーの使い方

プレーヤーウィンドウの下部にあるシークスライダーを使用して、セッションの録画内の別の位置にジャンプします。シークスライダーを録画内の表示したいポイントまでドラッグすることも、スライダーバーの任意のポイントをクリックして移動することもできます。

また、次のキーボードキーを使用してシークスライダーを制御できます。

キー：	シーク操作：
ホーム	冒頭へシークします。
終了日	末尾へシークします。
右矢印	5秒先へシークします。
左矢印	5秒前へシークします。
マウスホイールを1目盛り手前に動かす	15秒先へシークします。
マウスホイールを1目盛り奥に動かす	15秒前へシークします。
Ctrl+→	30秒先へシークします。
Ctrl+←	30秒前へシークします。
PgDn	1分先へシークします。
PgUp	1分前へシークします。
Ctrlキーを押しながらマウスホイールを1目盛り手前に動かす	90秒先へシークします。
Ctrlキーを押しながらマウスホイールを1目盛り奥に動かす	90秒前へシークします。
Ctrl+PageDown	6分先へシークします。
Ctrl+PageUp	6分前へシークします。

注： シークスライダーの速度を調整するには、**Session Recording Player**のメニューバーで、 **[ツール]** > **[オプショ**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ン] > [プレーヤー] の順に選択し、スライダーをドラッグしてシークの応答速度を変更します。応答速度を上げると、より多くのメモリが消費されます。録画のサイズやマシンのハードウェアによって、応答速度が低下する場合があります。

再生速度の変更

Session Recording Playerを設定して、標準の4分の1倍速から32倍速までの速度で、セッションの録画を再生できます。速度は指数的に増加します。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. [スタート] ボタンをクリックし、[Session Recording Player] を選択します。
3. **Session Recording Player**のメニューバーで、[再生] > [再生] の順に選択します。
4. 速度オプションを選択します。

すぐに速度が調節されます。速度を示す数字がプレーヤーウィンドウのボタンの下に表示されます。この速度を示す緑色のテキストは、プレーヤーウィンドウにも短時間表示されます。

録画されたセッションのアイドル期間のハイライト表示

録画されたセッションのアイドル期間とは、何も操作が行われていない部分です。Session Recording Playerでは、録画したセッションのアイドル期間を再生時にハイライトできます。 このオプションは、デフォルトで [オン] になっています。

Session Recording Playerでライブセッションを再生すると、アイドル期間がハイライトされない点に注意してください。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. [スタート] ボタンをクリックし、[Session Recording Player] を選択します。
3. **Session Recording Player**のメニューバーで、[表示] > [アイドル期間] と選択し、オプションボックスをオンまたはオフにします。

操作のない空白期間の省略

高速レビューモードを使用すると、録画されたセッション内で操作のない部分の再生を省略することができます。この設定により再生時間を短くできます。ただし、アニメーションを用いたマウスポインター、点滅するカーソル、秒針付きの時計など、動画による連続処理の再生は省略できません。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. [スタート] ボタンをクリックし、[Session Recording Player] を選択します。
3. **Session Recording Player**のメニューバーで、[再生] > [高速レビューモード] の順に選択します。

オプションがオンまたはオフに切り替わります。このオプションを選択するたびに、その状態がプレーヤーウィンドウに短時間表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

イベントとブックマークの使用

Dec 05, 2017

イベントとブックマークを使用して、録画されたセッション内を簡単に移動できます。

イベントは、イベントAPIおよびサードパーティ製のアプリケーションを使用して、セッションの録画中に挿入されます。イベントはセッションファイルの一部として保存されます。Session Recording Playerを使用して削除または変更することはできません。

ブックマークは、録画されたセッションにSession Recording Playerを使用して挿入するマーカーです。ブックマークは削除するまでは録画されたセッションに関連付けられますが、セッションファイルの一部としては保存されません。各ブックマークのデフォルトのラベルテキストは「**ブックマーク**」ですが、最長128文字までの任意のコメントテキストに変更できます。

イベントとブックマークはプレーヤーウィンドウの下部に丸印として表示されます。イベントの丸印は黄色で、ブックマークの丸印は青です。これらの丸印にポインターを合わせると、関連付けられているテキストラベルが表示されます。イベントとブックマークは、Session Recording Playerの**イベントとブックマーク**一覧にも表示できます。そのテキストラベルと録画されたセッションでの時刻と共に、時系列で一覧に表示されます。

イベントとブックマークを使用して、録画されたセッション内を簡単に移動できます。イベントまたはブックマークに移動することにより、それらが挿入されているポイントまでを省略して、録画されたセッション内を移動できます。

イベントとブックマークの一覧への表示

イベントとブックマークの一覧には、現在再生中の録画されたセッションに挿入されているイベントとブックマークが表示されます。イベントのみ、ブックマークのみ、または両方を表示できます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **イベントとブックマーク**の一覧にマウスポインターを移動し、右クリックしてメニューを表示します。
4. **[イベントのみ表示]**、**[ブックマークのみ表示]**、または **[すべて表示]** を選択します。

ブックマークの挿入

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. ブックマークを追加する、録画されたセッションの再生を開始します。
4. ブックマークを挿入する位置までシークスライダーを動かします。
5. プレーヤーウィンドウ内にマウスポインターを移動し、右クリックしてメニューを表示します。
6. 次の方法で、デフォルトのラベル「**ブックマーク**」でブックマークを追加するか、コメントを作成します。
   - デフォルトのラベル「**ブックマーク**」でブックマークを追加するには、**[ブックマークを追加]** を選択します。
   - 内容のわかるテキストラベルを作成してブックマークを追加するには、**[コメントを追加]** を選択します。ブックマークに割り当てるテキストラベルを最長128文字で入力します。**[OK]** をクリックします。

コメントの追加または変更

ブックマークを作成した後でコメントを追加したり、コメントを変更したりできます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. ブックマークを含む録画されたセッションの再生を開始します。
4. イベントとブックマークの一覧にブックマークが表示されていることを確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. **イベントとブックマーク**の一覧でブックマークを選択し、右クリックしてメニューを表示します。
6. **［コメントを編集］**を選択します。
7. 表示されるダイアログボックスに新しいコメントを入力して**［OK］**をクリックします。

ブックマークの削除

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **［スタート］ボタンをクリックし、［Session Recording Player］**を選択します。
3. ブックマークを含む録画されたセッションの再生を開始します。
4. イベントとブックマークの一覧にブックマークが表示されていることを確認します。
5. イベントとブックマークの一覧でブックマークを選択し、右クリックしてメニューを表示します。
6. **［削除］**を選択します。

イベントまたはブックマークへの移動

イベントまたはブックマークに移動すると、それらが挿入されているポイントまでを省略して、録画されたセッション内を移動できます。

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **［スタート］ボタンをクリックし、［Session Recording Player］**を選択します。
3. イベントまたはブックマークを含む録画されたセッションの再生を開始します。
4. 次の方法で、イベントまたはブックマークに移動します。
   - プレーヤーウィンドウの下部でイベントまたはブックマークを表す丸印をクリックし、イベントまたはブックマークに移動します。
   - **イベントとブックマーク**の一覧で、イベントまたはブックマークをダブルクリックします。次のイベントまたはブックマークに移動するには、一覧から任意のイベントまたはブックマークを選択して右クリックし、**［ブックマークへシーク］**を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

再生の表示形式の変更

Dec 05, 2017

オプションを使用して、プレーヤーウィンドウにセッションの録画を表示する形式を変更できます。セッションの録画をプレーヤーウィンドウまたは元のセッションのサイズに合わせて表示したり、全画面で再生したり、プレーヤーウィンドウを独立ウィンドウで表示したり、セッションの録画の周りに赤い枠を表示して、セッションをプレーヤーウィンドウの背景と区別しやすくしたりできます。

プレーヤーウィンドウの全画面表示

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[表示] > [全画面]** の順に選択します。
4. 元のサイズに戻すには、EscキーまたはF11キーを押します。

独立ウィンドウでのプレーヤーウィンドウの表示

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[表示] > [独立ウィンドウ]** の順に選択します。プレーヤーウィンドウを含む新しいウィンドウが開きます。ウィンドウをドラッグしてサイズを変更できます。
4. プレーヤーウィンドウをメインウィンドウに埋め込むには、メニューバーで **[表示] > [独立ウィンドウ]** の順に選択するか、**F10**キーを押します。

再生するセッションの画面サイズをプレーヤーウィンドウのサイズに合わせる

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[再生] > [表示モード] > [ウィンドウに合わせる]** の順に選択します。
   - **[ウィンドウに合わせる（高速描画）]** を選択すると、十分な画質を維持しながら画像を縮小します。高画質オプションを使用する場合より描画が高速で行われますが、画像とテキストの明晰さは低下します。高画質モードでパフォーマンスに問題が生じる場合は、このオプションを使用します。
   - **[ウィンドウに合わせる（高画質）]** を選択すると、明晰な画像とテキストを維持しながら画像を縮小します。このオプションを使用すると、高速描画オプションの場合より描画速度が遅くなることがあります。

再生するセッションの画面サイズを元のセッションのサイズに合わせる

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[再生] > [表示モード] > [セッションに合わせる]** の順に選択します。ポインターが手のひらの形に変化し、画面全体を表す小さなイメージがプレーヤーウィンドウの右上に表示されます。
4. 画面をドラッグします。小さなイメージに現在表示されている箇所が表示されます。
5. スクロールを停止するには、ウィンドウに合わせるオプションのどちらかを選択します。

セッションの録画の周りに赤い枠線を表示する

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[ツール] > [オプション] > [Player]** の順に選択します。
4. **[セッションの録画の周りに枠線を表示する]** チェックボックスをオンにします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ヒント： ヒント： **[セッションの録画の周りに枠線を表示する]** チェックボックスがオフの場合は、マウスポインターがSession Recording Playerウィンドウ内にあるときにマウスの左ボタンを押したままにすると、一時的に赤い枠線が表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの録画ファイルのキャッシュ

Dec 05, 2017

セッションの録画ファイルを開くたびに、録画が格納されている場所からファイルがダウンロードされます。同じファイルを頻繁にダウンロードする場合は、ファイルをワークステーションにキャッシュすることでダウンロード時間を節約できます。ワークステーションにキャッシュされるファイルは次のフォルダーに格納されます。

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

キャッシュに割り当てるディスク容量を指定できます。指定した容量まで録画ファイルが蓄積されると、最も古く使用されていない録画が削除され、新しい録画のための空き領域が作成されます。ディスク領域を解放するために、いつでもキャッシュを空にすることができます。

キャッシュの有効化

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[ツール] > [オプション] > [キャッシュ]** の順に選択します。
4. **[ダウンロードしたファイルをローカルコンピューターにキャッシュする]** チェックボックスをオンにします。
5. キャッシュに使用されるディスク容量を制限するには、**[使用するディスク容量を制限する]** チェックボックスをオンにして、使用する容量をメガバイト単位で指定します。
6. **[OK]** をクリックします。

キャッシュを空にする

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. **[スタート] ボタンをクリックし、[Session Recording Player]** を選択します。
3. **Session Recording Player**のメニューバーで、**[ツール] > [オプション] > [キャッシュ]** の順に選択します。
4. **[ダウンロードしたファイルをローカルコンピューターにキャッシュする]** チェックボックスをオンにします。
5. Session Recording Playerで、**[ツール] > [オプション] > [キャッシュ]** の順に選択します。
6. **[キャッシュの削除]** をクリックし、次に **[OK]** をクリックして操作を確定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recordingのトラブルシューティング

Dec 05, 2017

このトラブルシューティング情報には、Session Recordingコンポーネントのインストール中とインストール後に発生する可能性のある、次のような問題に対する解決策が含まれています。

- コンポーネントで相互接続できない。
- セッションを録画できない。
- Session Recording PlayerまたはSession Recording Policy Consoleの問題。
- 通信プロトコルに関連して問題が発生する。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Session Recording Agentから接続できないとき、「**Session Recording Brokerにポールメッセージを送信しています - この処理の実行中に例外が見つかりました。**」というイベントメッセージが、例外のテキストと共にログに記録されます。例外のテキストには接続に失敗した原因が記載されます。次のような原因があります。

- 「**基になる接続が閉じられました。SSL/TLSの安全なチャネルを確立できませんでした。**」この例外は、Session Recordingサーバーで使用している証明書を署名したCAが、Session Recording Agentが動作するサーバーに信頼されていないか、Session Recording Agentが動作するサーバーにCA証明書がインストールされていないことを示します。または、証明書の有効期限が切れているか失効している可能性があります。

  解決策：正しいCA証明書がSession Recording Agentをホストするサーバーにインストールされているか、信頼されているCAを使用していることを確かめます。

- 「**リモートサーバーがエラーを返しました。HTTP 403（アクセス不可）。**」これは、HTTP（セキュリティで保護されていないプロトコル）を使用して接続しようとしたときに表示される、標準のHTTPSエラーです。Session Recordingサーバーをホストするコンピューターでセキュリティで保護された接続のみを受け付けるため、接続が拒否されています。

  解決策： 解決策：［Session Recording Agentのプロパティ］を使用してSession Recording Brokerのプロトコルを**HTTPS**に変更します。

「**レコードポリシークエリの検証中に、Session Recording Brokerが不明なエラーを返しました。エラーコード5（アクセスが拒否されました）。 詳しくは、Session Recordingサーバー上のイベントログを参照してください。**」このエラーは、セッションが開始され録画ポリシーの評価要求が送信されると発生します。このエラーは、Session Recording承認コンソールの役割であるポリシークエリの役割から、デフォルトのメンバーであるAuthenticated Usersグループが削除された結果発生します。

解決策：Authenticated Usersグループをこの役割に再追加するか、各Session Recording Agentをホストする各サーバーをポリシークエリの役割に追加します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

「基になる接続が閉じられました。維持される必要があった接続が、サーバーによって切断されました。」このエラーは、Session Recordingサーバーが停止しているか、要求を受け付けられないことを示します。IISがオフラインまたは再起動中であることが原因か、サーバー全体がオフラインである可能性があります。

解決策：Session Recording Serverが開始されていること、サーバーでIISが実行中であること、およびサーバーがネットワークに接続していることを確かめます。

Session Recordingサーバーコンポーネントのインストールが、エラーコード2503および2502で失敗します。
解決策：C:\Windows\Tempフォルダーのアクセス制御リスト（ACL）を
チェックし、ローカルユーザーとローカルグループにこのフォルダーに対する書き込み権限が付与されていることを確認します。付与されていない場合は、書き込み権限を手動で付与します。

Session Recording ServerからSession Recordingデータベースに接続できないとき、次のいずれかのメッセージが表示されることがあります。

イベントソース：

SQL Serverへの接続を確立しているときにネットワーク関連またはインスタンス固有のエラーが発生しました。このエラーは、Session Recordingサーバーをホストするコンピューターのイベントビューアーにおいて、IDが2047のアプリケーションイベントログに表示されます。

「Citrix Session Recordingストレージマネージャーの説明: データベース接続を確立しています - この処理の実行中に例外が見つかりました。」 このエラーは、Session Recordingサーバーをホストするコンピューターのイベントビューアーのアプリケーションログに記録されます。

「Session Recording Serverに接続できません。Session Recording Serverが実行中か確認してください。」このエラーメッセージはSession Recordingポリシーコンソールを起動するときに表示されます。

解決策：

- Microsoft SQL Server 2008 R2、Microsoft SQL Server 2012、Microsoft SQL Server 2014、またはMicrosoft SQL Server 2016のExpress Editionがスタンドアロンサーバーにインストールされていますが、Session Recordingのサービスまたは設定が正しく設定されていません。サーバーでTCP/IPプロトコルを有効にしてSQL Server Browserサービスを実行する必要があります。これらの設定を有効にする方法について詳しくは、Microsoft社のドキュメントを参照してください。
- Session Recording管理ツールのインストール中に、サーバーとデータベースについて誤った情報が指定されています。Session Recordingデータベースをアンインストールし、正しい情報を指定して再インストールします。
- Session Recordingデータベースサーバーが停止しています。サーバーに接続できることを確かめます。
- Session RecordingサーバーまたはSession Recordingデータベースサーバーをホストするコンピューターで、もう一方のFQDNまたはNetBIOS名を解決できません。pingコマンドを使用して、名前を解決できることを確認します。
- Session Recordingデータベースのファイアウォールの構成をチェックし、SQL Serverの接続が許可されていることを確認します。詳しくは、Microsoftの記事https://msdn.microsoft.com/en-us/library/cc646023.aspxを参照してください。

ユーザー 'NT_AUTHORITY\ANONYMOUS LOGON' ログオン失敗。 このエラーメッセージは、サービスのログオンアカウントが誤って.\administratorになっていることを意味します。

解決策：ローカルシステムユーザーとしてサービスを再起動し、SQLサービスを再起動します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーションセッションが正常に録画されない場合は、まずSession Recording AgentとSession Recordingサーバーが動作するVDA for Server OS上のイベントビューアーで、アプリケーションイベントログを確認します。このログには有益な診断情報が含まれている可能性があります。

セッションが録画されない場合、次の問題が原因である可能性があります。

- **コンポーネント間の接続と証明書**。Session Recordingコンポーネントの間で通信ができない場合は、セッションの録画に失敗する可能性があります。録画の問題のトラブルシューティングをするには、すべてのコンポーネントが適切に設定されていて正しいコンピューターを参照していることと、すべての証明書が有効で適切にインストールされていることを確かめます。
- **Active Directoryドメインでない環境**。Session RecordingはMicrosoft Active Directoryドメインの環境で動作するように設計されています。Active Directory環境で運用していない場合は、録画で問題が発生する可能性があります。Session Recordingのすべてのコンポーネントは、必ずActive Directoryドメインに参加しているコンピューターで実行します。
- **セッション共有がアクティブなポリシーと競合している。**Session Recordingでは、アクティブなポリシーとエンドユーザーが最初に開いた公開アプリケーションを照合します。同じセッション上で次のアプリケーションを開くと、最初のアプリケーションに対して有効なポリシーが、次のアプリケーションにも適用されます。セッション共有がアクティブなポリシーと競合することを防ぐには、競合するアプリケーションを別のVDAs for Server OSで公開します。
- **録画が有効になっていない。**VDA for Server OSにSession Recording Agentをインストールすると、そのサーバーではデフォルトで録画が有効になります。録画を許可するアクティブな録画ポリシーを設定するまでは、録画はされません。
- **アクティブな録画ポリシーによって録画が許可されない。**セッションを録画するには、特定のユーザー、サーバー、または公開アプリケーションを対象に、アクティブな録画ポリシーでセッションの録画が許可されている必要があります。
- **Session Recordingサービスが実行されていない。**セッションを録画するには、VDA for Server OSでSession Recording Agentサービスが実行されており、Session Recordingサーバーをホストするコンピューターで Session Recordingストレージマネージャーサービスが実行されている必要があります。
- **MSMQが設定されていない。**Session Recording Agentが動作するサーバーとSession Recordingサーバーをホストするコンピューターで MSMQが適切に設定されていない場合は、録画の問題が起きる可能性があります。

Session Recording Playerで録画を再生できないときは、次のエラーメッセージが表示される可能性があります。

「**セッションの録画ファイルをダウンロードできませんでした。ライブセッションの再生は許可されていません。サーバーがこの機能を許可しない設定になっています。**」このエラーは、サーバーがこの操作を許可しないように設定されていることを示します。

解決策： **[Session Recording Server のプロパティ]** で **[再生]** タブをクリックし、 **[ライブ セッションの再生を許可する]** チェックボックスをオンにします。

- Session Recording Playerを使用して表示した場合に録画が破損しているか、または不完全である場合、Session Recording Agentのイベントログにも警告が記録されることがあります。

  イベントソース：Citrix Session Recordingストレージマネージャー

  説明：ファイルを録画中のデータ喪失。

  通常、この問題は、Machine Creation Services（MCS）またはProvisioning Services（PVS）で構成済みのマスターイメージとインストール済みのMicrosoft Message Queuing（MSMQ）を使用してVDAを作成する場合に発生します。この状況では、VDAでMSMQのQMIdが同じになります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

これを回避するには、各VDAに対し、一意のQMIdを作成します。詳しくは、「Session Recordingのインストール、アップグレード、およびアンインストール」のここを参照してください。

- 特定の録画ファイルを再生しているときに、Session Recording Playerがメッセージ「**再生中のファイルにより、内部システムエラー（エラーコード: 9）が元の録画中に発生したことが報告されました。エラーが発生した箇所までは再生できます。**」を表示して内部エラーをレポートすることがあります。

  この問題は通常、グラフィック指向セッションの録画中にSession Recording Agentのバッファーサイズが不十分だったために発生します。

  これを回避するには、Session Recording Agentでレジストリ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMBの値を大きな値に変更してから、マシンを再起動します。

Session RecordingデータベースまたはSession Recording Serverのインストール時に、データベースインスタンス名が正しくても、エラーメッセージ「**Database connection test failed. Please correct Database instance name**」が表示されて接続テストが失敗します。

そのような場合は、現在のユーザーに、権限制限エラーを修正するためのパブリックSQL Server役割権限があることを確認してください。

Windows Server 2008 R2 SP1では、Administrator Logging機能をインストールする前に、まず **[.Net Framework 3.5の機能]** > **[WCFアクティブ化]** > **[HTTPアクティブ化]** をインストールしてから、.Net Framework 4.5以降のバージョンをインストールします。これら2つの要件を逆の順番でインストールしないでください。順番に従わないと、Administrator Loggingが想定どおり機能しない可能性があります。Session Recordingの構成をサーバープロパティコンソールで変更しようとしたり、Session Recordingポリシーを必須のログが有効になった状態でポリシーコンソールで更新しようとしたりすると、操作がブロックされる場合があります。

この問題を解決するには、次の手順に従います。

1. ［インターネットインフォメーションサービス（IIS）マネージャー］を開いて **[アプリケーションプール]** ノードに移動します。
2. **[SessionRecordingLoggingAppPool]** を右クリックして、 **[基本設定]** ダイアログを開きます。
3. .NET Frameworkバージョンを.NET Framework v4.0に変更します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コンポーネント間の接続の確認

Dec 05, 2017

Session Recordingのセットアップ中にコンポーネント間の接続に成功しないことがあります。すべてのコンポーネントがSession Recordingサーバー（Broker）と通信を行います。デフォルトでは、IISのコンポーネントであるブローカーのセキュリティは、IISの既定のWebサイトの証明書を使用して保護されます。あるコンポーネントからSession Recordingサーバーに接続できないときは、ほかのコンポーネントから接続を試行しても失敗することがあります。

Session Recording AgentとSession Recording Server（ストレージマネージャーとブローカー）の接続エラーは、Session Recording Serverをホストするコンピューターの、イベントビューアーのアプリケーションログに記録されます。Session Recording Policy ConsoleとSession Recording Playerでは、接続に失敗したときに画面にエラーメッセージが表示されます。

1. Session Recording Agentがインストールされているサーバーにログオンします。
2. **[スタート]** ボタンをクリックし、 **[Session Recording Agentのプロパティ]** を選択します。
3. **[Session Recording Agentのプロパティ]** で、 **[接続]** をクリックします。
4. ［Session Recording Server］の値が、Session Recordingサーバーをホストするコンピューターの正しい名前であることを確認します。
5. ［Session Recording Server］の値として入力されているサーバーにVDA for Server OSから通信できることを確かめます。

注： イベントビューアーのアプリケーションログにエラーや警告が記録されていないか確認します。

注意： レジストリエディターの使用によって、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。

1. Session Recordingサーバーをホストするコンピューターにログオンします。
2. レジストリエディターを開きます。
3. HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Serverを表示します。
4. **SmAudDatabaseInstance**の値で、SQL Serverのインスタンスにインストールしたデータベースが正しく参照されていることを確かめます。

1. SQL管理ツールを使用して、インストールしたSession Recordingデータベースを含むSQLインスタンスを開きます。
2. Session Recordingデータベースのセキュリティ許可を開きます。
3. Session Recordingコンピューターアカウントにデータベースへのアクセス許可が与えられていることを確かめます。たとえば、Session Recordingサーバーをホストするコンピューターの名前がMISドメインの**SsRecSrv**である場合、データベースにコンピューターアカウントとして**MIS\SsRecSrv$**を指定する必要があります。この値はSession Recordingデータベースのインストール中に設定します。

Session Recording コンポーネントで通信に問題が起きたときは、 WebブラウザーでSession Recording BrokerのWebページにアクセスしてSession RecordingサーバーのIISサイトへの接続をテストすると、問題の原因が、プロトコルの誤設定なのか、証明書の 問題なのか、Session Recording Brokerの問題なのかを 判断するのに役立ちます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording AgentのIISの接続を確かめるには

1. Session Recording Agentがインストールされているサーバーにログオンします。
2. Webブラウザーを起動して次のアドレスを入力します。
   - HTTPSで接続する場合：**https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**（ここで、<*servername*>はSession Recordingサーバーをホストするコンピューターの名前です）
   - HTTPで接続する場合：**http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**（ここで、<*servername*>はSession Recordingサーバーをホストするコンピューターの名前です）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Session Recording PlayerのIISの接続を確かめるには

1. Session Recording Playerがインストールされているワークステーションにログオンします。
2. Webブラウザーを起動して次のアドレスを入力します。
   - HTTPSで接続する場合：**https://servername/SessionRecordingBroker/Player.rem?wsdll**（ここで、<*servername*>はSession Recordingサーバーをホストするコンピューターの名前です）
   - **HTTPで接続する場合：http://servername/SessionRecordingBroker/Player.rem?wsdl**（ここで、*servername* はSession Recordingサーバーをホストするコンピューターの名前です）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Session Recording Policy ConsoleのIISの接続を確かめるには

1. Session Recording Policy Consoleがインストールされているサーバーにログオンします。
2. Webブラウザーを起動して次のアドレスを入力します。
   - HTTPSで接続する場合：**https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**（ここで、<*servername*>はSession Recordingサーバーをホストするコンピューターの名前です）
   - HTTPで接続する場合：**http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**（ここで、<*servername*>はSession Recordingサーバーをホストするコンピューターの名前です）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

WebブラウザーにXMLドキュメントが表示された場合は、設定したプロトコルを使用して、Session Recordingポリシーコンソールが動作するコンピューターがSession Recordingサーバーをホストするコンピューターと接続していることが確かめられたことになります。

通信プロトコルにHTTPSを使用する場合は、Session Recordingサーバーを ホストするコンピューターにサーバー 証明書を設定する必要があります。すべてのコンポーネントのSession Recordingサーバーへの接続に、ルートCA（Certificate Authority：証明機関）が 必要です。この証明書をインストールしないと、 コンポーネント間の通信は失敗します。

IISの接続をテストするときのように、Session Recording BrokerのWebページにアクセスすることによって、証明書をテストすることができます。各コンポーネントのXMLページに アクセスできる場合は、証明書は 正しく設定されています。

ここでは、接続 エラーの原因になる、証明書によくある問題について説明します。

- **無効な証明書または 証明書の不足：**Session Recording Agentが動作するサーバーにサーバー証明書を信頼するためのルート証明書がインストールされていない場合は、HTTPSを介してSession Recordingサーバーを信頼できず、接続できません。 Session Recordingサーバー上のサーバー証明書がすべてのコンポーネントで信頼されていることを確かめてください。
- **名前の不一致。**Session Recordingサーバーをホストするコンピューターに割り当てられたサーバー証明書が、完全修飾ドメイン名を使用して作成されている場合、Session Recordingサーバーに接続するとき、接続するすべてのコンポーネント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

で完全修飾ドメイン名を使用する必要があります。 サーバー証明書がNetBIOS名を使用して作成されている場合、Session Recordingサーバーに接続するとき、接続するすべてのコンポーネントでNetBIOS名を使用するように設定します。

- **失効した証明書。**サーバー証明書が失効している場合、HTTPSを介したSession Recordingサーバーへの接続は失敗します。 Session Recordingサーバーをホストするコンピューターに割り当てられているサーバー証明書が有効で、失効していないことを確かめてください。 録画したセッションのデジタル署名に同じ証明書を使用している場合は、Session Recordingサーバーをホストするコンピューターのイベントログに、証明書が失効したことを示すエラーメッセージまたは失効日が近づいていることを示す警告メッセージが記録されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording Playerに障害が発生した場合の録画の検索

Dec 05, 2017

Session Recording Playerで録画を検索できないときは、次のエラーメッセージが表示される可能性があります。

- **「セッションの録画ファイルを検索できませんでした。リモートサーバー名を解決できませんでした。 servername」**ここで、servernameはSession Recording Playerで接続を試行しているサーバーの名前です。Session Recording PlayerはSession Recordingサーバーと通信することができません。この原因として、誤ったサーバー名が入力されているか、DNSでサーバー名を解決できていないという、2つの理由が考えられます。
  解決策： Session Recording Playerのメニューバーで、 **[ツール]** > **[オプション]** > **[接続]** の順に選択し、 **[Session Recording Server]** ボックスの一覧のサーバー名が正しいことを確認します。サーバー名が正しい場合は、コマンドプロンプトでpingコマンドを実行し、名前を解決できるかどうかを確認します。Session Recordingサーバーが停止しているかオフラインのときにセッションの録画ファイルを検索すると、「**リモートサーバーに接続できません**」というエラーメッセージが返されます。

- **リモートサーバーに接続できません。**このエラーは、Session Recordingサーバーが停止しているかオフラインのときに発生します。
  解決策：Session Recordingサーバーが接続していることを確かめます。

- **「アクセスが拒否されました。」**アクセス拒否のエラーは、ユーザーにセッションの録画ファイルを検索およびダウンロードする権限がない場合に発生します。
  解決策：Session Recording承認コンソールで、ユーザーをプレーヤーの役割に割り当てます。

- **「Playerの役割が割り当てられているときにアクセスが拒否されました。」**このエラーは、通常、Session Recording PlayerとSession Recordingサーバーを同じマシンにインストールし、UACを有効にしているときに発生します。Domain AdminsまたはAdministratorsユーザーグループにPlayerの役割を割り当てたときに、そのグループに含まれていない組み込みではない管理者ユーザーがSession Recording Playerで録画ファイルを検索するときに役割ベースのチェックを渡せないことがあります。
  解決策：

  + Session Recording Playerを管理者として実行します。

  + グループ全体ではなく特定のユーザーにPlayerの役割を割り当てます。

  + Session Recordingサーバーではなく Session Recording Playerを個別のマシンにインストールします。

- **「セッションの録画ファイルを検索できませんでした。「基になる接続が閉じられました。SSL/TLSの安全なチャネルを確立できませんでした。」** この例外は、Session Recordingサーバーで使用している証明書を署名したCA（Certificate Authority：証明機関）がクライアントデバイスに信頼されていないか、クライアントデバイスにCA証明書がインストールされていないために発生します。
  解決策：Session Recording Playerがインストールされているワークステーションに、正しい、つまり信頼されているCA証明書をインストールします。

- **「リモートサーバーがエラーを返しました。HTTP 403（アクセス不可）。」**このエラーは、HTTP（セキュリティで保護されていないプロトコル）を使用して接続しようとしたときに発生する、標準のHTTPSエラーです。デフォルトでは、セキュリティで保護されている接続のみを受け入れるように設定されるため、サーバーにより接続が拒否されます。
  解決策： **Session Recording Player**のメニューバーで、 **[ツール]** > **[オプション]** > **[接続]** の順に選択しま

© 1999-2017 Citrix Systems, Inc. All rights reserved.

す。 **[Session Recordings Server]** ボックスの一覧でサーバーを選択し、 **[変更]** をクリックします。プロトコルを **[HTTP]** から **[HTTPS]** に変更します。

セッションの録画を知らせる通知メッセージがエンドユーザーに表示されているのに、Session Recording Playerで検索しても録画が見つからない場合は、MSMQに問題がある可能性があります。キューがSession Recordingサーバー（ストレージマネージャー）に接続されていることを確認し、Webブラウザーを使用して接続エラーが発生しないか確認します（MSMQの接続プロトコルとしてHTTPまたはHTTPSを使用している場合）。

キューが接続されていることを確認するには

1. Session Recording Agentをホストするサーバーにログインして、発信キューを表示します。
2. Session Recordingサーバーをホストするコンピューターへのキューが接続された状態であることを確認します。
   - **接続を待っている**状態で、多くのメッセージがキューにあり、プロトコルがHTTPまたはHTTPSの場合は（**[Session Recording Agent のプロパティ]** の **[接続]** タブで選択されているプロトコルに対応します）、手順3を実行します。
   - **接続済み**の状態で、メッセージがキューにない場合は、Session Recordingサーバーをホストするサーバーに問題がある可能性があります。手順3を省略し、手順4を実行します。
3. キューに多くのメッセージがある場合は、Webブラウザーを起動して次のアドレスを入力します。
   - HTTPSで接続する場合：**https://servername/msmq/private$/CitrixSmAudData**（ここで、*<servername>*はSession Recordingサーバーをホストするコンピューターの名前です）
   - HTTPで接続する場合：**http://servername/msmq/private$/CitrixSmAudData**（ここで、*<servername>*はSession Recordingサーバーをホストするコンピューターの名前です）

   「**サーバーはセキュリティで保護された接続のみを受け付けます**」というようなエラーが返される場合は、 **[Session Recording Agent のプロパティ]** に一覧されているMSMQプロトコルをHTTPSに変更します。そうではなく、Webサイトのセキュリティ証明書に問題があるというエラーが返される場合は、TLSのセキュアチャネルのための信頼関係に問題がある可能性があります。その場合は、正しいCA証明書をインストールするか、信頼されているCAを使用します。
4. キューにメッセージがない場合は、Session Recordingサーバーをホストするコンピューターにログオンし、専用キューを表示します。**citrixsmauddata**を選択します。キューに多くのメッセージがある場合は（［メッセージ数］列を確認します）、Session Recording StorageManagerサービスが開始されていることを確認します。開始されていない場合は、サービスを再起動します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通信プロトコルの変更

Dec 05, 2017

セキュリティ上の理由から、HTTPを通信プロトコルに使用することはお勧めできません。デフォルトでは、Session RecordingはHTTPSを使用して通信するように設定されます。HTTPSではなくHTTPを使用する場合は、いくつかの設定を変更する必要があります。

1. Session Recording Serverをホストするコンピューターにログオンし、IISで、Session Recording Brokerの接続のセキュリティを保護しないようにします。
2. Session Recording Agentがインストールされている各サーバーの **[Session Recording Agentのプロパティ]** でプロトコル設定をHTTPSからHTTPに変更します。
   1. Session Recording Agentがインストールされている各サーバーにログオンします。
   2. **[スタート]** ボタンをクリックし、 **[Session Recording Agentのプロパティ]** を選択します。
   3. **[Session Recording Agentのプロパティ]** ダイアログボックスで **[接続]** タブをクリックします。
   4. **[Session Recording Broker]** で **[プロトコル]** ボックスの一覧から **[HTTP]** を選択し、 **[OK]** をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、 **[はい]** をクリックします。
3. Session Recording Playerの設定でプロトコルをHTTPSからHTTPに変更します。
   1. Session Recording Playerがインストールされている各ワークステーションにログオンします。
   2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
   3. **[Session Recording Player]** メニューバーで **[ツール]** > **[オプション]** > **[接続]** の順に選択し、サーバーを選択して **[変更]** をクリックします。
   4. **[プロトコル]** ボックスの一覧から **[HTTP]** を選択し、［OK］を2回クリックして、変更を受け入れてダイアログボックスを閉じます。
4. Session Recording Policy Consoleの設定でプロトコルをHTTPSからHTTPに変更します。
   1. Session Recording Policy Consoleがインストールされているサーバーにログオンします。
   2. **[スタート]** ボタンをクリックし、 **[Session Recording Policy Console]** を選択します。
   3. **[プロトコル]** ボックスの一覧から **[HTTP]** を選択し、［OK］をクリックして接続します。接続が確立するとこの設定が保存され、次にSession Recordingポリシーコンソールを起動するときに使用されます。

1. Session Recording Serverをホストするコンピューターにログオンし、IISで、Session Recording Brokerの接続のセキュリティを保護します。
2. Session Recording Agentがインストールされている各サーバーの **[Session Recording Agentのプロパティ]** でプロトコル設定をHTTPからHTTPSに変更します。
   1. Session Recording Agentがインストールされている各サーバーにログオンします。
   2. **[スタート]** ボタンをクリックし、 **[Session Recording Agentのプロパティ]** を選択します。
   3. **[Session Recording Agentのプロパティ]** ダイアログボックスで **[接続]** タブをクリックします。
   4. **[Session Recording Broker]** で **[プロトコル]** ボックスの一覧から **[HTTPS]** を選択し、 **[OK]** をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、 **[はい]** をクリックします。
3. Session Recording Playerの設定でプロトコルをHTTPからHTTPSに変更します。
   1. Session Recording Playerがインストールされている各ワークステーションにログオンします。
   2. **[スタート]** ボタンをクリックし、 **[Session Recording Player]** を選択します。
   3. **[Session Recording Player]** メニューバーで **[ツール]** > **[オプション]** > **[接続]** の順に選択し、サーバーを選択して **[変更]** をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. **[プロトコル]** ボックスの一覧から **[HTTPS]** を選択し、 **[OK]** を2回クリックして、変更を受け入れてダイアログボックスを閉じます。

4. Session Recording Policy Consoleの設定でプロトコルをHTTPからHTTPSに変更します。
    1. Session Recording Policy Consoleがインストールされているサーバーにログオンします。
    2. **[スタート]** ボタンをクリックし、 **[Session Recording Policy Console]** を選択します。
    3. **[プロトコル]** ボックスの一覧から **[HTTPS]** を選択し、 **[OK]** をクリックして接続します。接続が確立するとこの設定が保存され、次にSession Recordingポリシーコンソールを起動するときに使用されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

リファレンス：データベースレコードの管理

Dec 05, 2017

ICAログデータベース（ICLDB）ユーティリティは、データベース用のコマンドラインユーティリティで、セッションの録画のデータベースレコードを操作するために使用します。このユーティリティは、Session Recording Serverソフトウェアをホストするサーバーのdrive:\Program Files\Citrix\SessionRecording\Server\Binフォルダーに、Session Recordingと合わせてインストールされます。

次の表に、ICLDBユーティリティで使用できるコマンドとオプションの一覧を示します。コマンドは次の形式で入力します。

icldb [version | locate | dormant | import | archive | remove | removeall] <コマンドオプション> [/l] [/f] [/s] [/?]

注： ユーティリティのオンラインヘルプにさらに詳しい説明が記載されています。オンラインヘルプにアクセスするには、コマンドプロンプトでdrive:**\Program Files\Citrix\SessionRecording\Server\Bin**ディレクトリに移動し、**icldb /?**と入力します。特定のコマンドのオンラインヘルプにアクセスするには、**icldb *<コマンド>* /?**と入力します。

コマンド	説明
archive	指定された保有期間を過ぎたセッションの録画ファイルをアーカイブします。 このコマンドを使用してファイルをアーカイブします。
dormant	休止状態とみなされるセッションの録画ファイルの数またはファイル名を表示します。休止ファイルとは、データの損失のために不完全なセッションの録画ファイルです。 このコマンドを使用してデータの損失があるかどうかを検証します。休止状態のセッションの録画ファイルの検索対象として、データベース全体を指定することも、日、時間、または分単位で、録画が行われた期間を指定することもできます。
import	セッションの録画ファイルをSession Recordingデータベースにインポートします。 このコマンドを使用して、データベースレコードを失ったときにデータベースを再構築します。 また、このコマンドを使用して、データベースをマージします。2つのデータベースがある場合は、一方のデータベースからファイルをインポートできます。
locate	ファイルIDを条件として、セッションの録画ファイルを検索しフルパスを表示します。 このコマンドを使用して、セッションの録画ファイルの格納場所を検索します。 このコマンドは、特定のファイルを条件にデータベースが最新の状態かどうかを検証する手段としても使用できます。
削除	セッションの録画ファイルへの参照をデータベースから削除します。 このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。条件として使用する保有期間を指定します。 関連付けられている物理ファイルを削除することもできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

コマンド	説明
removeall	セッションの録画ファイルへのすべての参照をSession Recordingデータベースから削除し、データベースを元の状態に戻します。実際の物理ファイルは削除されません。ただし、Session Recording Playerでファイルを検索することはできなくなります。 このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。削除された参照はバックアップから復元しない限り元に戻せません。
ページで、	Session Recordingデータベースのスキーマバージョンを表示します。
/l	結果とエラーをWindowsのイベントログに記録します。
/f	プロンプトを表示せずにコマンドを強制的に実行します。
/s	著作権のメッセージを非表示にします。
/?	コマンドのオンラインヘルプを表示します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

構成ログ

Dec 05, 2017

構成ログ機能では、管理者によるサイト構成の変更やそのほかの管理操作がデータベースに記録されます。このログは、以下の目的で使用できます。

- 構成変更の履歴を確認して問題の診断およびトラブルシューティングを行う。
- 変更管理の補助および構成の追跡を行う。
- 管理アクティビティのレポートを生成する。

Citrix Studioでは、構成ログの基本設定を変更したり、構成ログを表示したり、HTMLおよびCSV形式のレポートを生成したりできます。日範囲および全文検索の結果により構成ログ表示をフィルターできます。必須ログ機能を有効にすると、ログが記録可能になるまで管理者による構成の変更が禁止されます。適切な権限を持つ管理者は、構成ログのエントリを削除できます。構成ログ機能では、ログの内容を編集することはできません。

構成ログでは、PowerShell SDKとConfiguration Logging Serviceが使用されます。Configuration Logging Serviceは、サイト内のすべてのController上で実行されます。任意のControllerに障害が発生しても、ほかのControllerが自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効で、サイト作成時に作成されたデータベース（サイト構成データベース）が使用されます。データベースには別の場所を指定できます。構成ログデータベースでは、サイト構成データベースと同じ高可用性機能がサポートされます。

構成ログにアクセスするには、［ログ基本設定を編集］および［構成ログを表示］権限が必要です。

構成ログの言語には、作成時のロケールが適用されます。たとえば、英語で作成されたログは、管理者側のロケールには関係なく英語で表示されます。

ログの内容

構成ログには、Studio、Director、およびPowerShellスクリプトから開始された構成の変更および管理アクティビティのログが記録されます。以下の項目に対する作成、編集、削除などの操作が構成ログに記録されます。

- マシン カタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者の役割とスコープ
- ホストのリソースおよび接続
- Studioで構成するCitrixポリシー

ログが記録される管理変更の例には次のものがあります。

- 仮想マシンまたはユーザーのデスクトップの電源管理
- StudioまたはDirectorからユーザーへのメッセージ送信

次の操作はログに記録されません。

- 仮想マシンのプール管理電源オンなどの自動操作。
- グループポリシー管理コンソール（GPMC）でのポリシー操作。これらの操作のログはMicrosoftのツールを使って表示できます。
- レジストリによる変更、データベースの直接的な変更、およびStudio、Director、PowerShell以外での変更。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 展開の初期化後、最初のConfiguration Logging Serviceインスタンスが Configuration Serviceに登録されたときに構成ログが有効になります。このため、構成の初期のアクティビティが記録されない場合があります（ハイパーバイザーの初期化時にデータベーススキーマが取得および適用される場合など）。

構成ログの管理

デフォルトでは、サイトの作成時に作成されたデータベース（サイト構成データベース）に構成ログが記録されます。Citrixは、以下の理由により、構成ログデータベース（および監視データベース）には別の場所を使用することを推奨しています。

- 構成ログデータベースのバックアップ方針が、サイト構成データベースのバックアップ方針と異なる場合があります。
- 構成ログ（およびMonitoring Service）で収集されるデータの量によっては、サイト構成データベース用の領域が不足する場合があります。
- データベースを分散させると、単一ポイント障害の問題が解消されます。

注： 構成ログをサポートしない製品エディションでは、Studioに［ログ］ノードが表示されません。

構成ログおよび必須ログの有効化および無効化

構成ログ機能はデフォルトで有効になっており、必須ログ機能は無効になっています。

1. Studioのナビゲーションペインで **[ログ]** ノードを選択します。
2. ［操作］ペインの **[基本設定]** を選択します。［ログ設定］ダイアログボックスが開き、データベースに関する情報と、構成ログおよび必須ログ機能の有効/無効が表示されます。
3. 望ましい操作を選択します。

    構成ログを有効にするには、 **[有効]** をクリックします。これがデフォルトの設定です。データベースに書き込みができない場合、ログ情報は破棄されますが構成内容は正しく反映されます。

    構成ログを無効にするには、 **[無効]** をクリックします。それまでに記録されたログの内容は、PowerShell SDKで読み取ることができます。

    必須ログ機能を有効にするには、 **[データベースが切断されている場合の構成変更を禁止する]** をクリックします。構成の変更や管理作業は通常ログに記録されるので、構成ログデータベースへの書き込みが可能になるまで、これらの作業はできなくなります。必須ログ機能は、構成ログが有効な場合、つまり **[有効]** が選択されている場合にのみ有効にできます。Configuration Logging Serviceに障害が発生して、しかも高可用性が無効な場合、必須ログが有効になります。このような場合、構成ログデータベースに記録されるようなタスクは実行できなくなります。

    必須ログ機能を無効にするには、 **[データベースが切断されていても構成変更を許可する]** をクリックします。構成ログデータベースにアクセスできない場合でも、管理者は構成の変更やそのほかの管理タスクを実行できます（管理タスクが優先されます）。これがデフォルトの設定です。

構成ログデータベースの場所の変更

注： 必須ログ機能が有効になっている場合、データベースの場所を変更することはできません。データベースの変更時に短時間データベースから切断されるためです。

1. サポートされるバージョンのSQL Serverを使用してデータベースサーバーを作成します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Studioのナビゲーションペインで **[ログ]** ノードを選択します。
3. ［操作］ペインの **[基本設定]** を選択します。
4. ［ログ設定］ダイアログボックスで **[ログデータベースの変更]** をクリックします。
5. ［ログデータベースの変更］ダイアログボックスで、新しいデータベースサーバーが入っているサーバーの場所を指定しま す。有効な書式については、「データベース」の記事を参照してください。
6. Studioで自動的にデータベースを作成する場合は、 **[OK]** をクリックします。確認のメッセージが表示され、 **[OK]** をクリックするとデータベースが自動的に作成されます。現在のStudioユーザーの資格情報を使ってデータベースへのアクセスが試行されます。アクセスに失敗すると、データベースにアクセスするための資格情報を入力する画面が開きます。アクセスに成功すると、データベーススキーマがデータベースにアップロードされます（資格情報はデータベース作成時のみ保持されます）。
7. データベースを手動で作成する場合は、 **[データベーススクリプトの生成]** をクリックします。生成されるスクリプトにはデータベースを手動で作成するためのコマンドが記述されます。スキーマをアップロードする前に、データベースが空であること、および1人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

変更前のデータベース内の構成ログデータは変更後のデータベースにインポートされません。構成ログデータベースの場所を変更する場合、変更前のデータベースの内容は集約されなくなります。変更後の構成ログデータベースの最初にデータベースの変更を示すログが記録されますが、変更前のデータベースの場所は記録されません。

構成ログの内容の表示

管理者が構成の変更などの管理アクティビティを開始すると、StudioやDirectorによって作成された高レベル操作がStudioの中央ペインの上部に表示されます。高レベル操作により1つまたは複数のサービスおよびSDKの呼び出しが実行されます。これは、低レベル操作です。中央ペインの上部で高レベル操作を選択すると、中央ペインの下部に低レベル操作が表示されます。

操作が完了する前に失敗すると、たとえば開始レコードに対応する停止レコードがないなど、データベースでログ操作が完結しない場合があります。このような場合、情報不足であることがログに示されます。時間の範囲を指定してログを表示する場合、未完結のログが表示される場合があります。たとえば、直近5日間のログを表示するときにその5日間に開始時間のみが含まれ、終了時間が含まれていない場合も、その操作のログが表示されます。

PowerShellコマンドレットを呼び出すスクリプトを使う場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログにより代わりの高レベルの操作が作成されます。

構成ログの内容を表示するには、Studioのナビゲーションペインで **[ログ]** ノードを選択します。デフォルトでは、中央ペインにログコンテンツが時系列順に（最新のエントリが最初に）表示されます。

表示条件	表示条件の指定方法
特定の文字列で検索	中央ペイン上部にある［検索］ボックスに文字列を入力します。入力した文字列を含んでいるエントリのみが表示されます。通常のログ表示に戻すには、［検索］ボックスの文字列をクリアします。
列見出し	列見出しをクリックして、表示をその列のデータで並べ替えます。
日範囲	中央ペインの上部で［検索］ボックスの横にあるドロップダウンの一覧から期間を選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

レポートの生成

構成ログデータをCSVおよびHTML形式のレポートとして書き出すことができます。

- CSV形式のレポートには、指定した期間のすべてのログデータが書き込まれます。データベースの階層データが単一のCSV
テーブルとして出力されます。データの特定の要素に基づいて並べ替えられたものではありません。書式も適用されず、読
み取りやすさについても考慮されていません。レポートファイル（MyReport）には、汎用的な書式でデータが書き出され
ます。CSVファイルはデータのアーカイブ化や、レポート機能またはMicrosoft Excelなどデータ操作ツールのデータソース
として使用されます。
- HTML形式のレポートには、指定した期間のログデータが判読可能な形式で書き込まれます。変更内容の確認が容易な、構
造的でナビゲーション可能なレポートです。HTMLレポートでは、概要（Summary）および詳細（Details）の2つのファイ
ルが生成されます。概要レポートには、各操作の実行日時、操作主、および操作結果など、より高レベルな情報が一覧で表
示されます。各操作項目の横にある［詳細］リンクをクリックすると詳細ファイルが開き、より低いレベルの操作に関す
る情報を参照できます。

構成ログレポートを生成するには、Studioのナビゲーションペインで**[ログ]** ノードを選択し、［操作］ペインの **[カスタムレポートの作成]** を選択します。

- レポートの日付の範囲を選択します。
- レポート形式として、［CSVファイル］、［HTML］、または［両方］を選択します。
- レポートを保存する場所を参照します。

構成ログの内容の削除

構成ログを削除するには、特定の委任管理権限およびSQL Serverデータベース権限が必要です。

- **委任管理** - 展開構成を読み取ることができる委任管理の役割が必要です。組み込みのすべての管理権限を実行できる管理者
には、この権限があります。カスタムの役割では、［そのほかの権限］カテゴリで［読み取り専用］または［管理］権限を
選択する必要があります。
構成ログデータを削除する前にバックアップを作成するには、［ログ］カテゴリで［読み取り専用］または［管理］権限
を選択する必要もあります。

- **SQL Serverデータベース** — データベースからレコードを削除するための権限を持つSQL Serverのログインアカウントが必
要です。次のいずれかの方法を使用します。
  - データベースに対するすべての権限を持つsysadminサーバーロールを持つSQL Serverデータベースログインを使用しま
す。また、serveradminまたはsetupadminサーバーロールでも削除操作を実行できます。
  - 高度なセキュリティが必要な環境では、データベースからレコードを削除する権限を持つデータベースユーザーにマッ
プされた非sysadminデータベースログインを使用します。
    1. SQL Server Management Studioで、sysadmin以外のサーバーロールを持つSQL Serverログインを作成します。
    2. 作成したログインをデータベースのユーザーにマップします。SQL Serverにより、ログインと同じ名前のユーザーが
データベースに作成されます。
    3. データベースロールのメンバーシップとして、このデータベースユーザーにConfigurationLoggingSchema_ROLEまた
はdb_ownerのロールを指定します。

  詳しくは、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには、以下の手順に従います。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Studioのナビゲーションペインで **[ログ]** ノードを選択します。
2. ［操作］ペインの **[ログの削除]** を選択します。
3. 削除する前にログのバックアップを作成するかどうかを確認するメッセージが表示されます。バックアップを作成する場合は、バックアップを保存する場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログを削除すると、その削除操作が最初のエントリとしてログに記録されます。このエントリには、いつだれがログを削除したのかが記述されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

イベントログ

Dec 05, 2017

次の記事には、XenAppおよびXenDesktopサービスによって記録できるイベントの一覧と説明が記載されています。

この情報は包括的ではありません。個別の特集記事で、追加のイベント情報を確認してください。

- Citrix Broker Serviceイベント
- Citrix FMA Service SDKイベント
- Citrix Configuration Serviceイベント
- Citrix Delegated Administration Serviceイベント

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Director

Dec 05, 2017

ここでは次のことについて説明します。

Directorについて

Directorの展開と構成

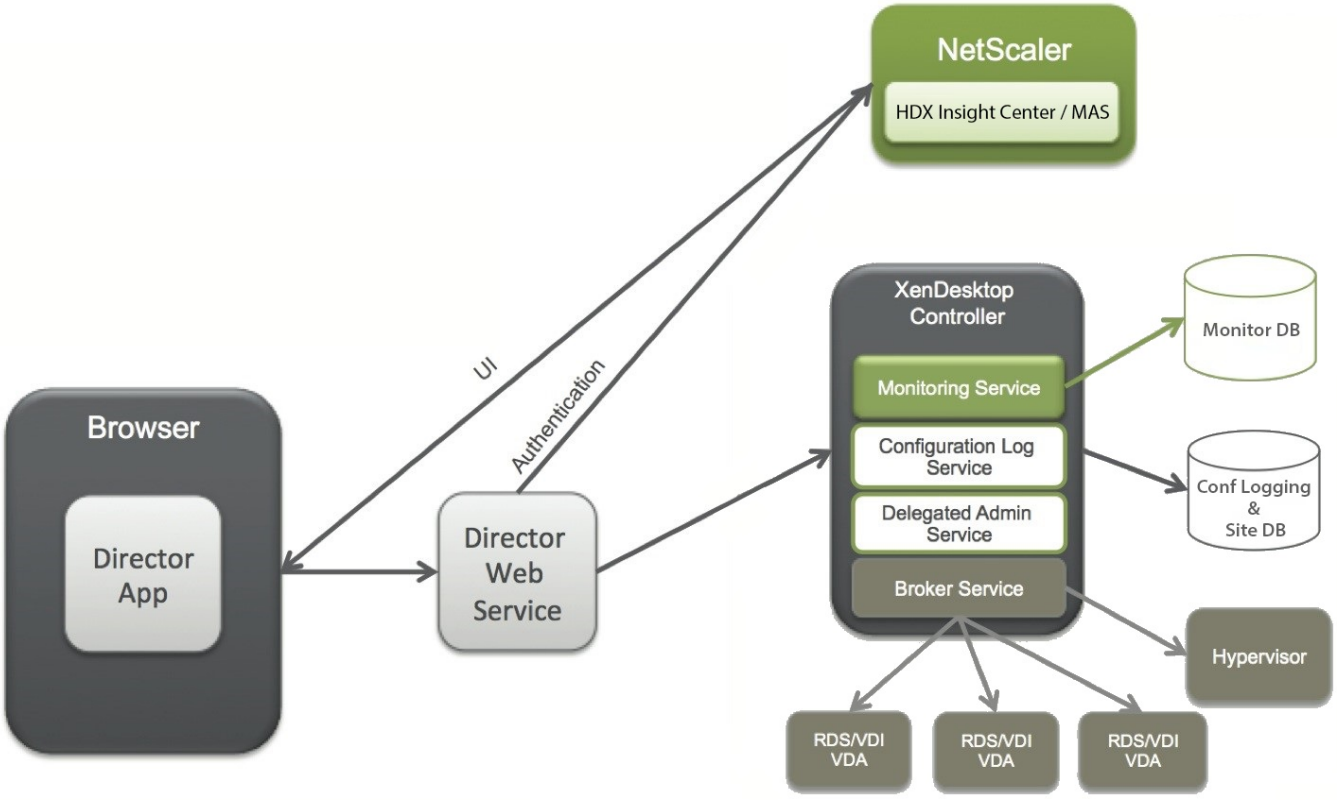
Directorのインストール

XenApp 6.5用のDirectorのインストール

Directorへのログオン

Directorでの統合Windows認証の使用

Directorは、XenAppとXenDesktopの監視およびトラブルシューティングのためのコンソールです。



Directorでは、以下の情報にアクセスできます。

- Broker Agentからのリアルタイムデータ。Analytics、Performance Manager、およびNetwork Inspectorの機能が統合されたコンソールを使用します。
  - Analyticsには、ヘルスおよびキャパシティのチェック機能と、NetScaler Insight CenterまたはNetScaler MASによる履歴傾向とネットワーク解析機能が含まれており、XenApp/XenDesktop環境のネットワークによるボトルネックを検出て

© 1999-2017 Citrix Systems, Inc. All rights reserved.

きます。
- 監視データベースに格納される履歴データ。構成ログデータベースへのアクセスで使用されます。
- NetScaler GatewayからのICAデータ。NetScaler Insight CenterまたはNetScaler MASが使用されます。
  - XenApp/XenDesktop環境の仮想アプリケーションやデスクトップを使用するエンドユーザーのユーザーエクスペリエンスを視覚化できます。
  - ネットワークデータをアプリケーションデータやリアルタイム測定値に関連付けて効率的にトラブルシューティングを施せます。
  - XenDesktop 7 Directorの監視ツールに統合されています。
- Personal vDiskデータ。ディスク割り当てのランタイム監視とヘルプデスク管理者によるPersonal vDiskのリセットが可能になります。
  - コマンドラインツールCtxPvdDiag.exeを使用すると、ユーザーのログ情報が単一ファイルに収集され、それをトラブルシューティングに役立てることができます。

Directorでは、XenApp/XenDesktopサイトのリアルタイムおよび履歴ヘルス監視を提供するトラブルシューティングダッシュボードが使用されます。この機能により、リアルタイムで問題を確認して、エンドユーザーがどのような問題に直面しているのかを判断できるようになります。

Delivery Controller（DC）、VDA、その他の依存するコンポーネントについてのDirectorの機能の互換性について詳しくは、「機能互換性マトリックス」を参照してください。

インターフェイスのビュー

Directorでは、管理者ごとに 異なる インターフェイス（ビュー）が表示されます。Citrix管理者の権限 により、表示される内容と実行できるコマンドが異なります。

たとえば、ヘルプ デスク管理者にはヘルプデスクタスク用のインターフェイスが表示されます。ヘルプデスク管理者 は、問題を報告しているユーザーをDirectorで検索し、アプリケーションやプロセスの状態など、そのユーザーに関する アクティビティを 表示できます。ヘルプデスク管理者は 応答しないアプリケーションやプロセスを終了したり、ユーザーのマシン上の操作をシャドウしたり、マシンを再起動したり、ユーザー プロファイルを再設定したりして問題を解決できます。

これに対して、すべての管理タスクの実行権限を持つ管理者はサイト全体を表示および管理でき、複数のユーザーやマシンに対してコマンドを実行できます。Dashboardには、セッションの状態、ユーザーのログオン、およびサイトインフラストラクチャなど、展開の主な要素に関する概要が表示されます。情報は1分ごとに更新されます。問題が発生すると、発生した問題の数や種類に関する詳細が自動的に表示されます。

Directorは、Delivery Controller上のWebサイトとしてデフォルトでインストールされます。必須要件およびそのほかの詳細については、このリリースのドキュメントの「システム要件」を参照してください。

このリリースのCitrix Directorは、XenApp 6.5以前の環境またはXenDesktop 7以前の環境と互換性がありません。

Directorで複数のサイトを監視する場合は、Controller、Director、およびそのほかのコアコンポーネントが動作すべてのサーバーのシステムクロックが同期している必要があります。システムクロックが同期していない場合、Directorにサイトの情報が正しく表示されないことがあります。

ヒント：XenApp 6.5ファームと、XenApp 7.5またはXenDesktop 7.xサイトの両方を監視する場合は、XenApp 6.5ファームを監視するためのDirectorコンソールとは別のサーバー上に新しいバージョンのDirectorをインストールすることをお勧めします。

重要：ユーザー名とパスワードがプレーンテキストで送信されないように、Director接続ではHTTPではなくHTTPSでの接続

© 1999-2017 Citrix Systems, Inc. All rights reserved.

のみを許可することを強く推奨します。特定のツールを使用すると、HTTP（非暗号化）ネットワークパケット内のプレーンテキストのユーザー名やパスワードを読み取ることができるため、ユーザーにとってセキュリティ上のリスクとなる場合があります。

権限を構成するには

Directorにログオンする管理者は、Active Directoryドメインユーザーで、以下の権限を持っている必要があります。

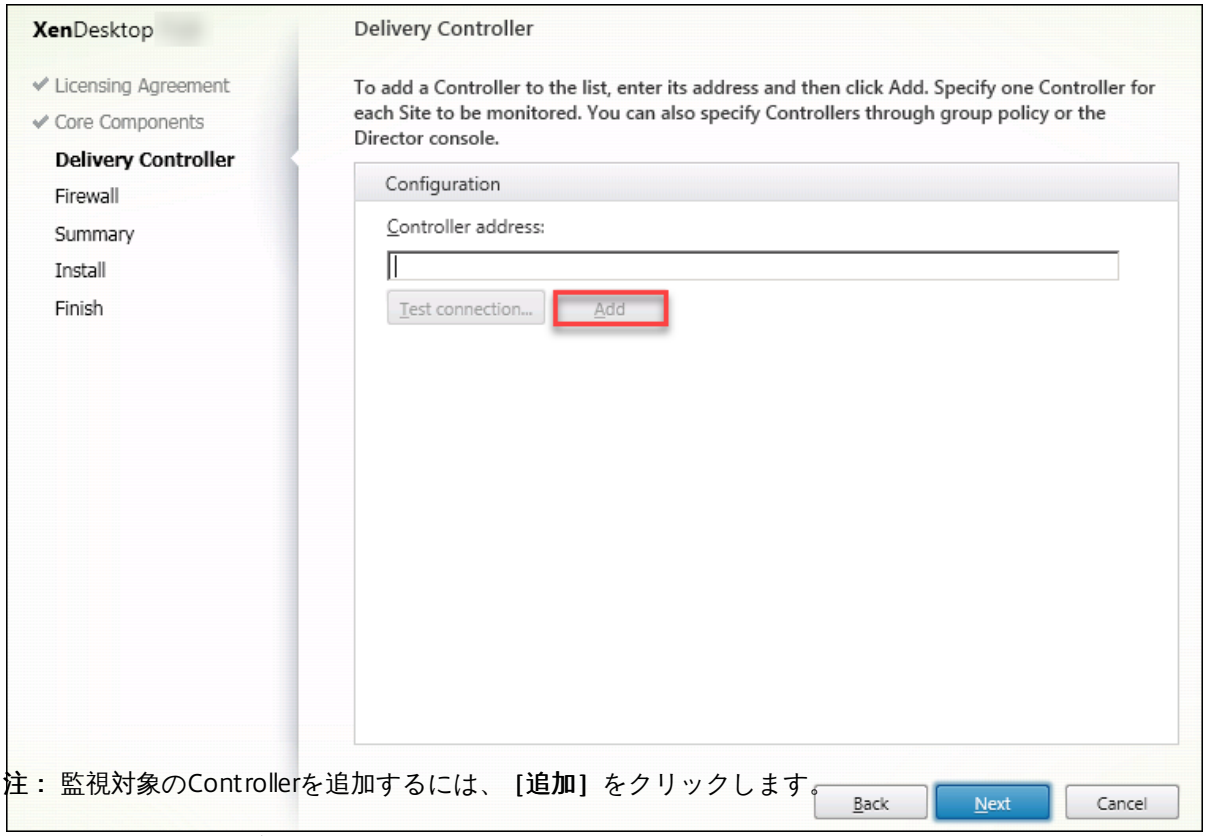
- 検索するすべてのActive Directoryフォレストを読み取る権限（「詳細構成」を参照）
- 構成済みの委任管理者の役割（「委任管理者とDirector」を参照）。
- ユーザーをシャドウするには、WindowsリモートアシスタンスのMicrosoftグループポリシーを使って管理者を構成する必要があります。また、次の点に注意してください。
  - VDAをインストールするすべてのユーザーデバイス上で、Windowsリモートアシスタンス機能が有効である必要があります。この機能は、デフォルトで有効になっています。
  - Directorをインストールするサーバーに、Windowsリモートアシスタンス機能がインストールされている必要があります。この機能は、デフォルトでインストールされています。ただし、デフォルトでは無効になっています。Directorを使ってエンドユーザーを支援する場合、この機能を有効にする必要はありません。セキュリティ上の理由から、この機能を無効にしておくことをお勧めします。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、適切なMicrosoftグループポリシー設定を使用して管理者に必要な権限を付与します。詳しくは、「CTX127388： Desktop Directorに対してリモートアシスタンスを有効にする方法」を参照してください。
- XenDesktop 7よりも前のバージョンのVDAがインストールされたユーザーデバイスについては、追加の構成が必要です。「XenDesktop 7よりも前のVDAに対する権限の構成」を参照してください。

DirectorはXenAppおよびDesktopに対応した全製品ISOインストーラーを使ってインストールします。このインストーラーは、前提条件をチェックし、不足しているコンポーネントをインストールして、DirectorのWebサイトをセットアップし、基本的な構成を行います。ISOインストーラーによるデフォルトの構成のままでも、一般的な展開を管理できます。インストール時にDirectorを含めなかった場合は、ISOインストーラーを再度実行してDirectorをインストールします。追加のコンポーネントをインストールするには、ISOインストーラーを再度実行して必要なコンポーネントを選択します。ISOインストーラーの使用について詳しくは、インストールに関するドキュメントで「コアコンポーネントのインストール」を参照してください。個々のMSIファイルではなく、全製品ISOインストーラーを実行して各コンポーネントをインストールすることをお勧めします。

Controller上にDirectorをインストールすると、Directorはlocalhostをサーバーアドレスとして自動的に構成され、デフォルトでローカルのControllerと通信します。

Controllerからリモートにある専用サーバー上にDirectorをインストールする場合には、Controllerの完全修飾ドメイン名（FQDN）またはIPアドレスを指定する必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



注：監視対象のControllerを追加するには、［**追加**］をクリックします。

Directorは、ここで指定したアドレスのControllerと通信します。監視する各サイトについてControllerのアドレスを1つずつ指定します。各サイトにあるほかのすべてのControllerは自動的に検出され、指定したControllerにエラーが発生した場合はほかのControllerにフォールバックされます。

注：Directorは、Controller間で負荷分散を行いません。

WebブラウザーとWebサーバー間の通信を保護するため、DirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。この手順については、Microsoft IISのドキュメントを参照してください。Director側では、TLSを有効にするために何らかの構成を行う必要はありません。

XenApp 6.5に対してDirectorをインストールするには、次の手順に従います。通常、DirectorはXenApp Controllerとは別のコンピューター上にインストールします。

1. XenAppのインストールメディアから、Directorをインストールします。 XenDesktop用のDirectorが既にインストールされている場合は、この手順をスキップし、次の手順に進みます。
2. 「詳細構成」の「**サイトをDirectorに追加するには**」の説明に従って、各Directorサーバー上のIIS管理コンソールで［アプリケーションの設定］のXenAppサーバーアドレスの一覧を更新します。
   XenAppサイトごとに1つのControllerのサーバーアドレスを指定します。そうすると、XenAppサイトのその他のControllerは自動的にフェールオーバー用に使用されます。Directorは、Controller間で負荷分散を行いません。
   重要： XenAppアドレスはService.AutoDiscoveryAddressesXAに指定し、デフォルト設定のService.AutoDiscoveryAddressesに指定しないでください。
3. Director WMIプロバイダーのインストーラーはDVDの**Support\DirectorWMIProvider**フォルダーに格納されています。適切なすべてのXenAppサーバー（Controllerおよびセッションを実行するワーカー）上にこれをインストールします。**winrm**が構成されていない場合は、**winrm qc**コマンドを実行します。
4. 「権限の構成」で説明されているように、各XenAppワーカーサーバーがWinRMクエリを受け入れるように構成します。
5. DirectorとXenApp間の通信で使用されるポート2513に対するファイアウォール例外を構成します。
6. WebブラウザーとWebサーバー間の通信を保護するため、DirectorをホストするIIS WebサイトでTLSを実装することをお

© 1999-2017 Citrix Systems, Inc. All rights reserved.

勧めします。
この手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorを構成する必要はありません。

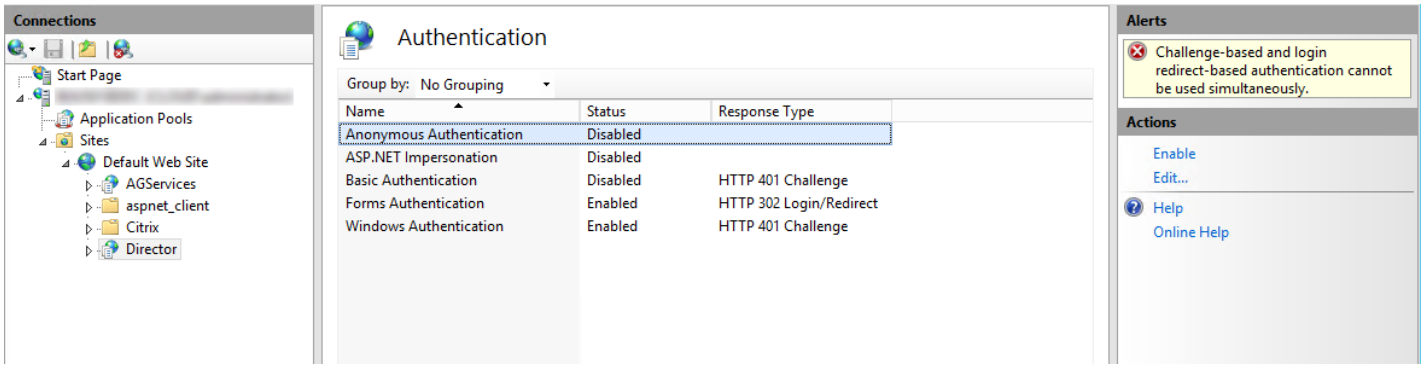
注：Directorがファーム内のすべてのXenAppワーカーを見つけることができるようにするには、ファームによって使用されるDNSサーバー上にXenAppサーバーがあるサブネットにリバースDNSゾーンを追加する必要があります。

Directorにログオンするには、Webブラウザーでhttps:///DirectorまたはHttp:///Directorにアクセスします。

複数サイト環境でいずれかのサイトがダウンしている場合、Directorへのログオンに時間がかかる場合があります。これは、ダウンしているサイトへの接続が試行されるためです。

統合Windows認証を使うと、ドメイン参加のユーザーは、Directorのログオンページに資格情報を再度入力しなくても、Directorに直接アクセスできます。Directorでの統合Windows認証の使用には、以下の前提条件があります。

- DirectorをホストしているIIS Webサイトで統合Windows認証を有効化します。Directorをインストールするときには、匿名認証とフォーム認証が有効化されています。Directorで統合Windows認証を使用するには、匿名認証を無効化し、Windows認証を有効化します。フォーム認証は、非ドメインユーザーを認証するために、有効化したままにしておく必要があります。
  1. IISマネージャーを起動します。
  2. **[サイト]** > **[既定のWebサイトのホーム]** > **[Director]** に移動します。
  3. **[認証]** を選択します。
  4. **[匿名認証]** を右クリックし、 **[無効化]** を選択します。
  5. **[Windows認証]** を右クリックし、 **[有効化]** を選択します。



- DirectorマシンのActive Directory委任アクセス許可を構成します。この作業は、DirectorとDelivery Controllerが異なるマシンにインストールされている場合のみ必要です。
  1. Active Directoryマシンで、Active Directory管理コンソールを開きます。
  2. Active Directory管理コンソールで、 **[ドメイン名]** > **[コンピューター]** の順に移動し、Directorマシンを選択します。
  3. セッションを右クリックして **[プロパティ]** を選択します。
  4. [プロパティ] で **[委任]** タブを選択します。
  5. **[任意のサービスへの委任でこのコンピューターを信頼する（Kerberosのみ）]** オプションを選択します。
- Directorへのアクセスに使用するブラウザーは、統合Windows認証をサポートしている必要があります。このため、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

FirefoxおよびChromeでは、さらに構成作業が必要になる場合があります。詳しくは、ブラウザーのドキュメントを参照してください。

- Monitoring Serviceでは、Directorのシステム要件に記載されているMicrosoft.NET Framework 4.5.1以降のバージョンが実行されている必要があります。詳しくは、「必要なシステム」を参照してください。

ユーザーがDirectorをログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。このログオンページから、認証の種類を**[自動ログオン]**または**[ユーザーの資格情報]**に設定できます。

Google Analyticsによる使用状況データ収集通知

Directorがインストールされると、DirectorサービスはGoogle Analyticsを使って使用状況に関するデータを収集します。［傾向］ページとそのタブの使用状況に関する統計と情報が収集されます。Directorをインストールすると、データ収集はデフォルトで有効になります。

Google Analyticsによるデータ収集を解除するには、Directorがインストールされているマシンのレジストリキー、HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstallを、「Citrix Insight Services」の「インストールとアップグレード分析」の説明に従って編集します。

メモ：HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstallレジストリキーはGoogle Analyticsと同様に、Citrix Insight Servicesによる使用状況に関するデータ収集も制御します。キーの値が変更されると、両方のサービスで収集は影響を受けます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

詳細構成:

Dec 05, 2017

ここでは次のことについて説明します。

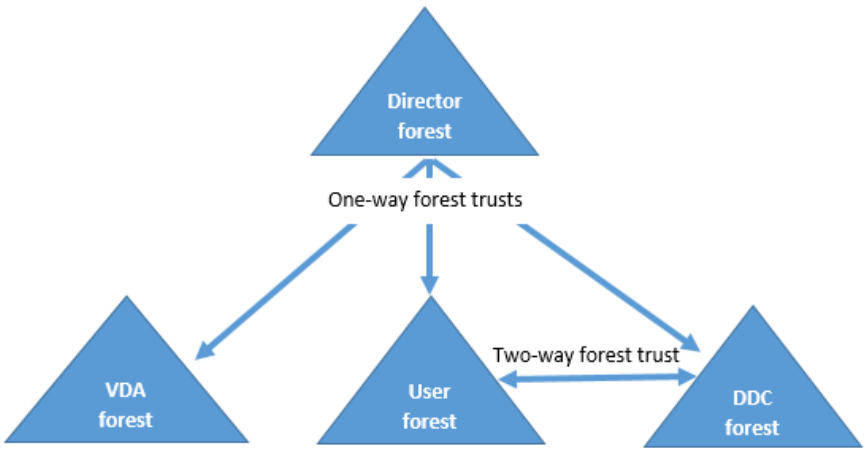
マルチフォレスト環境で動作するDirectorの推奨構成

Directorへのサイトの追加

アクティビティマネージャーで実行中のアプリケーションを非表示にする

Directorは、ユーザー、Domain Delivery Controllers（DDC）、VDA、およびDirectorが異なるフォレストに存在するフォレスト構成に広がるマルチフォレスト環境をサポートできます。このためには、フォレストと構成設定の間の信頼関係を適切にセットアップする必要があります。

推奨構成では、全ドメイン認証を使用してフォレスト間の送受信フォレスト信頼関係を作成する必要があります。



Directorからの信頼関係があると、管理者は異なるフォレストに存在するユーザーセッション、VDA、およびドメインコントローラーの問題をトラブルシューティングできます。

マルチフォレストをサポートするDirectorに必要な詳細構成は、インターネットインフォメーションサービス（IIS）マネージャーで定義する設定で制御します。
重要：IISの設定を変更すると、Directorサービスが自動的に再起動してユーザーをログオフします。
IISを使って詳細設定を構成するには、次の手順に従います。

1. インターネット インフォメーションサービス（IIS）マネージャーコンソールを開きます。
2. ［Default Web Site］ノードを開き、 ［Director］Webサイトを選択します。
3. **［アプリケーションの設定］** をダブルクリックします。
4. 編集する設定をダブルクリックします。

Platinumライセンスはデフォルトで90日間データを保持します。 構成について詳しくは、 「データの粒度と保持」を参照してください。

DirectorはActive Directoryを使ってユーザーを検索し、ユーザーおよびマシンの追加情報を照会します。Directorのデフォル

© 1999-2017 Citrix Systems, Inc. All rights reserved.

トでは、以下のドメインまたはフォレストが検索されます。

- 管理者のアカウント属しているドメインやフォレスト。
- DirectorのWebサーバーが属しているドメインやフォレスト（管理者が属しているものと異なる場合）。

Directorでは、Active Directoryグローバルカタログによるフォレストレベルでの検索が試行されます。管理者にフォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ほかのActive Directoryドメインまたはフォレストからのデータを検索または照会するには、対象のドメインまたはフォレストを明示的に設定する必要があります。次の設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性userおよびserverは、それぞれDirectorユーザー（つまり管理者）のドメインおよびDirectorサーバーのドメインを表しています。

ほかのドメインまたはフォレストからのデータを検索するには、次のようにドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),<ドメイン1>,<ドメイン2>
```

リストに追加した各ドメインについて、Directorによりフォレストレベルの検索が試行されます。管理者にフォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

注：マルチフォレスト環境では、Directorはドメインローカルグループを使用してXenDesktopデリバリーグループに割り当てられた他のフォレストからのユーザーのセッションの詳細を表示しません。

Directorがインストール済みの場合は、複数のサイトを監視できるように構成できます。これを行うには、各Directorサーバー上でIIS管理コンソールを使って［アプリケーションの設定］のサーバーアドレスの一覧を更新します。

各サイトのControllerのアドレスを次の設定に追加します。

Service.AutoDiscoveryAddresses = SiteAController,SiteBController

ここで*SiteAController*および*SiteBController*は、2つの異なるサイトのDelivery Controllerのアドレスです。

XenApp 6.5の場合は、各XenAppファームのControllerのアドレスを次の設定に追加します。

Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController

ここで*FarmAController*および*FarmBController*は、2つの異なるファームのXenApp Controllerのアドレスです。

XenApp 6.5サイトでは、次の方法でXenAppファームからControllerを追加することもできます。

DirectorConfig.exe / xenapp FarmControllerName

Directorのアクティビティマネージャーのデフォルトでは、そのユーザーのセッションで実行されているすべてのアプリケーションが一覧表示されます。この情報を表示するには、Directorのアクティビティマネージャー機能へのアクセス権限が必要です。この権限を持つ管理者の役割は、すべての管理権限を実行できる管理者、デリバリーグループ管理者、およびヘルプデ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

スク管理者です。

ユーザーのプライバシーと、ユーザーが使用しているアプリケーションを保護するために、［アプリケーション］タブでア
リケーションの一覧を非表示にできます。

警告：レジストリを誤って編集すると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. VDAで、レジストリキーHKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayedを変更します。デフォルトでは1に設定されています。値を0に変更すると、アクティビティマネージャーに情報が表示されなくなります。
2. Directorがインストールされたサーバー上で、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトの値はtrueで、これにより［アプリケーション］タブに実行中のアプリケーションの一覧が表示されます。値を「false」に変更すると、アプリケーションの一覧が表示されなくなります。このオプションは、VDAではなくDirectorのアクティビティマネージャーにのみ適用されます。
   次の設定で値を変更します。
   UI.TaskManager.EnableApplications = false

重要：実行中のアプリケーションの表示を無効にするには、これらの両方の値を変更してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

展開環境の監視

Feb 01, 2018

ここでは次のことについて説明します。

サイトの監視

セッションの監視

トラブルシューティングのためのデータのフィルター処理

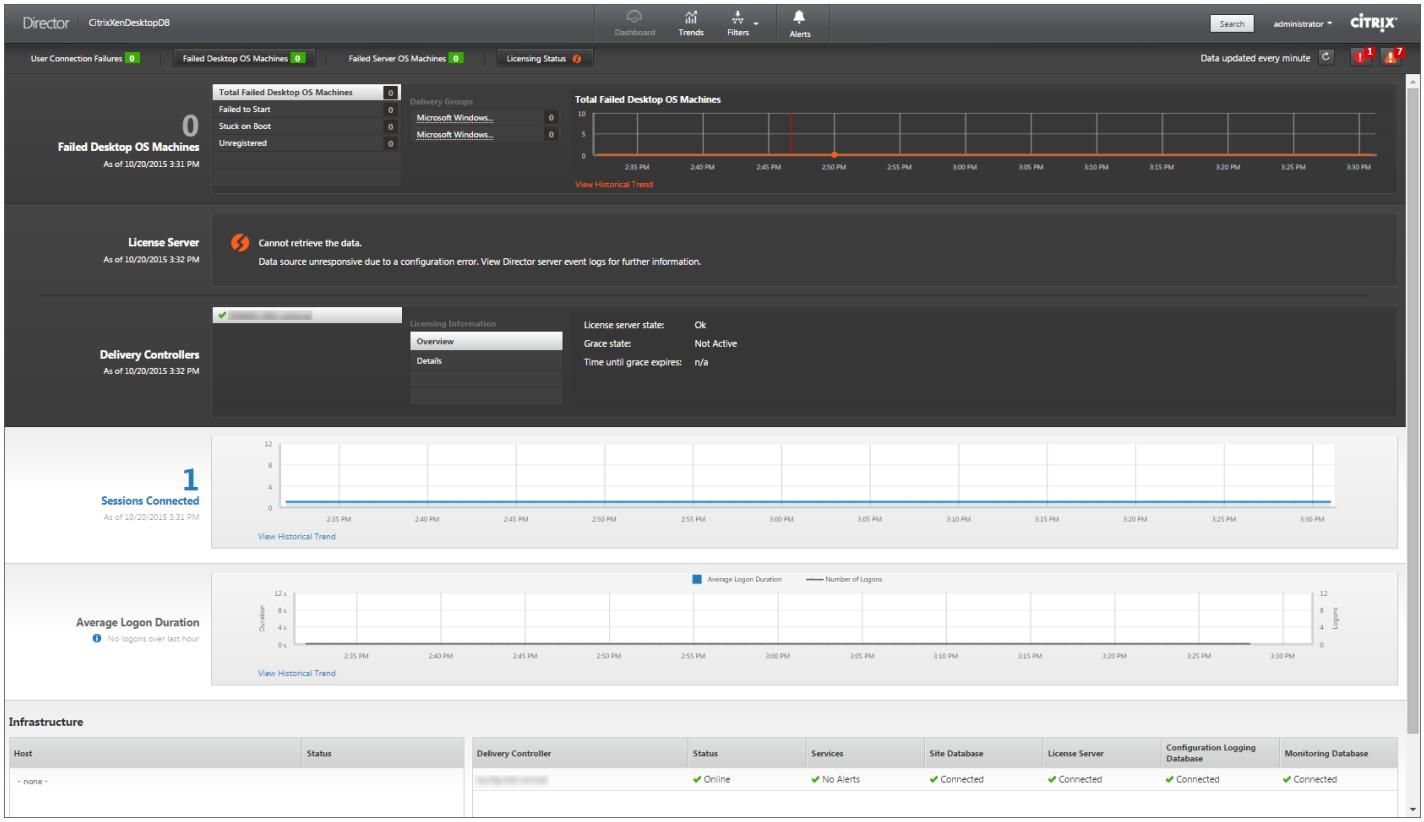
サイト全体の履歴傾向の監視

Hotfixの監視

ユーザーマシンの電源状態の制御

マシンへの接続の無効化

すべての管理権限を実行できる管理者としてDirector起動すると、サイトのヘルス状態や使用状況を監視するための[ダッシュボード]が開きます。



直近の60分間にエラーが発生していない場合、各パネルは閉じています。 エラーが発生している場合はそのエラーを示すパネルが自動的に開きます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注：組織のライセンスおよび管理者権限によって、表示されるオプションや機能は異なります。

パネル	説明
ユーザー接続エラー	過去60分間の接続エラーが表示されます。エラー総数の横にあるカテゴリをクリックして、各種のエラーの測定値を確認します。隣接する表には、発生したエラー数がデリバリーグループごとに表示されます。接続エラーには、アプリケーション制限に達したことによって発生したエラーも含まれます。アプリケーション制限について詳しくは、「アプリケーションの管理」を参照してください。
失敗したデスクトップOSマシンまたは失敗したサーバーOSマシン	過去60分間の総エラー数がデリバリーグループごとに表示されます。エラーの種類として、起動の失敗、起動時のスタック、および未登録があります。サーバーOSマシンの場合は、最大負荷に達しているマシンも含まれます。
ライセンスの状態	• ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートメッセージとそのアラートを解決するための操作が表示されます。 ライセンスサーバーのバージョン11.12.1以降が必要です。 • Delivery Controllerアラートには、Controllerから送信されたライセンス状態の詳細が表示されます。 XenApp 7.6またはXenDesktop 7.6以降のControllerが必要です。 アラートのしきい値は、Studioで設定できます。
接続セッション	すべてのデリバリーグループでの過去60分間の接続セッションが表示されます。
平均ログオン処理時間	過去60分間のログオン処理に関するデータが表示されます。左側にある大きなサイズの数値は、全体的な平均ログオン処理時間を示します。 この平均には、XenDesktop 7.0より前のバージョンのVDAへのログオンデータは含まれません。 詳しくは、「ユーザーログオンの問題の診断」を参照してください。
インフラストラクチャ	サイトのインフラストラクチャー覧 - ホストおよびコントローラー。 XenServerまたはVMwareのインフラストラクチャで、パフォーマンスアラートを表示できます。 たとえば、XenCenterでは、サーバーまたは仮想サーバーのCPU、ネットワークI/O、またはディスクI/Oの使用量が特定のしきい値を超えた場合にパフォーマンスアラートが発せられるように構成できます。アラートの送信間隔はデフォルトで60分ですが、必要に応じて変更できます。詳しくは、『Citrix XenServer 7.0管理者ガイド』でXenCenterのパフォーマンスアラートについて参照してください。

注： ホスト上でサポートされてない種類の測定値のアイコンは表示されません。たとえば、System Center Virtual Machine Manager（SCVMM）ホストを使用する環境では、ヘルス情報が表示されません。
以下に示すオプションを使って問題のトラブルシューティングを行います。

- ユーザーマシン電源の制御
- マシンへの接続の無効化

© 1999-2017 Citrix Systems, Inc. All rights reserved.

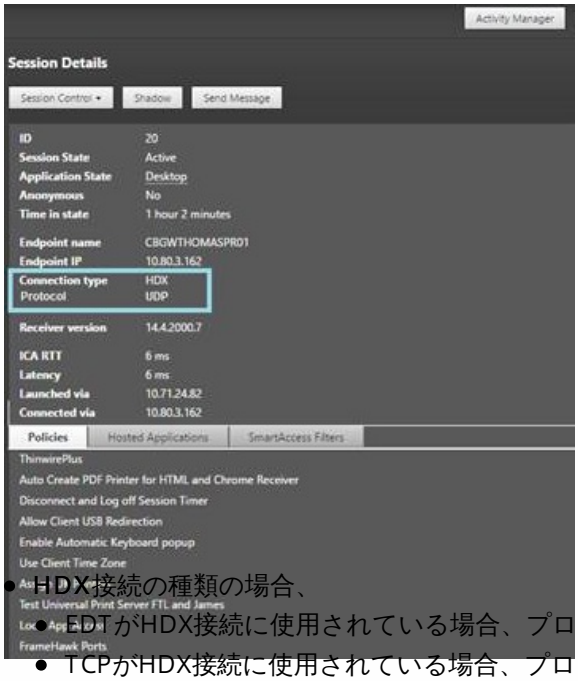
セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、サーバーとユーザーデバイス間の通信が切断されます。

アクション	説明
ユーザーが接続しているマシンまたはセッションを表示する	［アクティビティマネージャー］および［ユーザーの詳細］ビューで、ユーザーが接続しているマシンまたはセッションと、そのユーザーがアクセスしているすべてマシンおよびセッションの一覧を表示します。セッションの一覧にアクセスするには、そのユーザーのビューのタイトルバーにあるセッション切り替え用のアイコンをクリックします。詳しくは、「セッションの復元」を参照してください。
すべてのデリバリーグループで接続されたセッションの総数を表示する	［ダッシュボード］の［接続セッション］ペインには、すべてのデリバリーグループでの過去60分間の接続セッション数が表示されます。その合計数をクリックすると、［フィルター］ビューが開きます。ここでは、デリバリーグループごとのセッションデータや、すべてのデリバリーグループでの特定期間での使用量を視覚的に確認できます。
アイドル状態のセッションを終了する	［セッションフィルター］ビューにすべてのアクティブなセッションの関連データが表示されます。セッションに関連付けられているユーザー、デリバリーグループ、セッション状態、しきい値の時間を超えたアイドル時間に基づいてフィルターします。フィルターされた一覧で、ログオフまたは切断するセッションを選択します。詳しくは、「MSMQのトラブルシューティング」を参照してください。
長期間のデータを表示する	［傾向］ビューの［セッション］タブでは、長期間（つまり直近の60分よりも前）の接続セッションおよび切断セッションに関するデータを詳細に確認できます。この情報を表示するには、［履歴傾向の表示］をクリックします。

注：Virtual Delivery Agent 7より前のバージョンのVDA、またはLinux VDAを実行する場合、セッションに関する一部の情報がDirectorに表示されません。代わりに、利用できる情報がないというメッセージが表示されます。

［セッション詳細］パネルで現在のセッションのHDX接続の種類に使用されているトランスポートプロトコルを表示します。この情報はバージョン7.13以降のVDAで起動するセッションで利用できます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **HDX**接続の種類の場合、
  - EDTがHDX接続に使用されている場合、プロトコルは**UDP**と表示されます。
  - TCPがHDX接続に使用されている場合、プロトコルは**TCP**と表示されます。
- **RDP**接続の種類の場合、プロトコルは「**該当なし**」と表示されます。

アダプティブトランスポートが構成されている場合、セッショントランスポートプロトコルは、ネットワーク条件に応じて、EDT（UDP上）とTCPを動的に切り替えます。HDXセッションをEDTで確立できない場合は、TCPプロトコルにフォールバックします。

アダプティブトランスポート構成について詳しくは、「アダプティブトランスポート」を参照してください。

［ダッシュボード］で数値をクリックしたり［フィルター］メニューから事前定義のフィルターを選択すると、［フィルター］ビューが開きます。ここには、選択したマシンまたはエラーの種類に関するデータが表示されます。

事前定義のフィルターはそのままでは編集できませんが、それをカスタムフィルターとして保存してから編集することができます。さらに、すべてのデリバリーグループでのマシン、接続、セッション、アプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. 以下のビューを選択します。
   - **マシン**［デスクトップOSマシン］タブまたは［サーバーOSマシン］タブを選択します。これらのタブには構成されたマシンの数が表示されます。また、［サーバーOSマシン］タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。
   - **Sessions**：［セッション］ビューでセッション数を表示することもできます。 アイドル時間測定を使ってしきい値時間を超えてアイドル状態にあるセッションを特定します。
   - **接続**：直近の60分、24時間、または7日間の接続が表示されます。
   - **アプリケーションインスタンス**このビューでは、Server OSのVDAおよびDesktop OSのVDAの全てのアプリケーションインスタンスのプロパティが表示されます。セッションのアイドル時間測定機能は、Server OSのVDAのアプリケーションインスタンスに利用できます。
2. **［フィルター］**で特定の条件を定義します。
3. 必要に応じて、各ビューで追加のタブを使用してフィルターを実行します。
4. 必要に応じて追加の列を選択して、より詳細な情報を表示します。
5. フィルターに名前を付けて保存します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 複数のDirectorサーバーからフィルターにアクセスするには、これらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーには、Directorサーバーのアカウントを変更する権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスするよう構成されている必要があります。これを行うには、**IISマネージャー**を実行します。**[サイト]** > **[既定のWebサイト]** > **[Director]** > **[アプリケーションの設定]** の順に移動し、**Service.UserSettingsPath**の設定が共有フォルダーのUNCパスを反映するように変更します。
7. 後でフィルターを開くには、［フィルター］メニューでフィルターの種類（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存済みのフィルターを選択します。
8. **［マシン］**ビューまたは**［接続］**ビューでは、一覧でマシンを選択して電源制御操作を実行できます。［セッション］ビューでは、セッション制御を実行したりメッセージを送信したりできます。
9. **［マシン］**ビューおよび**［接続］**ビューで障害が発生したマシンまたは接続の**［エラーの理由］**をクリックすると、障害の詳細な説明と、障害をトラブルシューティングするために推奨される操作が表示されます。障害の理由と、マシンや接続の障害に対する推奨操作は、『Citrix Director 7.12 Failure Reasons Troubleshooting Guide』にあります。
10. **［マシン］**ビューでマシン名のリンクをクリックし、対応する**［マシンの詳細］**ページに移動します。マシンの詳細を表示するこのページでは、電源制御が提供され、CPU、メモリ、ディスクの監視、およびGPUの監視グラフが表示されます。また、**［履歴使用率の表示］**をクリックすると、マシンのリソース使用傾向が表示されます。詳しくは、「マシンのトラブルシューティング」を参照してください。
11. **［アプリケーションインスタンス］**ビューで、しきい値時間を超えた**［アイドル時間］**に基づいてソートまたはフィルターを行います。終了させるアイドル状態のアプリケーションインスタンスを選択します。ログオフまたはアプリケーションインスタンスを切断すると同一セッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
    注： ［アプリケーションインスタンスフィルター］ページと［セッションフィルター］ページのアイドル時間測定が利用できるのは、Director、Delivery Controller、VDAがバージョン7.13以降の場合です。

［傾向］ビューでは、各サイトのセッション、接続エラー、マシン障害、ログオンパフォーマンス、負荷評価、能力管理、マシン使用量、ソース使用、ネットワーク分析についての履歴傾向情報が表示されます。この情報を表示するには、**［傾向］**メニューをクリックします。

ズームインドリルダウン機能により、（グラフ内のデータポイントをクリックして）ある期間について着目し、その傾向に関連する詳細情報を表示させて、傾向チャートを参照できます。これにより、表示中の傾向により誰が、または何が影響を受けているかについてより詳細に把握できます。

各グラフのデフォルトの表示範囲を変更するには、［期間］フィルターを変更して適用します。

履歴傾向情報を必要とする期間を選択します。その期間を参照できるかは、Director環境により異なります。次を参照してください。

- Platinum Editionユーザーは、昨年（365日）までの傾向レポートを利用できます。
- Enterprise Editionユーザーは、先月（31日）までの傾向レポートを利用できます。
- Platinum Edition以外やEnterprise Edition以外のユーザーは、過去7日間の傾向レポート。

注：

- すべてのDirector展開環境で、期間を［先月］（**終わりは今日**）またはそれより短く設定すると、セッション、障害、およびログオンパフォーマンスの傾向情報をグラフやテーブルとして表示できます。期間に、終了日が設定可能な［先月］、または［昨年］を選択すると、傾向情報はグラフとして表示できますが、テーブルとしては表示できません。
- Monitoring Serviceによる傾向情報のクリーンアップ開始までのデフォルト値は、「データの粒度と保持」セクションで確認できます。Platinum Editionでは、クリーンアップが開始されるまでの日数をカスタマイズできます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アクション	説明
セッションの傾向の表示	［セッション］タブから、同時接続セッション数に関するより詳細な情報を表示するデリバリーグループと期間を選択します。
接続エラーの傾向の表示	［エラー］タブで、接続エラー情報を表示する接続、マシンの種類、エラーの種類、デリバリーグループ、および期間を選択します。
マシン障害の傾向の表示	［失敗したデスクトップOSマシン］タブまたは［失敗したサーバーOSマシン］タブで、障害情報を表示するエラーの種類、デリバリーグループ、および期間を選択します。
ログオンパフォーマンスの傾向の表示	［ログオンパフォーマンス］タブで、ログオンパフォーマンス情報（ログオン処理時間およびログオン数）を表示するデリバリーグループ、および期間を選択します。このビューには、仲介処理時間や仮想マシンの起動時間などのログオンフェーズにおける平均時間も表示されます。 このデータはユーザーのログオンに関するものであり、切断セッションへの再接続は含まれません。 グラフの下のテーブルに、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、いずれかの列を基準にレポートを並べ替えることができます。 詳しくは、「ユーザーログオンの問題の診断」を参照してください。
負荷評価の傾向の表示	［負荷評価基準インデックス］タブで、サーバーOSマシン間で分散された負荷に関する情報を表示します。このグラフでは、対象のデリバリーグループ、サーバーOSマシン、および期間を指定できます。
ホストされたアプリケーションの使用量の表示	この機能は、組織のライセンスによっては使用できない場合があります。 ［ホストされたアプリケーションの使用量］タブでデリバリーグループと期間を選択すると、最大同時使用量を示すグラフと、アプリケーションごとの使用量を示す表が表示されます。［アプリケーションごとの使用量］の表では、特定のアプリケーションについての詳細や、そのアプリケーションを使用しているユーザー、および使用していたユーザーの情報を表示できます。
デスクトップOSおよびサーバーOSの使用状況の表示	［傾向］ビューでは、サイト別およびデリバリーグループ別のデスクトップOSの使用状況が表示されます。サイトを選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 ［傾向］ビューでは、サイト別、デリバリーグループ別、およびマシン別のサーバーOSの使用状況も表示されます。サイトを選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンを選択すると、ユーザーごとの使用状況が表示されます。
仮想マシン使用量の確認	［マシン使用量］タブで［デスクトップOSマシン］または［サーバーOSマシン］を選択して、仮想マシンの使用状況をリアルタイムで表示させ、サイトのキャパシティニーズ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	に素早く対処することができます。 デスクトップOSの可用性 - デスクトップOSマシン（VDI）の現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。 サーバーOSの可用性 - サーバーOSマシンの現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。
リソース使用の表示	［リソース使用］タブで［デスクトップOSマシン］または［サーバーOSマシン］を選択して、各VDIマシンのCPUとメモリ使用量、およびIOPSとディスク遅延に関する履歴傾向を取得し、容量の計画に役立てることができます。 この機能の使用には、Delivery ControllerおよびVDAのバージョン7.11以降が必要です。 平均CPU、平均メモリ、平均IOPS、ディスク遅延、および最大同時セッション数を表示するグラフです。マシンにドリルダウンして、CPUを消費している上位10のプロセスに関するデータとチャートを表示できます。デリバリーグループ別および期間別でフィルターできます。過去2時間、24時間、7日間、月、年のCPU、メモリ使用量、最大同時セッション数のグラフを入手できます。平均IOPSとディスク遅延は、過去24時間、月、年のグラフが入手可能です。 **注：** • データを収集して［マシン使用率の履歴］ページの［上位10位のプロセス］テーブルに表示するには、監視ポリシーの［プロセスの監視を有効にします］設定を［許可］に設定する必要があります。このポリシーはデフォルトでは禁止されています。 • デフォルトではすべてのリソース使用データが収集されます。これは、ポリシーの［リソースの監視を有効にします］設定で無効にできます。 グラフの下のテーブルは、マシンごとのリソース使用状況データを示しています。 **注**：平均IOPSは、1日の平均を示します。最大IOPSは、選択した期間のIOPSの平均において最も高いIOPSが算出されます。（IOPSの平均は、選択した期間にVDAで収集されたIOPSの1時間当たりの平均です）。
ネットワーク分析データの表示	**注：** この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。この機能の使用には、Delivery Controllerバージョン7.11以降が必要です。 ［ネットワーク］タブで、ネットワークのユーザー、アプリケーション、およびデスクトップコンテキストビューを表示してネットワーク分析を行います。この機能は、DirectorがNetScaler Insight CenterまたはNetScaler MASでHDX Insightレポートを使用してICAトラフィックを詳細に分析できます。 詳しくは、「ネットワーク分析機能の構成」を参照してください。
アプリケーション障害の表示	［アプリケーション障害］タブで、 VDA上の公開アプリケーションに関連した障害が表示されます。 **注**：この機能の使用には、Delivery ControllerおよびVDAのバージョン7.15以降が必要です。Windows Vista以降が動作するデスクトップOSのVDA、およびWindows Server 2008以降が動作するサーバーOSのVDAがサポートされます。 詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーション障害履歴の監視」を参照してください。 デフォルトでは、サーバーOSのVDAからのアプリケーション障害のみが表示されます。監視ポリシーを使って、アプリケーション障害の監視の設定ができます。詳しくは、「監視のポリシー設定」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

カスタマイズされたレポートの作成	［カスタムレポート］タブには、監視データベースのリアルタイムデータおよび履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスがあります。 **注：**この機能の使用には、Delivery Controllerバージョン7.12以降が必要です。 以前に保存されたカスタムレポートクエリの一覧から［**実行**］をクリックしてCSV形式のレポートをエクスポートし、［**ODataのコピー**］をクリックして対応するODataクエリをコピーして共有し、［**編集**］をクリックしてクエリを編集します。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいて、新しいカスタムレポートクエリを作成できます。フィールド（たとえばマシン、デリバリーグループ、または期間）に基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。 コピーしたODataクエリに基づいて、新しいカスタムレポートクエリを作成できます。それには、OData Queryオプションを選択し、コピーしたODataクエリを貼り付けます。結果として得られたクエリを、後で実行するために保存できます。 **注：**ODataクエリを使用して生成したレポートのプレビューとエクスポートでは、列名はローカライズされず、英語で表示されます。

また、重要なイベントやアクションの発生は、フラグアイコンで示されます。フラグをクリックすると、発生したイベントたはアクションが表示されます。

注：

- XenDesktop 7よりも前のバージョンのVDAについてはHDX接続のログオンデータが収集されません。以前のバージョンのVDAについては、チャートデータが0として表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データがクリーンアップされるまでDirectorの［傾向］フィルターで選択できます。削除されたデリバリーグループを選択すると、保存まで使用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- デリバリーグループ間でアクティブなセッションがあるマシンを移動すると、移動後のデリバリーグループの**［リソース使用率］および［負荷評価基準インデックス］**テーブルで両方のデリバリーグループの統合された測定値が表示されます。

傾向データをエクスポートして、通常使用レポートおよび能力管理レポートを生成できます。エクスポートでは、PDF、Excel、およびCSVレポート形式がサポートされます。PDFとExcel形式のレポートには、傾向がグラフとテーブルとして表示されます。CSV形式のレポートには、処理してビューを生成したり、アーカイブしたりできる表形式のデータが含まれます。

レポートをエクスポートするには、次の手順に従います。

1. **［傾向］**タブに移動します。
2. フィルター基準と期間を設定して**［適用］**をクリックします。傾向グラフとテーブルにデータが入力されます。
3. **［エクスポート］**をクリックして、レポートの名前と形式を入力します。

Directorは、選択したフィルター基準に基づいてレポートを生成します。フィルター基準を変更した場合は、**［適用］**をクリックしてから**［エクスポート］**をクリックします。

注：大量のデータをエクスポートすると、Directorサーバー、Delivery ControllerおよびSQLサーバーのメモリとCPUの消費が著しく増加します。サポートされる同時エクスポート処理の数とエクスポートできるデータの量は、エクスポートのパフォ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マンスを最適にするため、デフォルトの上限に設定されています。

サポートされるエクスポート上限

エクスポートされるPDFとExcelのレポートは、選択されたフィルター基準によるグラフィカルなチャートが含まれています。ただし、すべてのレポート形式の表形式のデータは、行の数またはテーブルのレコード数のデフォルト値を超えた値は切り捨てられています。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Directorアプリケーションの設定をインターネットインフォメーションサービス（IIS）で構成して、デフォルトの上限を変更できます。

VHD形式	サポートされるデフォルトのレコード数	Directorアプリケーションの設定におけるフィールド	サポートされる最大レコード数
PDF	500	UI.Export Pdf Drilldown Limit	5000
Excel	100,000	UI.Export Excel Drilldown Limit	100,000
CSV	100,000（［セッション］タブでは10,000,000）	UI.Export Csv Drilldown Limit	100,000

エクスポートできるレコード数の上限を変更するには、次の手順に従います。

1. IISマネージャーコンソールを開きます。
2. ［Default Web Site］ノードを開き、［Director］Webサイトを選択します。
3. **［アプリケーションの設定］**をダブルクリックします。
4. フィールドを編集するか、新しいフィールドを追加します。

［アプリケーションの設定］でこれらのフィールドの値を追加すると、デフォルト値が上書きされます。

警告：サポートされる最大レコード数より多くフィールド値を設定すると、エクスポートのパフォーマンスが影響を受ける可能性があり、サポートもされません。

エラー処理

このセクションでは、エクスポート処理中に発生しうるエラーに対処するための情報を提供します。

- **Directorのタイムアウト**

  このエラーは、Directorサーバーでの、またはMonitor Serviceによるネットワーク問題や高いリソース使用率によって発生する可能性があります。

  デフォルトのタイムアウト時間は100秒間です。Directorサービスのタイムアウト時間を増やすには、インターネットインフォメーションサービス（IIS）のDirectorアプリケーションの設定で**Connector.DataServiceContext.Timeout フィールド**の値を設定します。

  1. IISマネージャーコンソールを開きます。

  2. ［Default Web Site］ノードを開き、［Director］Webサイトを選択します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. [アプリケーションの設定] をダブルクリックします。

4. 値Connector.DataServiceContext.Timeoutを編集します。

- モニターのタイムアウト

  このエラーは、Monitor Serviceによる、またはSQLサーバーでのネットワーク問題や高いリソース使用率によって発生する可能性があります。

  Monitor Serviceのタイムアウト時間を増やすには、Delivery Controllerで以下のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- 同時エクスポートまたはプレビュー処理上限

  Directorでは、エクスポートまたはプレビューの1つのインスタンスがサポートされます。**同時エクスポートまたはプレビュー処理上限**エラーが発生した場合は、次のエクスポート処理を後で実行してください。

  同時エクスポートまたはプレビュー処理の数を増やすことはできますが、Directorのパフォーマンスに影響する可能性があり、サポートもされません。

  1. IISマネージャーコンソールを開きます。

  2. ［Default Web Site］ノードを開き、［Director］Webサイトを選択します。

  3. [アプリケーションの設定] をダブルクリックします。

  4. 値UI.ConcurrentExportLimitを編集します。

- Directorのディスク容量不足

  各エクスポート処理には、Windows Tempフォルダーに最大2GBのハードディスク容量が必要です。容量をクリアするか、Directorサーバーにハードディスク容量を追加してからエクスポートを再試行してください。

特定のマシンのVDA（物理または仮想）にインストールされている Hotfixを確認するには、［マシンの詳細］ビューを選択します。

Directorで選択したマシンの電源の状態を制御するには、［電源制御］オプションを使用します。これらのオプションはデスクトップOSマシンに対してのみ実行でき、サーバーOSマシンに対しては使用できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注：この機能は、物理マシンまたはリモートPCアクセスを使用しているマシンに対しては使用できません。

コマンド	機能
再起動	仮想マシン上のすべてのプロセスを停止して、通常の再起動処理（ソフト再起動）を実行します。たとえば、起動に失敗したマシンを再起動するときにこのコマンドを使用します。
強制再起動	通常のシャットダウン処理を行わずに強制的に仮想マシンを再起動します。これは、物理サーバーの電源プラグを抜いてから電源を入れるのと同等の操作です。
シャットダウン	仮想マシン上のすべてのプロセスを停止して、通常のシャットダウン処理（ソフトシャットダウン）を実行します。
強制シャットダウン	通常のシャットダウン処理を行わずに強制的に仮想マシンをシャットダウンします。物理サーバーの電源プラグを抜くのと同等の操作です。実行中のプロセスを正しく停止できない場合があるため、この方法で仮想マシンをシャットダウンするとデータが失われる可能性があります。
サスペンド	仮想マシンを一時停止して、そのときの状態をデフォルトのストレージリポジトリ上にファイルとして保存します。この方法で仮想マシンを一時停止してからそのホストサーバーをシャットダウンし、ホストサーバーを再起動してから仮想マシンを元の実行状態に戻すことができます。
再開	一時停止状態の仮想マシンを再開して、元の実行状態に戻します。
起動	シャットダウン状態の仮想マシンを起動します（「コールドスタート」とも呼ばれます）。

電源制御操作に失敗した場合、アラート上にマウスポインターを置くと問題の詳細情報がポップアップメッセージとして表示されます。

メンテナンスモードでは、管理者がイメージの保守作業を行っている間、一時的にユーザーが接続できなくなります。

マシンをメンテナンスモードにすると、メンテナンスモードを解除するまでそのマシンへの接続が禁止されます。そのマシンにユーザーがログオンしている場合は、すべてのユーザーがログオフした後でメンテナンスモードに切り替わります。ユーザーのログオフを促すには、マシンのシャットダウンを通知するメッセージをユーザーに送信したり、電源制御機能を使って強制的にマシンをシャットダウンしたりできます。

1. ［ユーザーの詳細］ビューなどからマシンを選択するか、［フィルター］ビューでマシンのグループを選択します。
2. ［メンテナンスモード］をクリックしてマシンをメンテナンスモードにします。

メンテナンスモードのデスクトップにユーザーが接続を試みると、デスクトップを使用できないことを示すメッセージが表示されます。管理者がメンテナンスモードを解除するまで、新しい接続は許可されません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アラートおよび通知

Dec 05, 2017

ここでは次のことについて説明します。

アラートの監視

アラートポリシーの作成

アラートポリシーの条件

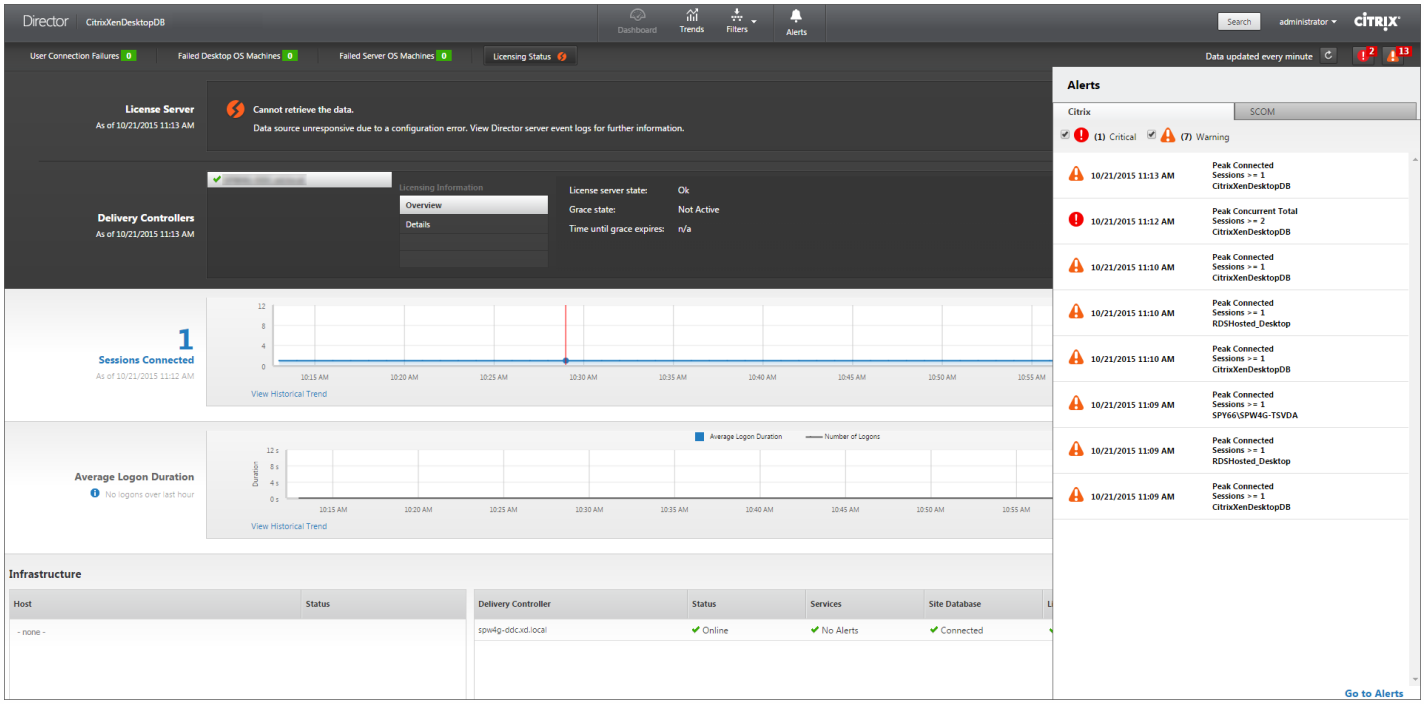
Octoblu webhookによるアラートポリシーの構成

SNMPトラップによるアラートポリシーの構成

SCOMアラート

SCOM統合の構成

アラートは、Directorのダッシュボードおよびそのほかの概要ビューに、警告および重大アラートシンボルと共に表示されます。アラートは、**Platinum**ライセンスを持つユーザーが使用できます。アラートは、1分ごとに自動的に更新されます。オンデマンドで更新することもできます。



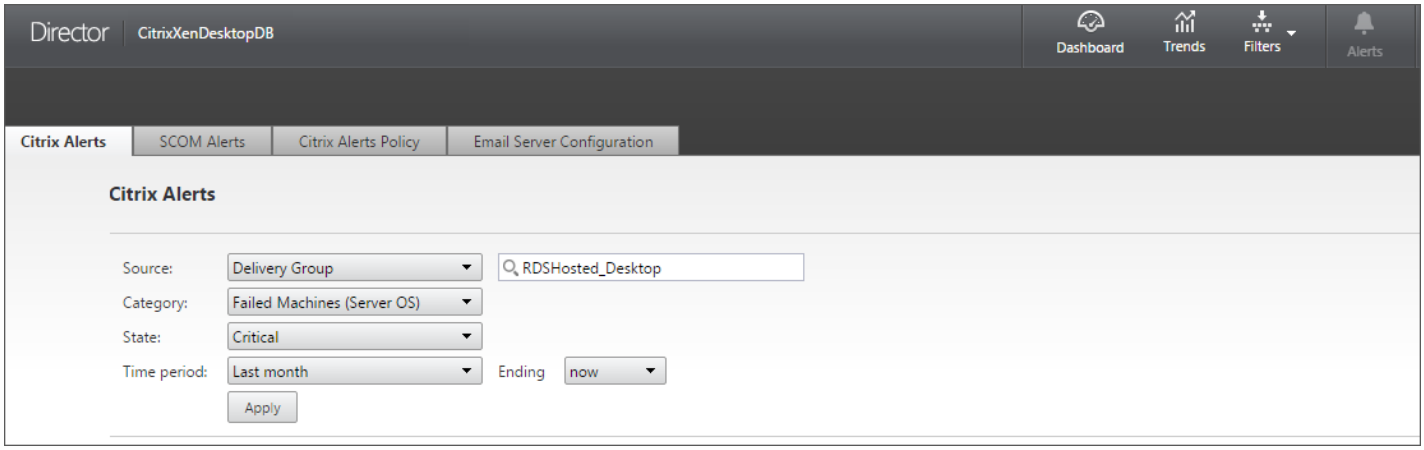
警告アラート（黄色の三角形）は、条件の警告しきい値に達した、またはしきい値を超えたことを示します。

重大アラート（赤の円）は、条件の重大しきい値に達した、またはしきい値を超えたことを示します。

サイドバーからアラートを選択し、サイドバーの下部にある**[アラートに移動]**リンクをクリックするか、［Director］ページの上部にある**[アラート]**を選択して、アラートに関するさらに詳細な情報を表示することができます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

［アラート］ビューで、アラートをフィルターおよびエクスポートできます。たとえば、先月特定のデリバリーグループで失敗したサーバーOSマシンや、特定のユーザーに対するすべてのアラートを特定することができます。詳しくは、「レポートのエクスポート」を参照してください。

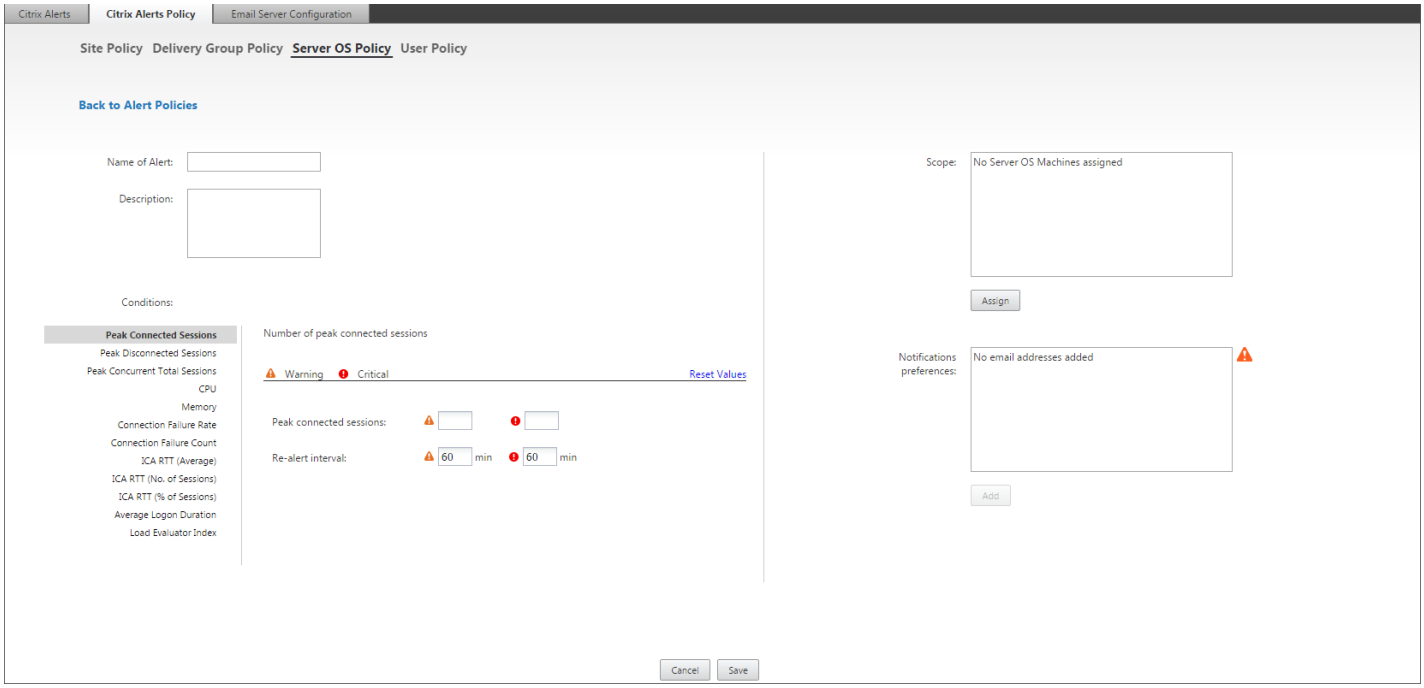


Citrixアラート。Citrixアラートは、Citrixコンポーネントで発生し、Directorで監視されるアラートです。Citrixアラートは、Director内で **[アラート]** > **[Citrixアラートポリシー]** の順に選択して構成することができます。設定した条件のしきい値を超過した場合のアラートに関して、個人およびグループにメールで送信される通知を構成の中で設定できます。通知は、Octoblu webhookまたはSNMPトラップとしても構成できます。 Citrixアラートのセットアップについて詳しくは、「アラートポリシーの作成」を参照してください。

SCOMアラート。SCOMアラートには、Microsoft System Center 2012 Operations Manager（SCOM）からのアラート情報が表示されます。これにより、Director内のデータセンターの稼働状態およびパフォーマンスがより包括的に示されます。詳しくは、「SCOMアラート」を参照してください。

サイドバーを展開する前にアラートアイコンの隣に表示されているアラートの数は、CitrixアラートとSCOMアラートの合計数です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



特定のセッション数基準のセットを満たした場合にアラートを生成するなどの目的で、新しいアラートポリシーを作成するには、以下の手順に従います。

1. **[アラート] > [Citrixアラートポリシー]** の順に選択し、［サーバーOSポリシー］などを選択します。
2. **[Create]** をクリックします。
3. ポリシーの名前と説明を入力し、アラートをトリガーするために満たす必要がある条件を設定します。たとえば、最大接続済みセッション数、最大切断セッション数、および最大同時セッション数に対して、警告とする数および重大とする数を指定します。警告値を重大値よりも大きくすることはできません。詳しくは、「アラートポリシーの条件」を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、アラートはこの間隔で再トリガーされます。アラートポリシーで設定されている場合は、メール通知が生成されます。クリアされたアラートの場合、再アラート間隔でメール通知が生成されることはありません。
5. スコープを設定します。たとえば、特定のデリバリーグループに対して設定します。
6. お知らせ設定で、アラートがトリガーされたときのメール通知の送信先を指定します。アラートポリシーでメールお知らせ設定を行うには、**[メールサーバーの構成]** タブでメールサーバーを指定する必要があります。
7. **[保存]** をクリックします。

Octoblu webhook構成について詳しくは、「Octoblu webhookによるアラートポリシーの構成」を参照してください。

SNMPトラップ構成について詳しくは、「SNMPトラップによるアラートポリシーの構成」を参照してください。

スコープに20件以上のデリバリーグループが定義されているポリシーを作成すると、構成が完了するまでにおよそ30秒かかる場合があります。完了するまで、スピナーアイコンが表示されます。

最大20の一意のデリバリーグループに対して、50以上のポリシー（合計で1000デリバリーグループターゲット）を作成すると、応答時間が遅くなることがあります（5秒以上）。

アクティブなセッションがあるマシンをデリバリーグループから別のデリバリーグループに移動すると、マシンパラメータで定義されたデリバリーグループアラートが誤って発信されることがあります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アラートポリシーの条件	説明および推奨される操作
最大接続済みセッション数	最大接続済みセッションの数。 • Directorセッションの傾向ビューで、最大接続済みセッション数をチェックします。 • セッションの負荷に対応するのに十分な処理能力があることを確認します。 • 必要に応じ、マシンを追加します。
最大切断セッション数	最大切断セッションの数。 • Directorセッションの傾向ビューで、最大切断セッション数をチェックします。 • セッションの負荷に対応するのに十分な処理能力があることを確認します。 • 必要に応じ、マシンを追加します。 • 必要に応じ、切断されたセッションからログオフします。
最大同時セッション数	最大同時セッションの数。 • Directorセッションの傾向ビューで、最大同時セッション数をチェックします。 • セッションの負荷に対応するのに十分な処理能力があることを確認します。 • 必要に応じ、マシンを追加します。 • 必要に応じ、切断されたセッションからログオフします。
CPU	CPU使用率の割合 • CPUを消費しているプロセスやリソースを特定します。 • 必要に応じてプロセスを終了します。プロセスを終了すると、保存されていないデータは失われます。 • すべてが想定どおりに機能している場合は、将来的にCPUリソースを追加します。 注：ポリシー設定 **[リソースの監視を有効にします]** はデフォルトで、VDAがインストールされているマシンでのCPUとメモリパフォーマンスカウンターの監視用に許可されています。このポリシー設定が無効にされると、CPUとメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。
メモリ	メモリ使用率の割合。 • メモリを消費しているプロセスやリソースを特定します。 • 必要に応じてプロセスを終了します。プロセスを終了すると、保存されていないデータは失われます。 • すべてが想定どおりに機能している場合は、将来的にメモリを追加します。 注：ポリシー設定 **[リソースの監視を有効にします]** はデフォルトで、VDAがインストールされているマシンでのCPUとメモリパフォーマンスカウンターの監視用に許可されています。このポリシー設定が無効にされると、CPUとメモリの条件に関するアラートはトリガーされません。詳

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	しくは、「監視のポリシー設定」を参照してください。
接続障害率	過去1時間の接続エラーの率。接続の合計試行回数に対する合計エラー数の割合に基づいて計算されます。 • Director接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。 • アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。
接続障害数	過去1時間の接続エラー数。 • Director接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。 • アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。
ICA RTT（平均）	平均ICA往復時間 • NetScaler HDX InsightまたはMASでICA RTTのブレークダウンをチェックして、原因を特定します。詳しくは、「NetScaler Insight Center - HDX Insight」または「NetScaler MAS - Analytics: HDX Insight」のドキュメントを参照してください。 • NetScalerが利用可能でない場合は、ICA RTTの［Directorのユーザー詳細］ビューおよび遅延をチェックして、これがネットワークの問題か、またはXenAppおよびXenDesktopの問題かを特定します。
ICA 往復時間（セッション数）	ICA往復時間を超過しているセッションの数。 • NetScaler HDX InsightまたはMASで、ICA RTTが高いセッションの数をチェックします。詳しくは、「NetScaler Insight Center - HDX Insight」または「NetScaler MAS - Analytics: HDX Insight」のドキュメントを参照してください。 • NetScalerが利用可能でない場合は、ネットワークチームと協力して原因を特定してください。
ICA RTT（セッションの割合）	平均ICA往復時間を超過しているセッションの割合。 • NetScaler HDX InsightまたはMASで、ICA RTTが高いセッションの数をチェックします。詳しくは、「NetScaler Insight Center - HDX Insight」または「NetScaler MAS - Analytics: HDX Insight」のドキュメントを参照してください。 • NetScalerが利用可能でない場合は、ネットワークチームと協力して原因を特定してください。
ICA RTT（ユーザー）	特定のユーザーによって開始されたセッションに適用されたICA往復時間。1つ以上のセッションでICA RTTがしきい値よりも高い場合は、アラートがトリガーされます。
失敗したマシン（デスクトップOS）	失敗したデスクトップOSマシンの数。 • Directorの［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。Citrix Scout診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

失敗したマシン（サーバーOS）	失敗したサーバーOSマシンの数。 • Directorの［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。Citrix Scout診断を実行して、原因を特定します。
平均ログオン処理時間	過去1時間に行われたログオンの平均ログオン処理時間。 • Directorのダッシュボードをチェックし、ログオン処理時間に関する最新の測定基準を取得します。短時間のうちに多数のユーザーがログインすると、ログオン処理時間が長引くことがあります。 • 原因を絞り込むため、ログオンのベースラインおよび内訳をチェックします。 詳しくは、「ユーザーログオンの問題の診断」を参照してください。
ログオン処理時間（ユーザー）	過去1時間に行われた指定されたユーザーのログオンに関するログオン処理時間。
負荷評価基準インデックス	過去5分間の負荷評価基準インデックスの値。 • Directorで、ピーク負荷（最大負荷）に達している可能性があるサーバーOSマシンをチェックします。 • ダッシュボード（失敗）および負荷評価基準インデックス傾向レポートを表示します。

メール通知は例外として、Octoblu webhookでアラートポリシーを構成してIoTサービスを開始できます。

注：この機能の使用には、Delivery Controllerバージョン7.11以降が必要です。

アラートを使用したIoTサービスの例としては、SMS通知の送信によるスタッフのサポートや、カスタムインシデント解決フラットフォームとの統合による追跡通知の支援などがあります。

PowerShellコマンドレットを使用して、HTTPコールバックまたはHTTP POSTでアラートポリシーを構成できます。webhooksのサポートのために拡張されます。

新しいOctobluワークフローの作成および対応するwebhook URLの取得について詳しくは、『Octoblu Developer Hub』を参照してください。

新しいアラートポリシーや既存のポリシーに対してOctoblu webhook URLを構成するには、次のPowerShellコマンドレットを使用します。

webhook URLで新しいアラートポリシーを作成する場合：



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description <Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーにwebhook URLを追加する場合：

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドのヘルプについては、たとえば次のようにPowerShellヘルプを使用します。

```
Get-Help  <Set-MonitorNotificationPolicy>
```

PowerShellを使用した通知ポリシーの構成について詳しくは、「Director 7.7： Powershellを使用したアラートと通知の管理と構成」を参照してください。

アラートポリシーから生成された通知によって、webhook URLへのPOSTコールでwebhookがトリガーされます。POSTメッセージには通知の情報がJSON形式で含まれます。

{"NotificationId" : <通知ID>,

"Target" : <通知ターゲットID>,

"Condition" : <違反された条件>,

"Value" : <条件のしきい値>,

"Timestamp": <通知が生成された時間（UTC）>,

"PolicyName": <アラートポリシーの名前>,

"Description": <アラートポリシーの説明>,

"Scope" : <アラートポリシーのスコープ>,

"NotificationState": <通知のステータス［critical］、［warning］、［healthy］、または［dismissed］>,

"Site" : <サイト名>}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SNMPトラップを構成されたアラートがトリガーされると、対応するSNMPトラップメッセージが構成済みのネットワークリスナーに転送され、さらに処理されます。Citrixアラートは、SNMPバージョン2以降のトラップをサポートします。現時点では、トラップメッセージを1つのリスナーに転送できます。

注：この機能の使用には、Delivery Controllerバージョン7.12以降が必要です。

SNMPトラップを構成するには、以下のPowerShellコマンドレットを使用します。

- 現時点のSNMPサーバー構成を取得する：

```
Get-MonitorNotificationSnmpServerConfiguration
```

- SNMPバージョン2のサーバー構成を設定する：

```
Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Comm
```

- SNMPバージョン3のサーバー構成を設定する：

```
$authpass = "<authentication password>" | ConvertTo-SecureString -AsPlainText -Force

$privpass = "<Privacy password>" | ConvertTo-SecureString -AsPlainText -Force

Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Engine
```

- 既存のアラートポリシーにSNMPトラップを有効化する：

```
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID>
```

- SNMPトラップ構成を持つ新しいアラートポリシーを作成する：

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -IsSnmpEnabled $true -Description <Policy description> -Enabled $true
```

DirectorからのSNMPトラップメッセージ内のOIDの構造は以下のようになります。
1.3.6.1.4.1.3845.100.1.
はDirectorに定義されたすべてのアラートポリシーに対して順次生成されます。そのため、OIDはユーザー環境ごとに一意です。

- 1.3.6.1.4.1.3845.100.1を使用すると、Directorからのすべてのトラップメッセージがフィルタリングされます。
- 1.3.6.1.4.1.3845.100.1. を使用すると、特定のアラートのトラップメッセージがフィルタリングされ、処理されます。

以下のコマンドレットを使用すると、ご使用の環境に定義されたアラートポリシーのUIDを取得できます。

```
Get-MonitorNotificationPolicy
```

SNMPトラップはSCOMに転送できます。それには、SCOMをDelivery Controllerとともに構成してトラップメッセージをリスンします。

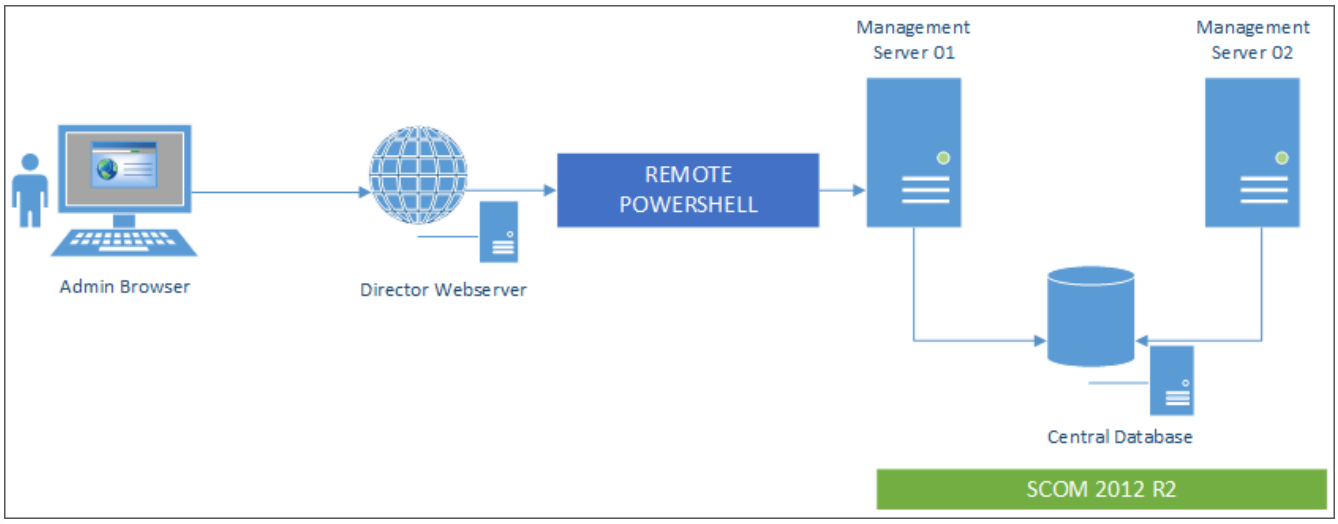
Directorとの統合により、SCOMからのアラート情報をDirectorのダッシュボードおよびその他の概要ビューで表示できるようになります。

SCOMアラートは、Citrixアラートと共に画面上に表示されます。SCOMアラートには、サイドバーの［SCOM］タブからアクセスしてドリルダウンすることができます。

1か月前までの過去のアラートを表示し、情報を並べ替えてフィルターし、フィルターされた情報をCSV、Excel、およびPDFレポート形式にエクスポートすることができます。 詳しくは、「レポートのエクスポート」を参照してください。

SCOM統合では、リモートPowerShell 3.0以上を使用してSCOM管理サーバーのデータをクエリし、ユーザーのDirectorセッションで永続的な実行空間接続を維持します。DirectorおよびSCOMサーバーのPowerShellバージョンが同じである必要があります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



SCOM統合の要件は、以下のとおりです。

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0以上（DirectorおよびSCOMサーバーのPowerShellバージョンは一致する必要があります）
- クアッドコアCPUと16GBのRAM（推奨）
- SCOMのプライマリ管理サーバーは、Directorのweb.configファイルで構成する必要があります。この処理は、DirectorConfigツールを使用して実行できます。

注：

- Director管理者アカウントをSCOMオペレーターの役割として構成することをお勧めします。これにより、管理者がDirectorで完全なアラート情報を取得できるようになります。そのように構成できない場合、DirectorConfigツールを使用してSCOM管理者アカウントをweb.configファイルに構成できます。
- 最適なパフォーマンスのために、構成するDirector管理者の数は、1つのSCOM管理サーバーにつき10人以下とすることをお勧めします。

Directorサーバーで、以下を実行します。

1. コマンド**Enable-PSRemoting**を実行して、PowerShellリモート処理を有効にします。

2. SCOM管理サーバーをTrustedHosts一覧に追加します。PowerShellプロンプトを開いて、次のコマンドを実行します。

    a. 最新のTrustedHosts一覧を取得します。

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

    b.SCOM管理サーバーのFQDNを、TrustedHostsの一覧に追加します。 は、Get-Itemコマンドレットから返された既存エントリのセットを表します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

3. DirectorConfigツールを使用して、SCOMを構成します。

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

SCOM管理サーバーで、以下を実行します。

1. SCOM管理者の役割に、Director管理者を割り当てます。

a. SCOM管理コンソールを開き、**[管理]** > **[セキュリティ]** > **[ユーザーロール]** の順に選択します。

b. ［ユーザーロール］では、新しいユーザー役割を作成するか、または既存のユーザー役割を変更することができます。SCOMデータへのアクセス方法を定義するSCOMオペレーターの役割には4つのカテゴリがあります。たとえば、読み取り専用の役割には、［管理］ペインが表示されず、規則、マシン、アカウントを検出または管理することができません。オペレーターの役割は、すべての管理権限を実行できる管理者の役割です。

注：Director管理者がオペレーター以外の役割に割り当てられている場合、以下の操作を実行できません。

i. 複数の管理サーバーが構成されており、プライマリ管理サーバーを利用できない場合、Director管理者はセカンダリ管理サーバーに接続できません。プライマリ管理サーバーはDirectorのweb.configファイルで構成されるサーバーであり、前述の手順3でDirectorConfigツールで指定されたサーバーです。セカンダリ管理サーバーは、プライマリサーバーのピア管理サーバーです。

ii. アラートのフィルター時に、Director管理者はアラートソースを検索できません。検索するには、オペレーターレベルの権限が必要です。

c. ユーザー役割を変更するには、役割を右クリックし、**[プロパティ]** をクリックします。

d. ［ユーザーロールのプロパティ］ダイアログで、指定したユーザー役割にDirector管理者を追加するか、またはそこからDirector管理者を削除することができます。

2. Director管理者を、SCOM管理サーバーの［Remote Management Users］グループに追加します。これにより、Director管理者がリモートPowerShell接続を確立できるようになります。

3. コマンド**Enable-PSRemoting**を実行して、PowerShellリモート処理を有効にします。

4. WS-Managementプロパティ制限を設定します。

a. MaxConcurrentUsersの変更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CLI

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

PS

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. MaxShellsPerUserの変更：

CLI

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

PS

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. MaxMemoryPerShellMBの変更

CLI

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

PS

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. SCOM統合が混在ドメイン環境で機能するよう、以下のレジストリエントリを設定します。

パス：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

値の名前：LocalAccountTokenFilterPolicy

種類：REG_DWord

値のデータ：1

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

SCOM統合がセットアップされると、メッセージ「Cannot get the latest SCOM alerts. View the Director server event logs for more information」が表示されることがあります。サーバーイベントログを使用して問題を特定し、解決することができます。次の原因が考えられます。

- DirectorまたはSCOMマシンで、ネットワーク接続が失われた。
- SCOMサービスが利用できないか、ビジー状態のため応答していない。
- 構成したユーザーの権限が変更されていたため、認証に失敗した。
- SCOMデータの処理中に、Directorでエラーが発生した。
- DirectorとSCOMサーバーのバージョンが不一致。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理権限の委任とDirector

Dec 05, 2017

管理権限の委任機能では、管理者、役割、およびスコープという3つの概念が使用されます。管理者の権限は、その管理者の役割とそのスコープに基づいて定義されます。たとえば、管理者にヘルプデスク管理者の役割を割り当てて、その役割のスコープとして特定のサイトのエンドユーザーを指定できます。

委任管理者の作成について詳しくは、「委任管理」を参照してください。

付与されている管理権限により、その管理者に表示されるDirectorのインターフェイスと実行可能なタスクが決定されます。権限により、次の内容が決定されます。

- その 管理者がアクセスできるDirectorの表示内容。これを「ビュー」と呼びます。
- その管理者が表示したり操作したりできるデスクトップ、 マシン、およびセッション。
- ユーザーセッションのシャドウや メンテナンスモードの有効化など、その 管理者が実行できるコマンド。

組み込みの役割および権限によっても、管理者がDirectorで実行できるタスクが決定されます。

管理者の役割	Directorでの権限
すべての管理権限を実行できる管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
読み取り専用管理者	すべてのビューに制限なくアクセスして、一般的な情報と、指定されているスコープのすべてのオブジェクトを表示できます。HDXチャネルからレポートをダウンロードして、［傾向］ビューのエクスポートオプションを使って傾向データをエクスポートできます。そのほかのコマンドは実行できず、ビューで設定を変更することはできません。
ヘルプデスク管理	［ヘルプデスク］および［ユーザーの詳細］ビューにのみアクセスでき、委任されたオブジェクトのみを表示できます。ユーザーセッションをシャドウしたり、そのユーザーに対してコマンドを実行したりできます。メンテナンスモードを有効にしたり解除したりできます。デスクトップOSマシンの電源制御オプションを使用できます。［ダッシュボード］ビュー、［傾向］ビュー、［アラート］ビュー、および［フィルター］ビューにはアク

© 1999-2017 Citrix Systems, Inc. All rights reserved.

者	セスできません。サーバーOSマシンの電源制御オプションは使用できません。
管理者のマシンカタログ管理者の役割	Directorでの権限 アクセスできません。この管理者は、Directorを使用したりデータを表示したりできません。マシン詳細ページ（マシンベースの検索）にはアクセスできます。
ホスト管理者	アクセスできません。この管理者は、Directorを使用したりデータを表示したりできません。

Director管理者のカスタム役割を構成するには

Studioでは、組織の要件に応じてDirector用のカスタムの役割を構成して、管理権限を柔軟に委任できます。 例えば、組み込みのヘルプデスク管理者の役割を制限して、この管理者がユーザーのセッションをログオフすることを禁止できます。

Director用のカスタムの役割を作成する場合は、その役割に以下の一般的な権限も付与する必要があります。

- DirectorにログオンするためのDelivery Controller権限 - 少なくとも管理者ノードでの読み取り専用アクセス
- デリバリーグループのデータをDirectorで閲覧するための権限 - 少なくとも読み取り専用アクセス

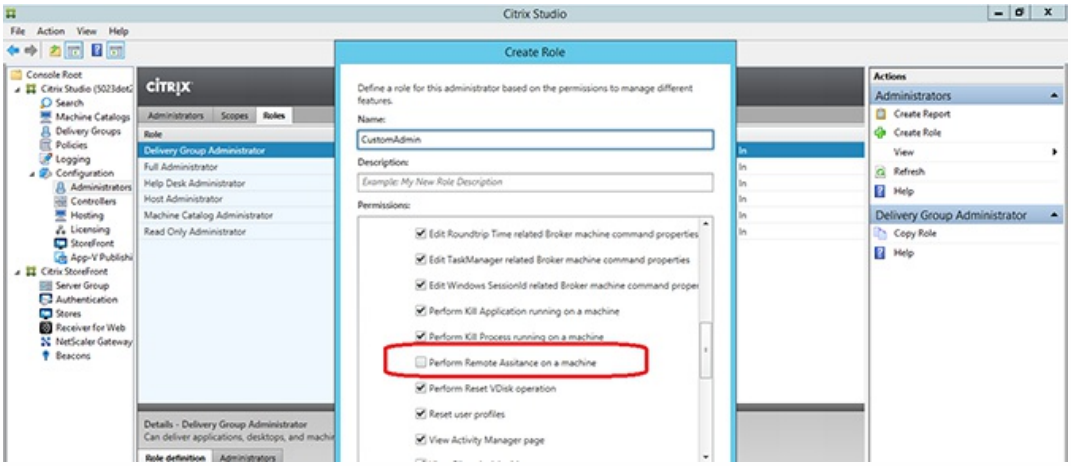
または、既存の役割をコピーしてカスタムの役割を作成し、異なるビューのための権限を追加することができます。 たとえば、ヘルプデスクの役割をコピーして、［ダッシュボード］ページや［フィルター］ページを表示するための権限を追加できます。

以下のDirector用の権限を追加します。

- マシンで実行中の アプリケーションの強制終了
- マシンで実行中の プロセスの強制終了
- マシン上でのリモート アシスタンス
- vDiskのリセット 操作
- ユーザープロファイルのリセット
- クライアント詳細 ページの表示
- ダッシュボードページの表示
- フィルターページの表示
- マシン 詳細ページの表示
- 傾向ページの表示
- ユーザー詳細 ページの表示

この例では、シャドウ機能（マシン上でのリモートアシスタンス）が無効になっています。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



権限は、UIで使えるようにするために、他の権限への依存関係を持つ場合があります。たとえば、**マシンで実行中のアプリケーションの強制終了**権限を選択すると、その役割のために権限を持つこれらのパネルのみで、**[アプリケーションの終了]**の機能が有効になります。以下のパネルの権限を選択することができます。

- フィルター ページの表示
- ユーザー詳細ページの表示
- マシン詳細ページの表示
- クライアント詳細ページの表示

さらに、他のコンポーネントの権限の一覧から、次のデリバリーグループ権限の追加を検討します。

- デリバリーグループメンバーシップによるマシンのメンテナンスモードの有効/無効。
- デリバリーグループメンバーシップによるWindowsデスクトップマシンの電源操作。
- デリバリーグループメンバーシップによるマシンのセッション管理。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Director展開環境の保護

Feb 01, 2018

この記事では、Directorの展開および構成時に使用すべき、システムのセキュリティを保護するための機能について説明します。

制限されたIIS構成でDirectorを構成できます。これはデフォルトのIIS構成ではありません。

ファイル拡張子

一覧にないファイル拡張子を禁止することができます。

Directorは要求のフィルタリングに、次のファイル拡張子が必要です。

- .aspx
- .css
- .html
- .js
- png
- .svc

Directorは要求のフィルタリングに、次のHTTP動詞が必要です。次の一覧にない動詞を禁止できます。

- GET
- POST
- ヘッド

Directorは次を必要としません。

- ISAPIフィルター
- ISAPI拡張
- CGIプログラム
- FastCGIプログラム

重要：

- Directorには完全な信頼が必要です。グローバル.NET信頼レベルを［High］またはそれ以下に設定しないでください。
- Directorは個別のアプリケーションプールを保持します。Directorの設定を変更するには、Directorサイトを選択し変更します。

Directorがインストールされると、そのアプリケーションプールには［サービスとしてログオン］のログオン権限と［プロセスのメモリ クォータの増加］、［セキュリティ監査の生成］、［プロセス レベル トークンの置き換え］の権限が付与されます。これはアプリケーションプールが作成された時の通常のビヘイビアーです。

通常、これらのユーザー権利を変更する必要はありません。これらの権限はDirectorでは使用されず自動的に無効になります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

実稼働環境では、Directorとサーバーの間で通信されるデータを保護するために、インターネットプロトコルセキュリティ（IPsec）またはHTTPSプロトコルを使用することをお勧めします。IPsecは、インターネットプロトコルの標準機能拡張のセットです。インターネットプロトコルは、データ整合性と再生の保護により通信の認証と暗号化の機能を提供します。IPsecはネットワーク層のプロトコルセットであるため、上位レベルのプロトコルでそのままIPSecを使用できます。HTTPSは、TLS（Transport Layer Security）プロトコルを使用して強力なデータ暗号化機能を提供します。

注：

- 実稼働環境では、Directorへのすべての接続が保護されるようにしてください。
- Directorからの通信を保護するには、個別に各接続を構成する必要があります。
- SSLプロトコルは、推奨されていません。代わりにより安全なTLSプロトコルを使用します。
- IPsecではなくTLSを使用して、NetScalerとの通信を保護する必要があります。

DirectorとXenAppおよびXenDesktopサーバーの（監視およびレポート機能のための）通信を保護する方法について詳しくは、「データアクセスセキュリティ」を参照してください。

DirectorとNetScalerの（NetScaler Insightのための）通信を保護する方法について詳しくは、「ネットワーク分析機能の構成」を参照してください。

Directorとライセンスサーバーの通信を保護する方法について詳しくは、「ライセンス管理コンソールの保護」を参照してください。

Director と同じWebドメイン（ドメイン名とポート）にWebアプリケーションを展開すると、これらのWebアプリケーションの脆弱性によりDirector展開環境のセキュリティが低下する可能性があります。セキュリティ境界を分離してセキュリティを強化するため、WebアプリケーションとWebドメインにDirectorを展開することをお勧めします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenDesktop 7よりも前のVDAに対する権限の構成

Dec 05, 2017

XenDesktop 7よりも前のバージョンのVDAがある場合、Directorには展開からの情報に加えて、Windowsリモート管理（WinRM）によるリアルタイム状態と測定値が提供されます。

さらに、この手順を使用してXenDesktop 5.6 Feature Pack1のリモートPC用にWinRMを構成します。

デフォルトでは、デスクトップマシンのローカル管理者（一般的にはドメイン管理者および特権のあるそのほかのユーザー）だけが、リアルタイムデータを表示するための権限を持っています。

WinRMのインストールと構成については、 CTX125243を参照してください。

ほかのユーザーがリアルタイムデータを確認できるようにするには、そのユーザーに権限を付与する必要があります。 例えば、HelpDeskUsersというActive Directoryセキュリティグループのメンバーである複数のDirectorユーザー（HelpDeskUserA、HelpDeskUserBなど）がいるとします。 グループにはStudioでヘルプデスク管理者の役割が割り当てられており、必要なDelivery Controller権限が付与されています。 ただし、このグループはデスクトップマシンからの情報にもアクセスする必要があります。

この場合、次のいずれかの方法で必要な権限を構成できます。

- Directorユーザーに権限を付与する（偽装モデル）
- Directorサービスに権限を付与する（信頼されたサブシステムモデル）

Directorユーザーに権限を付与するには（偽装 モデル）

Directorでは、デフォルトで偽装モデルが使用されます。つまり、デスクトップマシンへのWinRM接続は、DirectorユーザーのIDを使って実行されます。 つまり、このユーザーにはデスクトップに対する適切な権限が必要です。

必要な権限は、次のいずれかの方法で構成できます（これらの方法について詳しくは後述します）。

1. ユーザーをデスクトップマシン上の ローカル管理者グループに追加する。
2. Directorで必要な 特定の権限をユーザーに付与する。この方法では、デスクトップマシンのすべての管理 権限を Director ユーザー（HelpDeskUsersグループなど）に付与しなくても、必要な権限だけを付与できます。

Directorサービスに権限を付与するには（信頼されたサブシステム モデル）

Directorユーザーにデスクトップマシン上の権限を付与する代わりに、WinRM接続にサービスIDが使用されるようにして、そのサービスIDに適切な権限のみを付与できます。

このモデルでは、DirectorのユーザーにはWinRMを呼び出す権限を付与しません。 ユーザーはDirectorを使ってデータにアクセスできるだけです。

IISのDirectorアプリケーションプールは、サービスIDとして実行するように構成されています。 デフォルトでは、APPPOOL\Director仮想アカウントが使用されます。 リモート接続を実行すると、このアカウントがサーバーのActive Directoryコンピューターアカウント（MyDomain\DirectorServer$など）として表示されます。 このアカウントに適切な権限を付与する必要があります。

複数のDirector Webサイトが展開されている環境では、各Webサーバーのコンピューターアカウントを、適切な権限で構成されているActive Directoryセキュリティグループに追加する必要があります。

WinRMに対してユーザーのIDではなくサービスIDを使用するようにDirectorを設定するには、 詳細構成」の説明に従って次

© 1999-2017 Citrix Systems, Inc. All rights reserved.

の設定を構成します。

Service.Connector.WinRM.Identity = Service
必要な権限は、次のいずれかの方法で構成できます。

1. サービス アカウントをデスクトップマシン上のローカル管理者グループに追加する。
2. Directorで必要な特定の権限をサービス アカウントに付与する（後述）。この 方法では、デスクトップ マシンのすべての管理権限をサービスアカウントに付与しなくても、必要な権限だけを付与できます。

特定のユーザーまたはグループに権限を割り当てるには

DirectorがWinRMでデスクトップマシンからの情報にアクセスできるようにするには、以下の権限が必要です。

- WinRM RootSDDLの読み取りおよび実行権限
- 以下のWMI名前空間権限：
  - root/cimv2 - リモートアクセス
  - root/citrix - リモートアクセス
  - root/RSOP — リモートアクセスおよび実行
- 以下のローカルグループのメンバーシップ：
  - パフォーマンスモニターユーザー
  - イベントログリーダー

これらの権限を自動的に付与するには、x86\Virtual Desktop AgentおよびX64\Virtual Desktop Agentフォルダーのインストールメディア、およびC:\inetpub\wwwroot\Director\toolsフォルダーに収録されているConfigRemoteMgmt.exeツールを使用します。すべてのDirectorユーザーに上記の権限を付与する必要があります。

Active Directoryセキュリティグループ、ユーザー、またはコンピューターアカウントに上記の権限を付与したり、アプリケーションやプロセスを終了するための権限を付与したりするには、管理特権でコマンドプロンプトを開き、次の引数を指定してこのツールを実行します。

ConfigRemoteMgmt.exe /configwinrmuser domain\name
ここで、 name はセキュリティグループ、ユーザー、またはコンピューターアカウントです。

ユーザーのセキュリティグループに必要な権限を付与するには次のコマンドを実行します。

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
特定のコンピューターアカウントに権限を付与するには次のコマンドを実行します。

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
アプリケーションやプロセスを終了したり、シャドウ機能を使用したりする権限を付与するには次のコマンドを実行します。

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
特定のユーザーグループに権限を付与するには次のコマンドを実行します。

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
このツールのオンラインヘルプを表示するには次のコマンドを実行します。

ConfigRemoteMgmt.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ネットワーク分析機能の構成

Dec 05, 2017

注： この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。

Directorは、NetScaler Insight CenterまたはNetScaler MASを統合して、ネットワーク分析機能およびパフォーマンス管理機能を提供します。

- ネットワーク分析機能では、NetScaler Insight CenterまたはNetScaler MASでHDX Insightレポートを使用してネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能を使用すると、DirectorでICAトラフィックを高度に分析できます。
- パフォーマンス管理機能により、履歴保持および傾向に関するレポートを生成できます。データの履歴保持とリアルタイム評価により、管理者はサーバーのキャパシティとヘルスに関する傾向レポートを作成できます。

Directorでこの機能を有効にすると、HDX Insightレポートにより以下の追加情報がDirectorに提供されます。

- ［傾向］ページの［ネットワーク］タブには、展開環境全体におけるアプリケーション、デスクトップ、ユーザーに対する遅延と帯域幅の影響が表示されます。
- ［User Details］ページには、特定のユーザーセッションに特化した遅延と帯域幅情報が表示されます。

制限事項

- ICAセッション往復時間（RTT）には、Receiver for Windows 3.4以降およびReceiver for Mac 11.8以降のデータが正確に表示されます。これらのバージョンよりも前のバージョンのReceiverについては、正確なデータが表示されません。
- ［傾向］ビューでは、XenDesktop 7よりも前のバージョンのVDAについてはHDX接続のログオンデータが収集されません。以前のバージョンのVDAについては、チャートデータが0として表示されます。

ネットワーク分析機能を有効にするには、DirectorでNetScaler Insight CenterまたはNetScaler MASをインストールし、構成する必要があります。Directorには、NetScaler MAS Version 11.1 Build 49.16以降が必要です。Insight CenterおよびMASは、Citrix XenServerで実行される仮想アプライアンスです。Directorでは、ネットワーク分析により、環境のトラフィック情報を収集します。

詳しくは、「NetScaler Insight Center」または「NetScaler MAS」のドキュメントを参照してください。

1. Directorがインストールされているサーバー上のコマンドラインプロンプトで、C:\inetpub\wwwroot\Director\toolsにあるDirectorConfigコマンドに/confignetscalerパラメーターを指定して実行します。
2. 画面上の指示に従って、NetScaler Insight CenterまたはNetScaler MASマシン名（完全修飾ドメイン名またはIPアドレス）、ユーザー名、パスワード、および接続の種類（HTTPまたはHTTPS）を入力して、NetScaler InsightまたはNetScaler MASとの統合を選択します。
3. 変更を確認するには、いったんログオフして再ログオンします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーの問題のトラブルシューティング

Dec 05, 2017

Directorの **[アクティビティマネージャー]** ページにある **[ヘルプデスク]** ビューを使って、ユーザーに関する情報を確認します。

- ユーザーのログオン、接続、およびアプリケーションの状態について確認する。
- ユーザーのマシンをシャドウする。
- ICAセッションを記録する。
- 次の表に示す方法で問題のトラブルシューティングを行い、必要な場合は問題を担当の管理者に報告する。

トラブルシューティングのヒント

ユーザーの問題	提案
ログオンに時間がかかる。断続的もしくは繰り返し失敗する	ユーザーログオンの問題の診断
アプリケーションが遅いまたは応答しない	アプリケーションエラーの解決
接続に失敗した	デスクトップ接続の復元
セッションが遅いまたは応答しない	セッションの復元
セッションの記録	セッションの記録
ビデオが遅いまたは画質が悪い	HDXチャネルシステムレポートの生成

注：［ユーザーの詳細］ビューの［マシンの詳細］パネルで、マシンがメンテナンスモードになっていないことを確認してください。

検索のヒント

Directorの［検索］フィールドにユーザー名を入力すると、Directorのサポートが構成されたすべてのサイトでActive Directoryユーザーが検索されます。

［検索］フィールドにマルチユーザーマシンの名前を入力すると、そのマシンの[マシンの詳細］ページが開きます。

［検索］フィールドにエンドポイントの名前を入力すると、そのエンドポイントに接続している認証が不要なユーザー（匿名ユーザー）セッションおよび認証が必要なセッションを検索でき、匿名ユーザーセッションのトラブルシューティングを行うことができます。匿名ユーザーセッションのトラブルシューティングを行うには、エンドポイント名が重複していないことが重要です。

検索結果には、現在マシンを使用していないユーザーや、マシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。

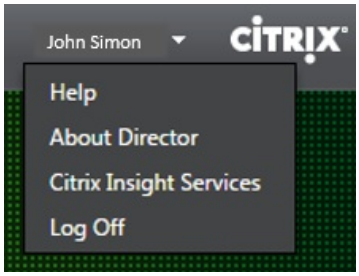
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 検索語の一部を入力すると、一致する候補が一覧で表示されます。
- ユーザー名、姓と名、または表示名などをスペースで区切って複数の文字列として入力すると、両方の文字列と一致する項目が検索されます。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert, Jones」などが検索されます。

ホームページに戻るには、Directorのロゴをクリックします。

Citrix Insight Servicesへのアクセス

Directorの［ユーザー］ボックスからCitrix Insight Services（CIS）にアクセスすることで、診断からさらなる洞察を得ることができます。CISで提供されるデータは、Call HomeやCitrix Scoutなどのソースから取得されます。



Citrixテクニカルサポートへのトラブルシューティング情報のアップロード

単一のDelivery ControllerまたはVirtual Delivery AgentからCitrix Scoutを実行し、選択したコンピューターのトラブルシューティングに必要なデータ要素やCitrix Diagnostics Facility（CDF）トレースをキャプチャします。Scoutは、CISプラットフォームにデータを安全にアップロードする機能を提供し、Citrixのテクニカルサポートのトラブルシューティングを支援します。CitrixのテクニカルサポートはCISプラットフォームを使用して、カスタマーから報告された問題解決する時間を短縮します。

Scoutは、XenAppまたはXenDesktopのコンポーネントと一緒にインストールされます。Windowsのバージョンに応じて、Scoutは、XenDesktop 7.1、XenDesktop 7.5、XenApp 7.5、XenDesktop 7.6、XenApp 7.6、XenDesktop 7.7、またはXenApp 7.7をインストール、またはこれらのバージョンにアップグレードしたときに、Windowsのスタートメニュー、またはスタート画面に表示されます。

スタートメニューやスタート画面からScoutを起動するには、［Citrix］の［Citrix Scout］を選択します。

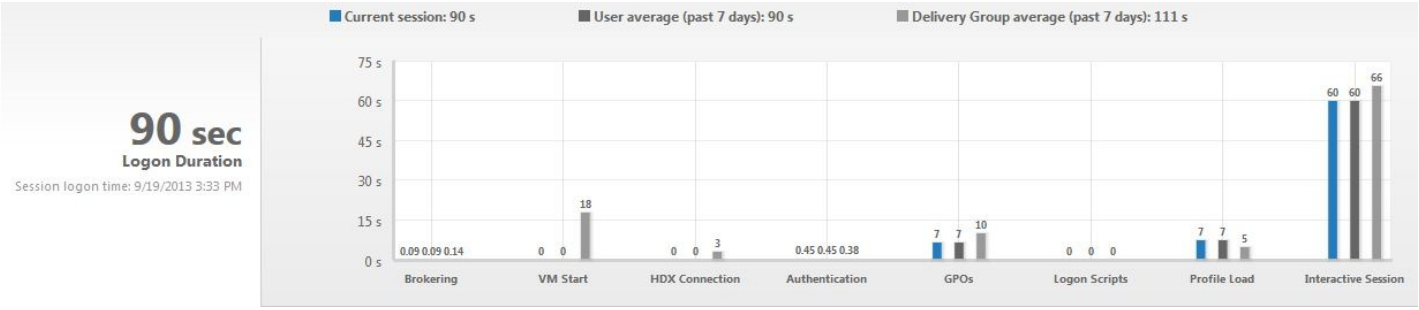
Scoutの使用と構成、および一般的な問題について詳しくは、CTX130147を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーログオンの問題の診断

Dec 05, 2017

ユーザーログオンの問題のトラブルシューティングを行うには、ログオン処理時間データを使用します。［ユーザーの詳細］ビューでは処理時間が数値として表示され、その下にログオンした時刻も示されます。また、ログオンプロセスの各フェーズのグラフも表示されます。



［ユーザーの詳細］ビューの［ログオン処理時間］パネル

ユーザーがXenAppおよびXenDesktopにログオンすると、Monitor Serviceにより、ユーザーがCitrix Receiverから接続した時点から、デスクトップが使用可能になった時点までのログオンプロセスの各フェーズが追跡されます。 左側の大きな数字は総ログオン時間であり、接続の確立およびDelivery Controllerからのデスクトップの取得にかかった時間と、仮想デスクトップの認証とログオンにかかった時間を合計して計算されます。処理時間の情報は、管理者のWebブラウザーのローカル時刻で秒単位（または秒の小数単位）まで表示されます。

ユーザーログオンの問題のトラブルシューティングを行うには、通常は次の手順を使用します。

1. ログオン状態のトラブルシューティングを行うには、**［ユーザーの詳細］**ビューの［ログオン処理時間］パネルを使用します。
   - ユーザーがログオン中の場合は、ここにログオンのプロセスが表示されます。
   - ユーザーがログオン済みの場合、ユーザーがそのセッションにログオンするときにかかった時間が［ログオン処理時間］パネルに表示されます。
2. ログオンプロセスの各フェーズを調査します。

ログオンプロセスのフェーズ	**説明**
仲介	ユーザーに割り当てるデスクトップを決定するのに要した時間です。
仮想マシンの起動	マシンの起動を必要とするセッションの場合、これは仮想マシンの起動にかかった時間です。
HDXコネクション	クライアントから仮想マシンへのHDX接続の設定で必要な手順を実行するためにかかった時間です。
認証	リモートセッションへの認証を実行するのにかかった時間

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	です。
GPO	仮想マシン上で［グループポリシー］設定が有効になっている場合、これはグループポリシーオブジェクトの適用にかかった時間です。
ログオンスクリプト	セッションでログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。
プロファイルロード	ユーザーまたは仮想マシンに対してプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。
対話型セッション	これは、ユーザープロファイルのロード後、キーボードやマウスの制御をユーザーに「渡す」までにかかった時間です。通常、ログオンプロセスのすべてのフェーズで最も長い時間であり、次のように計算されます。 対話型セッションの処理時間 = デスクトップ準備完了イベントのタイムスタンプ（VDAのEventId 1000）- ユーザープロファイルロード完了イベントのタイムスタンプ（VDAのEventId 2）

総ログオン時間は、これらの各フェーズを厳密に合計したものではありません。たとえば、複数のフェーズが並行して発生したり、一部のフェーズで追加処理が発生したりしてログオン処理時間が合計値よりも大きくなることがあります。

注：［ログオン処理時間］グラフには、ログオンフェーズが秒単位で表示されます。1秒未満の時間値はすべて、秒未満の値として表示されます。1秒を超える値は、0.5秒単位に丸められます。グラフは、Y軸の最高値を200秒として表示するように計計されています。200秒を超える値はすべて、実際の値を棒グラフの上に添えて表示されます。

グラフで異常または予期しない値を識別するには、現在のセッションの各フェーズで要した時間と、このユーザーの最近7日間の平均処理時間、およびこのデスクトップグループのすべてのユーザーの最近7日間の平均処理時間を比較します。

必要に応じて、担当管理者に報告します。たとえば、仮想マシンの起動に時間がかかり、ハイパーバイザーが問題の原因である可能性がある場合は、ハイパーバイザー管理者に問題を報告します。また、仲介処理に時間がかかる場合は、サイト管理者にDelivery Controllerの負荷分散のチェックを依頼します。

以下の問題について調査します。

- （現在の）ログオンを示すバーが表示されていない。
- 現在のログオン処理時間とこのユーザーの平均処理時間が大きく食い違う。次の原因が考えられます。
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムが更新された。
  - 構成が変更された。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロード時間が長くなります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ユーザーのログオン処理時間（現在値および平均値）とデリバリーグループの平均値が大きく食い違う。

必要な場合は、［**再起動**］をクリックしてユーザーに再ログオンしてもらい、仮想マシンの起動や仲介時に問題が発生するかどうかを確認します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーのシャドウ

Dec 05, 2017

Directorの ユーザーのシャドウ 機能を使用すると、ユーザーの仮想デスクトップまたはセッションを直接表示したり操作したりできます。 この機能を使用するには、そのマシンにユーザーが接続している必要があります。 ユーザーが接続している場合、ユーザーのタイトルバーにそのマシン名が表示されます。

1. ［ユーザーの 詳細］ビューで、ユーザーセッションを選択します。
2. 以下の操作で、 そのユーザーセッションに対するシャドウを開始します。
   - マシンを監視する場合は、 ［アクティビティマネージャー］ビューで ［シャドウ］をクリックします。
   - セッションを監視する場合は、 ［ユーザーの 詳細］ビューの ［セッション詳細］パネルで ［シャドウ］をクリックします。
3. 接続が初期化されると、 .msrcincidentファイルを開くか保存するかを確認するダイアログボックスが開きます。
4. デフォルトで選択されていない場合は、Remote Assistance Viewerでファイルを開きます。 ユーザーデバイス側には、確認のメッセージが表示されます。
5. ユーザーが ［はい］をクリックすると、マシンまたはセッションの共有が開始されます。

ユーザーがマウスやキーボードの制御を許可すると、管理者がシャドウセッションを制御できるようになります。

Microsoft Internet Explorerブラウザーでダウンロードしたマイクロソフトリモートアシスタンスファイル（msra）がリモートアシスタンスクライアントで自動的に開くように構成します。

これを行うには、グループポリシーエディターで [ファイルのダウンロード時に自動的にダイアログを表示] を有効にする必要があります。

［コンピューターの構成］ > ［管理用テンプレート］ > ［Windowsコンポーネント］ > ［Internet Explorer］ > ［インターネットコントロールパネル］ > ［セキュリティページ］ > ［インターネットゾーン］ > ［ファイルのダウンロード時に自動的にダイアログを表示］

デフォルトでは、ローカルイントラネットゾーンのサイトに対してこのオプションが有効になっています。Directorサイトがローカルイントラネットゾーンにない場合は、ローカルイントラネットゾーンに追加することを検討してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザーへのメッセージの送信

Dec 05, 2017

Directorでは、マシンに接続しているユーザーにメッセージを送信できます。たとえば、突発的にデスクトップの保守、ログオフ、再起動、プロファイルのリセットなどが必要になった場合に、ユーザーに緊急のメッセージを送信できます。

1. ［アクティビティマネージャー］ビューでユーザーを選択して、 ［詳細］をクリックします。
2. ［ユーザーの 詳細］ビューの ［セッション詳細］パネルで、 ［メッセージの 送信］をクリックします。
3. 送信する メッセージの ［件名］および ［メッセージ］を入力して、 ［送信］をクリックします。

メッセージが正しく送信されると、Directorに確認メッセージが表示されます。 マシンに接続しているユーザーにメッセージが表示されます。

メッセージの送信に問題が発生すると、Directorにエラーメッセージが表示されます。 そのエラーメッセージに従って問題を解決してください。 問題を解決したら、 件名およびメッセージを再入力して ［ 再試行］をクリックします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーションエラーの解決

Dec 05, 2017

［アクティビティマネージャー］ビューで［アプリケーション］タブをクリックします。ここでは、このユーザーがアクセスするすべてのマシン上のすべてのアプリケーションとその状態を確認できます。これには、現在接続しているマシンのローカルアプリケーションおよびホストされるアプリケーションが含まれます。

注：［アプリケーション］タブが灰色表示になっている場合は、このタブを有効にする権限を持つ管理者に問い合わせてください。

一覧には、セッション内で起動されたアプリケーションのみが表示されます。

サーバーOSマシンおよびデスクトップOSマシンでは、アプリケーションが切断セッションごとに一覧で表示されます。ユーザーが接続していない場合、アプリケーションは表示されません。

アクション	**説明**
応答していないアプリケーションを終了する	応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。アプリケーションが終了したら、ユーザーに再度起動するように通知します。
応答していないプロセスを終了する	必要な権限がある場合は、［プロセス］タブをクリックします。アプリケーションに関連するプロセス、またはCPUリソースやメモリを過度に消費しているプロセスを選択し、**［プロセスの終了］**をクリックします。 プロセスを終了するための権限がない場合、プロセスを終了することはできません。
ユーザーのマシンを再起動する	デスクトップOSマシンでは、選択したセッションで**［再起動］**をクリックします。 または、［マシンの詳細］ビューで電源制御を使ってマシンを再起動またはシャットダウンします。アプリケーションの状態を再確認するには、ユーザーに再度ログオンするように通知します。 サーバーOSマシンでは、［再起動］オプションを使用できません。代わりに、ユーザーをログオフして、再度ログオンさせます。
マシンをメンテナンスモードにする	パッチまたはそのほかの更新などによりマシンのイメージをメンテナンスする必要がある場合は、マシンをメンテナンスモードにします。**［マシンの詳細］**ビューで**［詳細］**をクリックして、メンテナンスモードのオプションをオンにします。担当の管理者に報告します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

デスクトップ接続の復元

Dec 05, 2017

Directorビューでは、タイトルバーにそのユーザーの接続状態が表示されます。

デスクトップ接続に問題が発生するとその原因が表示されるため、トラブルシューティング方法を判別することができます。

アクション	説明
マシンがメンテナンスモードでないことを確認する	［ユーザーの詳細］ページで、メンテナンスモードがオフであることを確認します。
ユーザーのマシンを再起動する	マシンを選択し、［再起動］をクリックします。ユーザーのマシンがCPUリソースを過度に消費しているためにマシンが応答しないまたは接続できない場合は、このオプションを使用します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの復元

Dec 05, 2017

セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、サーバーとユーザーデバイス間の通信が切断されます。

［ユーザーの詳細］ビューで、［セッション詳細］パネルのセッション障害のトラブルシューティングを実行します。現在のセッションがセッションIDで示され、詳細を確認できます。

アクション	説明
応答していないアプリケーションまたはプロセスを終了する	［Application］タブをクリックします。応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。同様に、応答していないプロセスを選択し、［プロセスの終了］をクリックします。また、メモリやCPUリソースを過度に消費しているプロセスを終了します。
Windowsセッションを切断する	［セッション制御］をクリックし、［切断］を選択します。このオプションは、仲介されたサーバーOSマシンに対してのみ使用できます。仲介されていないセッションでは無効です。
セッションからユーザーをログオフする	［セッション制御］をクリックし、［ログオフ］を選択します。

セッション障害が解決されたことを確認するために、ユーザーに再度ログオンさせます。また、ユーザーをシャドウしてセッションをより詳しく監視することもできます。

注：ユーザーデバイスでXenDesktop 7より前のバージョンのVDAが動作している場合、Directorはセッションに関する完全な情報を表示することができません。代わりに、情報を使用できないことを示すメッセージが表示されます。このメッセージは、［ユーザーの詳細］ページおよび［アクティビティマネージャー］に表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDXチャネルシステムレポートの生成

Dec 05, 2017

ユーザーのマシン上のHDXチャネルの状態を確認するには、[ユーザーの詳細] ビューの [HDX] パネルを使用します。このパネルは、HDXを使ってユーザーマシンに接続している場合にのみ操作できます。
情報を使用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分待つか、[更新] ボタンをクリックしてください。HDXデータはほかのデータより更新に時間がかかることがあります。

エラーまたは警告のアイコンをクリックすると、詳細が表示されます。

ヒント：このダイアログボックスでは、タイトルバーの左隅にある矢印をクリックしてほかのチャネルの情報を表示することもできます。
HDXチャネルシステムレポートは、主にCitrixサポートチームによるトラブルシューティング時に使用されます。

1. [HDX] パネルで、 [システムレポートのダウンロード] をクリックします。
2. 生成された XML形式のレポートファイルを表示したり保存したりできます。
   - XMLファイルを表示するには、 [開く] をクリックします。Directorに XMLファイルの内容が表示されます。
   - XMLファイルを保存するには、 [保存] をクリックします。 [名前を付けて 保存] ダイアログボックスで、ファイルの保存場所としてDirectorが動作するマシン上のフォルダーを指定します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personal vDiskのリセット

Dec 05, 2017

注意：Personal vDiskをリセットすると、設定がデフォルトの状態にリセットされ、そのディスク上のすべてのデータが削除されます。ただし、Personal vDiskのデフォルト設定（Cドライブからのプロファイルリダイレクトの設定）を変更しない限り、またはサードパーティ製プロファイル管理ソリューションを使用していない場合、Personal vDiskをリセットしてもプロファイルデータは保持されます。
Personal vDiskをリセットするには、そのPersonal vDiskを使用しているマシンが実行中である必要があります。ユーザーがログオンしていなくても構いません。

このオプションはデスクトップOSマシンに対してのみ使用できます。サーバーOSマシンでは無効です。

1. ［ヘルプ デスク］ビューでデスクトップOSマシンを選択します。
2. このビュー、 または ［ユーザーの詳細］ビューの ［個人設定］ パネルで、 ［Personal vDiskの リセット］をクリックします。
3. ［リセット］をクリックします。 ユーザーがログオフされることを警告する メッセージが表示されます。ログオンしていたユーザーは ログオフされ、マシンが再起動します。

リセットに成功すると、 ［ユーザーの 詳細］ビューの ［個人設定］パネルの ［Personal vDiskの状態］に ［実行中］と表示されます。リセットに失敗すると、 ［実行中］の右側に赤い Xが表示されます。この X上にマウスポインターを置くと、問題についての情報が表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ユーザープロファイルのリセット

Dec 05, 2017

注意：プロファイルをリセットすると、そのユーザーのフォルダーやファイルは保存され、新しいプロファイルにコピーされます。ただし、多くのユーザープロファイルデータは削除されます。たとえば、レジストリはリセットされ、アプリケーション設定も削除される場合があります。

1. Directorから、プロファイルをリセットするユーザーを検索し、このユーザーのセッションを選択します。
2. **[プロファイルのリセット]** をクリックします。
3. ユーザーに、すべてのセッションからログオフするように指示します。
4. ユーザーに再度ログオンするように指示します。ユーザープロファイルから保存されたフォルダーやファイルが新しいプロファイルにコピーされます。
   重要：複数のプラットフォーム上（Windows 8とWindows 7など）にユーザーのプロファイルが存在する場合は、問題が発生したデスクトップまたはアプリケーションに最初にログオンするよう指示します。これにより、正しいプロファイルがリセットされます。
   Citrixユーザープロファイルの場合、ユーザーのデスクトップが表示された時点でリセットされています。Microsoftの移動プロファイルの場合、フォルダーの復元処理に時間がかかる場合があります。この復元処理が完了するまで、ユーザーはログオンしていなければなりません。

注：これまでの手順では、XenDesktop（デスクトップVDA）を使用している前提になっています。XenApp（サーバーVDA）を使用している場合は、プロファイルのリセットを実行するためにログオンする必要があります。ユーザーはいったんログオフしてから再度ログオンし、プロファイルのリセットを完了させる必要があります。
プロファイルが正しくリセットされない場合（ユーザーがそのマシンに再ログオンできなかったり一部のファイルが見つからなかったりする場合など）、管理者が手作業で元のプロファイルを復元する必要があります。
ユーザーのプロファイルのフォルダーやファイルが保存され、新しいプロファイルにコピーされます。これらのフォルダーは、以下の順番でコピーされます。

- デスクトップ
- Cookies
- お気に入り
- ドキュメント
- マイピクチャ
- マイミュージック
- マイビデオ

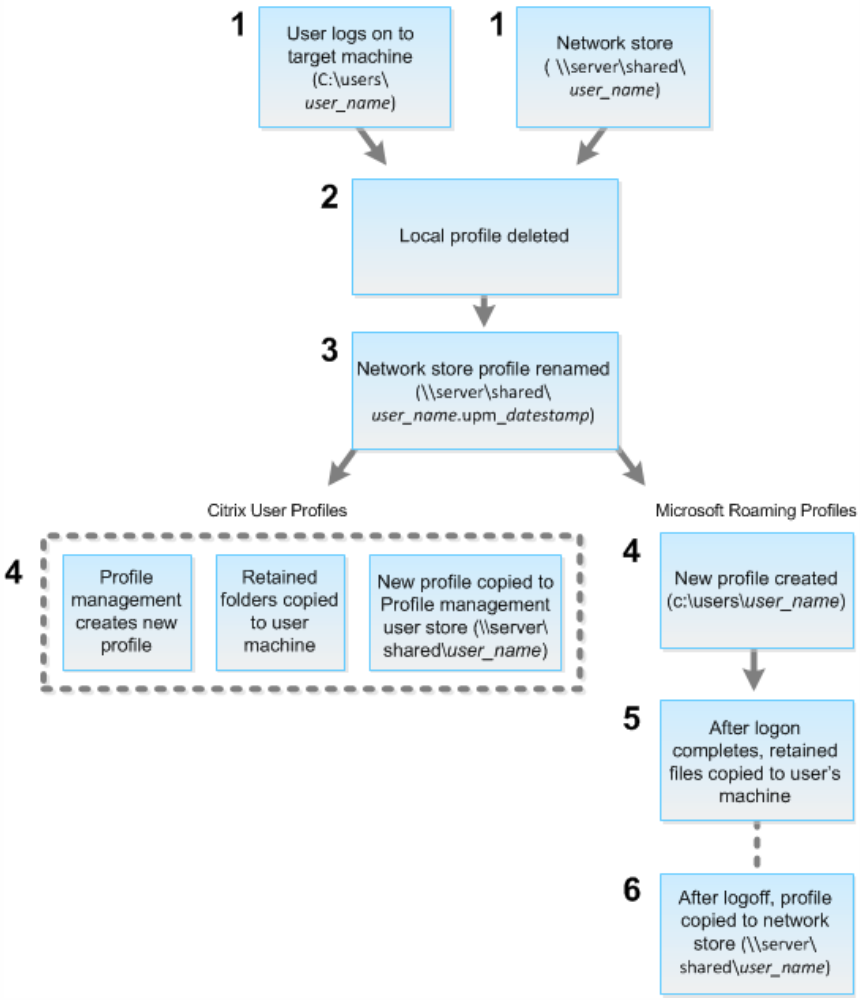
注：Windows 8以降では、プロファイルのリセット時にクッキーフォルダーはコピーされません。

リセットされたプロファイルはどのように処理されるか

いずれのCitrixユーザープロファイルまたはMicrosoft移動プロファイルもリセットできます。ユーザーがログオフした後に管理者がDirectorまたはPowerShell SDKでリセットコマンドを選択すると、使用されているユーザープロファイルが識別され、Directorにより適切なリセットコマンドが発行されます。DirectorはProfile managementを介してプロファイルのサイズ、種類、およびログオン時間などに関する情報を取得します。

これは、ユーザーログオン後の処理を説明した図です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Directorからのリセットコマンドにより、プロファイルの種類が指定されます。次に、Profile managementサービスによりその種類のプロファイルのリセットが試行され、適切なネットワーク共有（ユーザーストア）が検出されます。Profile managementにより処理されたユーザーのプロファイルに対して移動プロファイル用のコマンドが発行された場合は拒否されます（逆の場合も同様）。
2. ローカルプロファイルがある場合は削除されます。
3. ネットワークプロファイルの名前が変更されます。
4. 次の処理は、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoft移動プロファイルかにより異なります。
   - Citrixユーザープロファイルの場合、Profile managementのインポート規則によって新しいプロファイルが作成され、フォルダーがネットワークプロファイルにコピーされ、ユーザーは通常どおりにログオンできます。リセットに移動プロファイルが使用される場合は、移動プロファイル内のすべてのレジストリ設定がリセットプロファイル内に保持されます。
     注：必要な場合は、テンプレートプロファイルが移動プロファイルよりも優先されるようにProfile managementを構成することもできます。
   - Microsoft移動プロファイルの場合、Windowsにより新しいプロファイルが作成され、ユーザーがログオンするとフォルダーがユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルがネットワークストアにコピーされます。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーに、すべてのセッションからログオフするように指示します。
2. ローカルプロファイルが存在する場合はそれを削除します。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. ネットワーク共有上のアーカイブフォルダーを検索します。アーカイブフォルダーには、名前に日時と .upm_datestamp拡張子が含まれます。
4. 現在のプロファイルのフォルダー （拡張子 upm_datestampのないもの）を削除します。
5. アーカイブフォルダーの名前から日時拡張子を削除します。 プロファイルがリセット前の状態に戻りました。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

セッションの録画

Dec 05, 2017

Directorの［**ユーザーの詳細**］と［**マシンの詳細**］画面から、Session Recording制御を使って、ICAセッションを録画することができます。この機能は**Platinum**ライセンスを持つユーザーが使用できます。

DirectorConfigツールを使ってDirectorのSession Recordingを構成するには、「Session Recordingのインストール、アップグレード、およびアンインストール」の「Directorを構成してSession Recording Serverを使用する」を参照してください。
ログインユーザーにSession Recordingポリシーを変更する権限がある場合のみ、DirectorのSession Recording制御を使用できます。この権限は、「録画ポリシーの作成とアクティブ化」で説明されているように、Session Recording承認コンソールで設定できます。
注：DirectorまたはSession Recording Policy ConsoleによるSession Recordingの設定の変更は、次のICAセッションの起動時から有効になります。

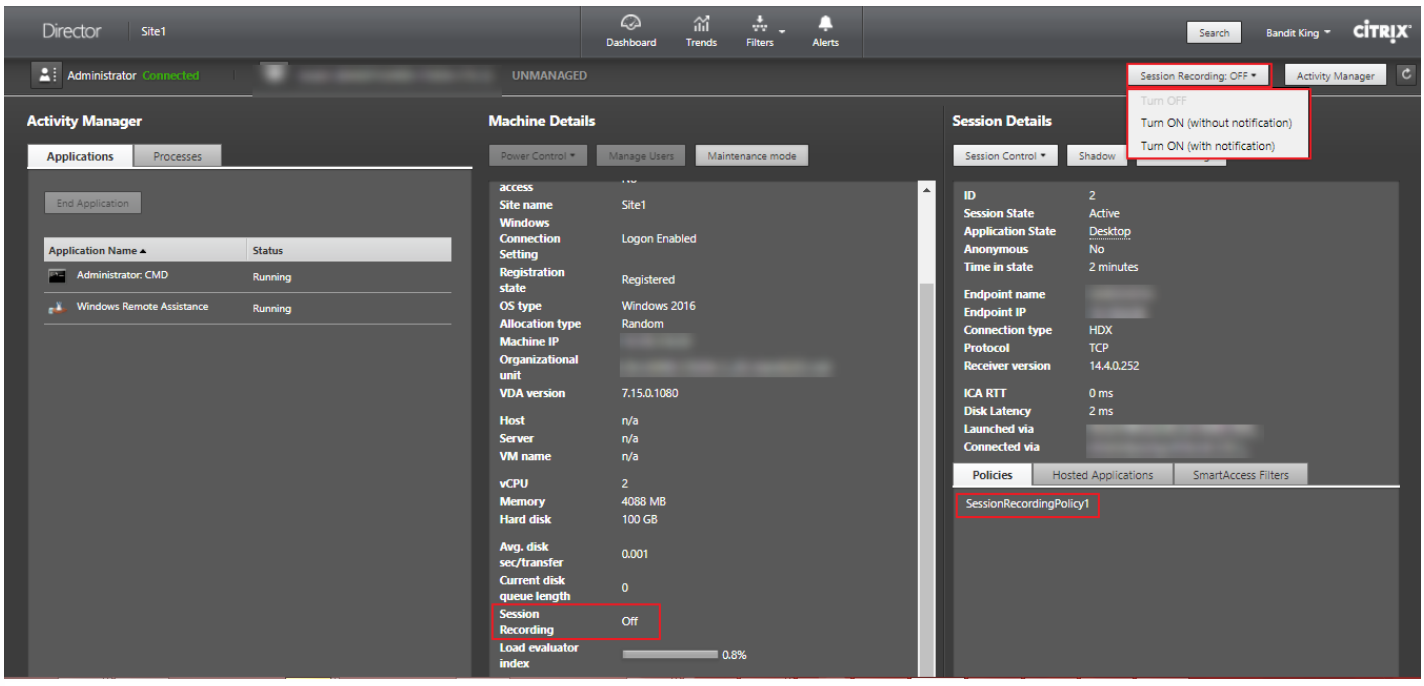
DirectorでのSession Recording制御

［**アクティビティマネージャー**］または［**ユーザーの詳細**］画面で、特定のユーザーに対してSession Recordingを有効にできます。サポートされるすべてのサーバーで特定のユーザーに対して以降のセッションが録画されます。

マシンの追加方法

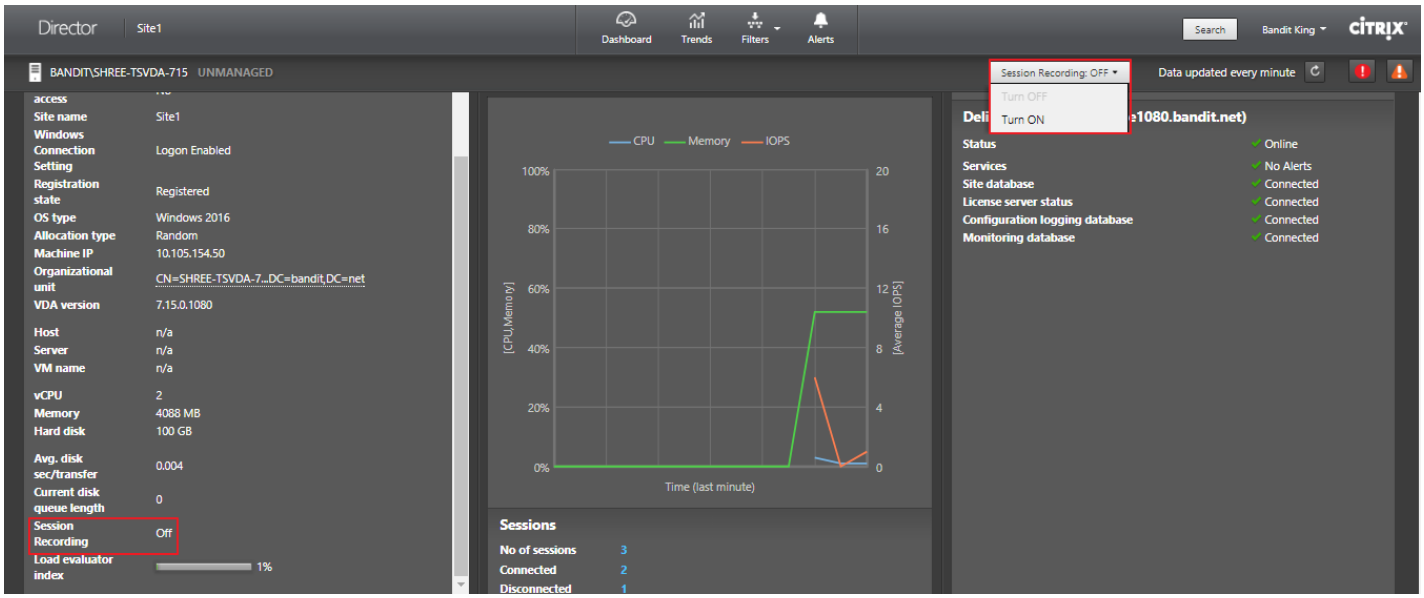
- オンにする（通知あり） - ICAセッションへのログオン時に録画されているセッションについてユーザーに通知されます。
- オンにする（通知なし） - ユーザーに通知されることなく、セッションは録画されます。
- オフにする - ユーザーのセッションの録画を無効にします。

ポリシーパネルには、アクティブなSession Recordingポリシーが表示されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

［マシンの詳細］ページから特定のマシンに対して、Session Recordingを有効にできます。そのマシンの以降のセッションが録画されます。［マシンの詳細］パネルには、そのマシンのSession Recordingポリシーの状態が表示されます。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

アプリケーションのトラブルシューティング

Dec 05, 2017

リアルタイムアプリケーション監視

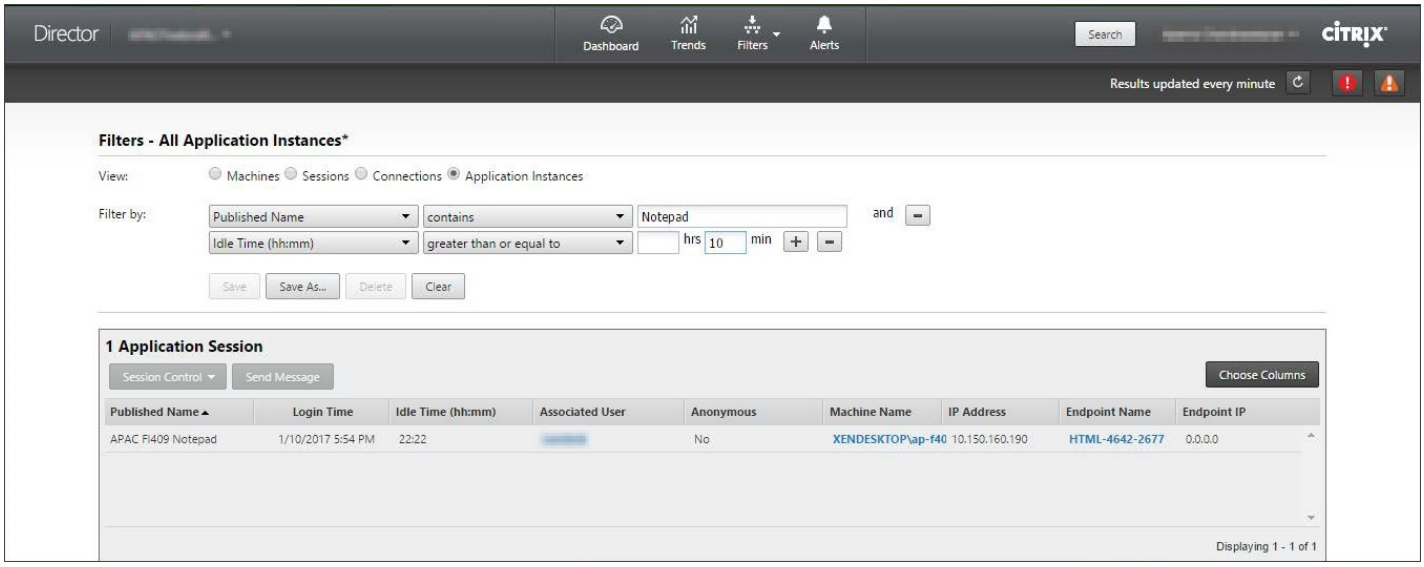
アイドル状態の時間の指標を使用して、特定の時間制限を超えてアイドル状態であるインスタンスを識別することで、アプリケーションとセッションをトラブルシューティングできます。

アプリケーションベースのトラブルシューティングの一般的な用途は、ヘルスケアのセクターです。このセクターでは、従業員間でアプリケーションライセンスが共有されています。このため、XenAppとXenDesktopの環境の削除、パフォーマンスの低いサーバーの再構成、またはアプリケーションの保守およびアップグレードを行うには、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

[アプリケーション インスタンス] フィルターページには、サーバーOS上とデスクトップOS上にあるVDAのすべてのアプリケーションインスタンスが表示されます。関連付けられたアイドル時間の測定値は、10分間以上アイドル状態になっているサーバーOSのVDAのアプリケーションインスタンスについて表示されます。

注：アプリケーションインスタンスの測定値は、すべてのライセンスエディションのサイトで確認できます。

一定時間以上アイドル状態になっているアプリケーションインスタンスを識別して、必要に応じてログオフするか接続を切断するためにこの情報を使用します。これを行うには、**[フィルター] > [アプリケーション インスタンス]** の順に選択し、保存済みのフィルターを選択するか **[すべてのアプリケーション インスタンス]** を選択し、独自のフィルターを作成します。



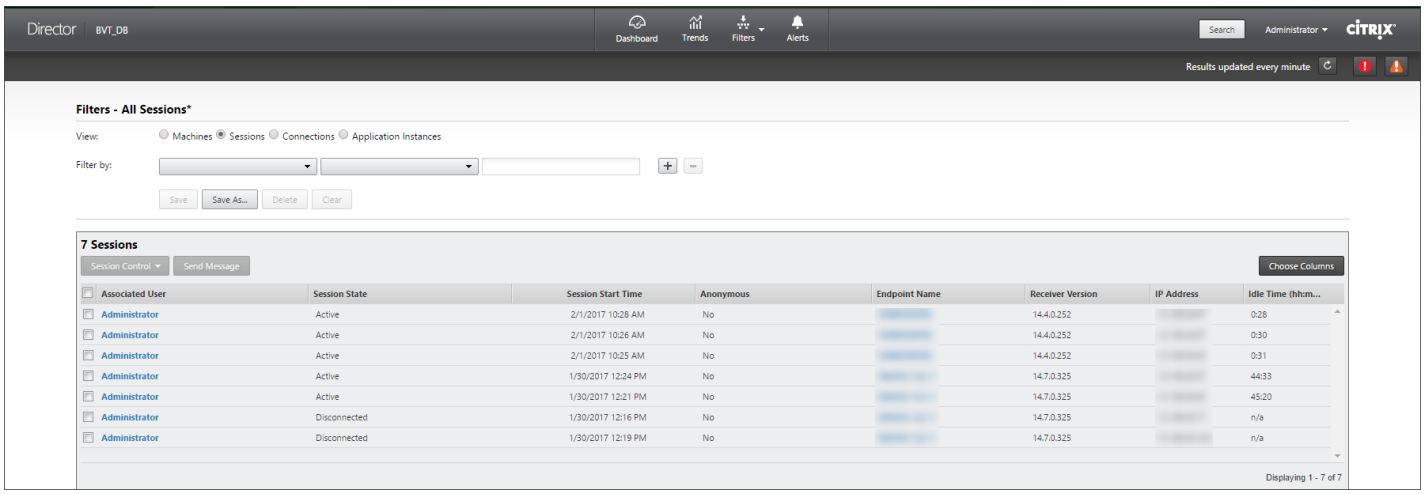
フィルターの例は次のようになります。**[フィルター基準]** 条件として **[公開名]**（アプリケーションの公開名）と **[アイドル時間]** を選択します。次に **[アイドル時間]** に **[次のもの以上]** を設定して特定の時間制限を指定、再利用のためのフィルターを保存します。フィルター後の一覧から、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**[セッション制御]** ドロップダウンリストから **[ログオフ]** または **[切断]** を選択してインスタンスを終了します。

注： ログオフするかアプリケーションインスタンスを切断すると、現在のセッションがログオフされるか切断されるため、同じセッションに属するすべてのアプリケーションインスタンスが終了されます。

[セッション] フィルターページでセッション状態とセッションのアイドル時間の指標を使用してアイドル状態のセッショ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ンを識別できます。 **[アイドル時間]** 列で並べ替えるか、特定の時間制限を超えてアイドル状態であるセッションを識別するフィルターを定義します。 アイドル時間は、10分間以上アイドル状態であるサーバーOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次のいずれかの場合、**[アイドル時間]** には **[なし]** と表示されます。

- アイドル状態の時間が10分未満の場合
- デスクトップOSのVDA上で起動されている場合
- バージョン7.12以前を実行するVDA上で起動されている場合

アプリケーション障害履歴の監視

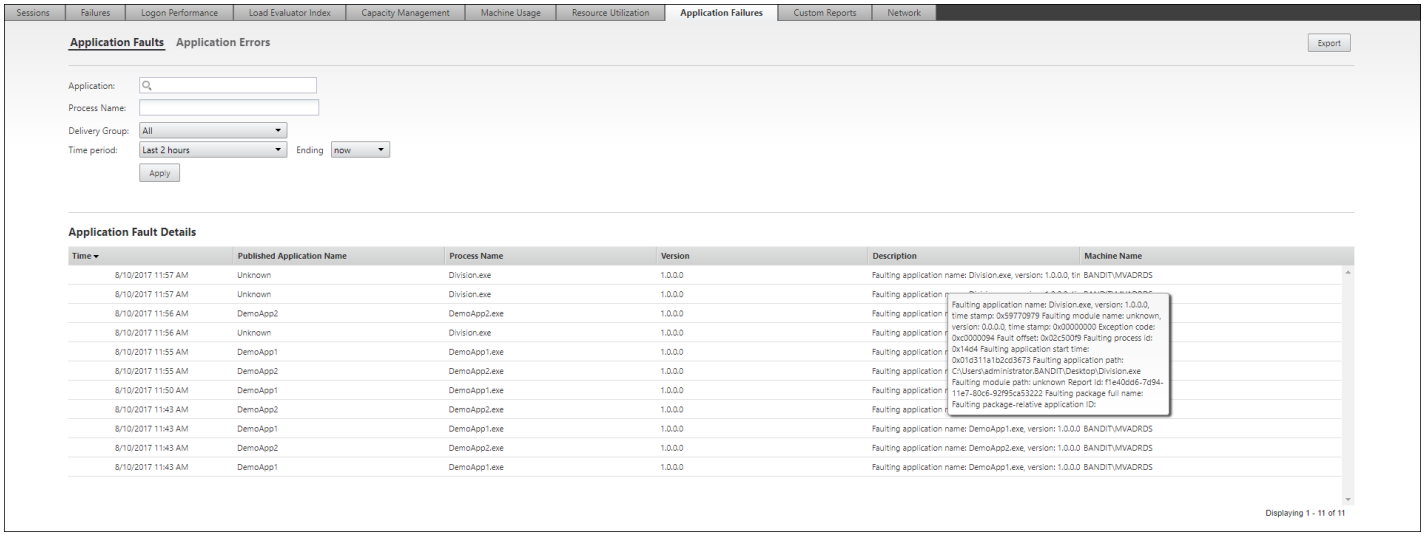
[傾向] -> **[アプリケーション障害]** タブで、 VDA上の公開アプリケーションに関連した障害が表示されます。

アプリケーション障害の傾向は、PlatinumおよびEnterprise Editionでは、過去2時間、24時間、7日間、および1か月間で使用できます。他のライセンスの種類では、過去2時間、24時間、および7日間で使用できます。ソースに「アプリケーションエラー」がある場合は、イベントビューアーに記録されているアプリケーション障害が監視されます。 **[エクスポート]** をクリックすると、CSV、Excel、またはPDFフォーマットのレポートが生成されます。

アプリケーション障害の監視についてのグルーミング保持の設定は、PlatinumおよびPlatinum Edition以外にはGroomApplicationErrorsRetentionDaysおよびGroomApplicationFaultsRetentionDaysがデフォルトで1日に設定されています。この設定は次のPowerShellのコマンドで変更できます。

Set-MonitorConfiguration -<設定名> <値>

© 1999-2017 Citrix Systems, Inc. All rights reserved.



障害はその重要度によって **[アプリケーション障害]** または **[アプリケーションエラー]** として表示されます。［アプリケーション障害］タブには、機能またはデータの損失に関連した障害が表示されます。［アプリケーションエラー］には、即座に関連しない問題が示されます。これは、将来問題が発生する可能性がある状況を意味しています。

障害は、**公開アプリケーション名**、**プロセス名**または**デリバリーグループ**、および**期間によってフィルターできます。**表には、障害またはエラーコードと簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

注：対応するアプリケーション名を派生できない場合、公開アプリケーション名は「不明」として表示されます。これは、通常、アプリケーションの起動がデスクトップセッションで失敗した場合、または依存している実行ファイルが原因で処理できない例外により失敗した場合に発生します。

デフォルトでは、サーバーOSのVDAでホストされたアプリケーションの障害のみが監視されています。アプリケーション障害の監視の有効化、デスクトップOSのVDA上のアプリケーション障害の監視の有効化、および障害の監視から除外されるアプリケーションの一覧の設定は、監視グループポリシーで変更が可能です。詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

マシンのトラブルシューティング

Dec 05, 2017

[フィルター] > [マシン] ビューで **[デスクトップOSマシン]** または **[サーバーOSマシン]** を選択して、サイトで構成されているマシンを表示します。［サーバーOSマシン］タブには負荷評価基準インデックスが表示されます。この測定値上にマウスポインターを置くと、各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。

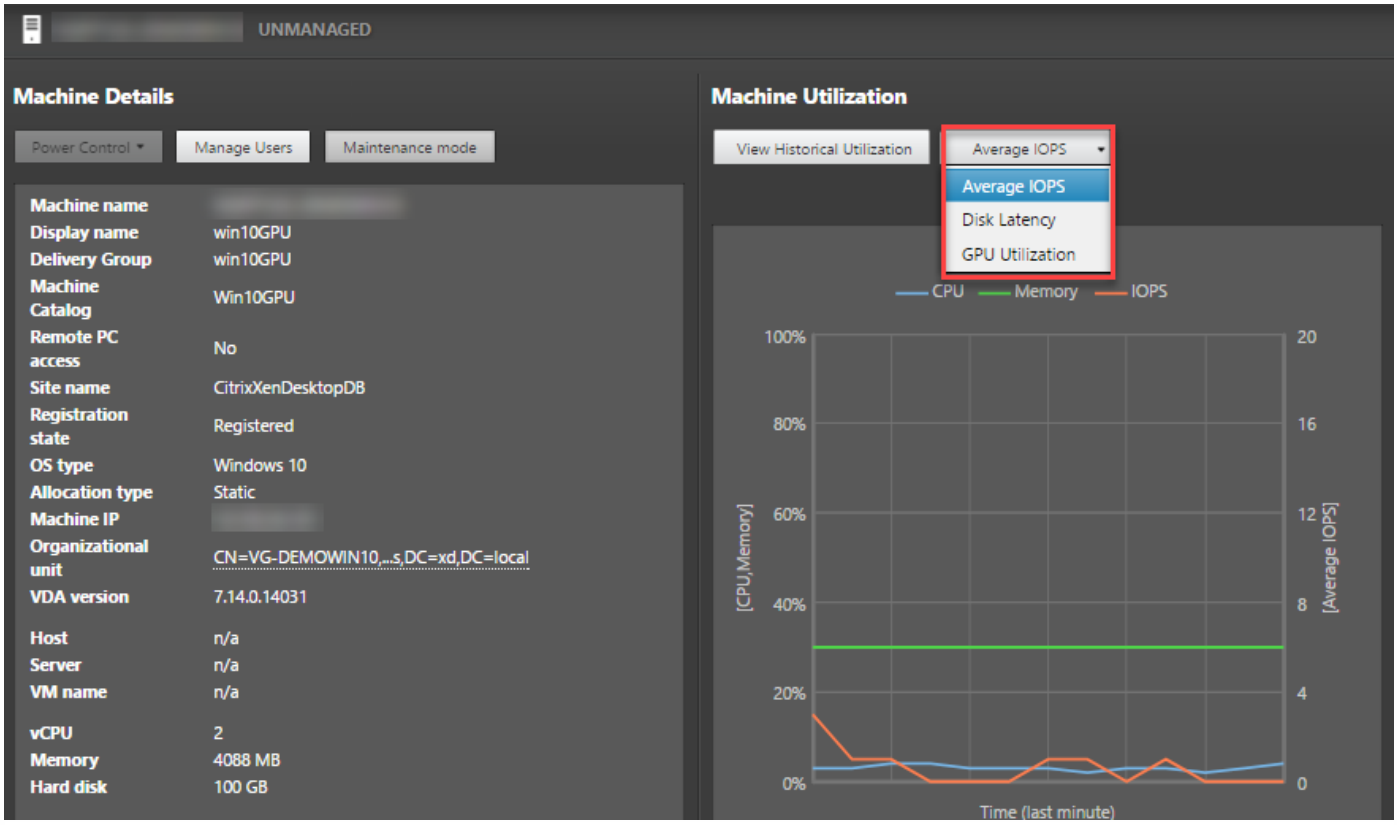
エラーが発生したマシンの **[エラーの理由]** をクリックすると、エラーの詳細な説明と推奨される解決手順が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、『Citrix Director 7.12 Failure Reasons Troubleshooting Guide』に記載されています。

マシン名のリンクをクリックし、**[マシンの詳細]** ページに移動します。［マシンの詳細］ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用済みのHotFixの詳細の一覧が表示されます。**[マシン稼働]** パネルには、マシンの稼働状況を示すグラフが表示されます。

マシンごとのリアルタイムのリソース使用状況

[マシン稼働] パネルには、CPUとメモリのリアルタイムの使用状況を示すグラフが表示されます。Delivery ControllerおよびVDAのバージョン**7.14**以降がインストールされているサイトでは、ディスクとGPUの監視グラフも表示されます。

重要なパフォーマンス測定値としてディスク監視グラフ、平均IOPS、ディスク遅延があり、VDAディスク関連の問題をモニターし解決する上で役立ちます。［平均IOPS］グラフには、ディスクの読み取りおよび書き込みの平均回数が表示されます。**[ディスク遅延]** を選択すると、データが要求されてディスクから返されるまでの時間をミリ秒単位で示すグラフが表示されます。



[GPU使用率] を選択するとGPU、GPUメモリ、およびエンコーダーとデコーダーの使用率がパーセント値として表示され、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

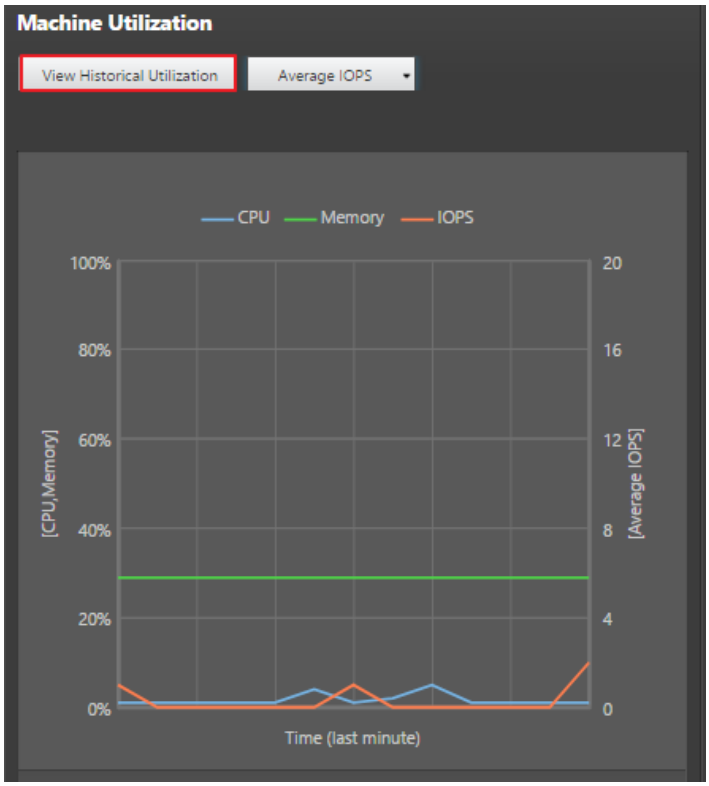
サーバーまたはデスクトップOSのVDAでのGPU関連の問題を解決できます。［GPU使用率］グラフは、NVIDIA Tesla M60 GPUを搭載した64ビットWindowsとDisplay Driverバージョン369.17以降が実行されているVDAでのみ使用できます。
VDAでGPUアクセラレーションを使用するには、HDX 3D Proを有効にする必要があります。詳しくは、「WindowsデスクトップOSのためのGPUアクセラレーション」および「WindowsサーバーOSのためのGPUアクセラレーション」を参照してください。
VDAが1つ以上のGPUにアクセスしている場合、［GPU使用率］グラフには個々のGPUから収集されたGPU測定値の平均が表示されます。GPU測定値は、個々のプロセスではなくVDA全体について収集されます。

マシンごとの過去のリソース使用状況

［マシン稼働］パネルの**［履歴使用率の表示］**をクリックすると、選択したマシンでの過去のリソースの使用状況を確認できます。
使用率グラフには、CPU、メモリ、最大同時セッション数、平均IOPS、ディスク遅延などの重要なパフォーマンス測定が表示されます。

注：データを収集して［マシン使用率の履歴］ページの［上位10位のプロセス］テーブルに表示するには、監視ポリシーの**［プロセスの監視を有効にします］**設定を［許可］に設定する必要があります。この設定はデフォルトでは［禁止］に設定されています。

デフォルトでは、CPUとメモリの使用率、平均IOPS、ディスク遅延に関するデータが収集されます。この収集は、**［リソースの監視を有効にします］**ポリシー設定で無効にできます。



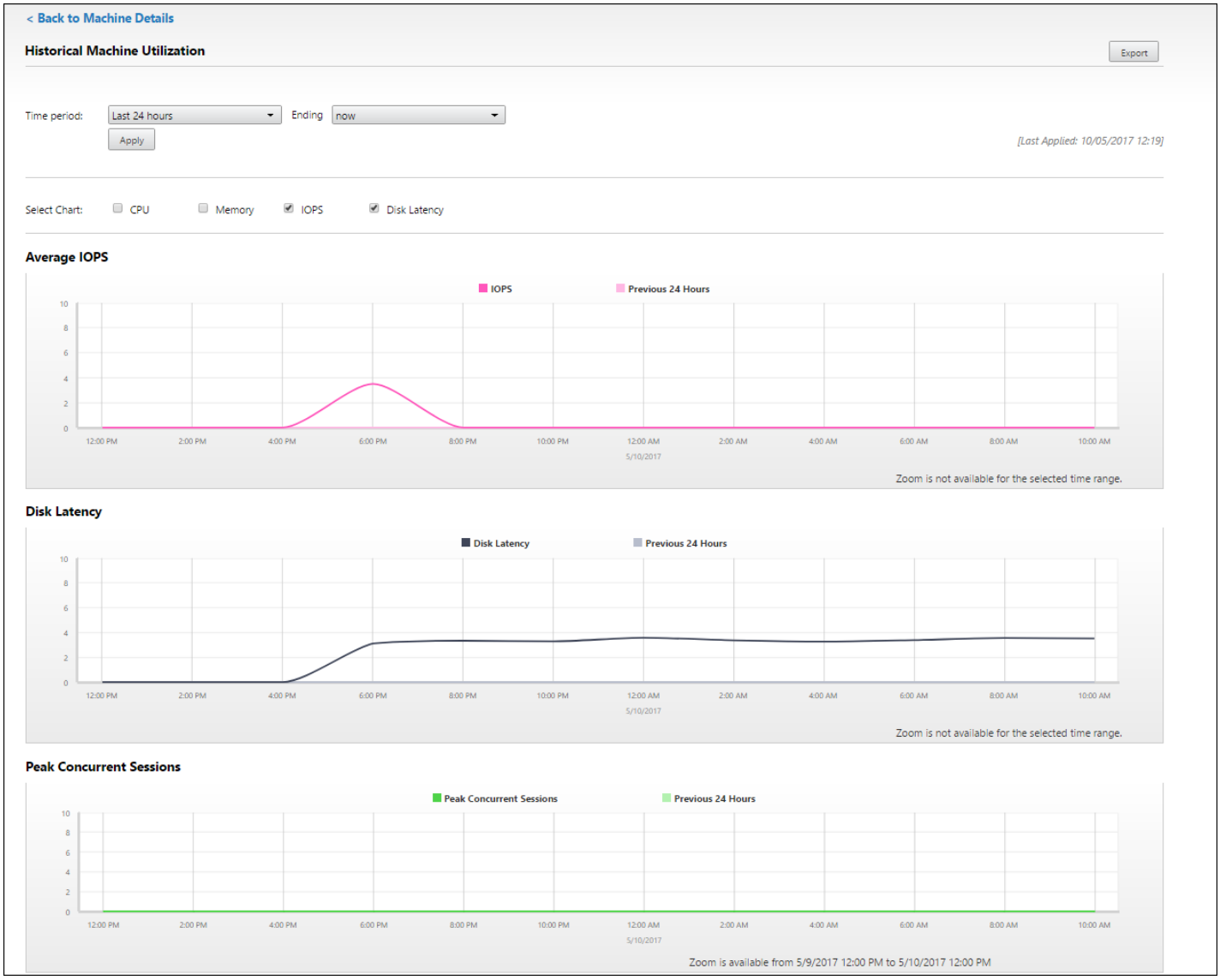
1. **［マシンの詳細］**ビューの**［マシン稼働］**パネルから、**［履歴使用率の表示］**を選択します。**［マシン使用率の履歴］**ページが開きます。

2. **［期間］**で、使用率を表示する期間を過去2時間、過去24時間、過去7日間、過去30日間、または過去1年から選択します。
注：現在、平均IOPSとディスク遅延のデータについては、過去24時間、過去30日間、過去1年についてのみ表示できます。カスタムの終了時刻は使用できません。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. **[適用]** をクリックして、目的のグラフを選択します。

4. グラフの他のセクションにマウスを合わせると、選択した期間の詳細が表示されます。



たとえば、 **[過去2時間]** を選択すると、基準期間は選択した時間範囲の2時間前になります。過去2時間と基準期間のCPU、メモリ、およびセッションの傾向を表示します。
[過去30日間] を選択すると、基準期間は先月になります。これを選択すると、先月から基準日時までの平均IOPSおよびディスク遅延が表示されます。

5. 選択した期間のリソース使用状況データをエクスポートするには、**[エクスポート]** をクリックします。詳しくは、「展開環境の監視」の「レポートのエクスポート」セクションを参照してください。

6. グラフの下には、CPUとメモリの使用率が上位10位のプロセスを示すテーブルが表示されます。選択した時間範囲のアプリケーション名、ユーザー名、セッションID、平均CPU、ピーク時のCPU、平均メモリ、ピーク時のメモリが表示される列から任意の列を選択してソートできます。［平均IOPS］列と［ディスク遅延］列は並び替えできません。

注：システムプロセスのセッションIDは「0000」と表示されます。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 特定プロセスのリソース消費に関する履歴傾向を表示するには、上位10位のプロセスから任意のプロセスを選択してドリダウンします。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

機能互換性マトリックス

Dec 05, 2017

各サイトでは、VDAやDelivery Controllerの以前のバージョンを使用できますが、Directorの最新バージョンの機能の一部が使用できない場合があります。さらに、機能が使用できるかどうかは、サイトのライセンスエディションによって異なります。Director、Delivery Controller、VDAは同じバージョンを保有されることをお勧めします。

注: Delivery Controllerのアップグレード後にStudioを開くと、サイトのアップグレードを要求するメッセージが表示されます。詳しくは、「**アップグレードの順序**」（「環境のアップグレード」セクション）を参照してください。

以下の表は、Directorの機能と、Delivery Controller（DC）、VDA、およびライセンスエディションで必要なその他の従属コンポーネントの最小バージョンの一覧です。

Directorのバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.15	アプリケーション障害の監視	DC 7.15 || VDA 7.15	すべて
7.14	アプリケーションを中心としたトラブルシューティング	DC 7.13 || VDA 7.13	すべて
	ディスクの監視:	DC 7.14 || VDA 7.14	すべて
	GPUの監視		
7.13	アプリケーションを中心としたトラブルシューティング	DC 7.13 || VDA 7.13	Platinum
	［セッション詳細］パネル上のトランスポートプロトコル	DC 7.x || VDA 7.13	すべて
7.12	ユーザーフレンドリな接続およびマシンの障害の説明	DC 7.12 || VDA 7.x	すべて
	Enterprise Editionでの履歴データ提供期間の延長		エンタープライズ
	カスタムレポート		Platinum
	SNMPトラップによるDirector通知の自動化		Platinum

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.11	リソース使用レポート	DC 7.11 || VDA 7.11	すべて
	CPU、メモリ、ICA RTTの状況に拡張されたアラート		Platinum
	エクスポートレポートの改善	DC 7.11 || VDA 7.x	すべて
	Citrix OctobluによるDirector通知の自動化		Platinum
	NetScaler MASとの統合	DC 7.11 || VDA 7.x || MASバージョン11.1ビルド49.16	Platinum
7.9	ログオン処理時間	DC 7.9 || VDA 7.x	すべて
7.7	予見的な監視およびアラート	DC 7.7 || VDA 7.x	Platinum
	SCOM統合	DC 7.7 || VDA 7.x || SCOM 2012 R2 || PowerShell 3.0以降*	Platinum
	Windows認証統合	DC 7.x || VDA 7.x	すべて
	デスクトップOSおよびサーバーOSの使用状況	DC 7.7 || VDA 7.x	Platinum
7.6.300	Framehawk仮想チャネルのサポート	DC 7.6 || VDA 7.6	すべて
7.6.200	セッションの録画の統合	DC 7.6 || VDA 7.x	Platinum
7	HDX Insightの統合	DC 7.6 || VDA 7.x || NetScaler Insight Center	Platinum

© 1999-2017 Citrix Systems, Inc. All rights reserved.

データの粒度と保持

May 07, 2018

データ値の集計

Monitor Serviceは、ユーザーセッション使用状況、ユーザーログオンの処理性能の詳細、セッションの負荷分散の詳細、および接続とマシンのエラー情報を含む、さまざまなデータを収集します。 データはカテゴリにより異なる方法で集計されます。OData Method APIを使って示されたデータ値の集計を理解することは、データの解釈に不可欠です。 次に例を示します。

- 接続セッション（Connected Session）やマシンエラー（Machine Failure）は一定の期間の状態を示すため、その期間内の最大値として公開されます。
- ログオン期間（LogOn Duration）は時間の長さを示す指標であるため、期間内の平均として公開されます。
- ログオン数（LogOn Count）および接続障害（Connection Failure）は一定の期間に発生した数を示し、期間内の合計値として公開されます

同時接続データの評価

重複しているセッションは同時発生していると考える必要があります。 ただし、間隔として1分を指定した場合、1分以内に発生するすべてのセッションは（重複しているかしていないかに関係なく）すべて同時であるとみなされます。つまり、間隔のサイズが非常に小さいため、精度の計算に関係するパフォーマンス上のオーバーヘッドを考慮する必要はありません。 2つのセッションがその1時間内の別々の1分間に発生する場合、それらは重複しているとはみなされません。

サマリーテーブルと生データの相関関係

データモデルでは、以下の2つの方法でメトリックスが示されます。

- サマリーテーブルでは、分単位、時間単位、および日単位のメトリックスを集計したものが示されます。
- 生データは、セッション、接続、アプリケーション、およびそのほかのオブジェクト内で記録された個々のイベントまたは現在の状態を示します。

データをAPIコール間またはそのデータモデル内で関連付けるときは、以下の概念および制限事項を考慮してください。

- **未完の間隔にはサマリーデータがありません。** メトリックスサマリーは長時間での履歴 傾向を示すためのものであり、完結した間隔のサマリーテーブルに集計されます。 データ収集の開始時や終了時のサマリーデータはありません。 1日（間隔=1440）の集計値の場合、最初と最後の未完の1日にはデータがないことを意味します。 これらの未完の間隔に生データが存在しても、そのデータが集計されることはありません。 各データ粒度の最初と最後の集計間隔は、各サマリーテーブルから最小と最大のSummaryDateを取得することで決定できます。 SummaryDate列は、間隔の開始時を示します。Granularity列はその集計データの間隔の長さを示します。
- **時間による関連付け。** 前述のように、メトリックスは完結した間隔のサマリーテーブルに集計されます。 これらの値は履歴傾向を知る目的で使用できますが、生イベントの方が集計された値よりも傾向分析に適切な状態を示している場合があります。 集計値と生データとを時間ベースで比較する場合、未完の間隔や間隔の最初と最後にサマリーデータがないことを考慮する必要があります。
- **欠落イベントまたは潜在 イベント** 集計期間で欠落または潜在しているイベントがあると、サマリーテーブルに集計されたメトリックスが正確でない場合があります。 Monitor Serviceでは現在の状態の正確な維持が試行されますが、過去にさかのぼって欠落イベントや潜在イベントをサマリーテーブルに再集計することはありません。
- **接続の高 可用性。** 接続の高可用性により、現在の接続のサマリーデータ数に差異が生じることがありますが、セッションインスタンスは生データ内で実行されています。
- **データの保持期間。** サマリーテーブルのデータは、生イベントデータとは異なるクリーンアップ（グルーミング）スケジュールで保持されます。 このため、サマリーテーブルまたは生テーブルのクリーンアップにより、データが消去されている場合があります。 データの保持期間は、サマリーデータの粒度によっても異なる場合があります。 低い粒度（分単

© 1999-2017 Citrix Systems, Inc. All rights reserved.

位）のデータは、高い粒度（日単位）のデータよりも早くクリーンアップされます。 特定の粒度のデータが消去されていても、より高い粒度のデータが存在している場合があります。 APIコールでは指定した粒度のデータのみが返されるため、データを取得できない場合でもその期間内のより高い粒度では取得できることがあります。

- **タイムゾーン。**格納されるメトリックスのタイムスタンプではUTCが使用されます。 サマリーテーブルは1時間区切りのタイムゾーンごとに集計されます。 1時間区切りのタイムゾーンに属さない場合は、データの集計先に不整合が生じることがあります。

データの粒度と 保持

Directorで取得される集計データの粒度は、要求された時間（T）の関数です。 以下の規則があります。

- 0 < T <= 1 時間の場合は分単位の粒度
- 0 < T <= 30日の場合は時間単位の粒度
- T > 31日 の場合は日単位の粒度

集計データから取得されないデータを要求すると、生のセッション（Session）および接続（Connection）情報から取得されます。このデータの量はすぐに大きくなるため、専用のスケジュールでクリーンアップされます。クリーンアップにより、意味のあるデータのみが長期間保持されます。これにより、レポートに必要な粒度を維持しながら良好なパフォーマンスが提供されます。Platinum Editionでは、クリーンアップが開始されるまでの日数をカスタマイズできます。

設定にアクセスするには、Delivery Controllerで以下のPowerShellコマンドを実行します。

コマンド　コピー

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -<setting name> <value>
```

クリーンアップは以下の設定により制御されます。

	設定名	対象データ	デフォルト値（Platinum、日数）	デフォルト値（Platinum以外、日数）
1	GroomSessionsRetentionDays	セッション終了後のセッションレコードと接続レコードの保有	90	7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2	GroomFailuresRetentionDays	MachineFailureLogレコードおよびConnectionFailureLogレコード	90	7
3	GroomLoadIndexesRetentionDays	LoadIndexレコード	90	7
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるMachineエンティティ、Catalogエンティティ、DesktopGroupエンティティ、およびHypervisorエンティティ。 関連するSessionレコード、SessionDetailレコード、Summaryレコード、Failureレコード、またはLoadIndexレコードも削除されます。	90	7
5	GroomSummariesRetentionDays	DesktopGroupSummaryレコード、FailureLogSummaryレコード、およびLoadIndexSummaryレコード。集計データ（日単位）	90	7
6	GroomMachineHotfixLogRetentionDays	VDAマシンおよびControllerマシンに適用されたHotfix	90	90
7	GroomMinuteRetentionDays	集計データ（分単位）	3	3
8	GroomHourlyRetentionDays	集計データ（時間単位）	32	7
1041	GroomApplicationInstanceRetentionDays	アプリケーションインスタンスの履歴	90	0

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10	GroomNotificationLogRetentionDays	通知ログレコード	90	
11	GroomResourceUsageRawDataRetentionDays	リソース使用率データ（生データ）	1	1
12	GroomResourceUsageMinuteDataRetentionDays	リソース使用率サマリーデータ（分単位）	7	7
13	GroomResourceUsageHourDataRetentionDays	リソース使用率サマリーデータ（時間単位）	30	7
14	GroomResourceUsageDayDataRetentionDays	リソース使用率サマリーデータ（日単位）	90	7
35	GroomProcessUsageRawDataRetentionDays	プロセス使用率データ（生データ）	1	1
16	GroomProcessUsageMinuteDataRetentionDays	プロセス使用率データ（分単位）	3	3
17	GroomProcessUsageHourDataRetentionDays	プロセス使用率データ（時間単位）	7	7
18	GroomProcessUsageDayDataRetentionDays	プロセス使用率データ（日単位）	30	7
19	GroomSessionMetricsDataRetentionDays	セッションメトリクスデータ	7	7
20	GroomMachineMetricDataRetentionDays	マシンメトリクスデータ	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	マシンメトリクスサマリーデータ	90	7
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

23	GroomApplicationFaultsRetentionDays	アプリケーション障害データ	1	1

注意：Monitor Serviceデータベースの値を変更した後でその値を適用するには、このサービスを再起動する必要があります。Monitor Serviceデータベースの値の変更は、Citrixサポート担当者からの指示があった場合のみ行ってください。

クリーンアップ（グルーミング）保持についての注意事項：

- Platinumライセンスがあるサイト – 前述のクリーンアップ保持設定を任意の日数更新できます。
  - 例外：GroomApplicationErrorsRetentionDaysおよびGroomApplicationFaultsRetentionDaysでは、31日間に制限されています。
- Enterpriseライセンスがあるサイト – すべての設定のクリーンアップ保持は31日間に制限されています。
- その他すべてのサイト – すべての設定のクリーンアップ保持は7日間に制限されています。

データを長期間保持すると、テーブルのサイズについて以下の影響が発生することがあります。

- **時間単位のデータ。**時間単位のデータを2年などの長期間保持すると、1000個のデリバリーグループがあるサイトではデータベースが以下の数式に基づいて増大します。
  「1000個のデリバリーグループ×24時間/日×365日/年×2年＝17,520,000行のデータ」集計テーブルのデータ量が多いため、パフォーマンスに大きな影響を及ぼします。ダッシュボードのデータがこのテーブルから取得されることを考慮すると、データベースサーバーに対する要求は高くなります。データ量が過度に多いと、パフォーマンスが大きく低下します。

- **セッションとイベントのデータ。**各セッションの開始時および接続/再接続時に収集されるデータです。大規模サイト（100,000ユーザーなど）では、このデータの量が急速に増加します。たとえば、これらのテーブルでは2年間で1TB以上のデータが保持され、高性能なエンタープライズレベルのデータベースが必要になります。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SDKおよびAPI

Dec 05, 2017

このリリースでは、複数のSDKおよびAPIを使用できます。詳しくは、開発者用のドキュメントを参照してください。そこから以下についてのプログラミングのための情報にアクセスできます。

- Delivery Controller
- Monitor Service OData
- StoreFront

Citrix Group Policy SDKにより、グループポリシーの設定およびフィルターを表示して構成できます。PowerShellプロバイダーを使用して、マシン、ユーザー設定、およびフィルターに対応する仮想ドライブを作成します。このプロバイダーは、New-PSDriveに対する拡張として表示されます。Group Policy SDKを使用するには、StudioまたはXenApp/XenDesktop SDKのいずれかをインストールする必要があります。詳しくは、「グループポリシーSDK」を参照してください。

Delivery Controller SDK。

このSDKは、Delivery ControllerまたはStudioと一緒にインストールされる多くのPowerShellスナップインで構成されています。

権限：シェルまたはスクリプトを実行するには、Citrix管理者の権限が必要です。Controllerのローカル管理者グループのメンバーには、XenAppまたはXenDesktopのインストールに必要な完全な管理権限が自動的に付与されますが、ローカル管理者アカウントを使うのではなく、適切な権限を持つCitrix管理者を作成することをお勧めします。Windows Server 2008 R2を実行している場合、ローカル管理者グループのメンバーとしてではなく、Citrix管理者としてシェルまたはスクリプトを実行する必要があります。

コマンドレットにアクセスして実行するには

1. PowerShellのシェルを開きます。 Studioを開き、［**PowerShell**］タブを選択して［**PowerShell の起動**］をクリックします。
2. スクリプト内でSDKコマンドレットを使用するには、PowerShell実行ポリシーを設定する必要があります。PowerShell実行ポリシーについて詳しくは、Microsoft社のドキュメントを参照してください。
3. Windows PowerShellコンソールで**Add-PSSnapin**コマンドレットを使って、必要なスナップインをPowerShell環境に追加します。

   V1およびV2は、スナップインのバージョンを示します（XenDesktop 5スナップインはV1、XenDesktop 7スナップインはV2です。たとえば、XenDesktop 7スナップインをインストールするには、コマンドAdd-PSSnapin Citrix.ADIdentity.Admin.V2を実行します）。すべてのコマンドレットをインポートするには、コマンドAdd-PSSnapin Citrix.*.Admin.V*を実行します。

スナップインを追加した後、コマンドレットおよび関連ヘルプにアクセスできるようになります。

注： 最新のXenAppおよびXenDesktop PowerShellコマンドレットヘルプを確認するには、次の手順に従います。

1. PowerShellコンソールからCitrixスナップイン：Add –PSSnapin Citrix.*.Admin.V*を追加します。
2. 「PowerShell Integrated Scripting Environment（ISE）」の手順に従ってください。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

グループポリシーSDK

Group Policy SDKを使用するには、StudioまたはXenApp/XenDesktop SDKのいずれかをインストールする必要があります。

グループポリシーSDKを追加するには、コマンド**Add-PSSnapin citrix.common.grouppolicy**を実行します（ヘルプにアクセスするには、「**help New-PSDrive -path localgpo:/**」と入力します）。

仮想ドライブを作成して設定を読み込むには、**コマンドNew-PSDrive [-PSProvider] CitrixGroupPolicy -Controller を実行します。**ここで、は接続して設定を読み込むサイトのControllerの完全修飾ドメイン名です。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenAppおよびXenDesktop 7.15 LTSRのCitrix VDIベストプラクティス

Jan 19, 2018

PDF Citrix VDI Handbook and Best Practices

In traditional business environments, workers suffer from productivity loss in many ways, including downtime during PC refreshes, patches and updates, or simply when they are away from the office. Application and desktop virtualization centralizes apps and desktops in the datacenter, rather than on local devices. This allows IT to deliver apps and desktops to users on demand, to any device, anywhere.

Take the following response from a desktop virtualization user:

Experience from the Field

"As a remote employee for [company], I struggled every time I needed to access the company's intranet, which forced me to VPN into the network. I also kept data on my local device because trying to access it over my broadband connection was too slow. Some coworkers did the same and lost data due to a virus, thankfully I was luckier.

Depending on my mood (and the weather), changing devices and locations was a challenge as I had to have my applications and data copied to many different endpoints. I know this was unsecure, but I didn't care because I was more concerned with flexibility.

Since moving to a virtual desktop, I'm able to use any device. I'm able to work from any location. And best of all, I don't have to worry about copying my data and applications onto all of my personal devices."

Unfortunately, organizations sometimes struggle to achieve this level of success. Why does one organization succeed while another organization struggles?

If we compare the factors between success and failure between desktop virtualization and other technology related projects, we see that there is little difference:

Lack of justification – Without a solid business reason, desktop virtualization is simply a new way to deliver a desktop. A business justification gives the project team a goal to strive towards.

Lack of a methodology – Many people who try and struggle to deploy a desktop virtualization solution do so because they jump right in without understanding or implementing the appropriate prerequisites. A structured methodology provides the path for the project.

Lack of experience – For many who embark on a desktop virtualization project, there is a lack of experience, which creates a lack of confidence in the design. Architects begin to second-guess themselves and the project stalls.

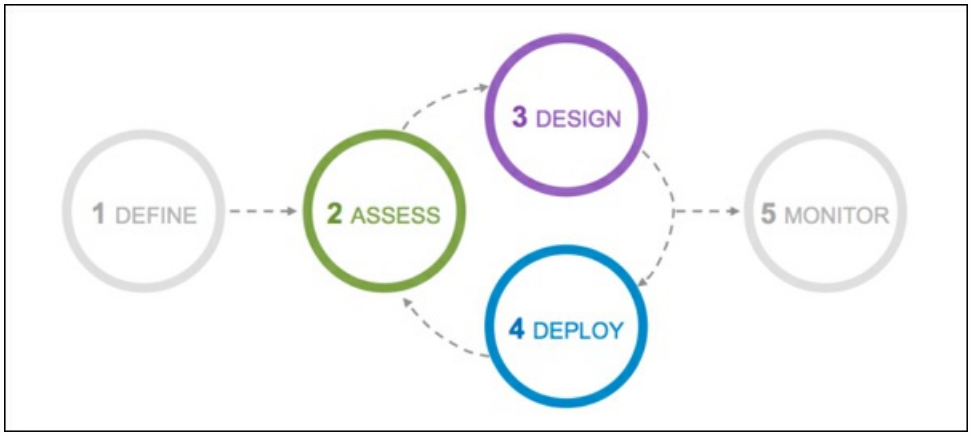
Our hope is that this handbook can alleviate the anxiety associated with desktop virtualization by showing how challenges can be resolved in a manner that is technically sound, but also feasible and effective for organizations facing deadlines and other organizational challenges.

Citrix has successfully employed the methodology, experience and best practices shared within this handbook across thousands of desktop virtualization projects.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Methodology

The Citrix VDI Handbook follows the Citrix Consulting methodology. A proven methodology that has been successfully employed across thousands of desktop virtualization projects. Each phase includes guidance on the important questions to ask, what tools to use and tips to help you succeed. The Citrix Consulting methodology consists of five phases:



1. Define – Builds the business case for desktop virtualization by creating a high-level project roadmap, prioritizing activities and estimating storage and hardware requirements.

2. Assess – Key business drivers are rated so that work effort can be prioritized accordingly. In addition, the current environment is reviewed for potential problems and to identify use cases for the project. This information will be used to set the direction of the Citrix deployment, upgrade, or expansion.

3. Design – Define architecture required to satisfy key business drivers and success criteria identified during the assess phase. Topics such as environment scalability, redundancy and high availability are addressed.

4. Deploy – During the deploy phase, the infrastructure is installed and configured as described in the design phase. All components of the infrastructure should be thoroughly unit and regression tested before users are provided with access to the environment.

5. Monitor – Define architectural and operational processes required to maintain the production environment.

The Citrix Consulting methodology follows an iterative Assess > Design > Deploy process for each major initiative of your project. In doing so, your organization is left with tangible improvements to the environment at the end of each engagement. For example, high priority user groups can progress through the assess, design and deploy phases earlier than other user groups.

> **注意**
>
> The VDI Handbook provides content on the Assess, Design and Monitor phases of the Citrix Consulting methodology.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

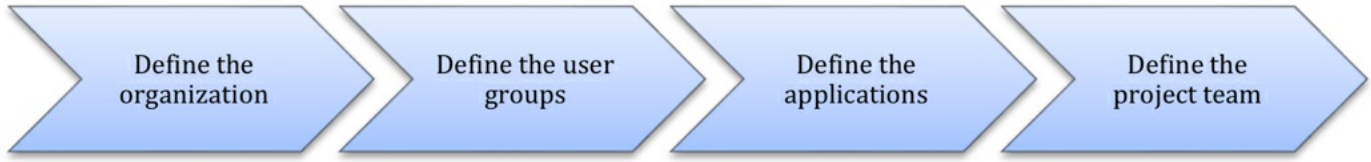
Assess

Jan 29, 2018

Creating an app and desktop delivery solution begins with a proper assessment. Architects that fail to properly assess the current environment find that they require the assess information later on, forcing them to backtrack, which can potentially stall and put the project at risk.

By gathering all of the information from the outset, the architect will gain an appreciation for the current environment and be able to work from the beginning on properly aligning business and user requirements with the overall solution.

The assess phase is a four-step, simple to follow process:



Step 1: Define the Organization

The first step in your virtual desktop project should be to understand and prioritize the strategic imperatives of the organization. This enables the project management team to define success criteria and allows the design team to create a tailored and optimized architecture.

Requirements can be captured during meetings or by distributing questionnaires. Meetings are more time consuming, but allow for follow-up questions to be asked and help to simplify the prioritization process. It is important that this exercise be completed jointly by both business managers and IT decision makers since both groups will have significantly different viewpoints.

Take the following examples of what certain organizations faced, which drove their selection of desktop virtualization.

Experience from the Field

- Finance – A large financial institution had a base of operations in the city designated as the host city for an upcoming G8 summit. As these types of meetings historically include riots, protests and other issues that can disrupt business and the safety of their employees, the financial organization needed an alternative allowing their users to work from the safety of their homes.
- Agriculture – Due to thin margins, an agriculture organization wanted to save money by extending the life of desktop PCs while still being able to run the latest applications.
- Healthcare – A large healthcare organization was in need of a solution to simplify application updates as the main application required updates on a weekly basis. Due to the distributed nature of the endpoint devices, the organization was in need of a better application delivery solution.

These are just a few examples, but they demonstrate how organizations think about their priorities. Most organizations do not focus on technology, they focus on the needs of the user and of the organization. These needs can be met with technical solutions but it is imperative the team understands the “Why” of the project.

In addition to the three real-world examples, the following table identifies a few other priorities often stated from many

© 1999-2017 Citrix Systems, Inc. All rights reserved.

organizations:

Requester	Requirement
Business Managers	**Better IT agility and responsiveness** – Flexible desktop solution that is capable of accommodating periods of change such as rapid growth or downsizing. For example, enabling the business to setup project offices or temporary points of sale very rapidly without long delays, hardware acquisitions or IT notification periods. **Bring your own device** – Empower employees to choose their own devices to improve productivity, collaboration and mobility. **Collaboration** – With an increase in both globalization and mobility, team members are often dispersed across multiple physical locations. Powerful collaboration capabilities are required to ensure high levels of productivity, efficiency and quality. **Work from anywhere** – The business needs to support home workers in order to attract and retain top talent, and / or travelling employees
IT decision makers	**Better desktop management** – Simplify the management of desktop infrastructure. IT is not as proactive as they would like and spend too much time "fighting fires". **Increase security** – Data theft or the loss of devices containing sensitive data is a big risk and preventive measures are a top priority. **Extend desktop hardware lifecycle** – Replacing workstations every three to five years in order to keep up with the requirements of the operating system or the applications has been very costly. **Reducing IT Management Scope** – Improve IT efficiency by focusing on only the aspects driving the business while offloading remaining functions to 3rd parties via cloud or service providers. **Improving user experience** - Increasing performance or enabling features which would otherwise not be possible with a geographically dispersed user population

The prioritization process should be completed in collaboration with the project team, business managers and IT managers so that all views are considered.

Step 2: Define the User Groups

Although there are multiple approaches towards defining user groups, it is often easiest to align user groups with departments as most users within the same department or organizational unit consumes the same set of applications.

User Segmentation

Depending on the size of the department, there might be a subset of users with unique requirements. Each defined user group should be evaluated against the following criteria to determine if the departmental user group needs to be further divided into more specialized user groups.

- Primary datacenter – Each user will have a primary datacenter or cloud resource location assigned that will be used to host their virtual desktop, data, and application servers. Identify the datacenter that the user should be assigned to rather than the datacenter they are currently using. Users will be grouped based on their primary datacenter so that a unique design can be created for each one.
- Personalization – Personalization requirements are used to help determine the appropriate VDI model for each user group. For example, if a user group requires complete personalization, a personal desktop will be recommended as the optimal solution. There are three classifications available:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personalization	Requirement
None	User cannot modify any user or application settings, for example - kiosk.
Basic	User can modify user-level settings of desktops and applications.
Complete	User can make any change, including installing applications.

- Security – Security requirements are used to help determine the appropriate desktop and policy (or policies) for each user group. For example, if a user group requires high security, a hosted pooled desktop or a local VM desktop will be recommended as the optimal solution. There are three classifications available:

Security level	Description
Low	Users are allowed to transfer data in and out of the virtualized environment.
Medium	All authentication and session traffic should be secured; users should not be able to install or modify their virtualized environment.
High	In addition to traffic encryption, no data should leave the data center (such as through printing or copy/paste); all user access to the environment should be audited.

- Mobility – Mobility requirements are used to help determine the appropriate desktop model for each user group. For example, if a user group faces intermittent network connectivity, then any VDI model requiring an active network connection is not applicable. There are four classifications available:

Mobility	Requirement
Local	Always uses the same device, connected to an internal, high-speed and secured network.
Roaming Local	Connects from different locations on an internal, high-speed, secured network.
Remote	Sometimes connects from external variable-speed, unsecure networks.
Mobile	Often needs access when the network is intermittent or unavailable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Desktop Loss Criticality – Desktop loss criticality is used to determine the level of high availability, load balancing and fault tolerance measures required. For example, if there is a high risk to the business if the user's resource is not available, the user should not be allocated a local desktop because if that local desktop fails, the user will not be able to access their resources. There are three classifications available:

Desktop loss criticality	Requirement
Low	No major risk to products, projects or revenue.
Medium	Potential risk to products, projects or revenue.
High	Severe risk to products, projects or revenue.

- Workload – Types and number of applications accessed by the user impacts overall density and the appropriate VDI model. Users requiring high-quality graphics will either need to utilize a local desktop implementation or a professional graphics desktop. There are three classifications available:

User type	Characteristics
Light	1-2 office productivity apps or kiosk.
Medium	2-10 office productivity apps with light multimedia use.
Heavy	Intense multimedia, data processing or application development.

> **注意**
>
> Performance thresholds are not identified based on processor, memory or disk utilization because these characteristics will change dramatically following the application rationalization and desktop optimization process. In addition, it is likely that the user's management tools and operating system will change during the migration process. Instead, workload is gauged based on the number and type of applications the user runs.

Experience from the Field

- Utility company – A large utility company collected data on every user in their organization. During the user segmentation process, it was realized that the organization's existing role definitions were sufficiently well defined that all the users within a role shared the same requirements. This allowed a significant amount of time to be saved by reviewing a select number of users per group.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Government – A government organization discovered that there was significant deviation between user requirements within each role, particularly around security and desktop loss criticality. As such, each user needed to be carefully reviewed to ensure that they were grouped appropriately.

Assign VDI Models

As with physical desktops, it is not possible to meet every user requirement with a single type of VDI. Different types of users need different types of resources. Some users may require simplicity and standardization, while others may require high levels of performance and personalization. Implementing a single VDI model across an entire organization will inevitably lead to user frustration and reduced productivity.

Citrix offers a complete set of VDI technologies that have been combined into a single integrated solution. Because each model has different strengths, it is important that the right model is chosen for each user group within the organization.

The following list provides a brief explanation of each VDI model.

- Hosted Apps – The hosted apps model delivers only the application interface to the user. This approach provides a seamless way for organizations to deliver a centrally managed and hosted application into the user's local PC. The Hosted Apps model is often utilized when organizations must simplify management of a few line-of-business applications. Hosted apps includes a few variants:
  - Windows Apps – The Windows apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - VM Hosted Apps – The VM hosted apps model utilizes a desktop-based Windows operating system, resulting in a single user accessing a single VM model. This model is often used to overcome application compatibility challenges with a multi-user operating system, like Windows 2008, Windows 2012 and Windows 2016.
  - Linux Apps – The Linux apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - Browser Apps – The browser apps model utilizes a server-based Windows operating system to deliver an app as a tab within the user's local, preferred browser. This approach provides a seamless way for organizations to overcome browser compatibility challenges when users want to use their preferred browser (Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, etc.) but the web application is only compatible with a specific browser.
- Shared Desktop – With the shared desktop model, multiple user desktops are hosted from a single, server-based operating system (Windows 2008, 2012, 2016, Red Hat, SUSE, CentOS and Ubuntu). The shared desktop model provides a low-cost, high-density solution; however, applications must be compatible with a multi-user server based operating system. In addition, because multiple users share a single operating system instance, users are restricted from performing actions that negatively impact other users, for example installing applications, changing system settings and restarting the operating system.
- Pooled Desktop – The pooled desktop model provides each user with a random, temporary desktop operating system (Windows 7, Windows 8 and Windows 10). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, pooled desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Personal Desktop – The personal desktop model provides each user with a statically assigned, customizable, persistent desktop operating system (Windows 7, Windows 8, Windows 10, Red Hat, SUSE, CentOS and Ubuntu). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, personal desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Pro Graphics Desktop – The pro graphics desktop model provides each user with a hardwarebased graphics processing unit (GPU) allowing for higher-definition graphical content.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Local Streamed Desktop – The local streamed desktop model provides each user with a centrally managed desktop, running on local PC hardware.
- Local VM Desktop – The local VM desktop model provides each user with a centrally managed desktop, running on local PC hardware capable of functioning with no network connectivity.
- Remote PC Access – The remote PC access desktop model provides a user with secure remote access to their statically assigned, traditional PC. This is often the fastest and easiest VDI model to deploy as it utilizes already deployed desktop PCs.

Each user group should be compared against the following table to determine which VDI model best matches the overall user group requirements. In many environments, a single user might utilize a desktop VDI model and an app VDI model simultaneously.

In this table:

- Y indicates "Recommended"
- N indicates "Not Recommended"
- o indicates "Viable"

Segmentation Characteristic	Hosted Apps	Hosted Shared Desktop	Hosted Pooled Desktop	Hosted Personal Desktop	Hosted Pro Graphics Desktop	Local Streamed Desktop	Local VM Desktop	Remote PC Access
Workload								
Light	**Y**	**o**	**o**	**o**	**N**	**o**	**o**	**o**
Medium	**o**	**Y**	**Y**	**o**	**o**	**o**	**o**	**o**
Heavy	**N**	**N**	**N**	**o**	**Y**	**Y**	**Y**	**o**
Mobility								
Local	**Y**	**Y**	**Y**	**o**	**o**	**Y**	**o**	**o**
Roaming Local	**Y**	**Y**	**Y**	**o**	**o**	**N**	**o**	**o**
Remote	**Y**	**Y**	**Y**	**o**	**o**	**N**	**o**	**Y**
Mobile	**N**	**N**	**N**	**N**	**N**	**N**	**Y**	**N**
Personalization								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

None	**Y**	**Y**	**Y**	**N**	**o**	**o**	**o**	**o**
Basic	**Y**	**Y**	**Y**	**N**	**o**	**o**	**o**	**o**
Complete	**N**	**N**	**N**	**Y**		**N**	**Y**	**Y**
Security								
Low	**o**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
Medium	**Y**	**Y**	**Y**	**o**	**o**	**o**	**o**	**o**
High	**o**	**o**	**Y**	**N**	**o**	**Y**	**Y**	**N**
Desktop Loss Criticality								
Low	**o**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
Medium	**Y**	**Y**	**Y**	**o**	**o**	**o**	**o**	**N**
High	**Y**	**Y**	**Y**	**N**	**o**	**o**	**N**	**N**

Don't forget to follow these top recommendations from Citrix Consulting based on years of experience:

Citrix Consulting Tips for Success

1. Start with Windows apps, shared and pooled desktops – As you can see in the VDI capability table above, the Windows apps, hosted shared and pooled desktop models can be used in the majority of situations. The local streamed and local VM desktop models should only be used on an exception basis. By reducing the number of VDI models required, you will help to reduce deployment time and simplify management.
2. Perfect match – It may not be possible to select a VDI model that is a perfect match for the user group. For example, you can't provide users with a desktop that is highly secure and offers complete personalization at the same time. In these situations, select the VDI model which is the closest match to the organization's highest priorities for the user group.
3. Desktop loss criticality – There are only three VDI models that meet the needs of a high desktop loss criticality user group (backup desktops available) – none of which allow for complete personalization. If a high-desktop loss criticality user group also requires the ability to personalize their desktop they could be provided with a pool of backup desktops (hosted shared, pooled) in addition to their primary desktop. Although these desktops would not include customizations made to their primary desktop, they would allow users to access core applications such as mail, Internet and Microsoft Office.
4. Consider Operations & Maintenance – The ongoing support of each VDI model should be factored in when deciding on a VDI model. For example, pooled desktops can be rebooted to a known good state which often leads to reduced

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

maintenance versus a personal desktop where each desktop is unique.

Step 3: Define the Applications

Once the users have been divided up in to groups the next step is to determine which applications they require. This is a two-step process:

1. Application rationalization – Help to simplify the application assessment by removing redundant applications from the inventory that were captured during the data capture.

2. Link apps to users – Use the results from the data capture process to map applications to user groups.

Application Rationalization

The number of applications identified during the inventory is often surprising, even for organizations that believe they have a high-level of control over applications. To help reduce complexity as well as overall time required, it's important to take the time to consolidate the list of applications. The following guidelines will help ensure that your application list is consolidated appropriately:

- Multiple versions – Different versions of the same application may have been identified during the inventory. There are various reasons for this, including an inconsistent patching or upgrade process, decentralized application management, limited licenses and situations where users require specific application versions for compatibility with other applications, macros and document formats. Where possible, work with the application owners to reduce the number of versions required. The leading practice is to standardize on a single version of each application, typically the latest.
- Non-business applications – Applications that are not required by the business should be removed from the application inventory to reduce resource requirements and to help simplify the overall project. Non-business related applications are typically found in an application inventory when users have been provided with the ability to install their own applications and typically include games, communication clients, screen savers, peripheral software and media players.
- Legacy applications – The inventory may identify legacy applications that have since been retired or that are no longer required within the business. These applications may not have been removed from the desktops because there is no established process to do so or because there are always more high-priority activities to complete. These applications should be consolidated during the rationalization stage of the application assessment.
- Management applications – The antivirus, application delivery, monitoring, inventory, maintenance and backup applications will be completely re-designed across the organization during the desktop virtualization project. These applications should also be consolidated during this stage.

Experience from the field:

Government: A government organization identified that there were 2,660 applications installed across their desktop estate. Most of which were installed by users with local administrative rights. By following the application rationalization recommendations above, it was possible to reduce the number of applications required to 160.

Application Categorization

Each application included in the project should be categorized based on certain criteria, which will help determine the most appropriate way to host and integrate the app. Each application can be installed directly into the image, virtualized in an isolated container and streamed to the desktop (Microsoft App-V), captured in a unique layer and attached to the virtual machine (Citrix App Layering) or installed locally on the user's endpoint device and seamlessly integrated into the user's virtual desktop (Citrix Local App Access). Due to the uniqueness of every application, many large-scale deployments simultaneously utilize multiple approaches. Each application should be categorized as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Common Apps - Every organization includes a suite of applications utilized by almost every user, Microsoft Office for example. This suite of applications is often the most utilized application in a desktop VDI model.
- Departmental Apps - A certain set of applications are only relevant for a unique business unit or department. For example, an engineering department will often require software development applications.
- User Apps - Often making up the largest grouping of apps are the apps used by very few individual users. In a traditional PC implementation, these applications are installed by the user as a temporary requirement or a personal requirement, often not directly impacting the business.
- Management Apps – Many desktop deployments include a combination of antivirus, monitoring, inventory, maintenance and backup applications. Many of these applications have unique virtualization requirements and are often required across the entire organization.

Application Characterization

Workload	Requirement
Resource intensive	Application requires 1 GB or more of RAM or averages 50% or more CPU utilization.
None	The application is not resource intensive.

The following characteristics should be identified for each application so that the right application delivery model can be selected during the design phase of the project:

- Complex – An application should be classified as complex or technically challenging if it is difficult to set up, has extensive dependencies on other applications or requires a specialized configuration, for example an Electronic Medical Records (EMR) application. Complex applications need to be identified during the application assessment because they are not generally appropriate for installation in a pooled/personal desktop model or delivery by application streaming. Delivering complex applications as a hosted app often helps to reduce the complexity of the base desktop image.
- Demanding – Collecting application resource requirements allows the virtualization infrastructure to be sized and an appropriate application delivery model to be selected. For example, demanding or resource intensive applications will not be delivered via a pooled/personal desktop model because there is limited control over how the resources are shared between users. There are two classifications available in the user assessment worksheet:

- Mobile – Some user groups may require the ability to work while mobile, sometimes when offline. If so, it is important that the design can determine which applications will work without a network connection and which ones will not. Applications that require backend infrastructure such as web and database servers are not typically available offline.
- Peripherals – If applications require connectivity with peripheral devices, identify the interface required so that it can be made available to the application when it is run from a virtual session.
- Restrictions – Application access may need to be restricted due to insufficient licenses /resources and to protect sensitive data / tools. For example, applications with a limited number of licenses should not be installed on a base image that is shared with unlicensed users. There are three restricted access categories in the application assessment workbook:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restricted Access	Requirement
No	There are no restrictions for the application and it can be accessed by any user within the organization.
User Group	The application may be installed on a multi-user operating system but only a specific group of users should be provided with an icon.
Virtual machine	Application should only be installed on a virtual machine that is accessible by authorized users, often because of licensing requirements.

Step 4: Define the Project Team

Desktop virtualization is a fundamental change that requires close collaboration between various business and technical teams in order to be successful. For example, the virtualization and desktop teams need to work together to ensure that the virtual desktop image meets user needs while also being optimized for the datacenter. Failure to build a cohesive project team that consists of the right roles and skillsets can negatively impact performance, availability, user experience and supportability while also increasing costs and risk.

The following tables identify the business and technical roles required during an enterprise virtual desktop deployment. Although the list may seem quite large, many of these roles are only required for a short time and multiple roles may be performed by a single person. The project manager and Citrix architect are considered to be full time roles with other team members being brought in only when required. The project manager role is key to ensuring that the right people are involved in the project at the right time.

Business Roles

Role	Description	Example Responsibilities
Project sponsor	The project sponsor is a senior company executive who recognizes the benefits that desktop virtualization will bring to the business. The project sponsor role is often performed by the chief technology officer (CTO).	**Pre-project** • Promote desktop virtualization within business. • Identify members of the steering committee. **Secure funding** • Assess general costs associated with solution. • Identify and prioritize key business drivers.
		All steps • Define key project

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Project manager	The project manager directs the project team and is responsible for ensuring that project objectives are completed on time and within budget.	• Create and update project plan. • Track progress against plan. • Track expenditure against budget. • Maintain issue and risk register. • Manage scope changes. • Create weekly project reports. • Brief steering committee on progress. • Organize project workshops and meetings. • Ensure project teams are synchronized. • Ensure pre-requisites are in place. • Creates change control requests.
Business manager	Depending on company structure and size, business managers oversee planning and performance at a department, region or company level. A business manager understands the requirements necessary for their employees to be successful.	**Assess** • Assist with application consolidation project. • Provide details on connectivity requirements of user group, including offline usage. • Provide details on risk tolerance of user group. • Identify requirements for peripherals. **Deploy** • Promote benefits of desktop virtualization. • Assist with coordinating the rollout.
		Assess • Provide Citrix architect with detailed understanding of the current business

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Design Responsibilities
Business continuity manager	The business continuity manager ensures that an organization can continue to function after a disruptive event such as natural disaster, crime or human/computer error.	**Design** • Update business continuity plan to incorporate the new Citrix infrastructure. **Deploy** • Test business continuity plan.
Test manager	The test manager is responsible for ensuring that the test and user acceptance environments match the production environment as closely as possible. The test manager helps to reduce risk by ensuring that changes are fully tested before being implemented in production.	**Assess** • Provide Citrix architect with detailed understanding of current testing infrastructure and processes. **Design** • Work with Citrix architect to design an appropriate testing infrastructure and test plan for new Citrix environment. **Deploy** • Ensure that testing design is implemented correctly and new Citrix infrastructure is fully tested before rollout.
Application owners	An application owner is a subject matter expert on specific applications deployed within the business. Application owners are responsible for ensuring that problems with the applications are resolved and that upgrades/updates are performed without issue. Application owners are also responsible for managing support agreements with the application vendors.	**Assess** • Assist with application consolidation project. • Identify application licensing limitations. • Provide details on security restrictions. • Provide details on application dependencies. • Provide location of backend resources. **Deploy** • Provide installation pre-requisites and install guide

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		installing and testing applications in VDI environment
Service desk manager	The service desk manager helps to improve productivity and end-user satisfaction by ensuring that production issues are logged, escalated and resolved in a timely manner. The service desk manager is also responsible for reporting on common issues, call volumes and service desk performance.	**Assess** • Identify common issues with existing environment. • Provide details on support tools currently used. **Design** • Assist Citrix architect with designing a delegated administration model. • Participate in operations and support design workshops. • Work with training manager to identify training requirements. **Deploy** • Monitor helpdesk calls for rollout related issues.
Training manager	The training manager ensures that support staff and end-users are proficient with new areas of technology. The training manager also has responsibility for ensuring that the training plan is up-to-date and followed appropriately.	**Assess** • Determine current skill set for support staff and end users. **Design** • Create training plan for support staff and end users. **Deploy** • Implement training plan for support staff and end users.
		Design • Work with project manager to create communications plan. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		• desktop virtualization. • Inform users of key migration dates. • Ensure expectations are set accordingly.

Technical Roles

Role	Description	Example Responsibilities
Citrix desktop architect	The Citrix architect acts as the design authority for all Citrix products and liaises with other architects to ensure that the Citrix infrastructure is successfully integrated into the organization.	**Assess** • Work with project sponsor and key stakeholders to identify and prioritize key business drivers. • Oversee user segmentation and app. assessment. • Map VDI models to user groups. • Perform capabilities assessment to determine current state of readiness. • Identify areas of risk and provides remedial actions. **Design** • Create Citrix design that includes hardware and storage estimates. • Coordinate with other architects to integrate Citrix infrastructure into organization. • Work with monitoring architect to ensure that Citrix environment is monitored appropriately. • Create operations and support design. • Create implementation and rollout design. • Create test plan **Deploy** • Ensure that the Citrix environment is implemented in accordance with design. • Verify that implementation passes test plan. • Ensure that the Citrix design is implemented correctly.
Archive directory architect	Design authority on Microsoft Active Directory, including Organizational Units (OU) and Group Policy Objects (GPOs).	**Assess** • Provide Citrix architect with detailed understanding of current Active Directory architecture. **Design** • Work with the Citrix architect to design OU structure, group policies, permissions, service accounts, etc. for new Citrix environment. • Update Active Directory infrastructure design to reflect centralization of user data and accounts. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		correctly.
Role	**Description**	**Example Responsibilities**
Visualization architect	Design authority on server and desktop virtualization using Citrix XenServer, Microsoft Hyper-V, Nutanix Acropolis or VMware vSphere.	**Assess** • Provide Citrix architect with detailed understanding of current virtualization architecture **Design** • Work with Citrix architect to design hardware, networking, storage, high availability, etc. for server and desktop virtualization • Work with monitoring architect to ensure that virtualization environment is monitored appropriately **Deploy** • Ensure that the virtualization design is implemented correctly
Network architect	Design authority on networking, including routing, VLANs, DHCP, DNS, VPN and firewalls.	**Assess** • Provide Citrix architect with detailed understanding of current networking architecture. **Design** • Work with Citrix architect to design physical network, virtual networks, routing, firewalls, quality of service, remote access, network optimization, etc. for new Citrix environment. • Work with monitoring architect to ensure that network is monitored appropriately. **Deploy** • Ensure that network design is implemented correctly.
Desktop architect	Design authority on Microsoft desktop operating systems, including Windows XP, Windows 7 and Windows 8.	**Assess** • Provide Citrix architect with detailed understanding of current desktop environment. **Design** • Work with Citrix architect to design core desktop virtual image, core applications, desktop optimizations, etc. for new Citrix environment. • Work with monitoring architect to ensure that the virtual desktops are monitored appropriately. **Deploy** • Ensure that desktop design is implemented correctly.
		Assess • Provide Citrix architect with detailed understanding of current shared storage environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Storage architect	Design authority on storage solutions, including directattached storage, storageattached networks and network attached storage.	• Work with Citrix architect to design storage architecture, tiers, sizing, connectivity, etc. for new Citrix environment. • Work with monitoring architect to ensure that storage is monitored appropriately. **Deploy** • Ensure that storage design is implemented correctly.
Backup architect	Design authority on backup and recovery, including virtual machines, desktops, servers, user data and databases.	**Assess** • Provide Citrix architect with detailed understanding of current backup architecture and processes **Design** • Work with Citrix architect and disaster recovery architect to design backup architecture, process, schedule, retention, etc. for new Citrix environment **Deploy** • Ensure that backup design is implemented correctly
Application package architect	Design authority on packaging applications for deployment via the systems management team	**Assess** • Provide Citrix architect with detailed understanding of current application packaging process and status **Deploy** • Ensure that all required applications are packaged according to design
Monitoring architect	Design authority on monitoring, including hardware, network, servers, storage and security appliances.	**Assess** • Provide Citrix architect with detailed understanding of current monitoring architecture and processes. **Design** • Work with Citrix architect to design monitoring architecture, metrics, alerts, etc. for new Citrix environment and supporting infrastructure. **Deploy** • Ensure that monitoring design is implemented correctly. • Provide regular reports on capacity and trends during rollout .
System management	Design authority on systems management, including server/desktop build process, patching and automated	**Assess** • Provide Citrix architect with a detailed understanding of the current systems management processes. **Design** • Works with Citrix architect to define server/desktop build process, patching and application delivery

© 1999-2017 Citrix Systems, Inc. All rights reserved.

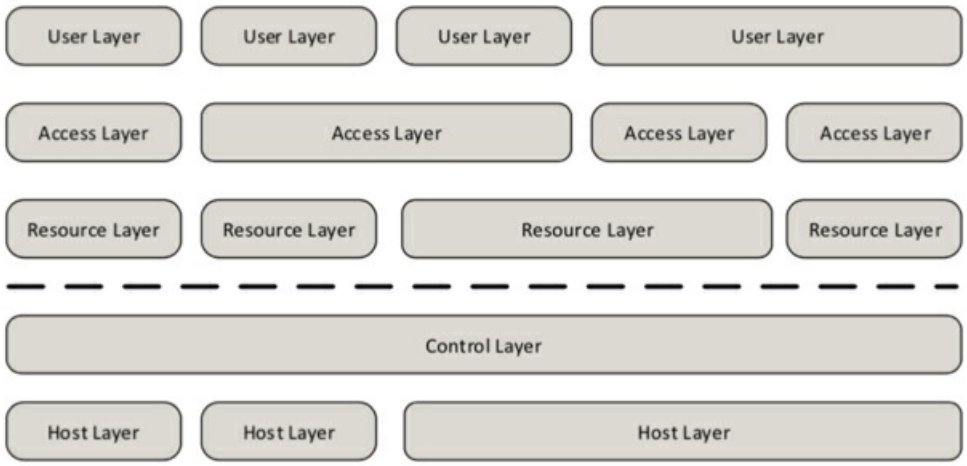
Role	Description	Example Responsibilities
		Deploy • Ensure that the systems management design is implemented correctly.
Security architect	Design authority on security, including desktops, servers, networks and VPNs.	**Assess** • Provide Citrix architect with detailed understanding of current security policy. **Design** • Work with Citrix architect to design security standards for new Citrix environment, including authentication, encryption, port numbers, firewall rules, etc. **Deploy** • Ensure that security design is implemented correctly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design

Jan 30, 2018

Designing a desktop virtualization solution is simply a matter of following a proven process and aligning technical decisions with organizational and user requirements. Without the standardized and proven process, architects tend to randomly jump from topic to topic, which leads to confusion and mistakes. The recommended approach focuses on working through five distinct layers:



The top three layers are designed for each user group independently, which were identified during the user segmentation section of the assess phase. These layers define the users' resources and how users access their resources. Upon completion of these three layers, the foundational layers (control and hardware) are designed for the entire solution.

This process guides the design thinking in that decisions made higher up impact lower level design decisions.

Layer 0: Conceptual Architecture

The conceptual architecture helps define the overarching strategies for the entire solution based on business objectives and organizational structure.

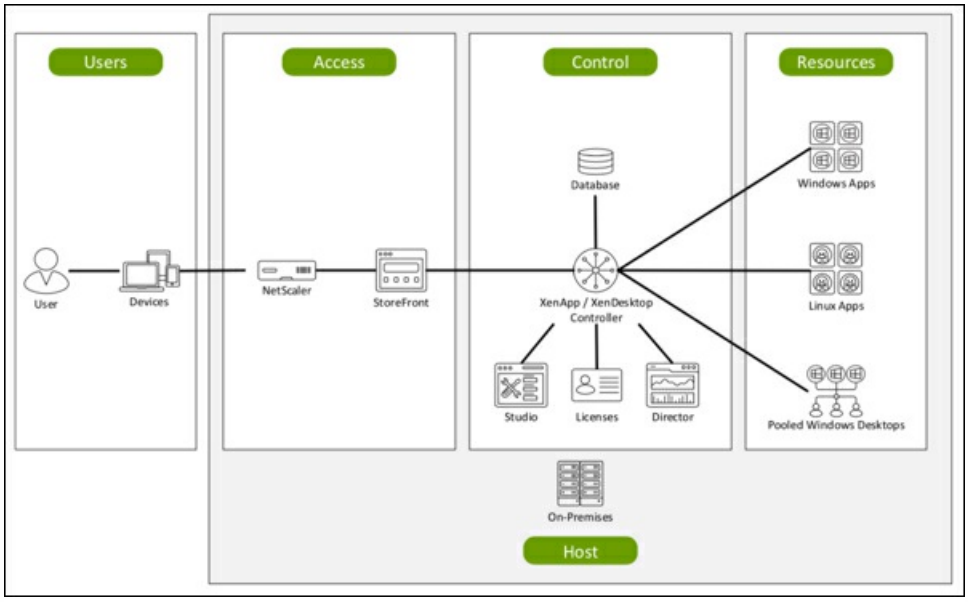
Although an organization's conceptual architecture will change over the coming years, it is worthwhile to start the design phase by defining the long-term objectives around delivery models and the physical, geographical distribution of solution.

Decision: Delivery Model

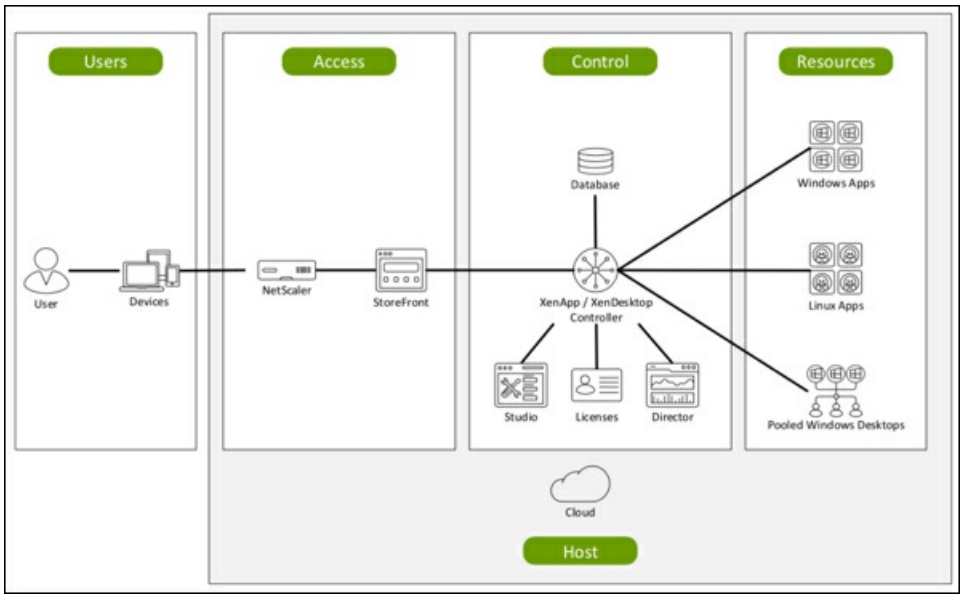
A XenDesktop and XenApp solution can take on many delivery forms. The organization's business objectives help select the right approach. Even though the infrastructure remains the same for all delivery models, the local IT team's management scope changes.

- **On Premises** - All components hosted from the organization's local data center. The onpremises model requires the local IT team to manage every aspect of the solution.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

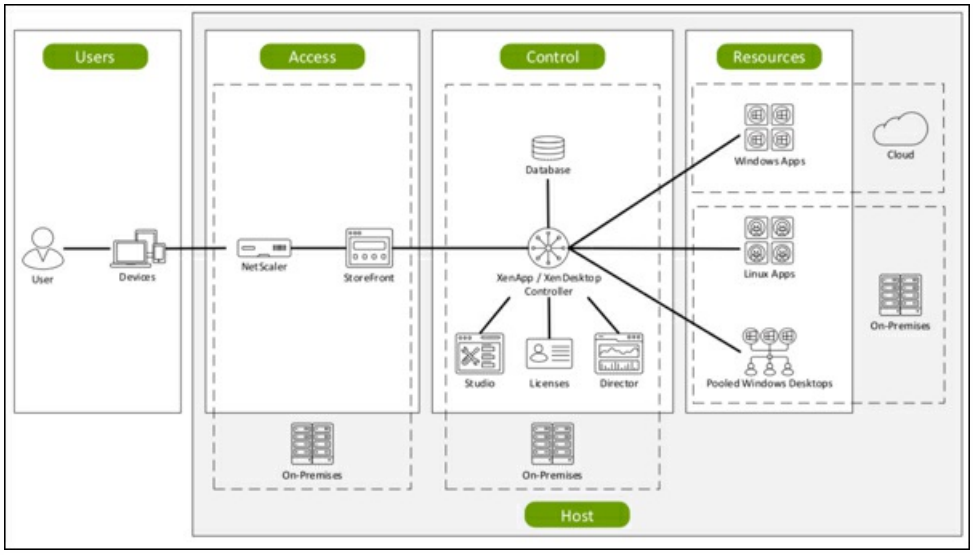


- **Public Cloud** - All components hosted from a public cloud infrastructure using Infrastructure as a Service (IaaS). The public cloud model eliminates hardware management from the local IT team's management scope.

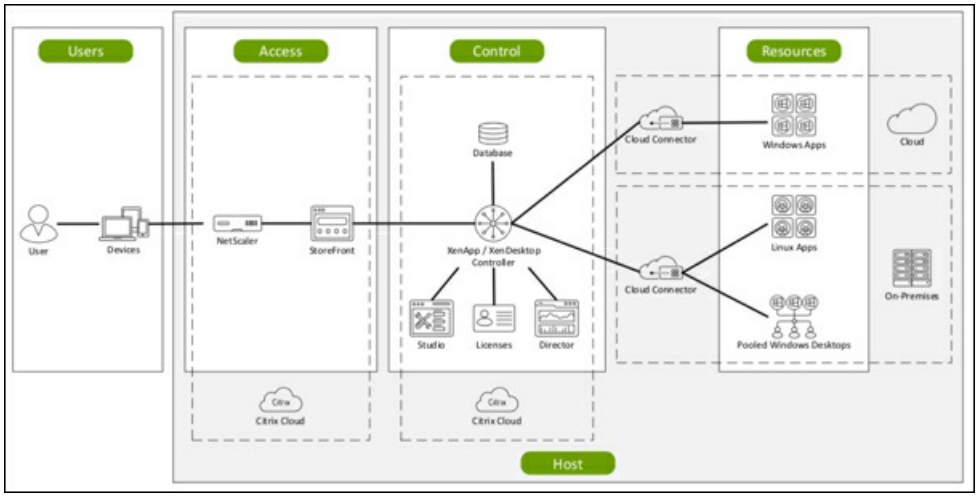


- **Hybrid Cloud** - A single implementation executes from an on-premises data center as well as the public cloud. Even though components of the solution are using different hosting providers, the entire solution is a single solution using the same code and managed as a single entity. The local IT team continues to manage all aspects of the solution except for the hardware associated with the cloud-hosted resources.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Citrix Cloud** - The XenApp and XenDesktop Service offering from Citrix Cloud breaks a typical deployment into multiple management domains. The access and control layer components are hosted and managed in the Citrix cloud by Citrix while the resource layer components continues to be managed by the local IT team either as an on-premises, public cloud or hybrid cloud model. Citrix manages the hardware, sizing and updates to the access and control components while the local IT team manages the resources. In addition, if the public cloud hosts the resources, the local IT team does not have to manage the resource hardware. Citrix Cloud continues to expand the number of offerings to help solve specific user cases. To learn more and understand the full array of offerings, please explore the workspace services within the Citrix Cloud.

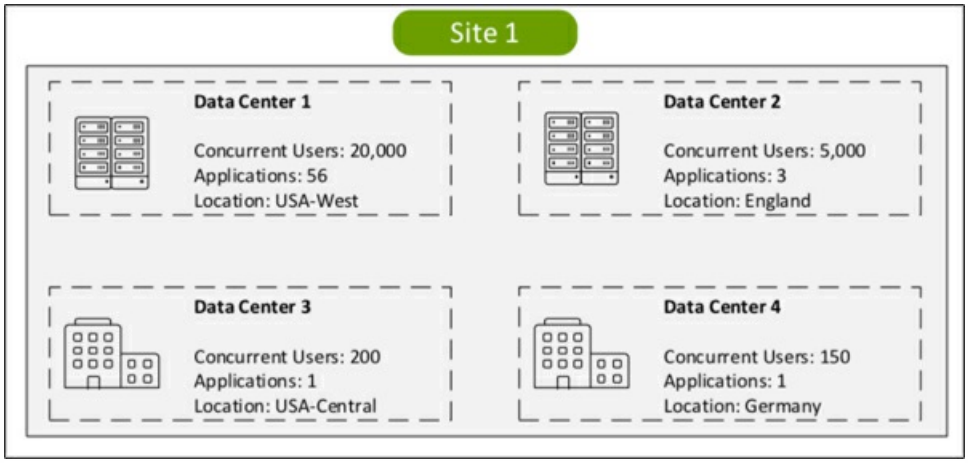


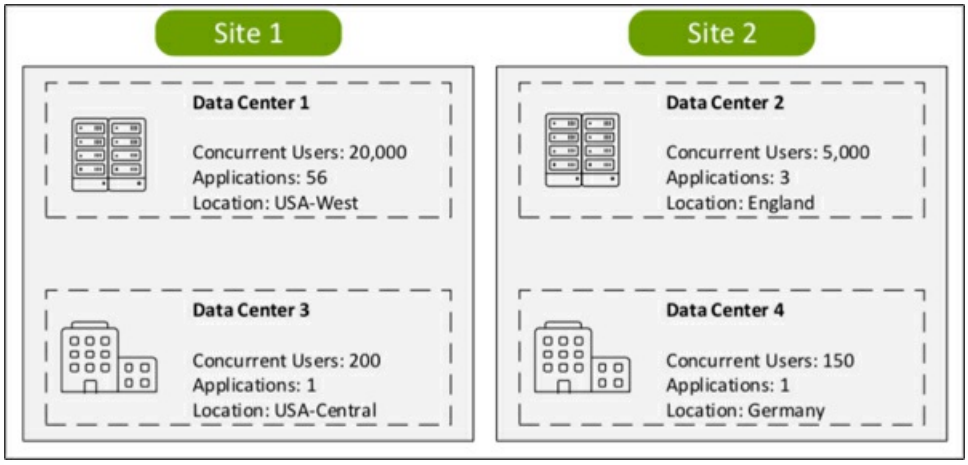
Decision: Site Topology

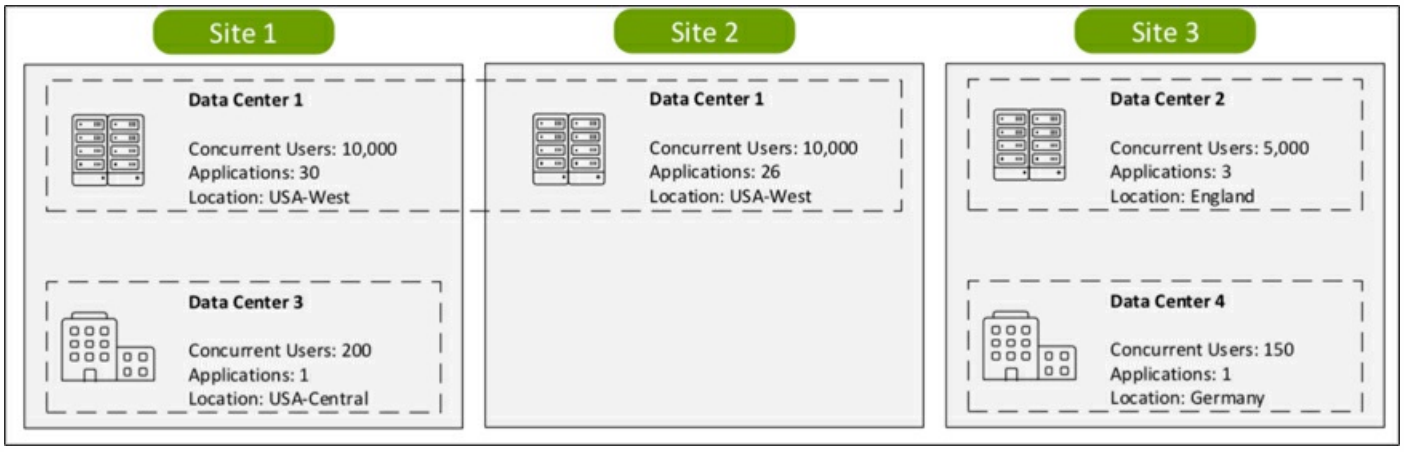
A XenApp and XenDesktop site groups desktops and applications together to form a single architectural and management entity. All persistent and dynamic data for the site, including site configuration, desktop assignments, and session state, is stored in a site's database.

A site can be contained within a single location, span across multiple locations or be a partial location. Through rigorous testing, a single XenApp/XenDesktop site can support 40,000 or more concurrent sessions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.







Zones subdivide single sites, often associated with geographical locations. There are several factors to consider when determining the overall topology of the XenApp and XenDesktop solution:

- **Risk Tolerance** – Create multiple XenDesktop sites to minimize the impact from a site-wide outage. For example, corruption of the XenDesktop site database could affect site-wide availability. For many organizations, the decreased risk from implementing multiple sites outweighs the additional management overhead and supporting infrastructure required.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Experience from the Field

Finance – A large financial institution hosts 10,000 desktops from a single datacenter. To reduce risk, it was decided that no site should exceed 5,000 desktops. Therefore, despite the desktops being connected by a fast and redundant network, two sites were created.

- **Security** – Although delegated administration is available, high-security organizations may require complete separation between environments to demonstrate compliance with specific service level agreements.

Experience from the Field

Retail – A retail organization required complete separation for employees responsible for managing financial data. To meet this requirement, two separate sites were created within the same datacenter – one for t he financial employees and a second for all other employees.

- **Administrative Boundaries** – Due to billing/charge back requirements or how IT is structured, multiple sites might be required to separate administrative boundaries.
- **Geographical Connectivity** – Although the implementation of zones does allow a single site to span geographical locations, there must be enough bandwidth between the satellite zone and primary zone for the site database to capture the session information. Higher latency or larger zones impacts response times for the user.

Variable	XenApp and XenDesktop 7.13	XenApp and XenDesktop 7.11
Latency (ms)	90	250
Concurrent requests	48	48
Average response time	3.7	7.6
Brokering requests per second	12.6	6.3
Time to launch 10,000 users	13 minutes	26 minutes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session count	Max concurrent sessions launches	Min site-to-site bandwidth	Max site-to-site round trip latency
Less than 50	20	1 Mbps	250 ms
50 to 500	25	1.5 Mbps	100 ms
500 to 1,000	30	2 Mbps	50 ms
1,000 to 3,000	60	8 Mbps	10 ms
Over 3,000	60	8 Mbps	5 ms

In general, administrators should minimize the number of XenDesktop sites and zones to reduce architectural complexity and administrative effort.

Decision: Image Management Strategy

A XenApp and XenDesktop solution requires the creation and management of master images. Organizations must decide early what strategy to pursue for image management.

Installed Images

An installed image requires the administrator to install the operating system and applications for each image. This approach is straightforward but creates a duplication of effort as the admin installs the same operating system and core applications across multiple master images.

Maintaining master images also includes duplication of effort as the same operating system version and core applications are part of multiple images, each requiring the same update process.

Scripted Images

Administrators can automate many of the tasks associated with installed images with scripting or automation tools. Many operating system and application installs support automated scripting, which mitigates the duplication of effort impact on the administrator's time with installed images.

Unfortunately, learning, creating, and maintaining a scripting framework for the entire image is challenging and time consuming. Scripting an entire build takes time and often results in unexpected failures if directory structures change, processes take too long to complete or a filename changes.

Layered Images

Each unique operating system (Windows 10, Windows 2012R2 and Windows 2016), platform (XenApp/XenDesktop 7.13 VDA, XenApp/XenDesktop 7.14 VDA and XenApp/XenDesktop 7.15 VDA) and application (Microsoft Office, Adobe Acrobat, Google Chrome and Mozilla Firefox) is a layer. A master image is the merging of one operating system layer, one platform and many applications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A layered image approach eliminates the duplication of effort challenges associated with installed and scripted images. Each unique layer is available to any master image. When an application requires an update, that layer receives the updates and all master images utilizing the layer receives the update. If an organization requires ten unique Windows 10 images, each of the ten images shares the same Windows 10 layer. When the administrator needs to upgrade the VDA from version 7.14 to 7.15 across ten images, the administrator only updates a single platform layer.

Initially, the layered image approach does require more time to deploy because the administrator must build the organization's library of layers. However, once the layers are available, the time to maintain the images is drastically reduced.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology user layer

Jan 30, 2018

The top layer of the design methodology is the user layer, which each unique user group defines.

The user layer appropriately sets the overall direction for each user group's environment. This layer incorporates the assessment criteria for business priorities and user group requirements in order to define effective strategies for endpoints and Citrix Receiver. These design decisions affect the flexibility and functionality for each user group.

Endpoint Selection

There are a variety of endpoints devices available, all with differing capabilities, including:

- Tablet based
- Laptop
- Desktop PC
- Thin client
- Smartphone

The user's primary endpoint device must align with the overall business objectives as well as each user's role and associated requirements. In many circumstances, multiple endpoints may be suitable, each offering differing capabilities.

Decision: Endpoint Ownership

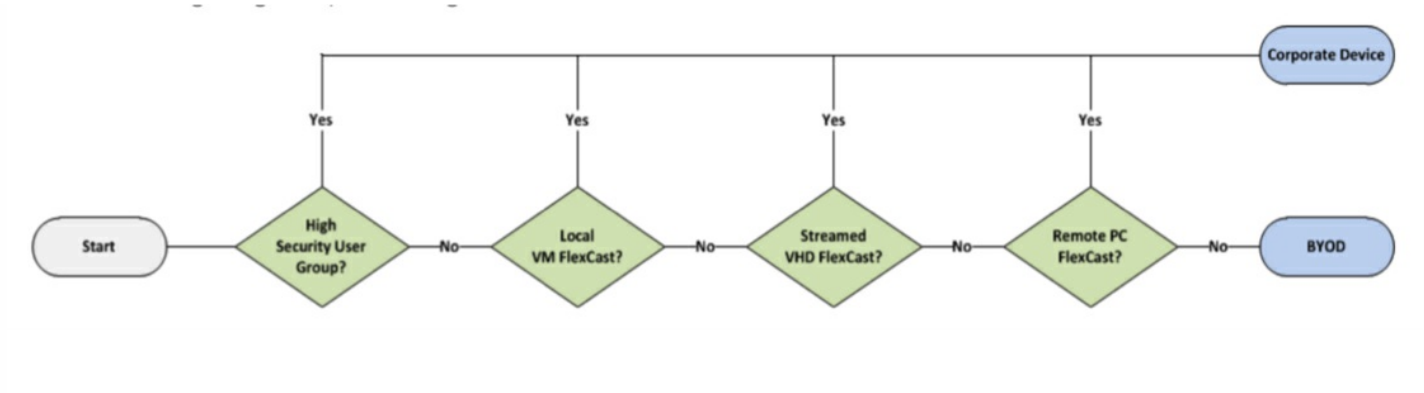
In many organizations, endpoint devices are corporate owned and managed. However, more and more organizations are now introducing bring your own device (BYOD) programs to improve employee satisfaction, reduce costs and to simplify device management. Even if BYOD is a business priority, it does not mean that every user should be allowed to use a personal device in the corporate environment.

Certain user requirements, which were identified during the user segmentation, can greatly impact the suitability of personal devices:

- **Security** – Users requiring a high-level of security might not be able to bring a personal device into the secured environment for risk of data theft.
- **Mobility** – Users operating in a disconnected mode might not be able to use a personal device, as the local VM desktop VDI model associated with this type of requirement can have specific hardware requirements, or special maintenance requirements.
- **Desktop loss criticality** – Users with a high desktop loss criticality rating might require redundant endpoints in the event of failure. This would require the user to have an alternative means for connecting in the event their personal device fails, likely making these users poor candidates for a BYOD program.
- **VDI models** – A personal device should not be recommended for user groups utilizing a local VDI model like a local streamed desktop, local VM desktop or Remote PC Access. These VDI models typically require a specific hardware configuration or installation that will restrict device selection.

The following diagram provides guidance on when user owned devices could be used:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Decision: Endpoint Lifecycle

Organizations may choose to repurpose devices in order to extend refresh cycles or to provide overflow capacity for contract workers. Endpoints now offer more capabilities allowing them to have longer useful lifespans. In many cases, these hardware capabilities vastly outstrip the needs of a typical user. When coupled with the ability to virtualize application and desktop workloads, this provides new options to administrators such as repurposing existing workstations. These options go well beyond the simple three-year PC refresh cycle. However, the benefits of repurposing or reallocating a workstation should be balanced against the following considerations.

- **Minimum standards** – While cost factors of repurposing existing workstations may be compelling, certain minimum standards should be met to guarantee a good user experience. At a minimum, it is recommended that repurposed workstations have a 1GHz processor, 1GB of RAM, 16GB of free disk space and a GPU that is capable of supporting HDX features.
- **Business drivers** – Priorities underpin the success of any major project. Those organizations that have prioritized reducing capital expenditure by means of prolonging the hardware refresh cycle can benefit from repurposing hardware. Conversely, if an organization's business drivers include reducing power consumption as part of an overall green initiative, purchasing newer endpoints may be beneficial in order to take advantage of the latest generation of power management capabilities available in the most modern devices.
- **Workload** – The type of work and VDI model for an end user can determine whether they are a good candidate for a repurposed endpoint, or may be better served with a new device. If the work performed by the individual involves locally installed applications, the individual may be best served by a new endpoint that offers the most powerful and recently updated processor and graphics architecture. However, if a user is largely performing tasks associated with virtualized applications that do not involve the latest multimedia capabilities such as webcams, VoIP and media redirection, then a repurposed workstation should be a viable alternative.

The following planning matrix outlines considerations when repurposing existing hardware:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Endpoint provisioning criteria	Repurpose existing	Procure new
Capital restrained environment	X	
High number of virtualized applications	X	
Desire to prolong hardware refresh cycle	X	
High failure rate among existing desktops		X
Outmoded client-side feature set		X
Power consumption or green initiative(s)		X

Decision: Unified Endpoint Management (UEM)

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices. Administrators need to:

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define WiFi parameters for office locations.
- Integrate certificates to secure communications.

Managing the distributed endpoints is only part of the challenge. Administrators need to define levels of access. Administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

UEM Solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. UEM also allows for the management of corporate data and resources, separately from personal data.

Decision: Mobile Device Management (MDM)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices, which is knows as Mobile Device Management (MDM).

MDM solutions, like Citrix XenMobile, enables organizations to protect devices and data on devices at a system level. For example,

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define Wi-Fi parameters for office locations.
- Integrate certificates to secure communications.

MDM is typically suitable for corporate-owned mobile devices because most users with personal devices do not want to give the IT team that much control over their personal devices.

Decision: Mobile Application Management (MAM)

With a distributed workforce accessing the XenApp and XenDesktop environment across numerous devices, administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

MAM solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data.

MAM is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected.

Decision: Endpoint Form Factor

The capabilities of endpoints have grown along with efficiencies offered in thin client form factors. Even mid-range thin clients now have graphics capabilities that allow utilization of HDX features such as multi-monitor support while offering management and power efficiency benefits. Citrix has developed a three-tiered classification for thin clients based on their HDX capabilities: HDX Ready, HDX Premium, and HDX 3D Pro, which can be used to help narrow the field of appropriate thin client devices based on the use case requirements. This expansion of capabilities has given IT administrators more options and flexibility than ever before.

Most organizations will likely deploy a mixture of fully featured clients as well as thin clients. However, certain endpoint devices are more appropriate when used in combination with certain VDI models as explained in the following table.

In the table:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Yes** indicates recommended.
- **No** indicates not recommended.
- o indicates viable.

VDI model	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Hosted Windows Apps	Yes	Yes	Yes	Yes	Yes
Hosted Browser Apps	Yes	Yes	Yes	Yes	Yes
Hosted Shared Desktop	Yes	Yes	Yes	o	o
Hosted Pooled Desktop	Yes	Yes	Yes	o	o
Hosted Personal Desktop	Yes	Yes	Yes	o	o
Hosted Pro Graphics Desktop	Yes	Yes	o	o	o
Local Streamed Desktop	No	Yes	No	No	No
Local VM Desktop	No	o	Yes	No	No
Remote PC Access	No	Yes	Yes	o	o

Experience from the Field

- **Large systems integrator** – A large systems integrator recommended that a customer deploy a single type of low-end, limited capability endpoint for all users. Upon deployment to production, users immediately complained that they received a poor user experience when viewing multimedia content over the WAN. At great cost, the systems integrator and customer re-assessed the environment and chose to deploy endpoints that supported HDX MediaStream. The mistake caused a schism between systems integrator and the customer, resulting in lost time, capital and the end of a business relationship that was fostered over many years. It is critical that the endpoints assigned to each user group can support their requirements.

Receiver Selection

Citrix Receiver is an easy-to-install software client that provides access to applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.

The following section provides a series of design decisions that should be considered when deploying Citrix Receiver.

Decision: Receiver Type

© 1999-2017 Citrix Systems, Inc. All rights reserved.

While most organizations should simply deploy the latest Citrix Receiver compatible with their endpoint, it is important to recognize that there are certain differences between editions. The following table should be referenced to determine the most appropriate edition of Citrix Receiver for each user group. For the latest feature matrix, please refer to Receiver Feature Matrix.

Decision: Initial Deployment

There are several deployment options available for delivering Citrix Receiver to an endpoint. Although it is usually a best practice to have a full version of Citrix Receiver deployed to an endpoint to provide the greatest level of functionality, it is important to consider fallback options such as the HTML5 Receiver for those situations where the installation of Citrix Receiver is simply not possible. Note that although the HTML5 Receiver can be used as a fallback option, like the Java client was with Web Interface, it is not generally recommended as the primary Receiver for enterprises to standardize on due to the limited feature set and common browser restrictions around unsecured WebSockets connections (see CTX134123 for more information).

Experience from the Field

- **Furniture distributor** – A furniture distributor maintains a configurator application for various furniture options. The configurator application is accessed via a limited functionality kiosk that is deployed at various furniture outlets, including small, independent retailers with little to no IT staff present. The kiosks are completely locked down in many situations, to the point where even the running of Java applications is limited. The kiosks do feature a modern browser (Google Chrome), and therefore, are able to utilize the HTML5 Receiver in order to provide access to the configurator application.
- **County government** – A government IT organization provides services to all agencies operating in the county. A mixture of full desktops are applications are deployed to both Windows based desktops and iPads. Since the desktops are joined to the Active Directory domain, GPOs are utilized to deploy and configure Citrix Receiver. Mobile users accessing the Citrix environment via an iPad install and configure Receiver from the App Store. To allow for seamless provisioning, email based discovery was configured. This allows users to configure Receiver for both internal and external access through NetScaler Gateway by entering in their email address.

The following mechanisms are commonly used to deploy and update Citrix Receiver:

- **StoreFront** – If Citrix StoreFront is available, administrators can deploy Citrix Receiver via a Receiver for Web site by enabling the “Client Detection” feature. When deployed, a Receiver for Web site enables users to access StoreFront stores through a web page. If the Receiver for Web site detects that a user does not have a compatible version of Citrix Receiver, the user is prompted to download and install Citrix Receiver. The Receiver clients can be hosted on the StoreFront server, or users can be directed to citrix.com for the latest Receiver files.
- **Internal download site** – Users may be prevented from downloading software from the Internet, even if they have permission to install applications. Administrator can create an internal website for supported Citrix Receivers or host them on a common software distribution point for a more seamless user experience. This could be an alternative to enabling Client Detection on the StoreFront Receiver for Web site, which can result in an inconsistent user experience depending on browser’s ActiveX settings.
- **Markets and stores** – Citrix Receiver is available on the Windows, Android and iOS stores.
- **Enterprise software deployment** – Many organizations employ an enterprise software deployment (ESD) or Mobile Application Management (MAM) solution. ESD/MAM solutions can be used to deploy Citrix Receiver to managed endpoint devices. Employee-owned devices can only be managed if the user successfully registered the device with the management tool.
- **Master image** – Most organizations have a group of master desktop images, which are deployed to each business owned desktop, laptop, server, or virtual desktop. A common mechanism to ensure access to virtual desktops and applications is to include a supported version of Citrix Receiver in the master image. Subsequent updates to Citrix

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiver are handled either by enterprise software deployment tools or manually.

- **Group policy** – For customers without a robust ESD solution, it is possible to deploy and configure Citrix Receiver via Microsoft Group Policy. Sample start-up scripts that deploy and remove Citrix Receiver are available on Citrix XenApp and XenDesktop media:

  Citrix Receiver and Plugins\Windows\Receiver\Startup_Logon_Scripts

- **Manual install** – All supported versions of Citrix Receiver are available from the Citrix Receiver Download site. Upon landing on this site, client detection is performed and a platform and operating system specific link is provided to allow users to download an appropriate edition of Citrix Receiver. It is important to note that no configuration will be accomplished via this download, so users will receive the first time use prompt to enter a server URL or email address. This option is likely to be utilized in a BYOD environment.

Selecting the appropriate deployment method is based on the type of Citrix Receiver selected. The following table should be referenced to help identify the appropriate deployment options for Citrix Receiver.

In the table,

- **Y** indicates "recommended.
- **N** equals "not recommended.

Deployment options	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Base image	Y	Y	Y	N	N
EDS/MAM	N	Y	Y	N	N
Group Policy	N	Y	Y	N	N
Receiver for Web site	N	Y	Y	N	N
Internal download site	N	Y	Y	N	N
App store	N	N	N	Y	Y

Decision: Initial Configuration

Citrix Receiver must be configured in order to provide access to enterprise resources. The method of configuration varies by Citrix Receiver edition, the form factor of the device, and lastly the access method (local or remote) that is involved. Several methods may be viable for an organization. The method utilized is contingent on the resources (people, systems, time) available as well as larger organizational initiatives such as BYOD programs.

The following methods can be used to configure Citrix Receiver:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Email based discovery** – The latest releases of Citrix Receiver can be configured by entering an email address. Email based discovery requires Citrix StoreFront as well as an SRV DNS record which points to the FQDN of the StoreFront server.

  Note: Any DNS platform should support email-based discovery, however only Windows DNS has been explicitly tested.

  For remote access, NetScaler Gateway must be utilized with the corresponding SRV record in external DNS. A valid server certificate on the NetScaler Gateway appliance or StoreFront server must be present in order to enable email-based account discovery. This configuration assumes that the portion of the email address after the "@" is the DNS namespace that should be queried for this SRV record. This can be challenging for customers with different external and internal namespaces or email addresses that are different from DNS namespaces.

- **Group policy** – Microsoft Group Policy can be used to configure Citrix Receiver. This can be done via start up scripts used to deploy Receiver by ensuring there is a value for the SERVER_LOCATION=Server_URL parameter or by using the ADMX/ADML template files included with the installation of Citrix Receiver to set the StoreFront Account List option in conjunction with another Receiver deployment method. Provide the URL of the server running Citrix StoreFront in the format https://baseurl/Citrix/storename/discovery.
- **Provisioning file** – For environments running StoreFront, it is possible to provide users with a provisioning file that contains store information. Provisioning files are exported from the StoreFront console. The file is saved with a "*.cr" extension and can then be placed on a shared network resource, a Receiver for Web site, or other web based resource or emailed to users. The file can then be launched from an endpoint, which automatically configures Citrix Receiver to use the store(s). If users browse to the Receiver for Web site and select the "Activate" option under their username, this also automatically downloads this same ".cr" file and configure the Receiver client for users.
- **Manually** – If allowed, it is usually possible to configure Citrix Receiver manually by entering the server URL. This method should be reserved for administrators or users that have advanced knowledge.
- **Studio** – In addition to the above methods, in order to configure Receiver deployed on a virtual desktop or server image (within a XenDesktop or XenApp environment), it is possible to set the StoreFront address via the properties of the Delivery Group.

Decision: Updates

Citrix Receiver is in active development. As such, periodic updates are released that provide enhanced functionality or address user issues. As with any actively developed product, the latest version of these products should be deployed to the endpoints so that users benefit from the latest functionality and to maintain compliance with product support lifecycles. There are multiple methods available to update Citrix Receiver and, if applicable, associated plug-ins.

- **Auto-Update** – Receiver for Windows 4.8+ and Receiver for Mac 12.6+ includes an autoupdate capability that automatically checks for newer versions of Receiver. The autoupdate service can be configured to allow users to defer updates as well as to skip any updates that are not long-term service release (LTSR) versions. Receiver for iOS and Android are automatically updated through their appropriate store.
- **Enterprise software deployment** – ESD tools provide an organization with direct control over the time/frequency of Receiver updates to managed devices. Additional thought must be given to updating unmanaged devices and endpoints outside of the corporate firewall.
- **Manual updates** – When no automated solution is available, manual methods can be used to update Citrix Receiver. Whether deployed on Receiver for Web site, StoreFront, an internal Citrix Receiver site, or an external site, these options will require user involvement in updating Citrix Receiver. Due to the involved nature of manual updates coupled with the opportunity for a user mistake, this option should only be considered as a last resort.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology access layer

May 07, 2018

The second layer of the design methodology is the access layer, which is defined for each user group.

Creating an appropriate design for the access layer is an important part of the desktop virtualization process. This layer handles user validation through authentication and orchestrates access to all components necessary to establish a secure virtual desktop connection.

The access layer design decisions are based on the mobility requirements of each user group as well as the endpoint devices used.

Authentication

Getting access to resources is based on the user's identity. Defining the authentication strategy takes into account the user's entry point into the environment as well as how the user will authenticate.

Decision: Authentication Provider

Traditionally, users required an Active Directory username and password to get access to their XenApp and XenDesktop resources. As most organizations standardized on an on-premises Active Directory deployment, this particular requirement was simple to achieve.

Organizations are using external contractors, which requires an account to get access to the XenApp and XenDesktop resources.Organizations are investigating the use of a third party identity provider (IdP) like Azure Active Directory, Google, LinkedIn, etc., instead of managing their own.

With the implementation of Citrix Federated Authentication Service, XenApp and XenDesktop supports the use of a third party IdP. An administrator can have a contractor use their Google account to gain access to their approved applications and desktops, simplifying onboarding.

Decision: Authentication Point

Before a user connects to a virtual resource, they must first authenticate. The place of authentication is often determined by the user group's mobility requirements, which were defined during the user segmentation process. There are two authentication points available in XenDesktop:

- **StoreFront** – Citrix StoreFront provides authentication and resource delivery services for Citrix Receiver, enabling centralized enterprise stores to deliver desktops, applications and other resources.
- **NetScaler Gateway** – NetScaler Gateway is an appliance providing secure application access and granular application-level policy controls to applications and data while allowing users to work from anywhere.

The following table lists preferred authentication points according to user group mobility requirements:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Group's Mobility Requirement	Preferred Authentication Point
Local	StoreFront
Roaming Local	StoreFront
Remote	NetScaler Gateway
Local	NetScaler Gateway

Authentication for user groups with a mobility requirement of remote or mobile may occur directly on StoreFront where required. For example, DMZ security policies may prohibit access from the NetScaler Gateway to the domain, which is required to support Smartcard client certificate authentication. Access to StoreFront for authentication may then be delivered via a NetScaler SSL_BRIDGE virtual server, which provides a conduit for https traffic. Typically, the virtual server would be hosted alongside a NetScaler Gateway on the same NetScaler configured to provide HDX Proxy access to the virtual desktop environment. Although such a use case may sometimes be necessary, the recommended best practice is to authenticate external users via NetScaler Gateway.

Decision: Authentication Policy

Once the authentication point has been identified, the type of authentication must be determined. The following options are the primary methods available:

- **StoreFront** – Supports a number of different authentication methods, although not all are recommended depending on the user access method, security requirements and network location. Note that by default StoreFront authenticates users directly with Active Directory, not via XML as Web Interface did. StoreFront 3.0+ can be optionally configured to delegate authentication to XML if required (such as if the StoreFront servers are in a domain that does not trust the user domains).
  - **User name and password** – Requires users to logon directly to the site by entering a user name and password.
  - **Domain pass-through** – Allows pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores.
  - **NetScaler Gateway pass-through** – Allows pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
  - **Smart card** – Allows users to authenticate using smart cards and PINs through Citrix Receiver for Windows and NetScaler Gateway. To enable smart card authentication, user accounts must be configured either within the Microsoft Active Directory domain containing the StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain. Multi-forest deployments involving one-way trust or trust relationships of different types are not supported.
  - **Anonymous** – Allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. Local anonymous accounts are created on demand on the Server VDA when sessions are launched. This requires a StoreFront store configured for authenticated access, a Server OS based VDA, and a XenApp Delivery Group configured for unauthenticated users.
- **NetScaler Gateway** – The NetScaler Gateway supports several authentication methods. The list below includes those

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily used in virtual desktop environments. Each may be used individually, but are often combined to provide multi-factor authentication.

- **LDAP** – The lightweight directory access protocol (LDAP) is used to access directory information services such Microsoft Active Directory. NetScaler Gateway uses LDAP to authenticate users and extract their group membership information.
- **RADIUS (token)** – Remote authentication dial in user service (RADIUS) is a UDP based network security protocol that provides authentication, authorization and accounting. A network access server (NetScaler Gateway in this case) forwards credentials to a RADIUS server that can either check the credentials locally, or check them against a directory service. The RADIUS server could then accept the connection, reject the connection, or challenge and request a second form of authentication such as a token.
- **Client certificate** – Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of a client certificate presented to the virtual server. Client certificates are usually disseminated to users in the form of smartcards or common access cards (CACs) that are read by a reader attach to each user's device.

The authentication type for a user group is often determined based on security requirements as well as the authentication point used. The following table helps define the appropriate solution for each user group based on the level of security required:

Authentication Point	Security Requirement	Authentication Type
StoreFront	• Low • Medium • High	Low: • LDAP user name and password • Pass-through Medium • LDAP user name and password • Pass-through High: LDAP and/or Smartcard
NetScaler Gateway	• Low • Medium • High	Low: LDAP user name and password Medium: LDAP user name and password High: • LDAP and Token • LDAP and Smartcard • Token and Smartcard

Experience from the Field

- **Retail** – A small private retail company provides virtual desktop users with access to non-sensitive data such as marketing catalogs and email. They are not required to adhere to security regulations such as Sarbanes Oxley. Therefore, LDAP authentication has been implemented based on user name and password.
- **Financial** – A medium financial enterprise provides their virtual desktop users with access to confidential data such as banking transaction records. They are governed by security regulations such as the Statement on Accounting Standards (SAS) 70 and are required to utilize multi-factor authentication for remote access users. LDAP authentication has been implemented based on user name and password along with RADIUS authentication using tokens.
- **Government** – A large federal institution provides virtual desktop users with access to highly confidential data such as

© 1999-2017 Citrix Systems, Inc. All rights reserved.

private citizens' personal records. They are subject to regulation by Department of Defense (DOD) security standards. LDAP authentication has been implemented based on user name and password, along with Client Certificate authentication using CAC cards.
- **Healthcare** - A hospital is using XenApp to deliver their EMR application to users. ThinClient devices on stationary and mobile carts are being used by doctors and nurses to capture and retrieve patient data. Unauthenticated access has been configured to prevent medical staff from having to authenticate to the domain as well as the EMR application.

StoreFront

Citrix StoreFront authenticates users to XenApp and XenDesktop resources. StoreFront enumerates and aggregates available desktops and applications into a single interface that users access through Citrix Receiver for Windows, iOS, Android, or the StoreFront web site.

Decision: High Availabiity

If the server hosting StoreFront is unavailable, users will not be able to launch new virtual desktops, published applications or manage their subscriptions. Therefore at least two StoreFront servers should be deployed to prevent this component from becoming a single point of failure. By implementing a load balancing solution, users will not experience an interruption in their service. Options include:

- **Hardware load balancing** – An intelligent appliance, which is capable of verifying the availability of the StoreFront service and actively load balance user requests appropriately. Citrix NetScaler is a great example of a hardware load balancer. Citrix NetScaler is an ideal load balancer, coming pre-configured with StoreFront health checks.
- **DNS round robin** – Provides rudimentary load balancing across multiple servers without performing any checks on availability. If a StoreFront server becomes unavailable, DNS round robin would still route users to the failed server. Because of this, DNS round robin is not recommended by Citrix.
- **Windows network load balancing** – A Windows service capable of performing rudimentary checks to verify the server is available but cannot determine the status of individual services. This can cause users to be forwarded to StoreFront servers which are not able to process new requests. The user would then not be able to access applications or desktops.

Decision: Delivery Controller Reference

To provide users with desktops and applications, StoreFront must be configured with the IP address or DNS name of at least one Controller in each XenDesktop and XenApp site. For fault tolerance, multiple controllers should be entered for each site and/or farm specified. By default, StoreFront treats a list of servers in failover order (active/passive).

For large deployments or environments with a high logon load an active distribution of the user load (active/active) is recommended. This can be achieved by means of a load balancer with built-in XML monitors, such as Citrix NetScaler or by configuring StoreFront to load balance the list of Controllers instead of treating them as an ordered list.

Decision: Beacons

Citrix Receiver uses beacons (websites) to identify whether a user is connected to an internal or external network. Internal users are connected directly to StoreFront for authentication while external users are connected via Citrix NetScaler Gateway. It is possible to control what a user sees by restricting applications due to which beacon they have access to.

The internal beacon should be a site that is not resolvable externally. By default, the internal beacon is the StoreFront base URL. This will have to be adjusted if the same external and internal URL is configured. The external beacon can be any external site that produces an http response. Citrix Receiver continuously monitors the status of network connections (for example, link up, link down or change of the default gateway). When a status change is detected, Citrix Receiver first verifies that the internal beacon points can be accessed before moving on to check the accessibility of external beacon

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

points. StoreFront provides Citrix Receiver with the http(s) addresses of the beacon points during the initial connection/configuration download process and provides updates as necessary. It is necessary to specify at least two highly available external beacons that can be resolved from public networks.

Decision: Resource Presentation

By default, StoreFront allows users to choose (subscribe) to the resources they want to regularly use after they logon (favorites). This approach, deemed “Self-Service,” allows users to restrict the resources that they see on their home screen to the ones that they use on a regular basis. The resources chosen by every user for each store are recorded by the subscription store service and stored locally on each StoreFront server (synced automatically between servers in the same server group) so that they can be displayed on the Citrix Receiver home screen from any device that the user connects from. Although by default subscriptions are per store and per server group, administrators can configure two stores within a server group to share a subscription database and/or sync subscriptions between two identically named stores in two separate server groups on a defined schedule if required.

Administrators should determine which applications should always be displayed to users on their home screen or the featured tab. In general, these applications are common applications such as the Microsoft Office Suite and any other applications that every user in an environment may need. StoreFront can filter/present these resources using Keywords defined within the published application properties Description field.

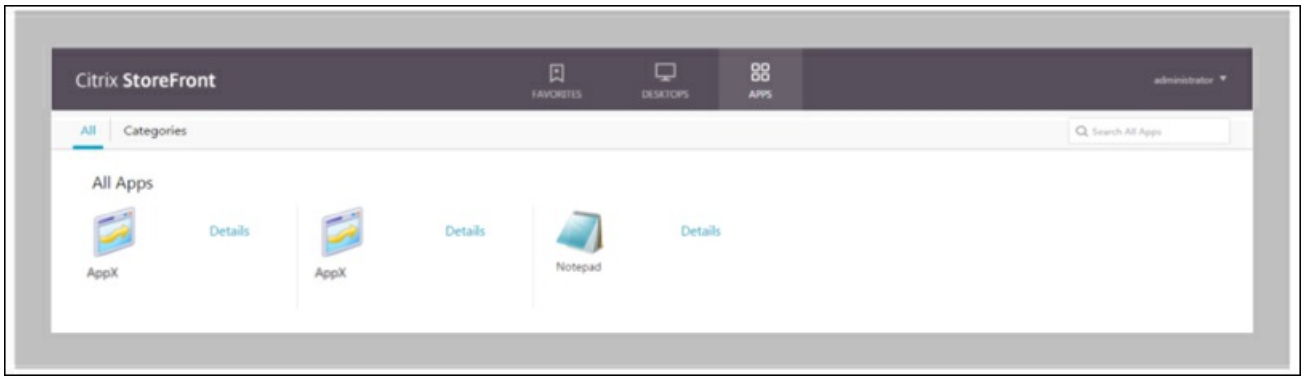
The following table explores the Keyword options:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Keyword	Description
Auto	Automatically subscribes all users of a store to an application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application. Users can choose to subsequently remove this subscription if desired.
Mandatory	New in StoreFront 2.5, the Mandatory keyword will make applications automatically be subscribed to users of the store. However, users will not have the option to remove the application. This setting is useful when creating a core set of applications which must always be presented to all users.
Featured	Advertise applications to users or make commonly used applications easier to find by listing them in the Receiver Featured list.
Prefer	Specify a locally installed application should be used instead of an application available in Receiver. Receiver searches for the specified name/path to determine if the application is installed locally. If it is, Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Receiver window, Receiver starts the locally installed (preferred) application. If a user uninstalls a preferred application outside of Receiver, the application is unsubscribed during the next Receiver refresh. If a user uninstalls a preferred application from the Receiver window, Receiver unsubscribes the application but does not uninstall it.
TreatAsApp	By default, XenDesktop VDI desktops and XenApp hosted shared desktops are treated like other desktops by Receiver for Web sites. By using the keyword "TreatAsApp," the desktop will be displayed in the application views of Receiver for Web sites rather than the desktop views. Users are required to subscribe before they can access the desktop.
Primary	When in a multi-site deployment, using this keyword ensures that an application is delivered from a designated site. If an application is available from multiple sites, with the same name, the application from the secondary site will only be displayed if the application is not available from the primary site.
Secondary	A same property as the "Primary" keyword, except it designates an application in the secondary site.

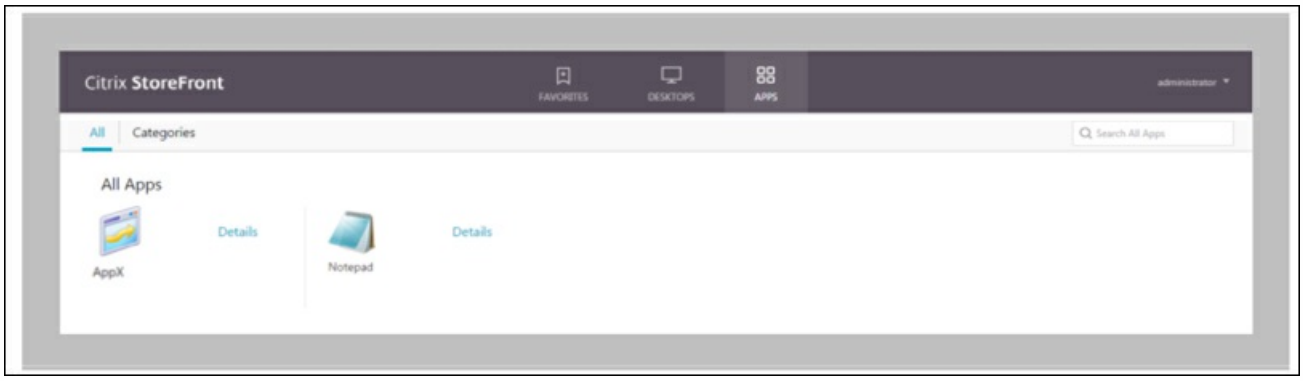
Decision: Aggregation Groups

If the XenApp/XenDesktop solution includes multiple delivery sites, StoreFront merges the available resources together so the user has a single interface for all published resources. However, if multiple sites publish the same resources, the user might experience confusion as a single application appears multiple times.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFront aggregation groups define how the resources in multiple sites merge to provide the user with a single, easy to understand view. StoreFront aggregates duplicate published resources into a single icon.



The administrator must determine how to load balance users across the different XenApp/XenDesktop sites when the icon is an aggregation. The options are:

- **Load Balancing** – Used when the duplicate sites are created based on capacity recommendations. StoreFront distributes user requests across all configured sites.
- **Failover** – Used when geographies need to have resources available in the event of an outage or when migrating users from one site to another site (like a XenApp migration project).

It is advisable to document the users, stores and aggregation methods during the design phase.

User Group	Available Store(s)	Load Balancing Stores	Failover Stores
NA_FinanceUsers	NA_West_Store NA_East_Store EMEA_Store	NA_West_Store NA_East_Store	EMEA_Store
EMEA_SalesUsers	EMEA_Store NA_East_Store	EMEA_Store	NA_East_Store

Decision: Scalability

The number of Citrix Receiver users supported by a single StoreFront server depends on the resources assigned and level of user activity. Note that Receiver for Web users will consume more RAM on average than native Receiver users, but a minimum of 4 GB of RAM is recommended per StoreFront server in all cases as a baseline. Additionally, more sites/farms enumerated per store will increase both CPU utilization and server response time, with XenApp IMA farms having a greater scalability impact than XenApp/XenDesktop FMA site.

StoreFront deployment	CPU Usage	Simultaneous activities
Standalone deployment • 4CPUs	75%	291 per second

© 1999-2017 Citrix Systems, Inc. All rights reserved.

• 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	90%	375 per second
Cluster StoreFront deployment 2 Nodes each with: • 4 CPUs • 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	75%	529 per second
	90%	681 per second

Tests have shown diminishing returns after a single StoreFront deployment grows beyond 3-4 StoreFront nodes with a maximum of 5-6 servers supported in a single server group.

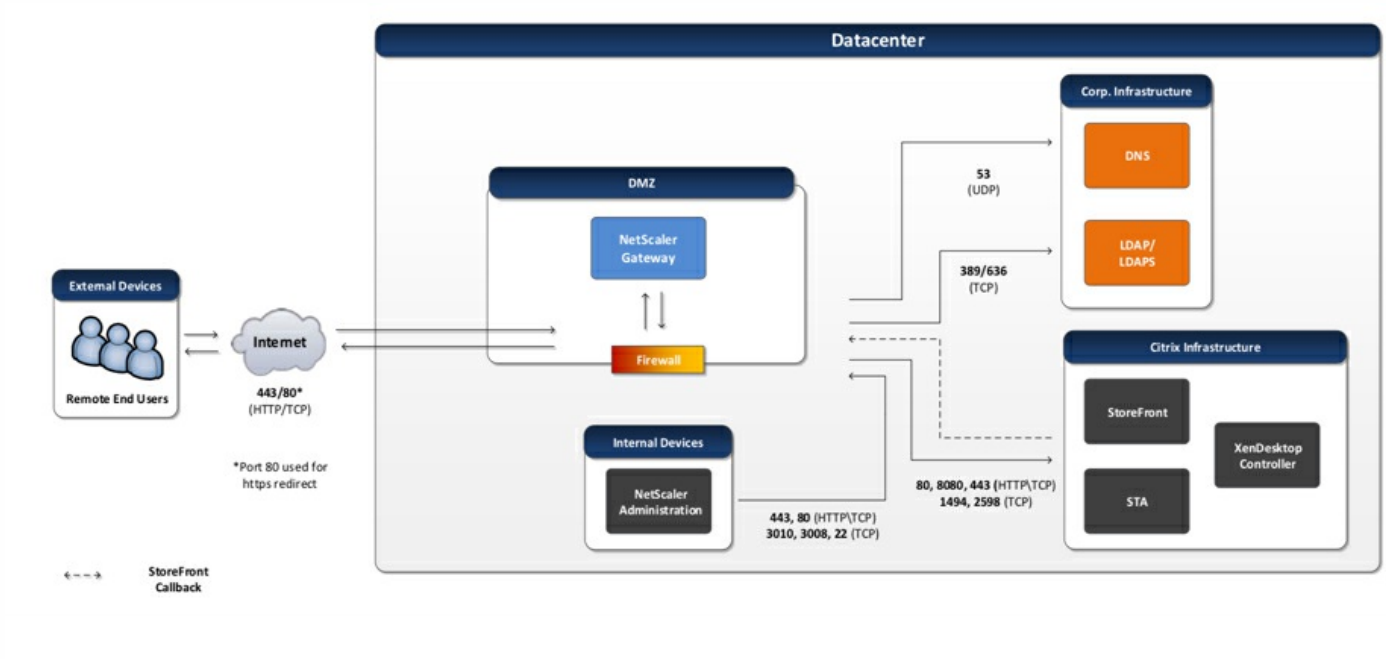
NetScaler Gateway

User groups utilizing NetScaler Gateway as their authentication point have additional design decisions to consider. These design decisions are not applicable for non-NetScaler Gateway authentication points.

Decision: Topology

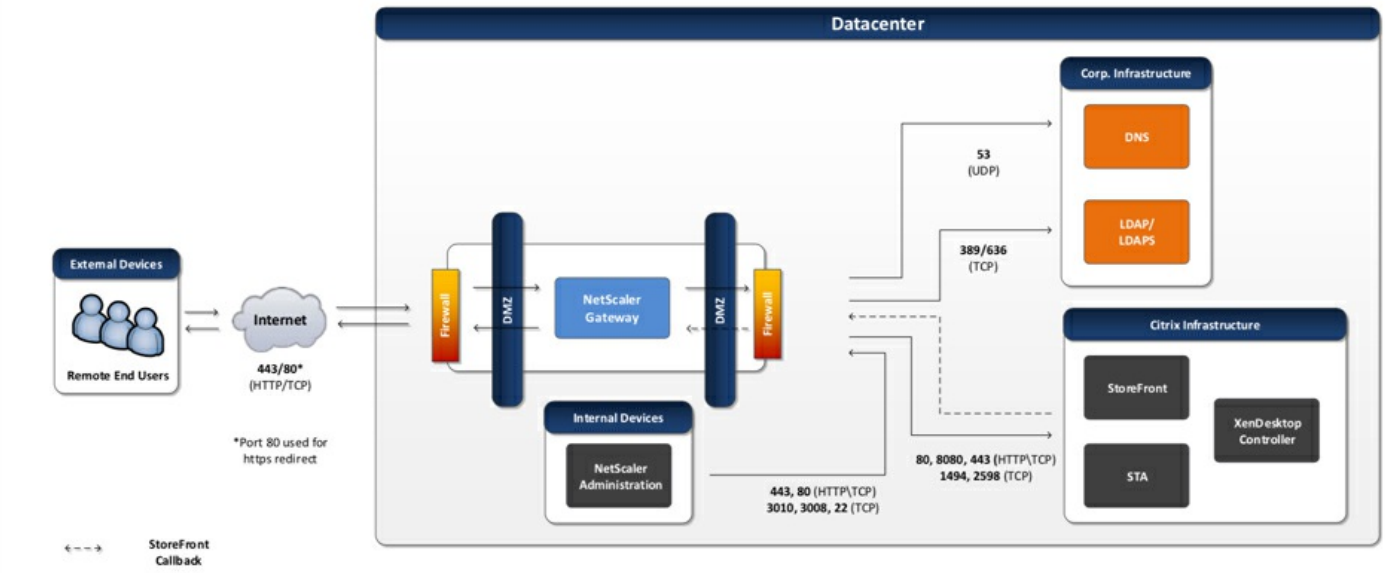
Selection of the network topology is central to planning the remote access architecture to ensure that it can support the necessary functionality, performance and security. The design of the remote access architecture should be completed in collaboration with the security team to ensure adherence to corporate security requirements. There are two primary topologies to consider, each of which provides increasing levels of security:

- **1-Arm (normal security)** – With a 1-arm topology, the NetScaler Gateway utilizes one physical or logical bonded interface, with associated VLAN and IP subnet, to transport both frontend traffic for users and backend traffic for the virtual desktop infrastructure servers and services.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **2-Arm (high security)** – With a 2-arm topology, the NetScaler Gateway utilizes two or more physically or logically bonded interfaces, with associated VLANS and IP subnets. Transport of the frontend traffic for users is directed to one of these interfaces. The frontend traffic is isolated from backend traffic, between the virtual desktop infrastructure servers and services, which is directed to a second interface. This allows the use of separate demilitarized zones (DMZs) to isolate frontend and backend traffic flows along with granular firewall control and monitoring.



Decision: High Availabiity

If the NetScaler Gateway is unavailable, remote users will not be able to access the environment. Therefore at least two NetScaler Gateway hosts should be deployed to prevent this component from becoming a single point of failure.

When configuring NetScaler Gateway in a high availability (active/passive) pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway.

Note that in firmware 10.5 and above, clustering is also possible with multiple NetScaler Gateway instances to provide high availability, although support for spotted versus stripped configurations varies by firmware and Gateway configuration (full SSL VPN versus ICA proxy).

(http://docs.citrix.com/en-us/netscaler/11-1/clustering/cluster-features-supported.html)

Decision: Platform

In order to identify an appropriate NetScaler platform to meet project requirements, the key resource constraints must be identified. Since all remote access traffic will be secured using the secure sockets layer (SSL), transported by Hypertext Transfer Protocol (HTTP) in the form of HTTPs, there are two resource metrics that should be targeted:

- **SSL throughput** – The SSL throughput is the gigabits of SSL traffic that may be processed per second (Gbps).
- **SSL transactions per second (TPS)** – The TPS metric identifies how many times per second an Application Delivery Controller (ADC) may execute an SSL transaction. The capacity varies primarily by the key length required. TPS capacity is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily a consideration during the negotiation phase when SSL is first setup and it is less of a factor in the bulk encryption / decryption phase, which is the majority of the session life. While TPS is an important metric to monitor, field experience has shown that SSL throughput is the most significant factor in identifying the appropriate NetScaler Gateway.

The SSL bandwidth overhead average is often considered negligible relative to the volume of virtual desktop traffic and is not typically accounted for as part of required SSL throughput. However, making provisions for SSL bandwidth will help ensure the total throughput estimated is sufficient. The fixed bandwidth added to packet headers can vary according to the encryption algorithms used and the overall percentage of bandwidth may vary widely according to packet size. Ideally, the overhead should be measured during a proof of concept or pilot. However, in the absence of such data incrementing the workload bandwidth by 2% is a reasonable rule of thumb. Therefore, to determine the SSL throughput required by a NetScaler platform, multiply the maximum concurrent bandwidth for a datacenter by 1.02:

□□□ □*h*□□□□*h*□□□ = □□□□□□□ □□□□□□□□□□ □□□□□□□□*h* ∗ 1.02

For example, assuming 128Mbps maximum concurrent bandwidth, the appropriate NetScaler model can be determined as follows:

~130□□□□ = 128□□□□ ∗ 1.02

The SSL throughput value should be compared to the throughput capabilities of various NetScaler platforms to determine the most appropriate one for the environment. There are three main platform groups available, each of which provides broad scalability options.

- **VPX** – A NetScaler VPX device provides the same full functionality as hardware NetScaler. However, NetScaler VPXs can leverage 'off the shelf' servers for hosting and are suitable for small to medium sized environments. Typically, organizations create a baseline cap for the VPX instances at 500 users.
- **MPX** – A NetScaler MPX is the hardware version of the NetScaler devices. The MPX device is more powerful than the virtual NetScaler and can support network optimizations for larger scale enterprise deployments, particularly when SSL offload will be configured as this is done in software on the VPX versus dedicated SSL chips on the MPX.
- **SDX** – A NetScaler SDX is a blend between the virtual and physical NetScaler devices. An SDX machine is a physical device capable of hosting multiple virtual NetScaler devices. This consolidation of devices aids with reducing required shelf space and device consolidation. NetScaler SDXs are suitable for handling network communications for large enterprise deployments and/or multi-tenant hosting providers.

SSL throughput capabilities of the NetScaler platforms may be found in the Citrix NetScaler data sheet. Therefore, based on the example calculation above, a NetScaler MPX 5550 appliance would be sufficient to handle the required load. However, actually scalability will depend on security requirements. NetScaler SSL throughput decreases with the use of increasingly complex encryption algorithms and longer key lengths. Also, this calculation represents a single primary NetScaler. At a minimum, N+1 redundancy is recommended which would call for an additional NetScaler of the identical platform and model.

> **注意**
>
> The Citrix NetScaler data sheet typically represents throughput capabilities under optimal conditions for performance. However, performance is directly affected by security requirements. For example, if the RC4 encryption algorithm and a 1k key length are used, a VPX platform may be able to handle more than 500 HDX proxy connections. However, if a 3DES encryption algorithm and 2k key length are used (which are becoming more common), the throughput may be halved.

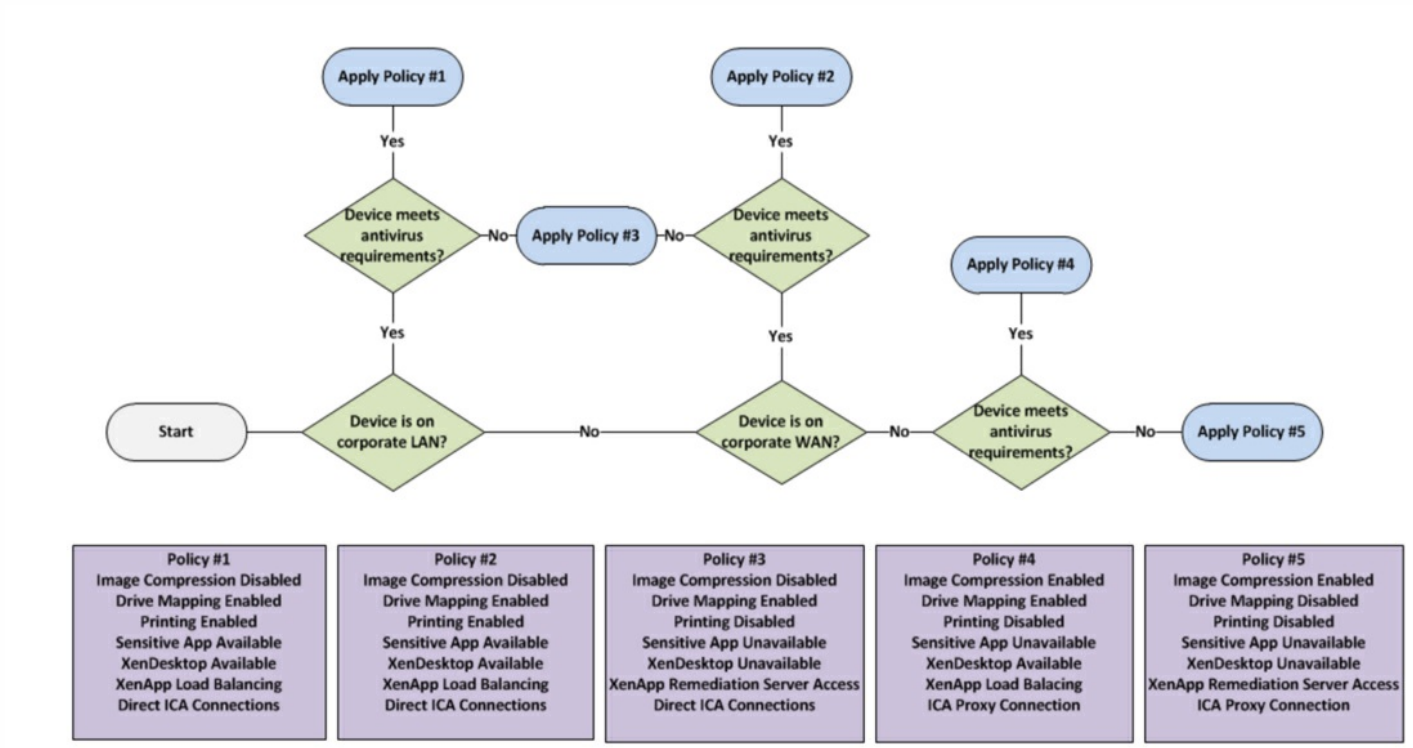
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Pre-Authentication Policy

An optional pre-authentication policy may be applied to user groups with NetScaler Gateway as their authentication point. Pre-authentication policies limit access to the environment based on whether the endpoint meets certain criteria through Endpoint Analysis (EPA) Scans.

Pre-authentication access policies can be configured to test antivirus, firewall, operating system, or even registry settings. These policies can be used to prevent access entirely or can be used by XenDesktop to control session features such as clipboard mapping, printer mapping and even the availability of specific applications and desktops. For example, if a user device does not have antivirus installed, a filter can be set to hide sensitive applications.

The following figure provides an overview of how multiple policies can be used to customize the features of a virtualization resource:



Experience from the Field

- **Retail** – A small private retail company use EPA to scan for the presence of updated antivirus definitions prior to allowing access.
- **Financial** – A medium financial enterprise use EPA scans of the Domain SID to verify that users are members of the enterprise domain prior to allowing access.
- **Government** – A large federal institution use EPA to scan endpoint devices to ensure that a specific certificate (or set of certificates) has been installed on the device prior to allowing access.

Decision: Session Policy

User groups with NetScaler Gateway as their authentication point must have corresponding session policies defined. Session policies are used to define the overall user experience postauthentication.

Organizations create sessions policies based on the type of Citrix Receiver used. For the purpose of session policy

© 1999-2017 Citrix Systems, Inc. All rights reserved.

assignment, devices are commonly grouped as either non-mobile (such as Windows, Mac and Linux OS based), or mobile (such as iOS or Android). Therefore, a decision on whether to provide support for mobile devices, non-mobile devices, or both should be made based on client device requirements identified during the assess phase.

To identify devices session policies, include expressions such as those discussed in this article.

- **Mobile devices** – The expression is set to REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver which is given a higher priority than the non-mobile device policy to ensure mobile devices are matched while non-mobile devices are not.
- **Non-mobile devices** – The expression is set to ns_true which signifies that it should apply to all traffic that is sent to it.

An alternative use of session policies is to apply endpoint analysis expressions. These session policies are applied post authentication yet mimic the previously mentioned pre-authentication policies. Use of session policies is an option to provide a fallback scenario to endpoints that do not meet full security requirements such read-only access to specific applications.

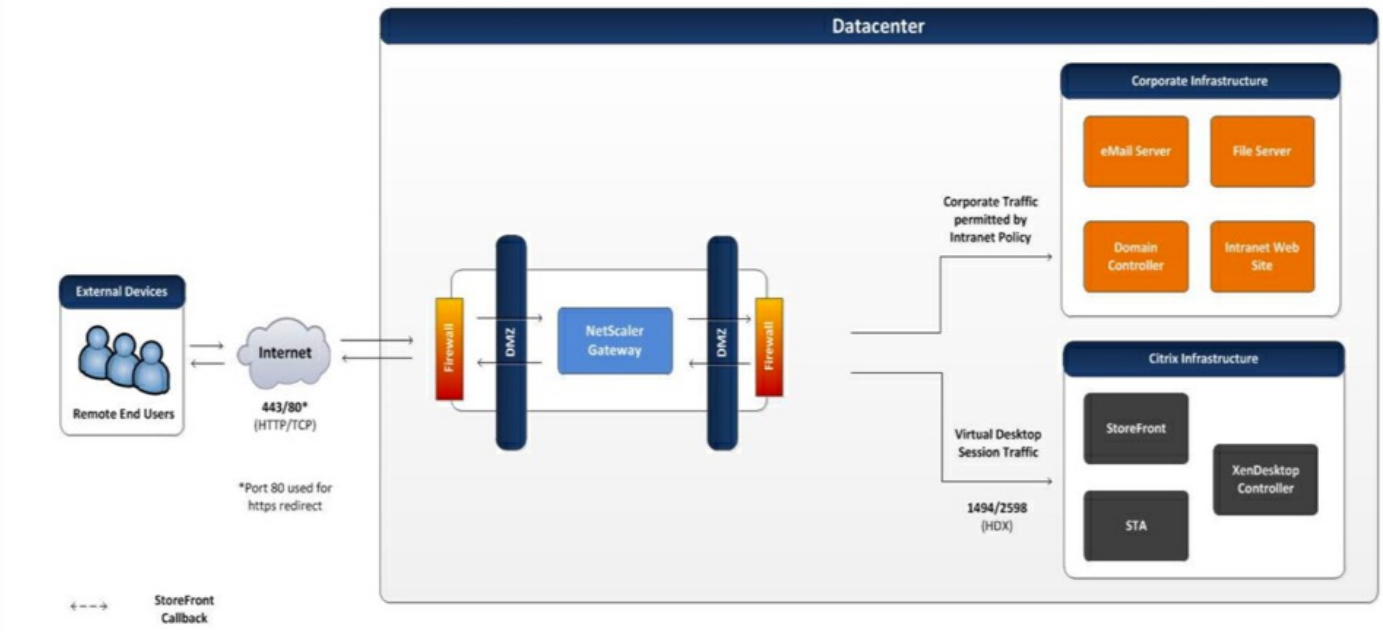
Decision: Session Profile

Each session policy must have a corresponding session profile defined. The session profile defines details required for the user group to gain access to the environment. There are two primary forms of session profiles that determine the access method to the virtual desktop environment:

- **SSLVPN** – Users create a virtual private network and tunnel all traffic configured by IP addresses through the internal network. The user's client device is able to access permitted intranet resources as if it were on the internal network. This includes XenDesktop sites and any other internal traffic such as file shares or intranet websites. This is considered a potentially less secure access method since network ports and routes to services outside of the virtual desktop infrastructure may be opened leaving the enterprise susceptible to risks that may come with full VPN access. These risks may include denial of service attacks, attempts at hacking internal servers, or any other form of malicious activity that may be launched from malware, Trojan horses, or other viruses via an Internet based client against vulnerable enterprise services via routes and ports.

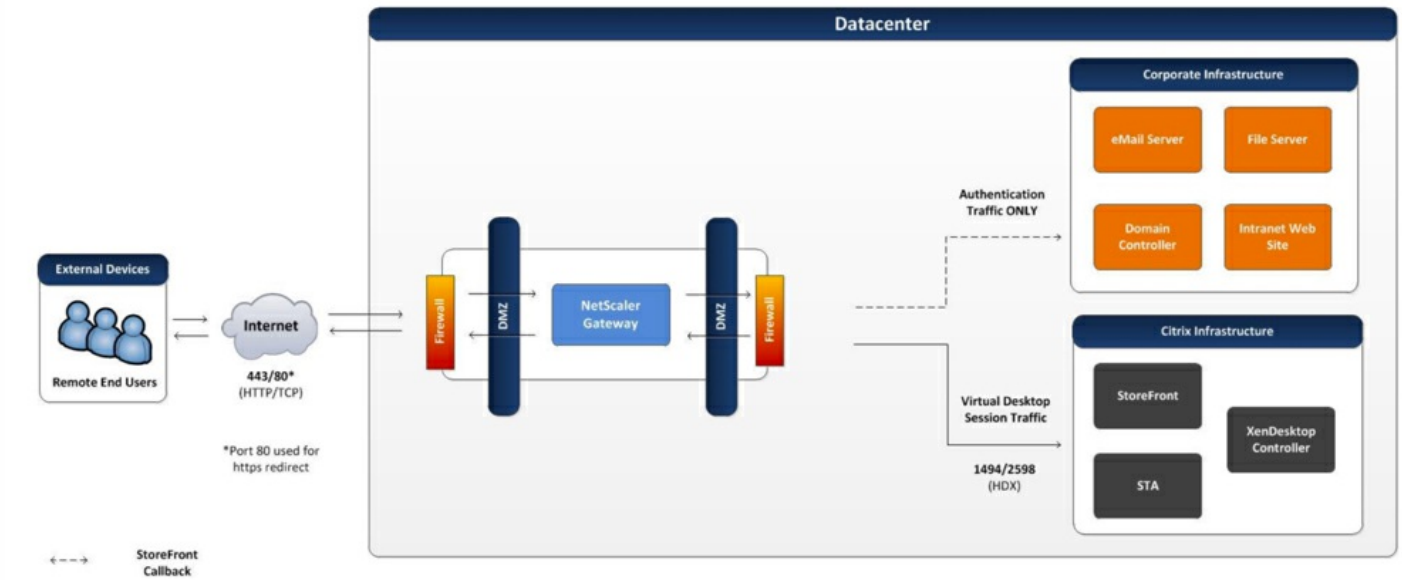
  Another decision to consider when SSLVPN is required is whether to enable split tunneling for client network traffic. By enabling split tunneling, client network traffic directed to the intranet by Citrix Receiver may be limited to routes and ports associated with specific services. By disabling split tunneling, all client network traffic is directed to the intranet, therefore both traffic destined for internal services as well as traffic destined for the external services (Internet) traverses the corporate network. The advantage of enabling split tunneling is that exposure of the corporate network is limited and network bandwidth is conserved. The advantage of disabling split tunneling is that client traffic may be monitored or controlled through systems such as web filters or intrusion detection systems

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **HDX proxy** – With HDX Proxy, users connect to their virtual desktops and applications through the NetScaler Gateway without exposing internal addresses externally. In this configuration, the NetScaler Gateway acts as a micro VPN and only handles HDX traffic. Other types of traffic on the client's endpoint device, such as private mail or personal Internet traffic do not use the NetScaler Gateway.

  Based on the endpoint and Citrix Receiver used, a decision must be made as to whether this method is supported for each user group. HDX Proxy is considered a secure access method for remote virtual desktop access since only traffic specific to the desktop session is allowed to pass through to the corporate infrastructure. Most Citrix Receivers support HDX Proxy and it is the preferred method:



Decision: Preferred Datacenter

Enterprises often have multiple active datacenters providing high availability for mission critical applications. Some virtual

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

desktops or applications may fall into that category while others may only be accessed from a specific preferred datacenter. Therefore, the initial NetScaler Gateway that a user authenticates to in a multi-active datacenter environment may not be within the preferred datacenter corresponding to the user's VDI resources. StoreFront is able to determine the location of the user's assigned resources and direct the HDX session to those resources; however, the resulting path may be sub-optional (WAN connection from the NetScaler Gateway to the virtual desktop/application resources as opposed to LAN connection).

There are static and dynamic methods available to direct HDX sessions to their virtual desktop resources in their primary datacenter. The decision regarding which method to select should be based on the availability of technology to dynamically assign sites links such as Global Server Load Balancing (GSLB) along with the network assessment of intranet and Internet bandwidth as well as Quality of Service (QoS) capabilities.

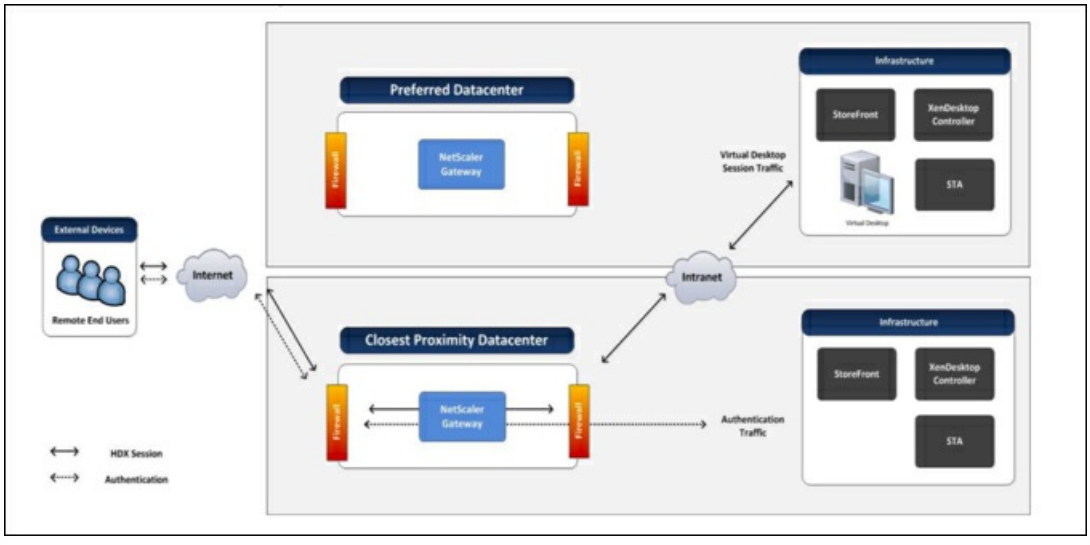
> **注意**
>
> For more information on configuring the static and dynamic methods of GSLB, please refer to Citrix Product Documentation - Configuring GSLB for Proximity.

Static

- **Direct** – The user may be given a FQDN mapped to an A record that is dedicated to the primary datacenter NetScaler Gateway(s) allowing them to access their virtual desktop directly wherever they are in the world. This approach eliminates a layer of complexity added with dynamic allocation. However, it also eliminates fault tolerance options such as the ability to access the virtual desktop through an alternative intranet path when a primary datacenter outage is limited to the access infrastructure.

Dynamic

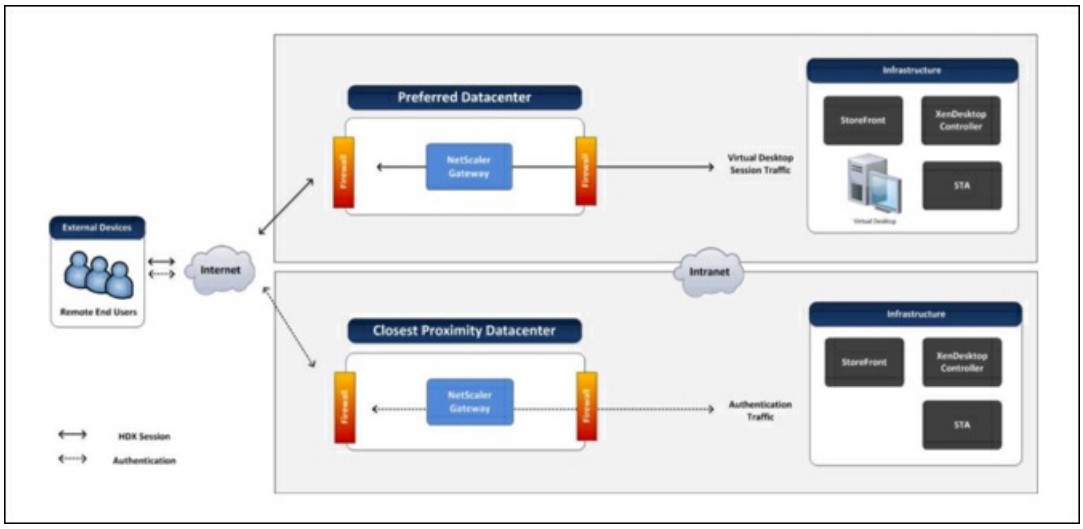
- **Intranet** – For most dynamic environments, the initial datacenter selected for authentication is the one closest to the user. Protocols such as GSLB dynamic proximity calculate the least latency between the user's local DNS server and the NetScaler Gateway. Thereafter, by default, the HDX session is routed through the same NetScaler Gateway to whichever datacenter is hosting the user's virtual desktops and applications. The advantage of this approach is that the majority of the HDX session would traverse the corporate WAN where quality of service may be used.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Internet** - Alternatively, the HDX session can be re-routed through an alternate NetScaler Gateway proximate to the backend VDI desktop / XenApp server, resulting in most of the HDX session travelling over the Internet. For example, a user with a dedicated desktop in the United Stated, traveling in Europe may be directed to a NetScaler Gateway hosted in a European datacenter based on proximity. However, when the user launches their desktop, an HDX connection will be established to the virtual desktop via a NetScaler Gateway hosted in the preferred datacenter in the United States.

  This conserves WAN network usage (at the cost of QoS) and is recommended in cases where the user's Internet connection may provide a more reliable experience than the corporate WAN.



Some customers will use a combination of these methods, such as geo-specific dynamic URLs such that fault tolerance is provided within a geographic area (such as North America) without incurring the complexity of global GSLB.

Site-to-Site Connectivity

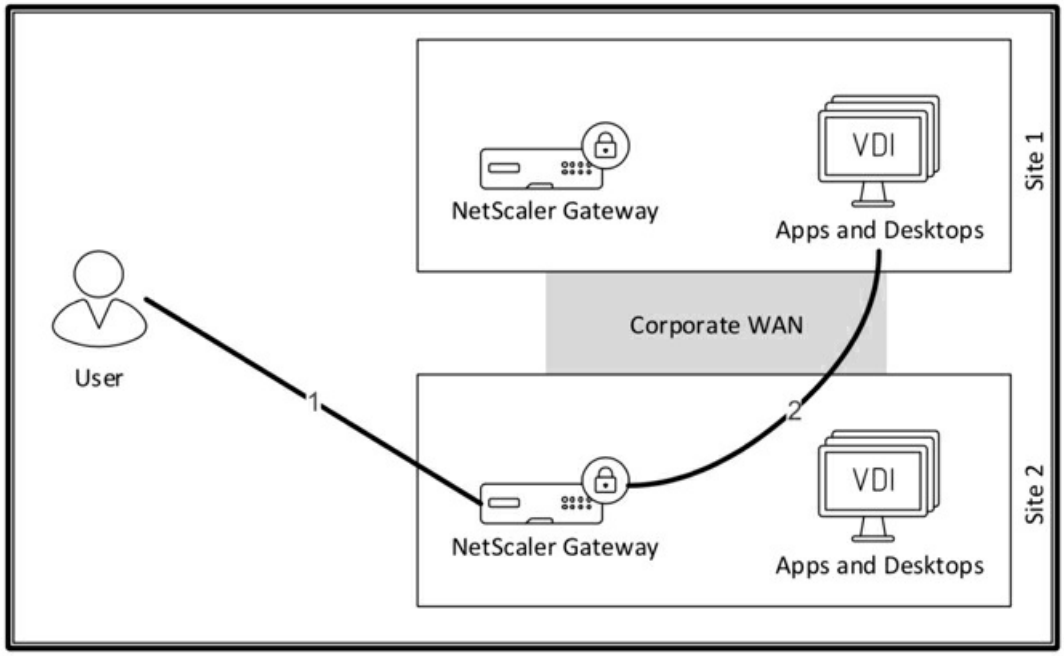
A XenApp and XenDesktop site is capable of spanning multiple locations, In order to successfully implement a multi-site solution, the design must take into account the site-to-site links and XenApp and XenDesktop session routing between locations in order to provide the best user experience.

Decision: HDX Optimized Routing

In a multi-site XenApp and XenDesktop solution, certain criteria, like fastest response time or closest proximity, routes users to the optimal site. These algorithms do not take into account the resources a user wants to access.

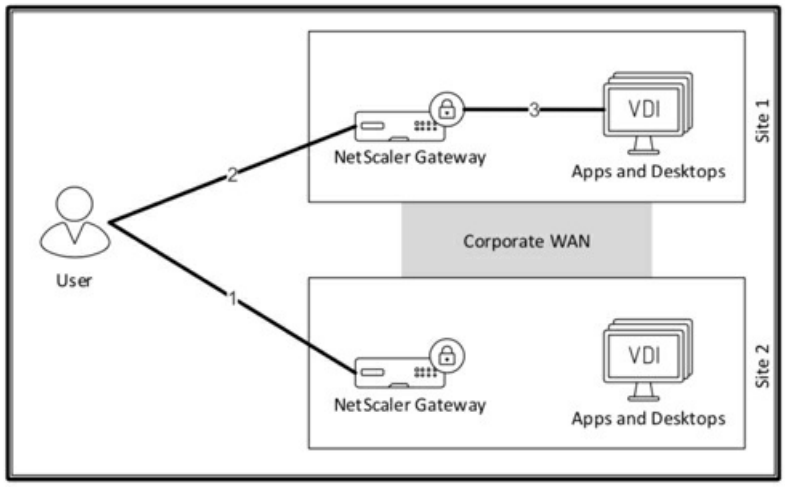
Improper routing of a user's session results in the following:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. User routed to the most preferred site, based on proximity or response time
2. NetScaler Gateway proxies the ICA traffic to the correct resource, which could be across the corporate WAN.

Ideally, optimized routing should resemble the following:



1. User routed to the most preferred site, based on proximity or response time
2. Based on the selected resource, NetScaler Gateway reroutes the session to a NetScaler Gateway in the preferred site.
3. NetScaler Gateway proxies the ICA traffic to the correct resource, which stays on the local LAN.

Using the optimized HDX routing option within StoreFront offloads traffic from the corporate WAN and places it on the public network

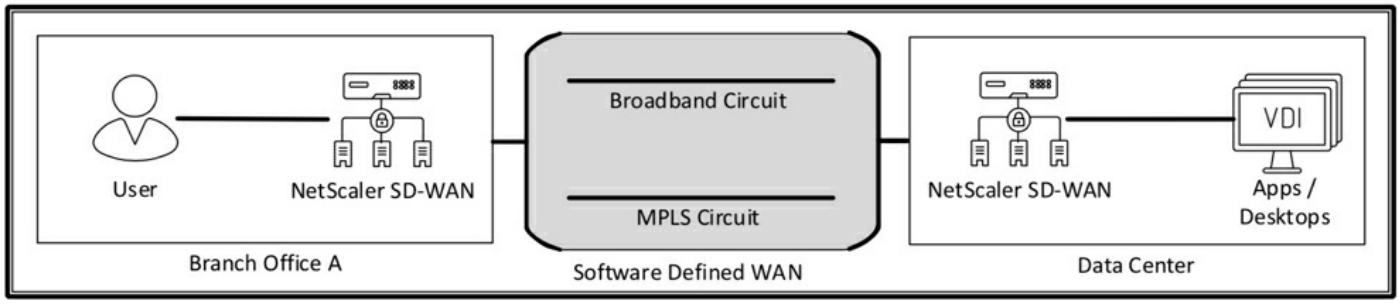
Decision: Virtual WAN

In branch office scenarios, a XenApp and XenDesktop design must evaluate the branch office's connection to the data centers hosting the application and desktop resources. If the WAN connection between the branch office and data center

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

is not able to meet the user requirements, the overall user experience degrades. Organizations have a couple of options on their WAN connections:

- **Scale Up** – Organizations can simply increase the size of the WAN pipe connecting the branch offices to the data center, typically at a sizable cost.
- **Scale Out** – Organizations can maintain their current WAN connection and augment it with multiple low-cost alternatives. The integration of all connections between the branch office and data center creates a software defined virtual WAN, like NetScaler SDWAN. The appliance sends duplicate network packets across all WAN connections defined within the virtual WAN. The appliance on the other end of the WAN uses the first arriving packet, discarding all subsequent packets. As the conditions of the multiple links change throughout the day, this approach guarantees the best experience possible.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology resource layer

May 07, 2018

The resource layer is the third layer of the design methodology and the final layer focused specifically on the user groups.

The overall user acceptance of the solution is defined by the decisions made within the resource layer. Profiles, printing, applications and overall desktop image design play a pivotal role in how well the desktop is aligned with the user group's requirements, which were identified within the assess phase.

User Experience

Perception is everything when it comes to a good VDI experience. Users expect an experience similar to or better than that of a traditional, physical desktop.

Codecs, transport protocols and self-service capabilities affects the overall experience. Poor quality graphics, lagging video or 120 second logon times can destroy the user experience. A proper user experience design can meet any network challenge.

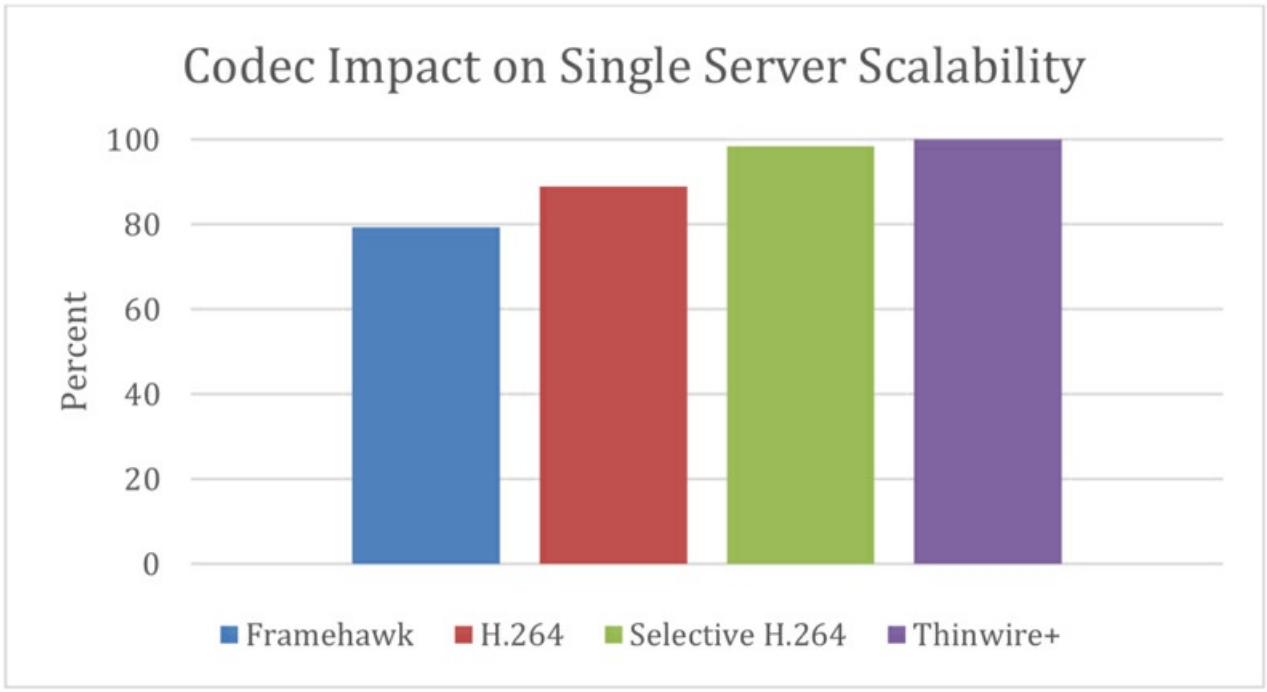
Decision: Display Protocol

Selecting the correct display protocol determines the quality of static images, video and text within the user's session as well as determining the impact on single server scalability. Administrators have the following options:

- Legacy - optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
- Desktop Composition Redirection – offloads desktop Windows manager DirectX commands to the endpoint, but only supports a Windows desktop VDA. Plus, in the 7.15 LTSR release, Desktop Composition Redirection is a depreciated feature.
- Framehawk – a UDP-based protocol that is able to provide high refresh rates in environments with high latency and high packet loss scenarios at the cost of greater network bandwidth utilization, commonly found on broadband wireless connections.
- H.264 – Often referred as the video codec, which provides the highest frame rates required for high quality video while saving network bandwidth. It does come at the expense of CPU processing time, reducing single server scalability. H.264 is the preferred codec when users predominately use multimedia applications.
- Thinwire – Based on the original Citrix patents from the 1990s that thinly transfers data over a wire. Use Thinwire in the majority of use cases as it provides a good user experience with minimal resource costs. There are two variations of Thinwire:
  - Legacy - Optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
  - Thinwire+ - Optimized for Desktop Windows Manager (DWM) graphics engine in Windows 8, Windows 10, Windows 2012 and Windows 2016
- Selective H.264 (Adaptive Display) - utilizes multiple codecs (H.264 and Thinwire+) simultaneously for portions of the screen
  - Do not use – Only uses Thinwire+ and not H.264. Best for users without server-rendered video or other graphically intense applications.
  - For entire screen – Only uses H.264. Best for users with heavy use of server-rendered video and 3D graphics, especially in low-bandwidth situations.
  - For actively changing regions – Uses H.264 for the portions of the screen that are constantly changing while the remainder of the screen uses Thinwire+. This is the best option for most users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Selecting the right codec not only has an impact on the overall user experience, but also on the scalability of the server.



Decision: Transport Protocol

There are three ways to transport the HDX protocol across the network:

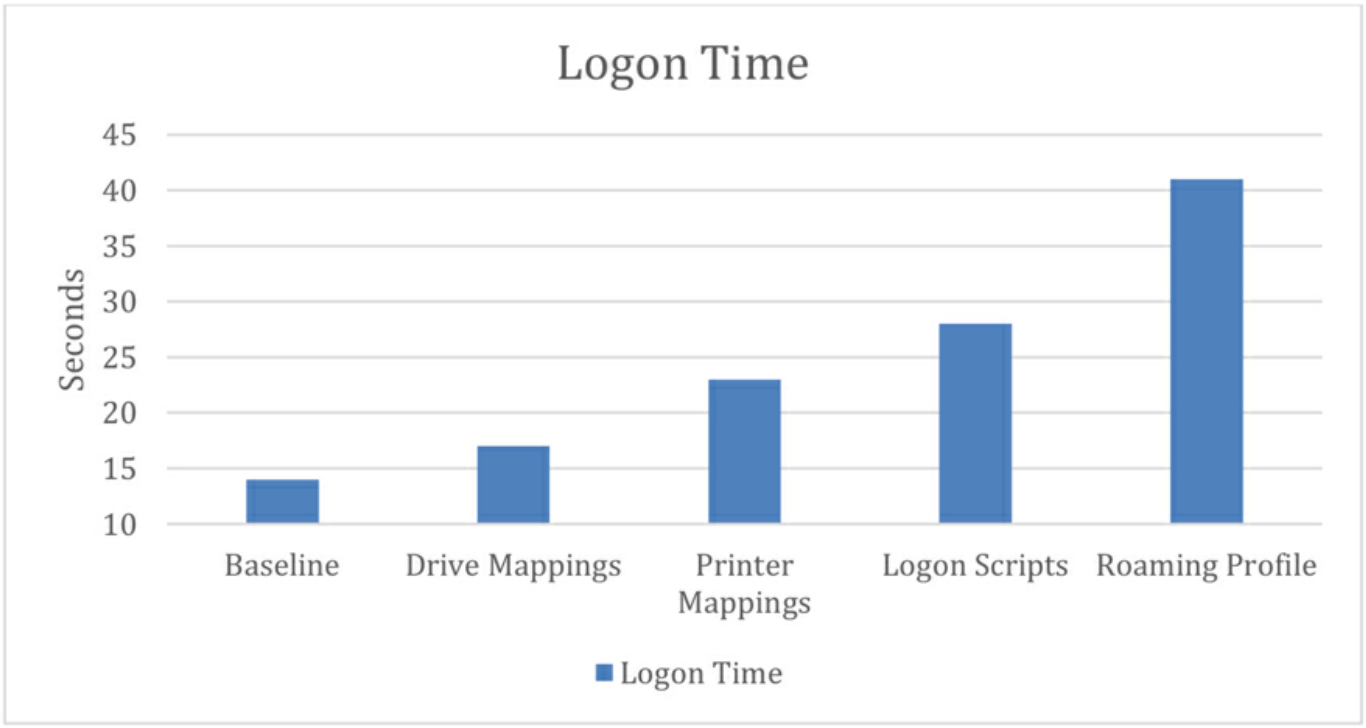
- **TCP** – Uses the industry standard TCP transport protocol. Common transport protocol over LAN and low-latency WAN connections, but suffers when connection distances increases, thus increasing latency and incurring more retransmissions.
- **EDT** – Uses a Citrix proprietary transport protocol called Enlightened Data Transport, based on UDP. Meant for high latency/packet loss networks, most common on long-distance WAN links. Provides a more interactive experience for the user without increasing CPU load on the server, but consumes more network bandwidth than TCP.
- **Adaptive Transport** – Uses TCP and EDT transport protocols. EDT used unless the network does not support transporting EDT over the network, which then automatically changes to TCP.

Most environments will use Adaptive Transport as the standard transport option unless the network does not have the appropriate firewall ports opened or NetScaler Gateway configured appropriately.
Decision: Logon Optimization

Every time a user logs onto a XenApp/XenDesktop session, the logon process must complete, which includes session initialization, user profile loading, group policy preferences execution, drive mapping, printer mapping, logon script execution and desktop initialization. Each process takes time and increases logon duration.

Most organizations include many mappings and complex logon scripts. When each of these items executes, the logon time drastically increases.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Workspace Environment Management removes drive mappings, printer mappings, logon scripts and roaming profiles from the standard logon process. With logon optimization, Workspace Environment Management applies the mappings/scripts/profiles in the background after the session and desktop initializes. The user receives the same environment but they receive their desktop interface faster. To learn more, review the following Logon Optimization video.

Most environments should enable logon optimization as a default configuration.

Decision: User Self Service

Self-service allows users to modify, update and troubleshoot their environments on their own without requiring help desktop intervention. Most organizations have policies in place that require users to change their passwords every 60-90 days. When users have multiple endpoint devices with saved passwords, it is extremely easy for their account to be locked out until each device is updated.

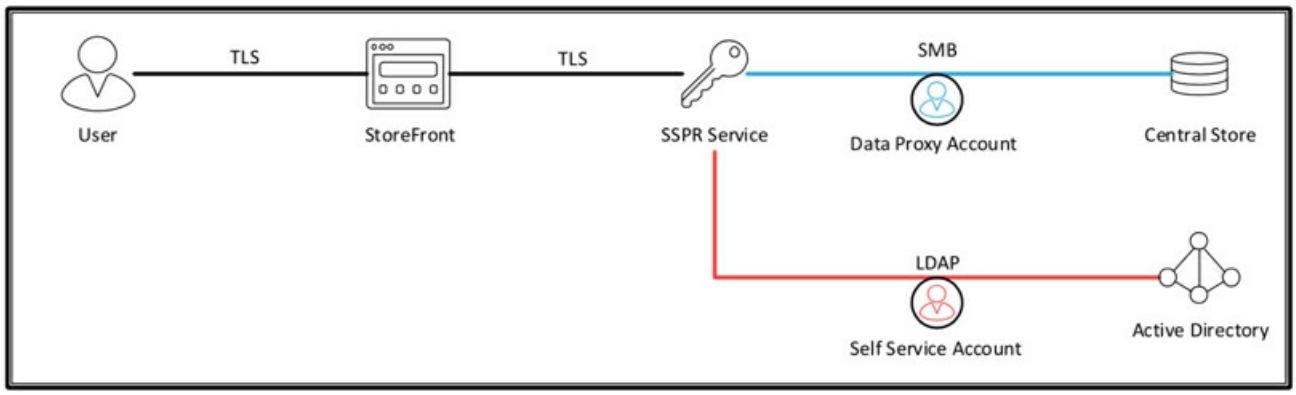
With StoreFront, can save time by self-servicing their own accounts with the following capabilities:

- **Account Unlock** – When the user's account is locked due to too many failed logon attempts, common with multiple devices, they can unlock their account if they know answers to their security questions.
- **Password Reset** – When users forgot their newly created password, they can reset their password if they know the answers to their security questions.

The self-service password reset architecture introduces the SSPR Service, Central Store and two accounts:

- **Data Proxy Account** – Responsible for accessing the central store, which contains encrypted answers to the user's security questions.
- **Self Service Account** – An Active Directory account with password reset and account unlock rights.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



In addition, properly designing self-service password reset requires the admin to create security questions that users will answer. Ideally, admins should create groups of questions around different categories then require users to answer a subset of questions for each group. The questions must be something the user knows that does not change and is not known by others.

User Profiles

A user's profile plays a critical role in delivering a consistently positive experience within a virtual desktop or virtual application scenario. Even a well-designed virtual desktop solution can fail if users are frustrated due to lengthy logon times or lost settings.

The user profile solution chosen must align with the personalization characteristics of the user group captured during the assess phase as well as the VDI model selected.

Decision: Profile Type

This section provides an overview on the different profile types available and provides guidance on the optimal user profile for each VDI model.

- **Local profiles** – Local profiles are stored on each server or desktop operating system and are initially created based on the default user profile. Therefore, a user accessing these resources would create an independent profile on each system. Users are able to retain changes to their local profile on each individual system, but changes are only accessible for future sessions on that system. Local profiles require no configuration; if a user logging into a server or desktop operating system does not have a profile path administratively defined, a local profile is created by default.
- **Roaming profiles** – Roaming profiles are stored in a centralized network repository for each user. Roaming profiles differ from local profiles in that the information in the profile (whether it is a printer, a registry setting, or a file stored in the documents folder) can be made available to user sessions accessed from all systems in the environment. Configuring a user for a roaming profile requires an administrator to designate the user's profile path (for virtual desktops) or terminal server profile path to a particular network share. The first time the user logs on to a server or desktop operating system, the default user profile is used to create the user's roaming profile. During logoff, the profile is copied to the administrator-specified network location.
- **Mandatory profiles** – Mandatory profiles are typically stored in a central location for many users. However, the user's changes are not retained at logoff. Configuring a user for a mandatory profile requires an administrator to create a mandatory profile file (NTUSER.MAN) from an existing roaming or local profile and assign users with a terminal services profile path. This can be achieved by means of Microsoft Group Policy, customizing the user properties in Active Directory or Citrix Profile Management.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Hybrid profiles** – Hybrid profiles combine a robust profile core (a mandatory profile or a local default profile) with user specific registry keys or files that are merged during logon. This technique enables administrators to tightly control which changes are retained and to keep the user profiles small in size. Furthermore, hybrid profiles address the last write wins issue using mature queuing techniques that automatically detect and prevent simultaneous writes that could potentially overwrite changes made in another session. Thus minimizing user frustration resulting from lost profile changes when accessing multiple servers or virtual desktops simultaneously. In addition, they capture and record only the changes within the profile, rather than writing the entire profile at logoff. A good example of a hybrid profile solution is Citrix Profile Management, which will be discussed in detail within this chapter.
  The following table compares the capabilities of each profile type.

  In the table:
  - **Y** indicates Functionality available.
  - **o** indicates Optional.
  - **N** indicates Functionality not available.

Feature	Local	Roaming	Mandatory	Hybrid
Central management / roams with user	N	Y	o	Yes
User settings are stored persistently	Y	Y	N	Yes
Granular capture of user settings	N	N	N	Yes

In order to select the optimal profile type for each user group it is important to understand their personalization requirements in addition to the VDI model assigned.

The following table provides recommendations on selecting the appropriate user profile type based on VDI resource:

In the table:

- **Y** indicates Recommended.
- **X** indicates Not Recommended.
- **o** indicates Viable.

	Local	Roaming	Mandatory	Hybrid
User setting persistence required (personalization characteristic: basic / complete)				
Hosted Windows App	X	Y	X	Y
Hosted Browser App	X	Y	X	Y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hosted Shared Desktop	X	Y	X	Y
Hosted Pooled Desktop	X	Y	X	Y
Hosted Personal Desktop	º	Y	X	Y
Hosted Pro Graphics Desktop	º	Y	X	Y
Local Streamed Desktop	X	Y	X	Y
Local VM Desktop	Y	º	X	º
Remote PC Access	Y	º	X	º
User setting persistence not required or not desired (personalization characteristic: none)				
Hosted Windows App	X	X	Y	X
Hosted Browser App	X	X	Y	X
Hosted Shared Desktop	X	X	Y	X
Hosted Pooled Desktop	Y	X	Y	X
Hosted Personal Desktop	X	X	Y	X
Hosted Pro Graphics Desktop	º	X	Y	X
Local Streamed Desktop	Y	X	Y	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Local VM Desktop	o	X	Y	X
Remote PC Access	o	X	Y	X

Decision: Folder Redirection

Redirecting special folders can supplement any of the described profile types. While redirecting profile folders, such as user documents and favorites, to a network share is a good practice to minimize profile size, architects need to be aware that applications may frequently read and write data to profile folders such as AppData, causing potential issues with file server utilization and responsiveness. It is important to thoroughly test profile redirection before implementation in production to avoid these issues. Therefore, it is important to research profile read / write activities and to perform a pilot before moving to production. Microsoft Outlook is an example of an application that regularly performs profile read activities, as the user signature is read from the user profile every time an email is created.

The following table provides general recommendations to help identify the appropriate folders to redirect:

In the table:

- **Y** indicates Recommended.
- **X** indicates Not Recommended.
- **o** indicates Viable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	X	o	X	o
Contacts	X	Y	X	o
Desktop	X	Y	X	o
Downloads	X	o	X	o
Favorites	o	Y	o	Y
Links	X	Y	X	o
My Documents	o	Y	o	Y
My Music	o	Y	o	o
My Pictures	o	Y	o	o
My Videos	o	Y	o	o
Saved Games	X	o	X	o
Searches	X	Y	X	o
Start Menu	X	X	X	X

Decision: Folder Exclusion

Excluding folders from being persistently stored as part of a roaming or hybrid profile can help to reduce profile size and logon times. By default Windows excludes the AppData\Local and AppData\LocalLow folders, including all subfolders, such as History, Temp and Temporary Internet Files. In addition, the downloads and saved games folders should also be excluded. All folders that are redirected should be excluded from the profile solution.

Decision: Profile Caching

Local caching of roaming or hybrid user profiles on a server or virtual desktop is default Windows behavior and can reduce login times and file server utilization / network traffic. With profile caching, the system only has to download changes made

© 1999-2017 Citrix Systems, Inc. All rights reserved.

to the profile. The downside of profile caching is that it can consume significant amounts of local disk storage on multi-user systems, such as a hosted shared desktop hosts.

In certain VDI models and configurations, the VDI resource is reset to a pristine state. Having locally cached profiles be deleted upon logoff is an unnecessary consumption of resources. Based on this, the leading recommendation is to not deleting locally cached profiles for the following VDI models:

- Hosted Personal Desktops
- Hosted Pooled Desktops – only in situations where a reboot occurs after logoff.
- Local VM Desktops
- Remote PC Access

Configuring the "Delay before deleting cached profiles" Citrix policy sets an optional extension to the delay before locally cached profiles are deleted at logoff. Extending the delay is useful if a process keeps files or the user registry hive open during logoff. This can also reduce logoff times for large profiles.

Decision: Profile Permissions

For security reasons, administrators, by default, cannot access user profiles. While this level of security may be required for organizations that deal with very sensitive data, it is unnecessary for most environments and can complicate operations and maintenance. Therefore, consider enabling the "Add the Administrators security group to roaming user profiles" policy setting. The configuration of this policy should be aligned with the security characteristics of the user groups captured during the assess phase. For more information on the permissions required for the file share hosting user profiles and data, please refer to Microsoft TechNet - Deploying Roaming Profiles.

Decision: Profile Path

Determining the network path for the user profiles is one of the most significant decisions during a user profile design process. In general, it is strongly recommended to leverage a redundant and high performance file server or NAS device. There are four topics that must be considered for the profile share:

- **Performance** – File server performance will affect logon and logoff times, and depending on other decisions such as redirected folders and profile streaming, can impact the user's experience within the session. For large virtual desktop infrastructures, a single file server cluster may not be sufficient to handle periods of peak activity. In order to distribute the load across multiple file servers, the file server address and share name will need to be adjusted.
- **Location** – User profiles are transferred over the network by means of the SMB protocol, which does not perform well on high-latency network connections. Furthermore, WAN connections are typically bandwidth constrained, which can add additional delay to the profile load process. Therefore, the file server should be located in close proximity to the servers and virtual desktops to minimize logon times.
- **Operating system platforms** – User profiles have a tight integration with the underlying operating system and it is not supported to reuse a single user profile on different operating systems or different platforms like 64-Bit (x64) and 32-Bit (x86).
  For more information, please refer to the Microsoft knowledge base article KB2384951 – Sharing 32 and 64-bit User Profiles. Windows 2008 and Windows Vista introduced a new user profile structure, which can be identified by .V2 profile directory suffix, which makes older user profiles incompatible with newer operating systems such as Windows 2012, 7 and 8. In order to ensure that a separate profile is used per platform, the profile directory has to be adapted.
- **Indexing capabilities** – To take full advantage of Windows Search functionality on a user's redirected data, Windows file servers that index the user's data must be used, as opposed to a share on a NAS appliance. This is important for use cases that are heavily dependent on Windows Search or are especially sensitive to perception of slowness or latency

© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are two methods that can be used to address these challenges that are based on Windows built-in technology:

- **User object** – For every user object in Active Directory, an individual profile path, which contains file server name and profile directory, can be specified. Since only a single profile path can be specified per user object, it is not possible to ensure that a separate profile is loaded for each operating system platform.
- **Computer group policy** or **system variables** – The user profile path can also be configured by means of computer specific group policies or system variables. This enables administrators to ensure that a user profile is dedicated to the platform. Since computer specific configurations affect all users of a system, all user profiles will be written to the same file server. To load balance user profiles across multiple servers dedicated XenDesktop delivery groups have to be created per file server.

Note: Microsoft does not support DFS-N combined with DFS-R for actively used user profiles.

For more information, please refer to the Microsoft articles:

- Information about Microsoft support policy for a DFS-R and DFS-N deployment scenario
- Microsoft Support Statement Around Replicated User Profile Data

When using Citrix Profile Management, a third option is available to address these challenges:

User object attributes and variables – Citrix Profile Management enables the administrator to configure the profile path by means of a computer group policy using attributes of the user object in Active Directory to specify the file server dynamically. In order to achieve this, three steps are required:

1. Create a DNS alias (for example, fileserver1) that refers to the actual file server
2. Populate an empty LDAP attribute of the user object (for example, l or UID) with the DNS Alias
3. Configure Citrix Profile Management by means of GPO to use a profile path that refers to the LDAP attribute (for example, if attribute UID is used the profile path becomes \\#UlD#\Profiles\profiledirectory)

In addition, Citrix Profile Management automatically populates variables to specify the profile path dynamically based on the operating system platform. Valid profile management variables are:

- !CTX_PROFILEVER! – Expands to v1 or v2 depending on the profile version.
- !CTX_OSBITNESS! – Expands to x86 or x64 depending on the bit-level of the operating system.
- !CTX_OSNAME! – Expands to the short name of the operating system, for example- Windows 7.

By combining both capabilities of Citrix Profile Management, a fully dynamic user profile path can be created, which can be load balanced across multiple file servers and ensure profiles of different operating system platforms are not mixed. An example of a fully dynamic user profile path is shown below:

\\#UID#\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!

Decision: Profile Streaming

Note: The following design decision only applies to those environments that use Citrix Profile Management.

With user profile streaming, files and folders contained in a profile are fetched from the user store (file server) to the local computer when a user accesses them. During the logon process, Citrix Profile Management immediately reports that the profile load process has completed reducing profile load time to almost zero.

Citrix recommends enabling profile streaming for all scenarios. If it is desired to keep a local cached copy of the user profile for performance reasons, it is recommended to enable the “Always Cache” setting and configure a size of 0. This ensures

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

that the user profile is downloaded in the background and enables the system to use this cached copy going forward.

Experience from the Field

- General – Some poorly written applications might load faster if their AppData has already been streamed to the VDI resource. Enabling the "Always Cache" option for profile streaming can help improve performance when the AppData folder is not redirected.

Decision: Active Write Back

Note: The following design decision only applies to those environments that use Citrix Profile Management.

By enabling the active write back feature, Citrix Profile Manager detects when an application has written and closed a file and copies the file back to the network copy of the profile during idle periods. In scenarios where a single user leverages multiple virtual desktops or hosted shared desktops simultaneously, this feature can be tremendously beneficial. However, Citrix Profile Management does not copy any registry changes back to the network, except during an ordered logoff. As such, there is a risk that the registry and files may get out of alignment on non-persistent systems, where locally cached profile information is wiped upon reboot. Therefore, it is recommended to disable active write back functionality for non-persistent scenarios.

Decision: Configuration Approach

Note: The following design decision only applies to those environments that use Citrix Profile Management.

Citrix Profile Management can be configured by means of an ".ini" file, Microsoft Group Policy and Citrix Policy (Citrix Profile Management 5.0 and newer). While each option offers the same configuration settings, Group Policy is recommended because it allows administrators to perform Windows and Citrix profile configurations from a single point, minimizing the tools necessary for profile management.

Note: With Citrix Profile Management 5.0 and newer, the desktop type is automatically detected and Citrix Profile Management policies set accordingly. For more information, please refer to Citrix Docs – How automatic configuration works.

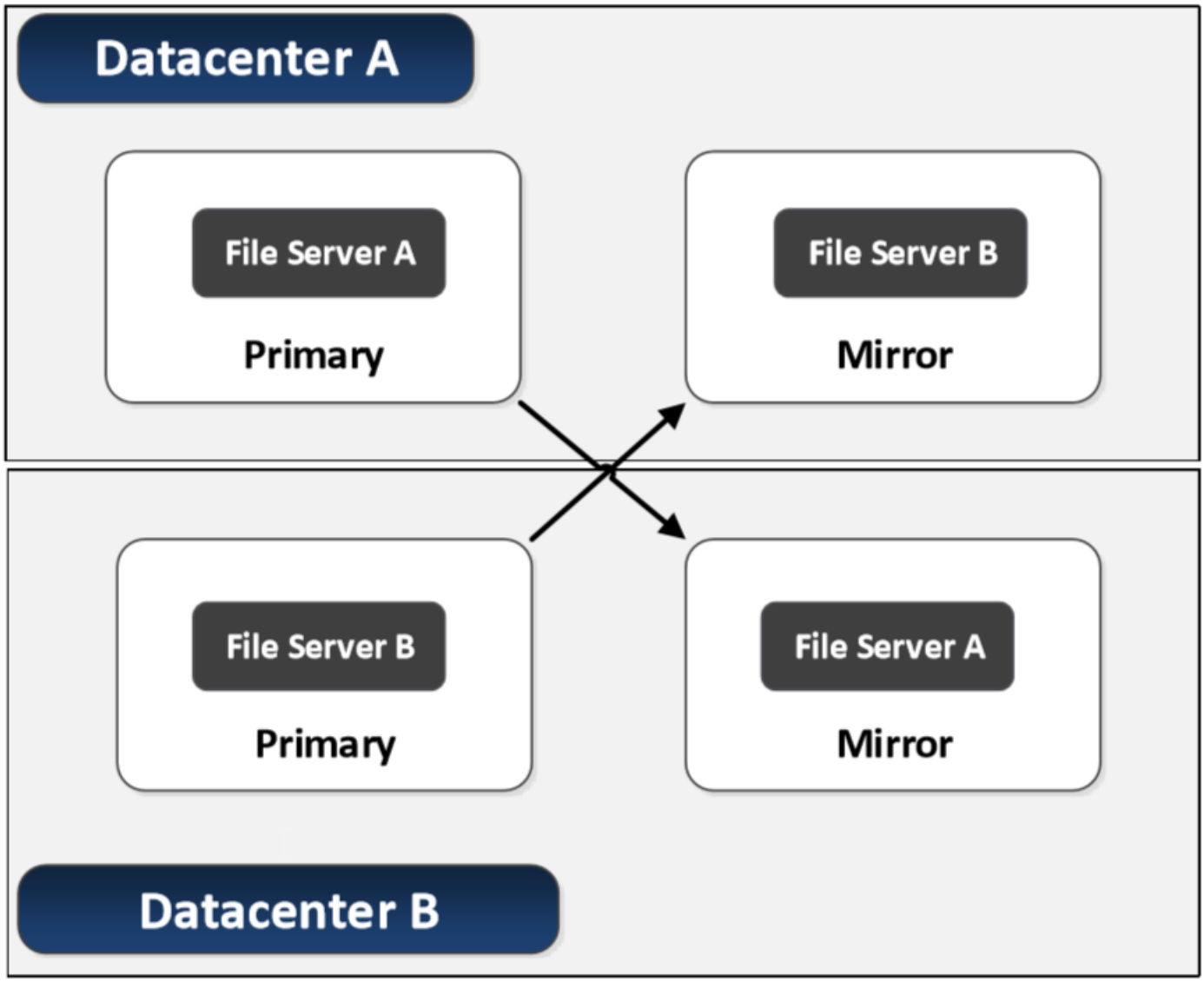
Decision: Replication

While having an active/active datacenter on a network level is easily accomplished with GSLB, the replication of user data makes having a fully active/active deployment complex in most situations. To have an active/active configuration where users are not statically assigned to a specific datacenter, will require users to have no form of personalization requirements. This will limit the user's ability to make any configuration changes and will not allow them to create any documents or persistent data. The exception to this is when a high-speed, low latency connection such as dark fiber is available between datacenters. This will let resources in both locations can point to the same file server allowing for a true active/active solution. Also, an active/active configuration can be accomplished when applications are used that rely solely on a backend database that is actively replicated between datacenters and do not store any data in the user profile.

For redundancy and failover purposes, user data such as Windows profiles and documents should be synchronized between datacenters. Although it is recommended to replicate user data between datacenters, the replication would be an active/passive configuration. This means the data can only be actively consumed from a single datacenter. The reason for this limitation is the distributed file locking method inside Windows that only allows a single user to actively write to a file. Therefore, active/active replication of user data is not supported. Any supported configuration consists of a one-way replication of data that is active in a single datacenter at any point in time.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For example, the figure below describes a scenario where user data is passively replicated from Datacenter A to Datacenter B. In this example, File Server A is the primary location for user data in Datacenter A and File Server B is the primary location in Datacenter B. One-way replication of the user data occurs for each fileserver to allow for the user data to be available in the opposite datacenter if a failover occurs. Replication technologies such as Microsoft DFS can be configured to mirror user profiles and documents to a file server in another datacenter. DFS Namespaces can also be used to have a seamless path for the location of the user data. However, implementing a replication solution like this requires an administrator familiar with Microsoft DFS and user profiles.



User Data

In order to be effective, users must access their data. The data must be in close proximity to the application for the user to have a good experience. As the distance between the application and data increases, latency also increases, which slows down any file operation (opening, saving, modifying).

In a VDI-based environment, administrators must understand where users store their data and impact of access.

Decision: User Data Location

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Users traditionally stored their data on their local device or on a network file server designated with a drive mapping. Due to IT storage space limitations or the inability to have the data follow the user to other mobile devices, users turned to free, cloud-based storage offerings like OneDrive, DropBox and Box. To get access to the data, the user would install the storage vendor's agent on their traditional Windows PC, allowing them direct access to the cloud-hosted storage repository.

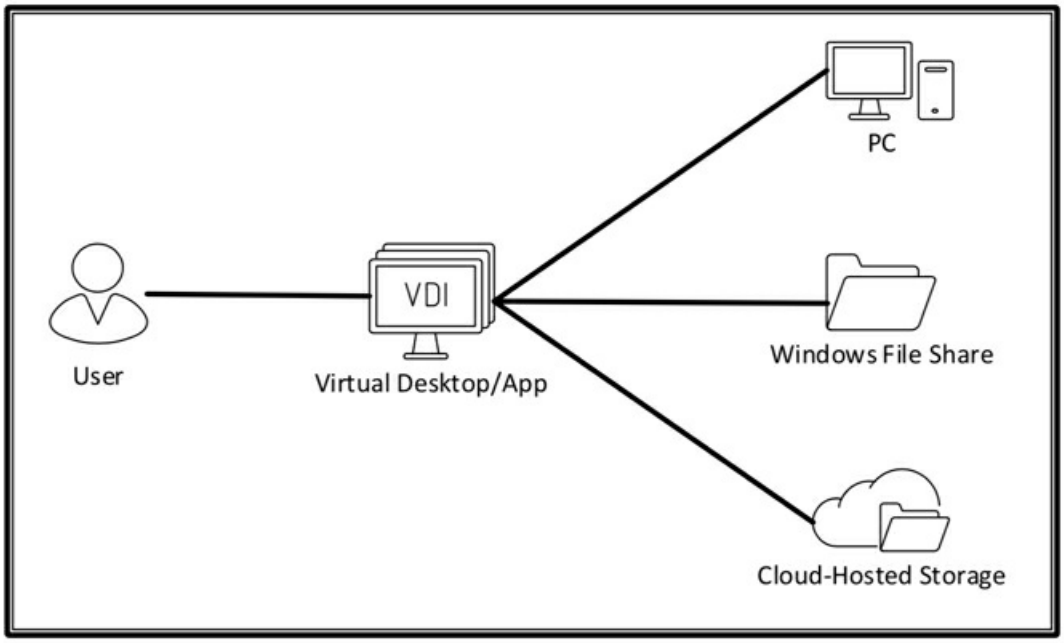
Administrators must design the solution to take into account user storage by looking at the following options:

- **Multi-Agent Strategy** – In VDI, users require the admin to install and configure the agent for each storage provider, which assumes the storage agent supports the non-persistent VDI model. Each agent is a new application that the admin must manage and maintain.
- **Storage Connector Strategy** – A single agent consolidates storage repositories from numerous cloud-hosted and on-premises providers into a single folder structure. For example, when a user connects to Citrix ShareFile, they see a consolidated folder structure containing their user data from the cloud (ShareFile, OneDrive, DropBox, Box and Google Drive) and from on-premises (SharePoint, Windows network shares and local endpoint shares).

Decision: User Data Access

A critical aspect to a successful VDI solution is for the user experience to remain the same as it was with a traditional PC. If users open files from within the application, that functionality must continue to function. If users navigate with Explorer to access a file, that functionality must continue to function.

A user's data can exist on the local PC, on a network file share and hosted in the cloud.



With local PC, on-premises network shares and cloud-hosted storage options available to users, administrators need to understand how users accessing their data affects the infrastructure and VDI experience.

- **Direct Data Access** – Users access a file on a remote server (on-premises Windows server or cloud-hosted storage provider). The distance between the application and file directly affects the experience. Longer distances equates to higher latency. Each file operation (navigate, open, close, save, etc.) takes more time as the latency between application and file storage increases. Windows file servers are often located in the same data center as the user's VDI desktop

© 1999-2017 Citrix Systems, Inc. All rights reserved.

making direct data access feasible; but cloud-hosted solutions and local PC Access will experience poor response times if the connection between the VDI desktop and the storage repository has high latency.

- **Local Synchronization** – With a traditional PC, users are accustomed to having files local, which mitigates any slow application response times due to extremely low latency. Many cloud-hosted solutions provide data synchronization to enable access speeds similar to a local storage model. Many of the cloud-hosted solutions provide full synchronization or user-configured partial synchronization of certain folders and files. With partial synchronization, only the synchronized files are visible and accessible on the device, causing user confusion. Full and partial synchronization increases VDI costs. Each session is an entirely new desktop requiring synchronization of user's folders/files, which takes time, network bandwidth and VDI storage space. Every file synchronized to the VDI desktop must be stored within the organization's data center for the duration of the VDI session.
- **On-Demand Synchronization** – When navigating Explorer, users see a complete, but virtual, file/folder structure even though those files/folders do not physically exist on the desktop. Selecting a file begins an automatic synchronization to the VDI desktop for that single file. At this point, file access is local, which creates a user experience like that of a traditional PC. When the user saves or closes the file, the file synchronizes back to the cloud. Only the files accessed synchronize, eliminating the waste incurred with the local data access model. Citrix ShareFile includes Drive Mapper, allowing the user to interact with their data via Explorer while utilizing on-demand synchronization when accessing a file. As only accessed files synchronize, the impact to the underlying storage infrastructure and associated storage costs are minimal.

In the table:

- **Y** indicates recommended.
- **N** indicates Not recommended.

	Direct Data Access	Local Synchronization	On-Demand Synchronization
Network File Server	Y		
Cloud-hosted	N	N	Y
Local PC	N	N	Y

Decision: Data Recovery

File corruption is an issue most users experience. Improperly shutting down the application or PC (hitting the power button instead of closing the application and shutting down the operating system gracefully) often causes many corruption issues.

A few options exist to provide users with data recovery options:

- **Multi-File** – With a traditional PC, users have few recovery options if the files are local. Users often manually create a new copy of the file each day in order to provide some level of recovery. This solution is hard to manage.
- **Backup/Restore** – Administrators can implement a backup and restore solution to help with file recovery. However, these solutions rarely work with local files and for a network file share, the backup process usually only runs nightly or weekly. In addition, restoring a corrupted file requires the user to call support.
- **Versioning** – Cloud-hosted options, like Citrix ShareFile, include file versioning, which automatically creates new versions

© 1999-2017 Citrix Systems, Inc. All rights reserved.

of the file as changes are saved. Versioning requires no user intervention and allows users to recover from corruption quickly and with little loss of data.



Uploaded	Title	Creator
7/20/17 3:22 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 2:15 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:16 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:08 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:07 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:1...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller

Policies

Policies provide the basis to configure and fine tune XenApp and XenDesktop environments, allowing organizations to control connection, security and bandwidth settings based on various combinations of users, devices or connection types.

When making policy decisions it is important to consider both Microsoft and Citrix policies to ensure that all user experience, security and optimization settings are considered. For a list of all Citrix-related policies, please refer to the Citrix Policy Settings Reference.

Decision: Preferred Policy Engine

Organizations have the option to configure Citrix policies via Citrix Studio or through Active Directory group policy using Citrix ADMX files, which extend group policy and provide advanced filtering mechanisms.

Using Active Directory group policy allows organizations to manage both Windows policies and Citrix policies in the same location, and minimizes the administrative tools required for policy management. Group policies are automatically replicated across domain controllers, protecting the information and simplifying policy application.

Citrix administrative consoles should be used if Citrix administrators do not have access to Active Directory policies. Architects should select one of the above two methods as appropriate for their organization's needs and use that method consistently to avoid confusion with multiple Citrix policy locations.

It is important to understand how the aggregation of policies, known as policy precedence flows in order to understand how a resultant set of policies is created. With Active Directory and Citrix policies, the precedence is as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Policy Precedence	Policy Type
Processed first (lowest precedence)	Local server policies
Processed second	Citrix policies created using the Citrix administrative consoles
Processed third	Site level AD policies
Processed fourth	Domain level AD policies
Processed fifth	Highest level OU in domain
Processed sixth and subsequent	Next level OU in domain
Processed last (highest precedence)	Lowest level OU containing object

Policies from each level are aggregated into a final policy that is applied to the user or computer. In most enterprise deployments, Citrix administrators do not have rights to change policies outside their specific OUs, which will typically be the highest level for precedence. In cases where exceptions are required, the application of policy settings from higher up the OU tree can be managed using “block inheritance” and “no override” settings. Block inheritance stops settings from higher-level OUs (lower precedence) from being incorporated into the policy. However, if a higher-level OU policy is configured with no override, the block inheritance setting will not be applied. Given this, care must be taken in policy planning, and available tools such as the “Active Directory Resultant Set of Policy” tool or the “Citrix Group Policy Modeling” wizard should be used to validate the observed outcomes with the expected outcomes.

> **注意**
>
> Some Citrix policy settings, if used, need to be configured through Active Directory group policy, such as Controllers and Controller registration port, as these settings are required for VDAs to register.

Decision: Policy Integration

When configuring policies, organizations often require both Active Directory policies and Citrix policies to create a completely configured environment. With the use of both policy sets, the resultant set of policies can become confusing to determine. In some cases, particularly with respect to Windows Remote Desktop Services (RDS) and Citrix policies, similar functionality can be configured in two different locations. For example, it is possible to enable client drive mapping in a Citrix policy and disable client drive mapping in a RDS policy. The ability to use the desired feature may be dependent upon the combination of RDS and Citrix policy. It is important to understand that Citrix policies build upon functionality available in Remote Desktop Services. If the required feature is explicitly disabled in RDS policy, Citrix policy will not be able to affect a configuration as the underlying functionality has been disabled.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

In order to avoid this confusion, it is recommended that RDS policies only be configured where required and there is no corresponding policy in the XenApp and XenDesktop configuration, or the configuration is specifically needed for RDS use within the organization. Configuring policies at the highest common denominator will simplify the process of understanding resultant set of policies and troubleshooting policy configurations.

Decision: Policy Scope

Once policies have been created, they need to be applied to groups of users and/or computers based on the required outcome. Policy filtering provides the ability to apply policies against the requisite user or computer groups. With Active Directory based policies, a key decision is whether to apply a policy to computers or users within site, domain or organizational unit (OU) objects. Active Directory policies are broken down into user configuration and computer configuration. By default, the settings within the user configuration apply to users who reside within the OU at logon, and settings within the computer configuration are applied to the computer at system startup, and will affect all users who logon to the system. One challenge of policy association with Active Directory and Citrix deployments revolves around three core areas:

- **Citrix environment specific computer policies** – Citrix servers and virtual desktops often have computer policies that are created and deployed specifically for the environment. Applying these policies is easily accomplished by creating separate OU structures for the servers and the virtual desktops. Specific policies can then be created and confidently applied to only the computers within the OU and below and nothing else. Based upon requirements, virtual desktops and servers may be further subdivided within the OU structure based on server roles, geographical locations or business units.
- **Citrix specific user policies** – When creating policies for XenApp and XenDesktop there are a number of policies specific to user experience and security that are applied based on the user's connection. However, the user's account could be located anywhere within the Active Directory structure, creating difficulty with simply applying user configuration based policies. It is not desirable to apply the Citrix specific configurations at the domain level as the settings would be applied to every system any user logs on to. Simply applying the user configuration settings at the OU where the Citrix servers or virtual desktops are located will also not work, as the user accounts are not located within that OU. The solution is to apply a loopback policy, which is a computer configuration policy that forces the computer to apply the assigned user configuration policy of the OU to any user who logs onto the server or virtual desktop, regardless of the user's location within Active Directory. Loopback processing can be applied with either merge or replace settings. Using replace overwrites the entire user GPO with the policy from the Citrix server or virtual desktop OU. Merge will combine the user GPO with the GPO from the Citrix server or desktop OU. As the computer GPOs are processed after the user GPOs when merge is used, the Citrix related OU settings will have precedence and be applied in the event of a conflict. For more information, please refer to the Microsoft TechNet article - Understand User Group Policy Loopback Mode.
- **Active Directory policy filtering** – In more advanced cases, there may be a need to apply a policy setting to a small subset of users such as Citrix administrators. In this case, loopback processing will not work, as the policy should only be applied to a subset of users, not all users who logon to the system. Active Directory policy filtering can be used to specify specific users or groups of users to which the policy is applied. A policy can be created for a specific function, and then a policy filter can be set to apply that policy only to a group of users such as Citrix administrators. Policy filtering is accomplished using the security properties of each target policy.

Citrix policies created using Citrix Studio have specific filter settings available, which may be used to address policy-filtering situations that cannot be handled using group policy. Citrix policies may be applied using any combination of the following filters:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filter Name	Filter Description	Scope
Access control	Applies a policy based on access control conditions through which a client is connecting. For example, users connecting through a Citrix NetScaler Gateway can have specific policies applied.	User settings
Citrix CloudBridge	Applies a policy based on whether or not a user session was launched through Citrix CloudBridge.	User settings
Client IP address	Applies a policy based on the IPv4 or IPv6 address of the user device used to connect the session. Care must be taken with this filter if IPv4 address ranges are used in order to avoid unexpected results.	User settings
Client name	Applies a policy based on the name of the user device used to connect the session.	User settings
Delivery group	Applies a policy based on the delivery group membership of the desktop running the session.	User settings
Delivery group type	Applies a policy based on the type of machine running the session. For example, different policies can be set depending upon whether a desktop is pooled, dedicated or streamed.	User and computer settings
Organizational unit	Applies a policy based on the OU of the desktop or server running the session.	User and computer settings
Tag	Applies a policy based on any tags applying to the desktop running the session. Tags are strings that can be added to virtual desktops in XenDesktop environments that can be used to search for or limit access to desktops.	User and computer settings
User or Group	Applies a policy based on the Active Directory group membership of the user connecting to the session.	User settings

> **注意**
>
> Citrix policies in XenDesktop 7.x provide a merged view of settings that apply at the user and computer level. In table 24, the Scope column identifies whether the specified filter applies to user settings, computer settings, or both.

Decision: Baseline Policy

A baseline policy should contain all common elements required to deliver a high-definition experience to the majority of users within the organization. A baseline policy creates the foundation for user access, and any exceptions that may need to be created to address specific access requirements for groups of users. It should be comprehensive to cover as many use cases as possible and should have the lowest priority, for example 99 (a priority number of “1” is the highest priority), in order to create the simplest policy structure possible and avoid difficulties in determining the resultant set of policies. The unfiltered policy set provided by Citrix as the default policy may be used to create the baseline policy as it is applied to all users and connections. In the baseline configuration, all Citrix policy settings should be enabled, even those that will be

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configured with the default value, in order to explicitly define desired/expected behavior, and to avoid confusion should default settings change over time.

Citrix Policy templates can be used to configure Citrix policies to effectively manage the end-user experience within an environment and can serve as an initial starting point for a baseline policy. Templates consist of pre-configured settings that optimize performance for specific environments or network conditions. The built-in templates included in XenDesktop are shown below:

Built-in Templates	Description
High definition user experience	Includes settings for providing high quality audio, graphics, and video to users.
High server scalability	Includes settings for providing an optimized user experience while hosting more users on a single server.
Optimized bandwidth for WAN	Includes settings for providing an optimized experience to users with low bandwidth or high latency connections.
Security and control	Includes settings for disabling access to peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices.

For more information on Citrix policy templates, please refer to Citrix Docs - Manage Citrix Policy Templates.

A baseline policy configuration should also include Windows policies. Windows policies reflect user specific settings that optimize the user experience and remove features that are not required or desired in a XenDesktop environment. For example, one common feature turned off in these environments is Windows update. In virtualized environments, particularly where desktops and servers may be streamed and non-persistent, Windows update creates processing and network overhead, and changes made by the update process will not persist a restart of the virtual desktop or application server. Also in many cases, organizations use Windows software update service (WSUS) to control Windows updates. In these cases, updates are applied to the master disk and made available by the IT department on a scheduled basis.

In addition to the above considerations, an organization's final baseline policy may include settings specifically created to address security requirements, common network conditions, or to manage user device or user profile requirements:

Printing

Citrix XenApp and Citrix XenDesktop support a variety of different printing solutions. In order to plan and successfully implement the proper printing solution it is important to understand the available technologies as well as their benefits and limitations.

Decision: Printer Provisioning

The process of creating printers at the start of a XenApp or XenDesktop session is called printer provisioning. There are multiple approaches available:

- **User Added** – Allowing users to manually add printers gives them the flexibility to select printers by convenience. The drawback to manually adding network-based printers is that it requires the users to know the network name or path of the printers. There is also a chance that the native print driver is not installed in the operating system and the Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Universal Print Driver is not compatible, thereby requiring the user to seek administrative assistance. Manually adding printers is best suited in the following situations:
  - Users roam between different locations using the same client device (i.e. laptop, tablet).
  - Users work at assigned stations or areas whose printer assignments will rarely change.
  - Users have personal desktops with sufficient rights to install necessary printer drivers.
- **Auto Created** – Auto-creation is a form of dynamic provisioning that attempts to create some or all of the available printers on the client device at the start of a user session. This includes locally attached printers as well as network-based printers. Auto-creating all client printers can increase the session logon time as each printer is enumerated during the logon process.
- **Session Based** – Session printers are a set of network-based printers assigned to users through a Citrix policy at the start of each session.
  - Proximity based session printers are filtered by IP subnet. The network printers created under this policy may vary based on where the user's endpoint device is located. Proximity printing is recommended in situations where: Users roam between different locations using the same endpoint device (i.e. laptop, tablet) and where thin clients are used, which do not have the ability to connect to network-based printers directly.
  - Session printers may be assigned using the "Session Printer" policy or the "Printer Assignments" policy. The "Session printer" policy is intended to be used to set default printers for a farm, site, large group, or OU. The "Printer Assignments" policy is used to assign a large group of printers to multiple users. If both policies are enabled and configured, the session printers will be merged into a single list.
- **Universal Printer** – The Citrix Universal Printer is a generic printer object that is autocreated at the start of a session and is not linked to a printing device. When using the Citrix Universal Printer, it is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. By default, the Citrix Universal Printer will print to the client's default printer, however the behavior can be modified to allow the user to select any of their compatible local or network-based printers.

The Citrix Universal Printer is best suited for the following scenarios:

- The user requires access to multiple printers both local and network-based which may vary with each session.
- The user's logon performance is a priority and the Citrix policy "Wait for printers to be created" must be enabled due to application compatibility.
- The user is working from a Windows based device or thin client.

> **注意**
>
> Other options for provisioning printers, such as Active Directory group policy, "follow-me" centralized print queue solutions, and other 3rd party print management solutions can be used to provision printers into a Citrix session.

Decision: Printer Drivers

Managing print drivers in XenApp and XenDesktop can be a tedious task, especially in large environments with hundreds of printers. In XenApp and XenDesktop there are several methods available to assist with print driver management.

- **User Installed** – When adding a printer within a XenApp or XenDesktop session and the native print driver is not available, the drivers can be installed manually, by the user. Many different print drivers can potentially be installed on different resources creating inconsistencies within the environment. Troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, user installed drivers is not recommended.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Automatic Installation** – When connecting a printer within a XenApp or XenDesktop session, a check is made to see if the required print driver is already installed in the operating system. If the print driver is not already installed, the native print driver, if one exists, will be installed automatically. If users roam between multiple endpoints and locations, this can create inconsistencies across sessions since users may access a different hosted resource every time they connect. When this type of scenario occurs, troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, automatic installed drivers is not recommended.
- **Universal Print Driver** – The Citrix Universal Printer Driver (UPD) is a device independent print driver, which has been designed to work with most printers. The Citrix Universal Printer Driver (UPD) simplifies administration by reducing the number of drivers required on the master image. For auto created client printers, the driver records the output of the application and sends it, without any modification, to the end-point device. The endpoint uses local, device-specific drivers to finish printing the job to the printer. The UPD can be used in conjunction with the Citrix Universal Print Server (UPServer) to extend this functionality to network printers.

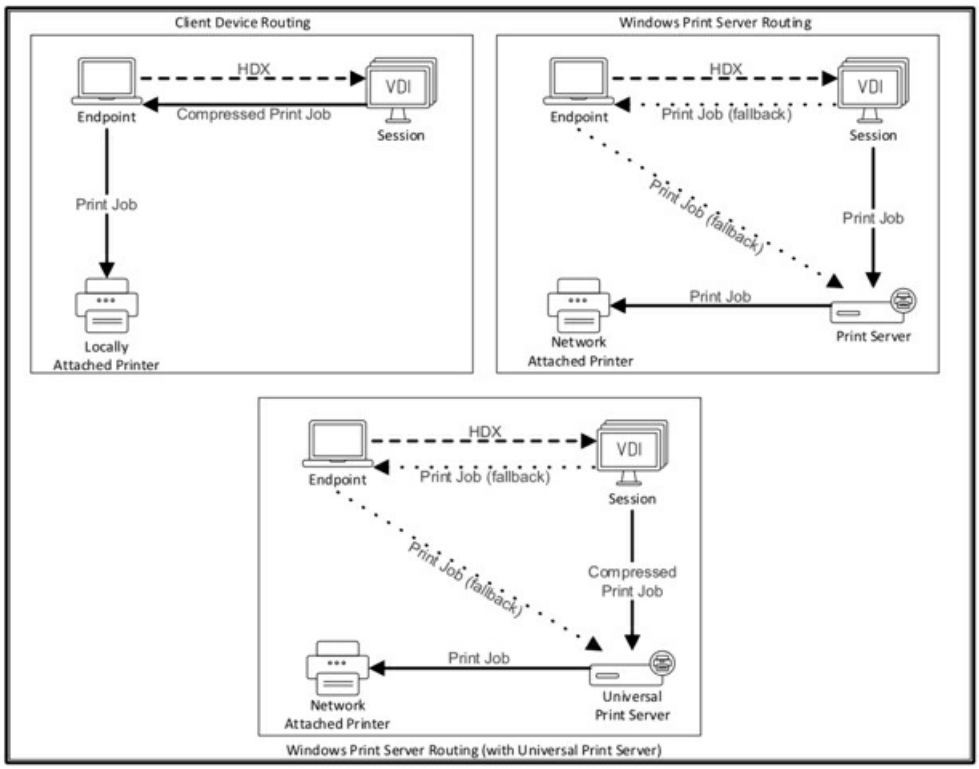
Decision: Printer Routing

Print jobs can be routed along different paths: through a client device or through a print server.

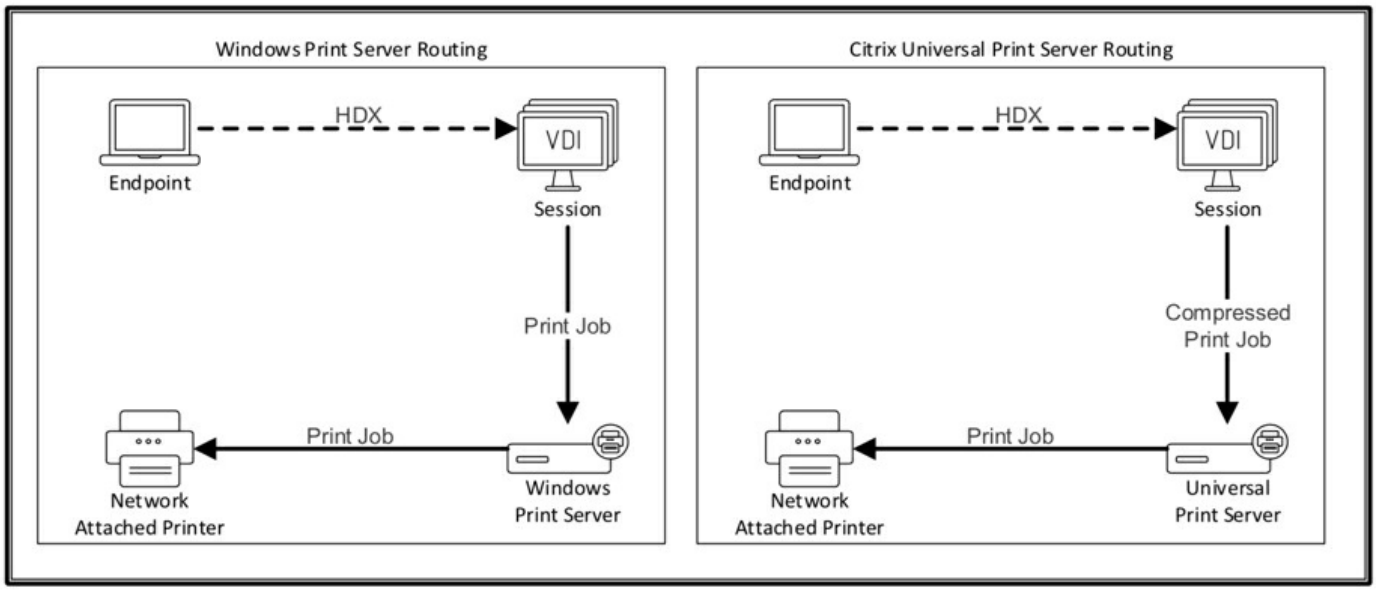
- **Client Device Routing** – Client devices with locally attached printers (printers attached through USB, LPT, COM, TCP, etc.) will route print jobs directly from the client device to the printer.
- **Windows Print Server Routing** – By default, print jobs sent to auto-created networkbased printers will be routed from the user's session to the print server. However, the print job will take a fallback route through the client device when any of the following conditions are true:
  - The session cannot contact the print server
  - The print server is on a different domain without a trust established.
  - The native print driver is not available within the user's session
- **Citrix Universal Print Server Routing** – Print job routing follows the same process as Windows Print Server Routing except that the Universal Print Driver is used between the user's session and the Citrix Universal Print Server.

The specifics with print job routing are based on the printer provisioning method. Auto-created and user-added printers can route print jobs based on the following diagrams:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



However, if the printers are provisioned as session printers, the print job routing options changes slightly. The jobs are no longer able to route through the user's endpoint device.



The recommended option is based on the network location of the endpoint device, the user's session and the print server.

- **Client Device Routing**
  - Use for locally attached printer implementations.
  - Use if a Windows endpoint device and printer are on the same high-speed, lowlatency network as the Windows Print

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server.

- **Windows Print Server Routing**
  - Use if the printer is on the same high-speed, low-latency network as the Windows Print Server and user session.
- **Windows Print Server Routing (with Universal Print Server)**
  - Use if non-Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.

Decision: Print Server Redundancy

Network-based printers, managed with a Microsoft print server or the Citrix Universal Print Server should be configured with redundancy in order to eliminate a single point of failure. The Citrix Universal Print Server redundancy should be defined within a Citrix Policy.

Experience from the Field

A print media company leverages Thin Clients and Windows-based workstations at the company headquarters. Network based printers are placed throughout the building (one per floor). Windows print servers reside in the datacenter and manage the network printers. XenDesktop and XenApp servers also reside in the datacenter.

A regional office has numerous Windows, Linux and Mac endpoints with network attached printers. A remote branch office has a few Windows workstations with locally attached printers.

Three different print strategies are applied:

- **Headquarters** - A Citrix Universal Print Server is used for printing within the XenApp and XenDesktop session. Native print drivers are not required on the Windows based workstations. A session printer policy is configured per floor which connects the floor printer as the default printer. The policies are filtered based on the subnet of the thin client for proximity printing. Quality of Service (QoS) policies are implemented. Inbound and outbound network traffic on ports TCP 1494 and TCP 2598 are prioritized over all other network traffic. This will prevent HDX user sessions from being impacted by large print jobs.
- **Regional Office** - A Universal Print Server is deployed within the regional office. The print job uses the Universal Print Driver and is compressed and delivered from the user's session to the Universal Print Server, across the WAN. The job is then sent to the network-attached printer in the office.
- **Branch Office** - Since all branch users work on Windows based workstations, auto-created client printers in conjunction with the Citrix Universal Printer Driver are used. Since the print job is delivered over ICA, the print data is compressed which saves bandwidth. The Citrix Universal Printer Driver ensures all printers connected to the client can be used within the XenApp or XenDesktop session without concern of the printer model used.

Applications

Properly integrating an application requires understanding compatibility and how the user/business requirements influences the appropriate delivery method.

Decision: Compatibility

VDI typically requires significant changes to be made to an organization's application delivery and management strategy. For example, many organizations will take the opportunity to upgrade their desktop operating system and to simplify management by reducing the number of applications installed into the base image using techniques such as application streaming and application layering. These are significant changes that require comprehensive compatibility testing. Important compatibility requirements that may need to be verified include:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Operating system** – The application must be compatible with the preferred operating system.
- **Multi-User** – Some applications may be more appropriate for delivery via a hosted shared desktop or a hosted Windows App. In these situations, the compatibility of the application must be verified against the multi-user capabilities of a server operating system like Windows Server 2012R2.
- **Application architecture** – It is important to understand whether the application includes 16-bit, 32-bit or 64-bit code so that an appropriate operating system can be selected. 16-bit code cannot be executed on a 64-bit operating system. However, a 16-bit application can be delivered to users as a Hosted Windows App from a 32-bit desktopbased operating system like x86 editions of Windows 7, 8 or 10.
- **Interoperability** – Some applications may experience complications if they coexist on the same operating system. Possible causes include shared registry hives, dll files or INI files as well as incompatible dependencies. Application interoperability issues should be identified so that appropriate remediation steps can be taken or an alternative delivery model selected.
- **Dependency** – Applications may need to interact with each other to provide the users with a seamless experience. For example, applications that present information in a PDF format require a suitable PDF viewer to be available. Many times, the dependent (child) applications are version specific to the parent application.
- **Application virtualization** – The use of application virtualization techniques, like streaming and layering, helps to simplify image management by reducing the number of applications installed into the base image. However, not all applications are suitable for streaming and layering because they may install device drivers, use COM+ or form part of the operating system.

Application compatibility can be achieved by doing a combination of manual, user testing, utilizing pre-verified lists maintained by the software vendor, or using an automated application compatibility solution, like Citrix AppDNA, which runs through thousands of tests to verify compatibility.

Decision: Application Delivery Method

It is unlikely that a single delivery method will meet all requirements. Based on the outcome of the application categorization assessment process and the overall image management strategy (installed images, scripted images and layered images), several application delivery methods can be considered.

Choosing one of the appropriate application delivery method helps improve scalability, management and user experience.

- **Installed app** – The application is part of the base desktop image. The install process involves dll, exe and other files copied to the image drive as well as registry modifications.
- **Streamed App (Microsoft App-V)** – The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings placed in a container on the virtual desktop and isolated from the base operating system and each other, which helps to address compatibility issues.
- **Layered App (Citrix App Layering)** – Each layer contains a single application, agent or operating system. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer; update the layer and all deployed images containing that layer are updated. App Layering has two different delivery options:
  - **Layered Image** – By integrating one OS layer, one platform layer (XenApp/XenDesktop VDA, Provisioning Services agent) and many application layers, an administrator can easily create new, deployable images.
  - **Elastic Layer** – A XenApp and XenDesktop user can dynamically receive a new app layer based at logon. On a XenApp host, an elastic layer is session-aware, where an attached layer is only available to a user's session granted access to the layer.
- **Hosted Windows App** - An application installed on a multi-user XenApp host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is executing remotely.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Local App** – An application deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it executes on the endpoint.

The following table provides recommendations on the preferred approaches for integrating applications into the overall solution.

In the table:

- **Y** indicates Recommended.
- **N** indicates Not Recommended.
- **o** indicates Viable.

App Category	Installed App	Streamed App	Layered App	Hosted Windows App	Local App
Common	Y	o	Y	o	N
Departmental	o	Y	Y	Y	N
User	N	o	Y	o	Y
Management	Y	N	Y	o	N

Experience from the Field

- **Energy** – An energy company installs applications on the base image for the majority of users and streams departmental applications as required.
- **Financial** – A banking customer maintains and deploys multiple desktop images containing user group focused applications as required by various departments.

Virtual Machines

Virtual resources require proper allocation of the processor, memory and disk. These decisions have a direct impact on the amount of hardware required as well as the user experience.

The key to successful resource allocation is to ensure that virtual desktops and applications offer similar levels of performance to physical desktops. Otherwise, productivity and overall user satisfaction will be affected. Allocating resources to the virtual machines above their requirements however is inefficient and expensive for the business.

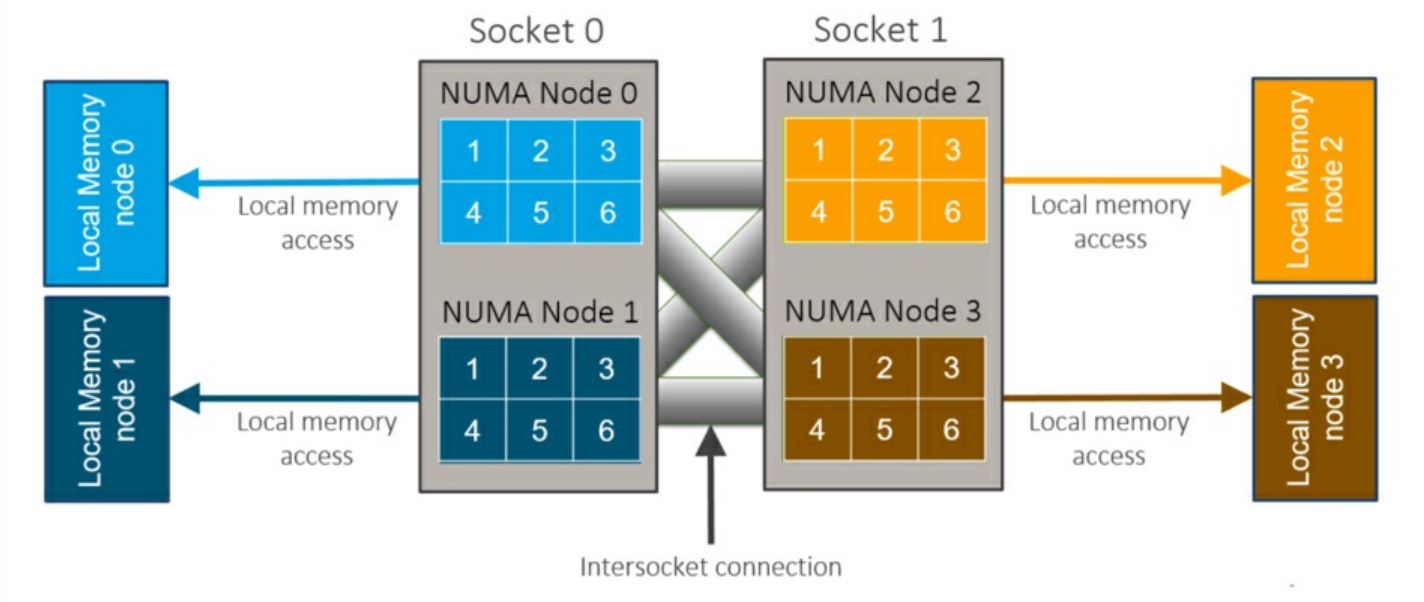
The resources allocated should be based on the workload characteristic of each user group, identified during the assess phase.

Decision: Virtual Processor (vCPU)

For hosted desktop-based VDI models (hosted pooled desktops and hosted personal desktops), the general recommendation is two or more vCPUs per virtual machine so that multiple threads can be executed simultaneously. Although a single vCPU could be assigned for extremely light workloads, users are more likely to experience session hangs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For hosted server-based VDI models (hosted Windows apps, hosted browser apps, hosted shared desktops), the proper vCPU allocation is based on the Non-Uniform Memory Access (NUMA) architecture of the processors.



Each socket is divided into one or more NUMA nodes. Hosted server-based VDI models will often utilize 4 or more processors. Allocating more vCPU than the NUMA node contains results in a performance hit. Allocating a portion of a NUMA node to a virtual machine results in a performance hit if the portion allocated is not easily divisible by the size of the NUMA node. It is often ideal to allocate the number of cores within a NUMA node to a virtual machine or allocate ½ of the cores to a virtual machine, while doubling the number of virtual machines.

User Workload	**Operating System**	**vCPU Configured for Scale**	**vCPU Configured for Experience**
Light	Windows 7	2 vCPU	2 vCPU
	Windows 10	2 vCPU	2 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Medium	Windows 7	2 vCPU	3 vCPU
	Windows 10	2 vCPU	3 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Heavy	Windows 7	3 vCPU	4 vCPU
	Windows 10	3 vCPU	4 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA

> **注意**
>
> Windows 2012 R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

Decision: CPU Optimization

In a shared and virtualized environment, a single user can monopolize CPU resources due to a runaway process or an intense data processing operation in Excel. If the processor is oversubscribed, it will not be able to fulfill other users' requests, resulting in a hung session.

Citrix Workspace Environment Management, a component of XenApp and XenDesktop, incorporates CPU optimization. When a process consumes a certain percentage of the CPU over a defined timeframe, the process priority lowers from normal to low or very low, giving all remaining processes a higher priority and overcoming the runaway process risk. CPU optimization will also remember processes that triggered CPU protection and automatically start the process at a lower priority on future launches.

Most environments should enable CPU optimization as a default configuration.

Decision: Virtual Memory (vRAM)

The amount of memory allocated to each resource is a function of the user's expected workload and application footprint. Assigning insufficient memory to the virtual machines will cause excessive paging to disk, resulting in a poor user experience; allocating too much RAM increases the overall cost of the solution.

The following table provides guidance on the virtual RAM that should be assigned based on workload.

User Workload	**Operating System**	**vRAM Configured for Scale**	**vRAM Configured for Experience**
Light	Windows 7	2 GB	3 GB
	Windows 10	2 GB	3 GB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2012R2	256 MB per user	
	Windows 2016	320 MB per user	
Medium	Windows 7	3 GB	4 GB
	Windows 10	3 GB	4 GB
	Windows 2012R2	512 MB per user	
	Windows 2016	640 MB per user	
Heavy	Windows 7	6 GB	8 GB
	Windows 10	6 GB	8 GB
	Windows 2012R2	1024 MB per user	
	Windows 2016	1280 MB per user	

注意

- Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.
- Memory allocation above 4GB requires a 64-bit operating system.
- If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

Decision: RAM Optimization

Even though users only work within a single application at a time, most have five or more applications running but idle. When a process moves from active to idle, the application and operating system releases a portion of the process's active working set of memory to free up system resources. However, this is only a small percentage of the applications working set. The rest remains locked for the application, severely limiting available system resources.

Using RAM Optimization within Citrix Workspace Environment Management, applications that are idle (have not been interacted with by a user) for a certain time are forced to release excess memory until they are no longer idle. When the application returns to an active state, the released memory is loaded back into the active working set.

Most environments should enable RAM optimization as a default configuration. A RAM optimization exclusion list is available if certain processes encounter issues with optimization.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Disk Cache

The amount of storage that each VM requires will vary based on the workload and the image type. If creating hosted personal desktop without leveraging an image management solution, each VM will require enough storage for the entire OS and locally installed applications.

Deploying machines through Machine Creation Services or Provisioning Services can substantially reduce the storage requirements for each virtual machine. Disk space requirements for the write cache and difference disk will depend on application usage and user behavior. However, the following table provides a starting point for estimating disk space requirements based on machine sized with vCPU and vRAM as per the following guidelines:

User Workload	**Operating System**	**Storage Space (Differencing Disk / Write Cache Disk)**
Light	Windows 7	10 GB
	Windows 10	10 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Medium	Windows 7	15 GB
	Windows 10	15 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Heavy	Windows 7	20 GB
	Windows 10	20 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB

Decision: RAM Cache

Provisioning Services and Machine Creation Services have the capability to utilize a portion of the virtual machine's RAM as a buffer for the storage cache. The RAM cache is used to improve the performance of traditional storage by sharing the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

virtual machine's non-paged pool memory.

User Workload	Operating System	RAM Cache Configured for Scale	RAM Cache Configured for Experience
Light	Windows 7	128 MB	256 MB
	Windows 10	128 MB	256 MB
	Windows 2012R2	2GB	
	Windows 2016	4GB	
Medium	Windows 7	256 MB	512 MB
	Windows 10	256 MB	512 MB
	Windows 2012R2	4GB	
	Windows 2016	8GB	
Heavy	Windows 7	512 MB	1024 MB
	Windows 10	512 MB	1024 MB
	Windows 2012R2	6GB	
	Windows 2016	10 GB	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意

- If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.
- If additional RAM is available on the host, the RAM Cache amounts can be increased to provide even greater levels of performance.

Decision: Storage IOPS

Storage performance is limited by the number of operations it can handle per second, referred to as IOPS. Under allocating storage IOPS results in a VDI desktop where apps, web pages and data are slow to load.

The following table provides guidance on the number of storage IOPS generated per user based on workload and operating system. Storage IO activity will be higher during user logon/logoff.

User Workload	**Operating System**	**Storage IOPS (without RAM-Based Cache)**	**Storage IOPS (with RAM-Based Cache)**
Light	Windows 7	10 IOPS	1 IOPS
	Windows 10	12 IOPS	1 IOPS
	Windows 2012R2	3 IOPS	0.5 IOPS
	Windows 2016	4 IOPS	1 IOPS
Medium	Windows 7	15 IOPS	1 IOPS
	Windows 10	20 IOPS	1.5 IOPS
	Windows 2012R2	4 IOPS	0.5 IOPS
	Windows 2016	6 IOPS	1 IOPS
Heavy	Windows 7	25 IOPS	2 IOPS
	Windows 10	35 IOPS	3 IOPS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2012R2	5 IOPS	0.5 IOPS
	Windows 2016	8 IOPS	1 IOPS

Decision: IO Prioritization

With shared environments, every user's IO process receives an equal share of resources. A user running some IO intensive task can affect mission critical applications. Citrix Workspace Environment Management allows administrators to define IO priorities for processes.

If a process requires more IO resources or the process is monopolizing IO resources, the process and process priority is manually increased or decreased via the console. This advanced configuration is only used in special circumstances.

Decision: Graphics (GPU)

Without a graphical processing unit (GPU), graphical processing is rendered with software by the CPU. A graphical processing unit (GPU) can be leveraged to improve server scalability and user experience or enable the use of graphically intensive applications. During the desktop design it is important to decide how the GPU (if used) will be mapped to the virtual machines. There are three methods available.

- **Pass-Through GPU** – Each physical GPU is passed through to a single virtual machine (hosted apps or hosted desktops).
- **Hardware Virtualized GPU** – Using a hypervisor's vGPU technology, an NVIDIA GRID or Intel Iris Pro is virtualized and shared between multiple machines. Each virtual machine has the full functionality of GPU drivers and direct access to the GPU.
- **Software Virtualized GPU** – The GPU is managed by the hypervisor and intercepts requests made by the VDI desktops. This process is used if a GPU is not installed within the host.

In the table:

- **Y** indicates Available.
- **X** indicates Not Supported.

	Pass-Through GPU	**Hardware Virtualized GPU (NVidia)**	**Hardware Virtualized GPU (Intel)**	**Hardware Virtualized GPU (AMD)**	**Software Emulated GPU**
Citrix XenServer					
XenDesktop	**Y**	**Y**	**Y**	**X**	**Y**
XenApp	**Y**	**Y**	**Y**	**X**	**Y**
Microsoft Hyper-V					
XenDesktop	**Y**	**X**	**X**	**X**	**Y**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp	**Y**	**X**	**X**	**X**	**Y**
VMware vSphere					
XenDesktop	**Y**	**Y**	**X**	**Y**	**Y**
XenApp	**Y**	**Y**	**X**	**Y**	**Y**

User groups with a heavy use of graphical applications will often require the use of a NVidia hardware virtualized GPU. User groups who rely on office-based applications can have an observable benefit with the use of a hardware virtualized GPU from Intel.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology control layer

May 07, 2018

The control layer is the fourth layer of the design methodology.

Active Directory

Decision: Forest Design

Multi-forest deployments, by default, do not have inter-domain trust relationships between the forests. An AD administrator can establish trust relationships between the multiple forests, allowing the users and computers from one forest to authenticate and access resources in another forest.

For forests that have inter-domain trusts, it is recommended that the appropriate settings be configured to allow the Delivery Controllers to communicate with both domains. When the appropriate trusts are not configured, multiple XenDesktop sites for each forest must be configured. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX134971 – Successfully Deploying XenDesktop in a Complex Active Directory Environment

Decision: Organizational Unit Structure

Infrastructure components for a XenApp and XenDesktop deployment should reside within their own dedicated organizational units (OUs); separating workers and controllers for management purposes. By having their own OUs, the objects inside will have greater flexibility with their management while allowing Citrix administrators to be granted delegated control.

A sample Citrix OU structure can be seen below.



Decision: User Groups

Whenever possible, permissions and authorization should be assigned to user groups rather than individual users, thereby eliminating the need to edit a large amount of resource permissions and user rights when creating, modifying, or deleting user accounts. Permission application example:

- An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- The same application published to 1,000 individual user accounts requires the validation of all 1,000 objects.

Database

The majority of Citrix products discussed within this document require a database. The following table outlines the usage on a per product basis:

In this table:

- **Y** indicates Available.
- **O** indicates Optional.

Product	Configuration Data	Runtime Data	Audit/Change Log Data	Monitoring Data
XenDesktop	Y	Y	Y	Y
Provisioning Services	Y		O	
Desktop Player	Y	Y	Y	

Decision: Edition

There are multiple editions of Microsoft SQL Server 2012: Express, Web, Standard, Business Intelligence, and Enterprise. Based on the capabilities of the various SQL Server editions available, the Standard edition is often used for hosting the XenApp and XenDesktop databases in production environments.

The Standard edition provides an adequate amount of features to meet the needs of most environments. For more information on the databases supported with Citrix products please refer to the Citrix Database Support Matrix. Different versions of Citrix products support different versions of the SQL server; therefore, it is important to check the support matrix to ensure the version of SQL server used is compatible with the Citrix product being deployed.

Decision: Database Server Sizing

The SQL Server must be sized correctly to ensure the performance and stability of an environment. Since every Citrix product uses SQL server in a different way, no generic all-encompassing sizing recommendations can be provided. Instead, per-product SQL server sizing recommendations are provided below.

XenApp and XenDesktop

XenApp and XenDesktop Brokers use the database as a message bus for broker communications, storing configuration data and storing monitoring and configuration log data. The databases are constantly in use and the performance impact on the SQL server can be considered as high.

Based on results from Citrix internal scalability testing the following SQL server specification for a server hosting all XenDesktop databases are recommended:

- 2 Cores / 4 GB RAM for environments up to 5,000 users
- 4 Cores / 8 GB RAM for environments up to 15,000 users

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 8 Cores / 16 GB RAM for environments with 15,000+ users

The database files and transaction logs should be hosted on separate hard disk subsystems in order to cope with a high number of transactions. For example, registering 20,000 virtual desktops during a 15-minute boot storm causes ~500 transactions / second and 20,000 users logging on during a 30-minute logon storm causes ~800 transactions / second on the XenDesktop Site Database.

Provisioning Services

In addition to static configuration data provisioning servers store runtime and auditing information in the database. Depending on the boot and management pattern, the performance impact of the database can be considered as low to medium.

Based on this categorization, a SQL server specification of 4 Cores and 4 GB RAM is recommended as a good starting point. The SQL server should be carefully monitored during the testing and pilot phase in order to determine the optimal configuration of the SQL server.

Decision: Instance Sizing

When sizing a SQL database, two aspects are important:

- **Database file** – Contains the data and objects such as tables, indexes, stored procedures and views stored in the database.
- **Transaction log file** – Contains a record of all transactions and database modifications made by each transaction. The transaction log is a critical component of the database and, if there is a system failure, the transaction log might be required to bring the database back to a consistent state. The usage of the transaction log varies depending on which database recovery model is used:
  - **Simple recovery** – No log backups required. Log space is automatically reclaimed, to keep space requirements small, essentially eliminating the need to manage the transaction log space. Changes to the database since the most recent backup are unprotected. In the event of a disaster, those changes must be redone.
  - **Full recovery** – Requires log backups. No work is lost due to a lost or damaged database data file. Data of any arbitrary point in time can be recovered (for example, prior to application or user error). Full recovery is required for database mirroring.
  - **Bulk-logged** – Requires log backups. This is an adjunct of the full recovery model that permits high-performance bulk copy operations. It is typically not used for Citrix databases.

For further information, please refer to the Microsoft Developer Network – SQL Server Recovery Models.

In order to estimate storage requirements, it is important to understand the disk space consumption for common database entries. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX139508 – XenDesktop 7.x Database Sizing.

XenDesktop General

XenApp 7.x and XenDesktop 7.x use three distinct databases:

- **Site Configuration database** – Contains static configuration and dynamic runtime data
- **Monitoring database** – Contains monitoring data which is accessible via Director
- **Configuration logging database** – Contains a record for each administrative change performed within the site (accessible via Studio)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Site Database

Since the database of a XenApp or XenDesktop site contains static configuration data and dynamic runtime data, the size of the database file depends not only on the physical size of the environment but also user patterns. The following factors all impact the size of the database file:

- The number of connected sessions
- The number of configured and registered VDAs
- The number of transactions occurring during logon
- VDA heartbeat transactions

The size of the Site Database is based on the number of VDAs and active sessions. The following table shows the typical maximum database size Citrix observed when scale testing XenApp and XenDesktop with a sample number of users, applications, and desktop delivery methods.

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	Hosted Pooled	30
10,000	N/A	Hosted Pooled	115
40,000	N/A	Hosted Pooled	390

> **注意**
>
> This sizing information is a guide only. Actual database sizes may differ slightly by deployment due to how databases are maintained.

Determining the size of the transaction log for the Site database is difficult due to factors that can influence the log including:

- The SQL Database recovery model
- Launch rate at peak times
- The number of desktops being delivered

© 1999-2017 Citrix Systems, Inc. All rights reserved.

During XenDesktop scalability testing, Citrix observed the transaction log growth rate at 3.5MB an hour when the system is idle, and a per user per day growth rate of ~32KB. In a large environment, transaction log usage requires careful management and a regular backup, to prevent excessive growth. This can be achieved by means of scheduled jobs or maintenance plans.

Monitoring Database

Of the three databases, the Monitoring database is expected to be the largest since it contains historical information for the site. Its size is dependent on many factors including:

- Number of Users
- Number of sessions and connections
- Number of workers
- Retention period configuration – Platinum customers can keep data for over a year (default 90 days). Non-platinum customers can keep data for up to 7 days (default 7 days).
- Number of transaction per second. Monitoring service tends to execute updates in batches. It is rare to have the number of transactions per second go above 20.
- Background transaction caused by regular consolidation calls from the Monitoring service.
- Overnight processing carried out to remove data outside the configured retention period.

The following table shows the estimated size of the Monitoring database over a period of time under different scenarios. This data is an estimate based on data seen within scale testing XenApp and XenDesktop (assuming a 5 day working week).

Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500
Estimates with 2 connections and 1 session per user with a 5 day work week					
Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	30	100	330	1,300

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	280	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

> **注意**
>
> The 100,000 HSD tests are based on a test environment consisting of:
>
> - 2 Delivery Controllers
> - 43 Hosted Shared Desktop workers
> - 3 SQL servers, configured with databases held within one Always On Availability Group.
>
> For more information please see the Citrix Support article – XenDesktop 7.x Database Sizing.

The size of the transaction log for the Monitoring Database is very hard to estimate, but XenApp and XenDesktop scalability testing showed a growth rate of about 30.5 MB an hour when the system is idle, and a per user per day growth rate of ~9 KB.

Configuration Logging Database

The Configuration Logging Database is typically the smallest of the three databases. Its size and the size of the related transaction log depends on the daily administrative activities initiated from Studio, Director or PowerShell scripts, therefore its size is difficult to estimate. The more configuration changes are performed, the larger the database will grow. Some factors that can affect the size of the database include:

- The number of actions performed in Studio, Director and PowerShell.
- Minimal transactions which occur on the database when no configuration changes are taking place.
- The transaction rate during updates. Updates are batched whenever possible.
- Data manually removed from the database. Data within the Configuration Logging Database is not subject to any retention policy, therefore it is not removed unless done so manually by an administrator.
- Activities that have an impact on sessions or users, for example, session logoff and reset.
- The mechanism used for deploying desktops.

In XenApp environments not using MCS, the database size tends to fall between 30 and 40MB. For MCS environments, database size can easily exceed 200MB due to the logging of all VM build data.

Temporary Database

In addition to the Site, Monitoring, and Configuration Logging databases, a system-wide temporary database (tempdb) is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

provided by SQL Server. This temporary database is used to store Read-Committed Snapshot Isolation data. XenApp 7.x and XenDesktop 7.x uses this SQL Server feature to reduce lock contention on the XenApp and XenDesktop databases. Citrix recommends that all XenApp 7.x and XenDesktop 7.x databases use Read-Committed Snapshot Isolation. For more information please see How to Enable Read-Committed Snapshot in XenDesktop.

The size of the tempdb database will depend on the number of active transactions, but in general it is not expected to grow more than a few MBs. The performance of the tempdb database does not impact the performance of XenApp and XenDesktop brokering, as any transactions that generate new data require tempdb space. XenApp and XenDesktop tend to have short-lived transactions, which help keep the size of the tempdb small.

The tempdb is also used when queries generate large intermediate result sets. Guidance and sizing the tempdb can be found on the Microsoft TechNet article Optimizing tempdb Performance.

Provisioning Services

The Provisioning Services farm database contains static configuration and configuration logging (audit trail) data. The record size requirements outlined below can be used to help size the database:

Configuration Item	DB Space Required (KB)	Number of Items (Example)	Total (KB)
Base farm configuration	112	-	112
User group w/ farm access	50	10	250
Site	4	5	20
Device collection	10	50	500
Farm view	4	10	40
Farm view to device relationship	5	1	5,000
Site View	4	5	20
Site view to device relationship	5	1	5,000
Device	2	5,000	10,000

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Device bootstrap	10	-	-
Device to disk relationship	35	1	175,000
Device printer relationship	1	-	-
Device personality data	1	-	-
Device status (when booted)	1	5,000	5,000
Device custom property	2	-	-
vDisk	1	20	20
vDisk version	3	5	300
Disk locator	10	1	200
Disk locator custom property	2	-	-
Server	5	10	50
Server IP	2	1	20
Server status (when booted)	1	20	20
Server custom property	2	-	-
vDisk store	8	5	40

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vDisk store to server relationship	4	1	40
Connection to XenServer (VirtualHostingPool)	4	-	-
vDisk update task	10	10	100
Administrative change (auditing enabled)	1	10,000	10,000
Total			**211,732KB (~212MB)**

During the PVS farm setup, a database with an initial file size of 20MB is created. Due to the nature of the data in the PVS farm database the transaction log is not expected to grow very quickly, unless a large amount of configuration is performed.

In contrast to XenApp, which also offers the ability to track administrative changes, the related information is not written to a dedicated database but directly to the Provisioning Services farm database. In order to limit the size of the Provisioning Services database it is recommended to archive the audit trail data on a regular schedule.

Decision: Database Location

By default, the Configuration Logging and Monitoring databases are located within the Site Configuration database. Citrix recommends changing the location of these secondary databases as soon as the configuration of the site has been completed, in order to simplify sizing, maintenance and monitoring. All three databases can be hosted on the same server or on different servers. An ideal configuration would be to host the Monitoring database on a different server from the Site Configuration and Configuration Logging databases since it records more data, changes occur more frequently and the data is not considered to be as critical as the other databases. For more information, please refer to Citrix Docs – Change secondary database locations.

> **注意**
>
> The location of the Configuration Logging database cannot be changed when mandatory logging is enabled.

Decision: High-Availability

The following table highlights the impact to XenApp, XenDesktop and Provisioning Services when there is a database outage:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Impact of Database Outage
Site configuration database	Users will be unable to connect or reconnect to a virtual desktop. **Note**: Local Host Cache allows users with Hosted Shared Desktops, Hosted Windows and Browser Applications, and Personal Desktops to reconnect to their applications and desktops even when the site database is unavailable.
Monitoring database	Director will not display any historical data and Studio cannot be started. Brokering of incoming user requests and existing user sessions will not be affected.
Configuration logging database	If allow changes when the database is disconnected has been enabled within XenApp and XenDesktop logging preferences, an outage of the configuration logging database will have no impact (other than configuration changes not being logged). Otherwise, administrators will be unable to make any changes to the XenApp and XenDesktop site configuration. Users are not impacted.
Provisioning Services farm database	When offline database support is enabled and the database becomes unavailable, the stream process uses a local copy of the database to retrieve information about the provisioning server and the target devices supported by the server. This allows provisioning servers and the target devices to remain operational. However, when the database is offline, the console and the management functions listed below become unavailable: • Auto Add target devices • vDisk creation and updates • Active Directory password changes • Stream process startup • Image update service • PowerShell and MCLI based management If offline database support has not been enabled, all management functions become unavailable and the boot and failover of target devices will fail.

> **注意**
>
> Please review HA options for 3rd party databases (for example, App-V, SCVMM or vCenter) with the respective software vendor.

In addition to the built-in database redundancy options, Microsoft SQL Server, as well as the underlying hypervisor (in virtual environments), offer a number of high availability features. These enable administrators to ensure single server outages will have a minimal impact (if any) on the XenApp and XenDesktop infrastructure. The following the SQL / hypervisor high availability features are available:

- **VM-level HA** – This high availability option is available for virtual SQL servers only, which need to be marked for High Availability at the hypervisor layer. In case of an unexpected shutdown of the virtual machine or the underlying hypervisor host, the hypervisor will try to restart the VM immediately on a different host. While VM-level HA can minimize downtimes in power-outage scenarios, it cannot protect from operating system level corruption. This solution is less expensive than mirroring or clustering because it uses a built-in hypervisor feature. However, the automatic failover process is slower, as it can take time detect an outage and start the virtual SQL server on another host. This may interrupt the service to users.
- **Mirroring** – Database mirroring increases database availability with almost instantaneous failover. Database mirroring can be used to maintain a single standby or mirror database, for a corresponding principal or production database.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Database mirroring runs with either synchronous operation in high-safety mode, or asynchronous operation in high-performance mode. In high-safety mode with automatic failover (recommended for XenDesktop) a third server instance, known as a witness, is required, which enables the mirror server to act as a hot standby server. Failover from the principal database to the mirror database happens automatically and is typically completed within a few seconds. It is a good practice to enable VM-level HA (or a similar automatic restart functionality) for at least the witness to ensure SQL service availability in case of a multi-server outage.

> **注意**
>
> Microsoft is planning to remove mirroring as a high availability option in a future release of SQL Server and is discouraging its use in new network development. Please refer to the Microsoft article – Database Mirroring (SQL Server) for more information

- **AlwaysOn Failover Cluster Instances** – Failover clustering provides high-availability support for an entire instance of Microsoft SQL Server. A failover cluster is a combination of two or more nodes, or servers, using a shared storage. A Microsoft SQL Server AlwaysOn Failover Cluster Instance, introduced in SQL Server 2012, appears on the network as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable. The transition from one node to the other node is seamless for the clients connected to the cluster. AlwaysOn Failover cluster Instances require a Windows Server Failover Clustering (WSFC) resource group. The number of nodes supported in the WSFC resource group will depend on the SQL Server edition. (Please refer to the table in the Decision: Edition earlier in this chapter.) For more information please refer to MSDN – AlwaysOn Failover Cluster Instances (SQL Server).
- **AlwaysOn Availability Groups** – AlwaysOn Availability Groups is an enterprise-level highavailability and disaster recovery solution introduced in Microsoft SQL Server 2012, which enables administrators to maximize availability for one or more user databases. AlwaysOn Availability Groups require that the Microsoft SQL Server instances reside on Windows Server failover clustering (WSFC) nodes. Similar to failover clustering a single virtual IP / network name is exposed to the database users. In contrast to failover clustering, shared storage is not required since the data is transferred using a network connection. Both synchronous and asynchronous replication to one or more secondary servers is supported. As opposed to mirroring or clustering secondary servers can be actively used for processing incoming read-only requests, backups or integrity checks. This feature can be used to offload user resource enumeration requests to a secondary SQL server in XenDesktop environments to essentially scale-out a SQL server infrastructure. Since the data on active secondary servers can lag multiple seconds behind the primary server, the read-only routing feature cannot be used for other XenDesktop database requests at this point in time. For more information, please refer to MSDN – AlwaysOn Availability Groups (SQL Server).

The following table outlines the recommended high availability features for Citrix databases:

In the table:

- **Y** indicates Recommended.
- **o** indicates Viable.
- **N** indicated Not Supported.
- **T** indicates for test environments only.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	VM Level - HA	Mirroring	AlwaysOn Failover Cluster Instances	AlwaysOn Availability Groups
Site database	T	Y	o	o
Configuration logging database	T	o	o	o
Monitoring database	T	Y	o	o
Provisioning Services farm database	T	Y	o	N
DesktopPlayer database	T	N	o	o

Citrix Licensing

Citrix offers organizations the flexibility of multiple licensing models that align with common usage scenarios. The different licensing models vary based on the Citrix product used, but can include per user/device and per concurrent user. Several Citrix products use the license server, while other products require a license to be installed on the product itself.

Citrix License Server

- XenDesktop
- XenApp
- Provisioning Services
- XenServer

On the product:

- NetScaler
- NetScaler Gateway

For more information on XenDesktop 7.x licensing, please refer to CTX128013 - XenDesktop Licensing.

For more information on Microsoft Licensing, please refer to the Microsoft document – Licensing Microsoft's Virtual Desktop Infrastructure Technology.

Decision: Sizing

Internal scalability testing has shown that a single virtual license server with two cores and 2GB of RAM can issue approximately 170 licenses per second or 306,000 licenses per half hour. If necessary, the specification of the license server can be scaled out to support a higher number of license requests per second.

Decision: High Availabiity

For a typical environment, a single license server is sufficient. Should the license server become unavailable, dependent Citrix products will enter a 30-day grace period, which provides more than enough time to resolve connectivity issues and/or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

restore or rebuild the license server.

> **注意**
>
> - If the license server and the Citrix product do not communicate within 2 heartbeats (5-10 min), the Citrix product will enter a grace period and will allow connections for up to 30 days. Once communication with the license server is re-established, the license server will reconcile the temporary and actual licenses.
> - A CNAME record in DNS is a convenient way to reference the license server. Using CNAMEs allows the license server name to be changed without updating the Citrix products.

If additional redundancy is required, Citrix supports the following high availability solutions for the license server.

- **Windows Clustering** – Cluster servers are groups of computers that work together in order to increase availability. Clustering allows the license server role to automatically failover in the event of a failure. For more information on clustering, please see the Citrix Docs article – Clustered License Servers.
- **Duplication of license server** – Create a VM level backup of the license server. This backup should not be stored on the same host as the license server. Instead, it should be stored in a safe location, such as a highly available storage solution, or backed up to tape or disk. The duplicate server is not active, and will remain on standby until the need arises to restore the active license server. Should the license server be restored using this backup, any new licenses must be re-downloaded to the server.

For more information, please refer to Citrix eDocs – Licensing Architecture Overview.

Each method allows an administrator to exchange a single license server for another without an interruption in service; assuming that the change occurs during the grace period and that the following limitations are considered.

- License files will reference the server specified during the allocation process. This means that the license files can only be used on a server with the same binding information (Hostname) as the server that was previously specified.
- Two Windows-based, domain joined license servers cannot share the same name and be active in the environment at the same time.
- Because license servers do not communicate with each other, any additional licenses must be placed on both the active and backup license server.

Decision: Optimization

License server performance can be optimized by tuning the number of “receive” and “processing” threads. If the thread count is set too low, requests will be queued until a thread becomes available. Conversely, if the thread count is set too high, the license server will become overloaded.

The optimal values are dependent on the server hardware, site configuration, and license request volume. Citrix recommends testing and evaluating different values to determine the proper configuration. Setting the maximum number of processing threads to 30 and the maximum number of receiving threads to 15 is a good starting point for large scale deployments.

This optimization will improve the Citrix License Server ‘s ability to provide licenses by increasing its ability to receive and process license requests.

For more information, please refer to the Citrix Docs – Improving Performance by Specifying Thread Use.

Delivery Controllers

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Server Sizing

Delivery Controller scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a controller can support. Each desktop startup, registration, enumeration and launch request impacts the controller's processor. As the storm increases in intensity, the CPU utilization of the controller will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Adding additional CPU cores to a Delivery Controller will lower the overall CPU utilization, thus allowing for greater numbers of desktops supported by a single controller. This is really only feasible when dealing with virtualized controllers as adding virtual CPUs is fairly easy and straightforward. The other alternative is to add another controller into the site configuration. The controller would have the same configuration as other controllers, and the load would be evenly distributed across all controllers, thus helping to reduce the overall load on each single controller.

Testing has shown that a single Delivery Controller, using the following configuration, can support more than 5,000 desktops.

Component	Specification
Processor	4 vCPU
Memory	4 GB RAM
Network	Bonded virtual NIC
Host Storage	40-GB shared storage
Operating System	Windows Server 2012 R2
XenDesktop	7

The following formula can be used to calculate the number of Delivery Controllers required for a Citrix site.

$$Number\ of\ Delivery\ Controllers = \frac{Number\ of\ Active\ Sessions\ per\ Site}{5{,}000} + 1$$

Decision: High Availability

If the server hosting the Delivery Controller is unavailable, users will not be able to access their virtual desktops or published applications. Therefore at least two Delivery Controllers (N+1 redundancy) should be deployed per zone on different physical servers to prevent this component from becoming a single point of failure. If one controller fails, the others can manage connections and administer the site.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The locations of all Delivery Controllers are specified on the VDA, allowing it to automatically failover if communication with one Delivery Controller is unavailable. The VDA checks the following locations, in order, stopping at the first place it finds the Delivery Controller:

1. A persistent storage location maintained for the auto-update feature. This location contains controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation.
   For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.
2. Policy settings (Delivery Controllers, Delivery Controller SIDs).
3. The Delivery Controller information under the VDA ListofDDCs registry key. The VDA installer initially populates these values, based on the information specified when installing the VDA.
4. OU-based discovery. This is a legacy method maintained for backward compatibility.
5. The Personality.ini file created by Machine Creation Services.

Citrix Consulting recommends utilizing the auto-update feature (enabled by default). This feature will simplify management of the environment by keeping VDA's updated when adding and removing Delivery Controllers.

Decision: Local Host Cache

Even if the SQL database is highly available, there is the risk of not having access to the database if the network connection between the delivery controller and SQL database fails, which is an important concern for sites that span geographical locations.

To overcome this risk, the delivery controllers can utilize the local host cache feature that creates a local copy of the SQL database, used only if the delivery controller loses contact with the database.

The following must be considered when using local host cache:

- **Elections** – When the zones loses contact with the SQL database, an election occurs nominating a single delivery controller as master. All remaining controllers go into idle mode. A simple alphabetical order determines the winner of the election.
- **Sizing** – When using local host cache mode, a single delivery controller is responsible for all VDA registrations, enumerations, launches and updates. The elected controller must have enough resources (CPU and RAM) to handle the entire load for the zone. A single controller can scale to 10,000 users, which influences the zone design.
  - **RAM** – The local host cache services can consume 2+GB of RAM depending on the duration of the outage and the number of user launches during the outage.
  - **CPU** – The local host cache can use up to 4 cores in a single socket.
  - **Storage** – During local host cache mode, storage space increased 1MB every 2-3 minutes with an average of 10 logons per second.
- **Power Options** – Powered off virtual resources will not start when the delivery controller is in local host cache mode. Pooled virtual desktops that reboot at the end of a session are placed into maintenance mode.
- **Consoles** – When using local host cache mode, Studio and PowerShell are not available.

Decision: XML Service Encryption

In a typical session, the StoreFront server passes credentials to the Citrix XML Service on a Delivery Controller. The Citrix XML protocol uses clear text to exchange all data, with the exception of passwords, which are transmitted using obfuscation.

If the traffic between the Storefront servers and the XenDesktop Controllers can be intercepted it will be vulnerable to the following attacks:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Attackers can intercept the XML traffic and steal resource set information and tickets.
- Attackers with the ability to crack the obfuscation can obtain user credentials.
- Attackers can impersonate the XenDesktop Controller and intercept authentication requests.

For most organizations, the Citrix XML traffic will be isolated on a dedicated physical or virtual datacenter network making interception unlikely. However, for safety consider using SSL encryption to send StoreFront data over a secure HTTP connection.

Decision: Server OS Load Management

Default Load Management policies are applied to all Server OS delivery groups. The default settings specify the maximum number of sessions a server can host at 250 and do not consider CPU and Memory usage. Capping session count does not provide a true indication of load, which can lead to an overburdening of Server OS delivery groups resulting in a degradation of performance or an underutilization of Server OS delivery groups resulting in an inefficient usage of resources.

Citrix Consulting recommends creating unique "custom" Load Management policies for each Delivery Group based on performance and scalability testing. Different rules and thresholds can be applied to each Delivery Group depending on the different resource bottlenecks identified during testing. For more information on the available Load Management policy configurations refer to Citrix Docs – Load Management policy settings.

If adequate testing cannot be performed prior to production, Citrix Consulting recommends implementing the following "custom" Load Management policy which can be applied to all servers as a baseline:

- **CPU Usage** - Full Load: 80%
- **CPU usage excluded process priority** – Below Normal or Low
- **Memory Usage** - Full Load: 80%
- **Memory Usage base load** – Report zero load (MBs): 786
- **Maximum number of sessions** – X

The "Maximum number of sessions" policy is included for capping purposes – this is considered a best practice for resiliency. Organizations can choose an initial value of 250 (denoted by "X" above). **It is highly recommended that this value and others be customized based on the results from scalability testing**.

Coud Connector

The XenApp and XenDesktop Service within Citrix Cloud utilize a set of services contained within the Citrix Cloud Connector. A redundant set of Cloud Connector virtual machines must be placed in each data center/resource location containing VDA hosts.

Decision: Server Sizing

Cloud Connector scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a cloud connector can support. Each desktop startup, registration, enumeration and launch request affects the cloud connector's processor. As the storm increases in intensity, the CPU utilization of the cloud connector will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Testing has shown that a single Cloud Connector Controller, using the following configuration, can support 5,000 desktops.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	On Premises Specifications	Azure Hosted Specifications
Number of VMs (with N+1 Fault Tolerance)	3	6 Standard_A2_V2 instances
Processors per VM	4 vCPU	2 vCPU
Memory per VM	4 GB RAM	4 GB RAM
Host Storage per VM	40 GB shared storage	200 GB temp storage
Operating System	Windows Server 2012 R2	Windows Server 2012 R2

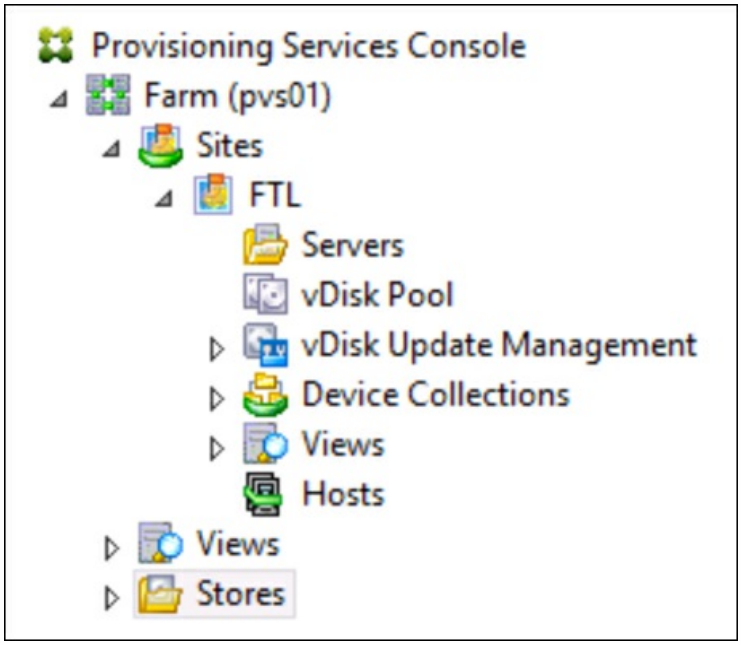
Provisioning Services

Citrix Provisioning Services (PVS) uses streaming technology to simplify the deployment of virtual and physical machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is performed on the master image.

Decision: Topology

A Provisioning Services farm represents the top level of the Provisioning Services infrastructure, which can be further broken down into sites. All provisioning servers in a farm share the same SQL database and Citrix license server.

Each site is a logical entity containing provisioning servers, vDisk pools and target device collections. Although all sites within a farm share the same database, target devices can only fail over to other provisioning servers within the same site.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are factors that must be considered when determining the overall Provisioning Services topology:

- **Network** – Provisioning servers are constantly communicating with the farm database to retrieve system configuration settings. Therefore, separate farms should be created for each physical location where target devices reside, unless they are connected to the database server by a fast and robust connection.
- **Administration** – Organizations may need to maintain the separation of administrative duties at a departmental, regional or countrywide basis. Additional Provisioning Services farms will add some complexity to the management of the environment. However, this overhead is typically limited to initial configuration, desktop creation and image updates.
- **Organization** – A practical reason for building multiple sites is due to organizational changes. For example, two companies may have recently merged through acquisition, but need to keep resources separate while integration takes place. Configuring the organization to use separate sites is one way to keep the businesses separate but managed centrally through the Provisioning Services console.

Only create additional sites if the business requirements warrant it. A single site per farm is easier to manage and requires no additional configuration.

Decision: Device Collections

Device collections provide the ability to create and manage logical groups of target devices. Creating device collections simplifies device management by allowing actions to be performed at the collection level rather than the target device level.



Device collections can represent physical locations, subnet ranges, chassis or different departments within an organization. Collections can also be used to logically separate production target devices from test and maintenance ones.

Consider creating device collections based on vDisk assignment so that the status of all target devices assigned to a particular vDisk can be quickly identified.

Decision: High Availability

Provisioning Services is a critical component of the virtual desktop infrastructure. The following recommendations should be followed to eliminate single points of failure:

- **Provisioning Server** – A minimum of two provisioning servers should always be implemented per site. Sufficient redundancy should be incorporated into the design so that a single server failure does not reduce the total number of target devices that can be supported per site. The Provisioning Services boot file should be configured for high availability. Up to four Provisioning Servers may be listed in the boot file. Target devices will try to contact the servers in the order that they are listed. The server that responds may not necessarily be the server that will provide streaming services to the target device. If Load Balancing is enabled, the target device may be reassigned to another server in the site that is less loaded than the others.
- **vDisks and Storage** – For vDisk stores hosted on local, Direct Attached Storage (DAS) or Storage Area Network (SAN),

© 1999-2017 Citrix Systems, Inc. All rights reserved.

replication should be used to synchronize the vDisks. If using Network Attached Storage (NAS), ensure that the vDisks are hosted on a highly available network share.

- **Networking** – The provisioning servers should have redundant NICs. If the provisioning server is deployed as a physical server, redundant NICs should be teamed and if the provisioning server is deployed as a virtual server, the underlying hypervisor should incorporate redundant NICs.

> **注意**
>
> The target devices will only failover to NICs that are on the same subnet as the PXE boot NIC.

Trivial File Transfer Protocol (TFTP) is a communications protocol used for transferring configuration or boot files between machines. Provisioning services can use TFTP to deliver the bootstrap file to target devices. There are several options available to make the TFTP service highly available. Some of the more commonly used options are:

- **DNS Round Robin** – A DNS entry is created for the TFTP service with multiple A records corresponding to the TFTP services running on the provisioning servers in the farm. This method is not recommended since the state of the TFTP service is not monitored. Clients could potentially be sent to a non-functioning server.
- **Hardware load balancer** – Use a hardware load balancer, such as Citrix NetScaler, to create virtual IPs that corresponds to the provisioning servers. The NetScaler can intelligently route traffic between the provisioning servers. In the event that one of the servers becomes unavailable, NetScaler will automatically stop routing TFTP requests to that server. This is the best method for making TFTP highly available, but can be complicated to setup.
- **Multiple DHCP Option 66 entries** – This method is easy to implement but requires a DHCP service that supports entering multiple entries in option 66. Microsoft DHCP server allows one option 66 entry so this method would not be feasible in environments with Microsoft DHCP services. If using a non-Microsoft DHCP server or appliance, check with the manufacturer to verify that multiple option 66 entries is supported.

There are other options available that can achieve the same result without having to use TFTP:

- **Proxy DHCP** – Use the provisioning servers PXE service to provide the bootstrap information. If one of the servers is down, the next available server in the farm can provide the bootstrap information. This method requires the provisioning servers to be on the same broadcast domain as the target devices. If there are other PXE services running on the network (Altiris, SCCM, etc.) then multiple VLANs may be required to keep the PXE services from interfering with each other.
- **Boot Device Manager** – Use the Boot Device Manager to create a bootstrap file that is either placed on the local hard drive, or used as a bootable ISO file. If the ISO file is used, configure the target devices to boot from the CD/DVD-ROM drive, and place the ISO file on a highly available shared network location or local storage of each target device. When either method is utilized, the TFTP service is not used at all.

High availability should always be incorporated into the Provisioning Services design. Although high availability may require additional resources and increased costs, it will provide a highly stable environment so that users experience minimal impact due to service outages.

Decision: Bootstrap Delivery

A target device initiates the boot process by first loading a bootstrap program which initializes the streaming session between the target device and the provisioning server. There are three methods in which the target device can receive the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

bootstrap program:

Using DHCP Options –

1. When the target device boots, the target device sends a broadcast for IP address and boot information. DHCP will process this request and provide an IP as well as scope option settings 66 (the name or IP address of the Provisioning Services TFTP server) and 67 (the name of the bootstrap file).

> **注意**
>
> If using a load balancer for the TFTP service then the address of the load balancer is entered in option 66.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server. The target device downloads the boot file from the provisioning server.

3. The target device boots the assigned vDisk image.

> **注意**
>
> Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP servers in order to receive PXE broadcasts.

Using PXE Broadcasts –

1. When a target device boots from the network, the target device sends a broadcast for an IP address and boot information. DHCP will process this request and provide an IP address. In addition, all provisioning servers that receive the broadcast will return boot server and boot file name information. The target device will merge the information received and start the boot process.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server which responded first. The target device downloads the boot file from the provisioning server.

> **注意**
>
> - Make sure no other PXE services are in use on the same subnet, such as the Altiris PXE service, or isolate using VLANs otherwise conflicts may occur with Provisioning Services.
> - Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP and PVS servers in order to receive PXE broadcasts.

Using Boot Device Manager – The Boot Device Manager (BDM) creates a boot file that target devices obtain through a physical CD/DVD, a mounted ISO image or as a virtual hard disk assigned to the target device. A BDM partition can be upgraded in one of three ways:

- By collection

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- By a group of highlighted devices
- By a single device

A summary of the advantages and disadvantages for each delivery method is listed in the following table:

Delivery Method	Advantages	Disadvantages
DHCP Options	Easy to implement	Requires changes to production DHCP service. DHCP service may only allow one option 66 entry. Requires UDP/DHCP helper for targets on different subnets.
PXE	Easy to implement	Can interfere with other running PXE services on the same subnet. Requires UDP/DHCP helper for targets on different subnets.
BDM ISO	Does not require PXE or TFTP services	Extra effort required to boot physical target devices. BDM ISO is regarded as a single point of failure if a single file is used.
BDM Partition	The BDM boot partition upgrade does not require PXE, TFTP, or TSB; it's considered a single stage bootloader, at boot time it automatically finds all relevant PVS server information and does not need external services provided by PXE, TFTP, or TSB.	An extra 8MB partition is created for each target device.

> **注意**
>
> When configuring the bootstrap file, up to four provisioning servers may be listed. The order in which the provisioning servers appear in the list determines the order which the provisioning servers are accessed. If the first server does not respond, the next server in the list is contacted.

Decision: vDisk Format

Provisioning Services supports the use of fixed-size or dynamic vDisks:

- **Fixed-size disk** – For vDisks in private mode, fixed-size prevents disk fragmentation, and offers improved write

© 1999-2017 Citrix Systems, Inc. All rights reserved.

performance over dynamic disks.

- **Dynamic disk** – Dynamic disks require less storage space than fixed-size disks, but offer significantly lower write performance. Although vDisks in Shared mode do not perform writes to the vDisk, the time required to complete vDisk merge operations will increase with dynamic disks. This is not a common occurrence as more environments choose to create new vDisks when updating.

Since most reads will be to the System Cache in RAM, there is no significant change in performance when utilizing fixed-size or dynamic disks. In addition, dynamic disks require significantly less storage space. Therefore, dynamic disks are recommended.

Decision: vDisk Replication

vDisks hosted on a local, Direct Attached Storage or a SAN must be replicated between vDisk stores whenever a vDisk is created or changed. Provisioning Services supports the replication of vDisks from stores that are local to the provisioning server as well as replication across multiple sites that use shared storage. The replication of vDisks can be performed manually or automatically:

- **Manual** – Manual replication is simple, but can be time consuming, depending on the number of vDisks and vDisk stores. If an error occurs during the replication process, administrators can catch them straight away and take the appropriate steps to resolve them. The risk of manual replication is vDisk inconsistency across the provisioning servers which will result in load balancing and failover to not work properly. For example, if a vDisk is replicated across three servers and then one of the vDisks is updated, that vDisk is no longer identical and will not be considered if a server failover occurs. Even if the same update is made to the other two vDisks, the timestamps on each will differ, and therefore the vDisks are no longer identical.
- **Automated** – For large environments, automated replication is faster than the manual method due to the number of vDisks and vDisk Stores required. Some automated tools, such as Microsoft DFS-R, support bandwidth throttling and Cross File Remote Differential Compression (CF-RDC), which use heuristics to determine whether destination files are similar to the file being replicated. If so, CF-RDC will use blocks from these files to minimize the amount of data transferred over the network. The risk of automated replication is that administrator do not typically monitor replication events in real-time and do not respond quickly when errors occur, unless the automation tool has an alerting feature. Some tools can be configured to automatically restart the copy process in the event of a failure. For example, Robocopy supports “resume copying” in the event that the network connection is interrupted.

For medium and large projects, use a tool to automate vDisk replication. Select a tool that is capable of resuming from network interruptions, copying file attributes and preserving the original timestamp.

> **注意**
>
> Load balancing and high availability will not work unless the vDisks have identical timestamps.

Decision: Server Sizing

Generally, a Provisioning Server is defined with the following specifications:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Specification
Model	Virtual
Processor	4 - 8 vCPU
Memory	2GB + (# of vDisks * 2GB)
Network	10 GBps NIC
Network	40 GB shared storage
vDisk Storage	Depending on number of images/revisions
Operating System	Windows Server 2012 R2

Model

Citrix Provisioning Services can be installed on virtual or physical servers:

- **Virtual** – Offers rapid server provisioning, snapshots for quick recovery or rollback scenarios and the ability to adjust server resources on the fly. Virtual provisioning servers allow target devices to be distributed across more servers helping to reduce the impact from server failure. Virtualization makes more efficient use of system resources.
- **Physical** – Offers higher levels of scalability per server than virtual servers. Physical provisioning servers mitigate the risks associated with virtual machines competing for underlying hypervisor resources.

  In general, virtual provisioning servers are preferred when sufficient processor, memory, disk and networking resources can be made available and guaranteed to be available.

> **注意**
>
> For high availability, ensure that virtual Provisioning Servers are distributed across multiple virtualization hosts. Distributing the virtual servers across multiple hosts will eliminate a single point of failure and not bring down the entire Provisioning Services farm in the event of a host failure.

CPU

Provisioning Services is not CPU intensive. However, under allocating the number of CPUs does impact the optimization of the network streams. The number of streams that a Provisioning Services server can run concurrently can be determined by the following formula:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

□□□ □□□□□□ □□ □□□□□□□ = # □□ □□□□□ ∗ # □□ □*h*□□□□/□□□□

By default, the Streaming Service is configured with 20 sequential network ports, and 8 threads per port. Therefore, by default, a provisioning server can support 160 concurrent targets. If more than 160 streams are required, Provisioning Services continuously switches between streaming different target devices

Ideally, if the environment needs to support more than 160 concurrent targets, the number of ports, and threads per port can be adjusted in the Provisioning Services console. Best performance is attained when the threads per port is not greater than the number of cores available on the provisioning server. If the provisioning server does not have sufficient cores, the server will show a higher CPU utilization, and target devices waiting for requests to be processed will have a higher read latency.

Even though Provisioning Services is not CPU intensive, allocating 2 CPUs will require a larger contiguous network port range.

- Small environments (up to approximately 500 virtual machines) 4 vCPUs are recommended.
- Larger environments 8 vCPUs are recommended.

RAM

The Windows operating system hosting Provisioning Services partially caches the vDisks in memory (system cache) reducing the number of reads required from storage. Reading from storage is significantly slower than reading from memory. Therefore, Provisioning Servers should be allocated sufficient memory to maximize the benefit from this caching process.

The following formula can be used to determine the optimal amount of memory that should be allocated to a provisioning server:

□□□□□ □□□□□□ □□□ = 2□□ + (# □□ □□□□□□ ∗ 2□□)

Network

Unlike most other XenApp and XenDesktop components, Provisioning Services does not bottleneck the CPU. Provisioning Services scalability is based on network throughput.

The following table shows the approximate amount of data that Provisioning Services requires to boot different operating systems:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Operating system	Avg Boot Data Usage (MB)
Windows 10 x64	240
Windows 8 x86	178
Windows 8 x64	227
Windows 7 x86	166
Windows 7 x64	210
Windows 2012	225
Windows 2012 R2	232
Windows 2008 R2	251
Windows Vista x86	190
Windows Vista x64	240

Determining how much time will be required to boot the target devices can be estimated using the following formula:

$$Seconds\ to\ Boot = \frac{(Number\ of\ Targets\ *\ MB\ Usage)}{\text{Network Throughput}}$$

Operating System	Number of VMs	Network Throughtput	Time to boot
Windows 10 x64	500	1 GBps	960 Seconds (16 minutes)
Windows 10 x64	500	10 GBps	96 Seconds (1 minute, 36 seconds)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A 10Gbps network is recommended for use with Provisioning Services. If a 10Gbps network is not available, consider link aggregation to provide additional bandwidth to the provisioning servers, or a dedicated physical streaming network.

> **ヒント**
>
> Firewalls can add latency and create bandwidth bottlenecks in Provisioning Services environments. If the use of firewalls cannot be avoided, refer to the Citrix whitepaper CTX101810 – Communication Ports Used By Citrix Technologies, for the list of ports that should be enabled for full functionality.

Growth

As the farm grows, administrators will need to decide whether to add more resources to the provisioning servers or to add more provisioning servers to the farm.

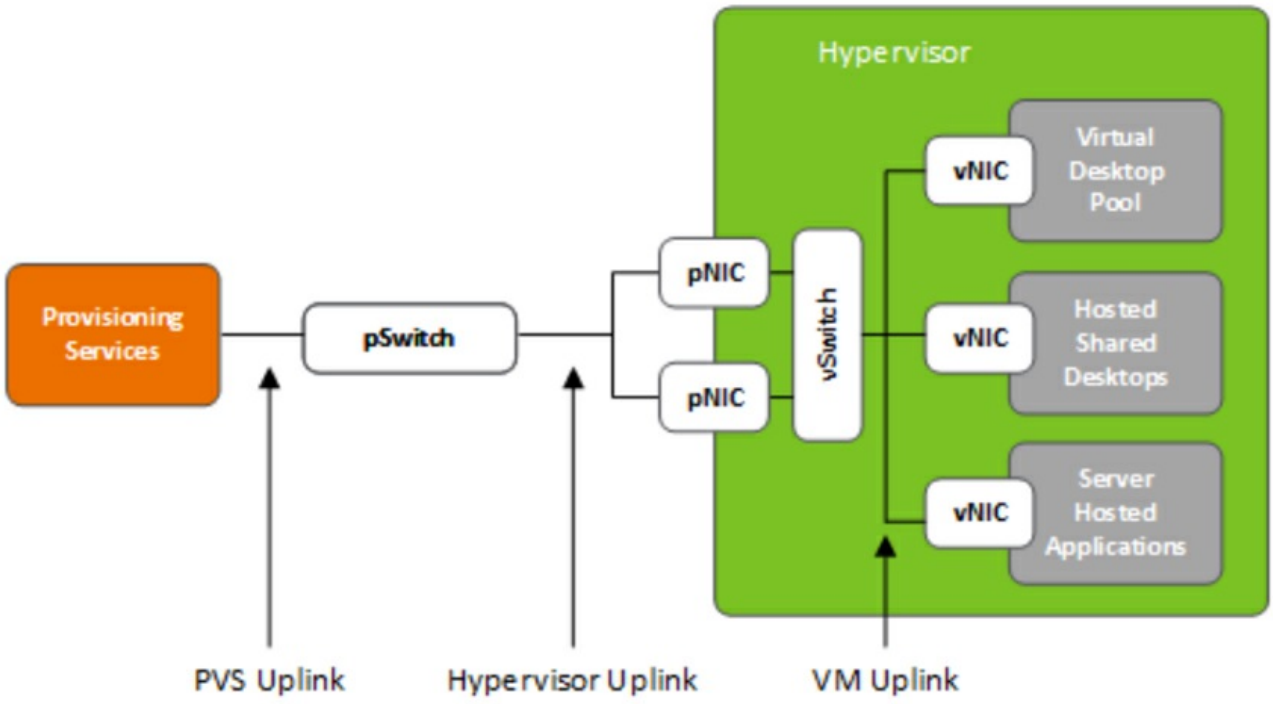
There are a number of environmental factors that need to be considered when determining whether the Provisioning Servers should be scaled up or scaled out:

- **Redundancy** – Spreading user load across additional less-powerful servers helps reduce the number of users affected from a single provisioning server failure. If the business is unable to accept the loss of a single high-specification server, consider scaling out.
- **Failover times** – The more target devices connected to a single provisioning server, the longer it will take for them to failover in the event that the server fails. Consider scaling out to reduce the time required for target devices to failover to another server.
- **Data center capacity** – The data center may have limited space, power and/or cooling available. In this situation, consider scaling up.
- **Hardware costs** – Initially, it may be more cost effective to scale up. However, there will be a point where scaling out actually becomes more cost effective. A cost analysis should be performed to make that determination.
- **Hosting costs** – There may be hosting and/or maintenance costs based on the number of physical servers used. If so, consider scaling up to reduce the long-term cost of these overheads.

Decision: Network Configuration

As mentioned before it is essential that the network is sized correctly to prevent network bottlenecks causing high disk access times and directly affecting virtual desktop performance. The following diagram outlines a common Provisioning Services network infrastructure:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



The following network configuration is recommended for the network sections outline within the diagram:

- **PVS Uplink** – All disk access from the target devices will be transferred via the PVS network uplink. This means hundreds or even thousands of devices will use this network connection. Therefore, it is vital that this connection is redundant and can failover without any downtime. Furthermore, Citrix recommends a minimum bandwidth of 1Gbps per 500 target devices. For virtual provisioning servers a respective QoS quota or a dedicated physical network uplink should be configured to ensure best performance.
- **Hypervisor Uplink** – Used by all PVS target devices hosted on a particular hypervisor host. Therefore, redundancy with transparent failover is strongly recommended. Unless the target devices run a very I/O intensive workload or perform I/O intensive tasks (e.g. booting) simultaneously, a bandwidth of 1Gbps is sufficient for this uplink.
- **VM Uplink** – All network traffic for a virtual machine, including PVS streaming traffic, will traverse this virtual network connection. Unless the workload is extremely I/O intensive a bandwidth of 100 Mbps is sufficient to handle even peak loads during I/O intensive tasks, such as booting from vDisk. For example, a Windows 2012 R2 Server will read approximately 232MB during a period of 90 seconds from the vDisk until the Windows Logon Screen is shown. During this period an average data rate of 20.5 Mbps with peaks up to 90 Mbps can be observed.

The following switch settings are recommended for Provisioning Services:

- **Disable Spanning Tree** or **Enable PortFast** – In a switching environment the Spanning Tree Protocol (STP) places ports into a blocked state while it transmits Bridged Protocol Data Units (BPDUs) and listens to ensure the BPDUs are not in a loopback configuration. The port is not placed in a forwarding state until the network converges, which depending on the size of the network, may incur enough time to cause Preboot Execution Environment (PXE) timeouts. To eliminate this issue, disable STP on edgeports connected to clients or enable PortFast.
- **Storm Control** - Storm Control is a feature available on Cisco switches that allows a threshold to be set whereby, multicast, broadcast, or unicast traffic may be suppressed. Its purpose is to prevent malicious or erroneous senders from flooding a LAN and affecting network performance. PVS Servers may send a large amount of traffic by design that falls within a storm control threshold, therefore the feature should be configured accordingly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Broadcast Helper** – The broadcast helper is required to direct broadcasts from clients to servers that would otherwise not be routed. In a PVS environment it is necessary to forward PXE boot requests when clients are not on the same subnet as the servers. If possible the recommended network design is to have PVS servers residing on the same subnet as the target devices. This mitigates the risk of any service degradation due to other networking infrastructure components.

The following network interface features should be taken into consideration when selecting a network interface for Provisioning Services:

- **TCP Offloading** – Offloading I/O tasks to the network interface reduces CPU usage and improves overall system performance, however, PVS Streaming Services can be negatively impacted when Large Send Offload is enabled due to the extra work placed on the network adapter. Many network adapters will have Large Send Offload and TCP checksum offload enabled by default.

> 注意
>
> If Large Send Offload is enabled and the switch that the traffic is passing through does not support the frame size sent by the Large Send Offload engine, the switch will drop the frame causing data retransmission. When retransmitting, the operating system will segment the frames instead of the network adapter, which can lead to severe performance degradation.

- **Receive Side Scaling (RSS)** – Receive side scaling enables packets received from a network adapter to be balanced across multiple CPUs which allows incoming TCP connections to be load balanced, preventing bottlenecks from occurring to a single CPU. In Windows Server 2008 R2 and Windows Server 2012/2012 R2, RSS is enabled by default.

> 注意
>
> For more information on PVS networking best practices please refer to Best Practices for Configuring Provisioning Services Server on a Network.
>
> For Provisioning Services implementations on low bandwidth networks (1Gbps or slower), performance may be improved by isolating streaming traffic from other network traffic on the LAN.
>
> Microsoft does not support NIC teaming with Hyper-V on Windows Server 2008 R2; however, third party solutions are available. Microsoft does support NIC teaming with Hyper-V on Windows Server 2012/2012 R2. All support queries regarding teaming with Hyper-V should be directed to the NIC OEM.

Decision: Subnet Affinity

The Provisioning Services Subnet Affinity is a load balancing algorithm that helps to ensure target devices are connected to the most appropriate provisioning server. When configuring subnet affinity, the following options are available:

- **None** – Ignore subnets; uses the least busy server.
- **Best Effort** – Uses the least busy server/NIC combination from within the same subnet. If no server/NIC combination is available within the subnet, select the least busy server from outside the subnet. If more than one server is available within the selected subnet, perform load balancing between those servers. This is the default setting.
- **Fixed** – Use the least busy server/NIC combination from within the same subnet. Perform load balancing between servers within that subnet. If no server/NIC combination exists in the same subnet, do not boot target devices assigned

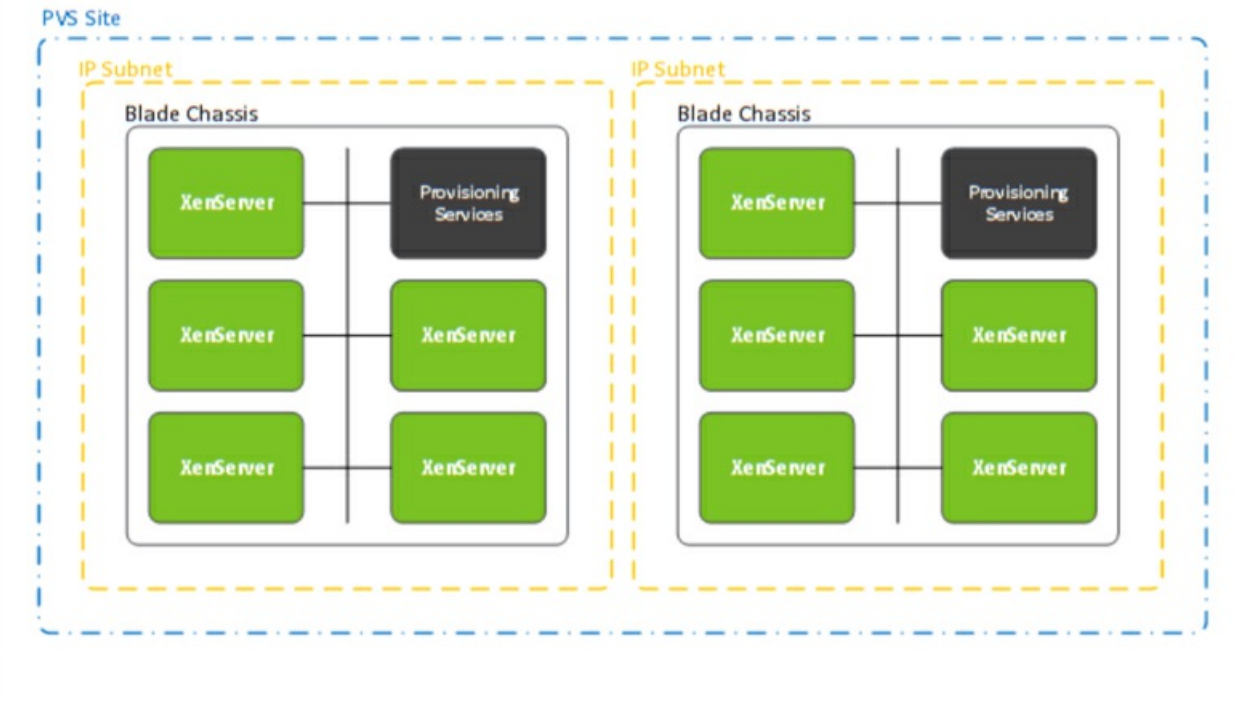
© 1999-2017 Citrix Systems, Inc. All rights reserved.

to this vDisk.

The following examples show common network configurations for physical provisioning servers. Similar configurations can be implemented for virtual provisioning servers without compromising on performance or functionality.

Blade Design

The provisioning servers and the target devices that they support reside within the same chassis. In most cases, the chassis will have a dedicated 10Gbps switch shared among all blade servers within the chassis.

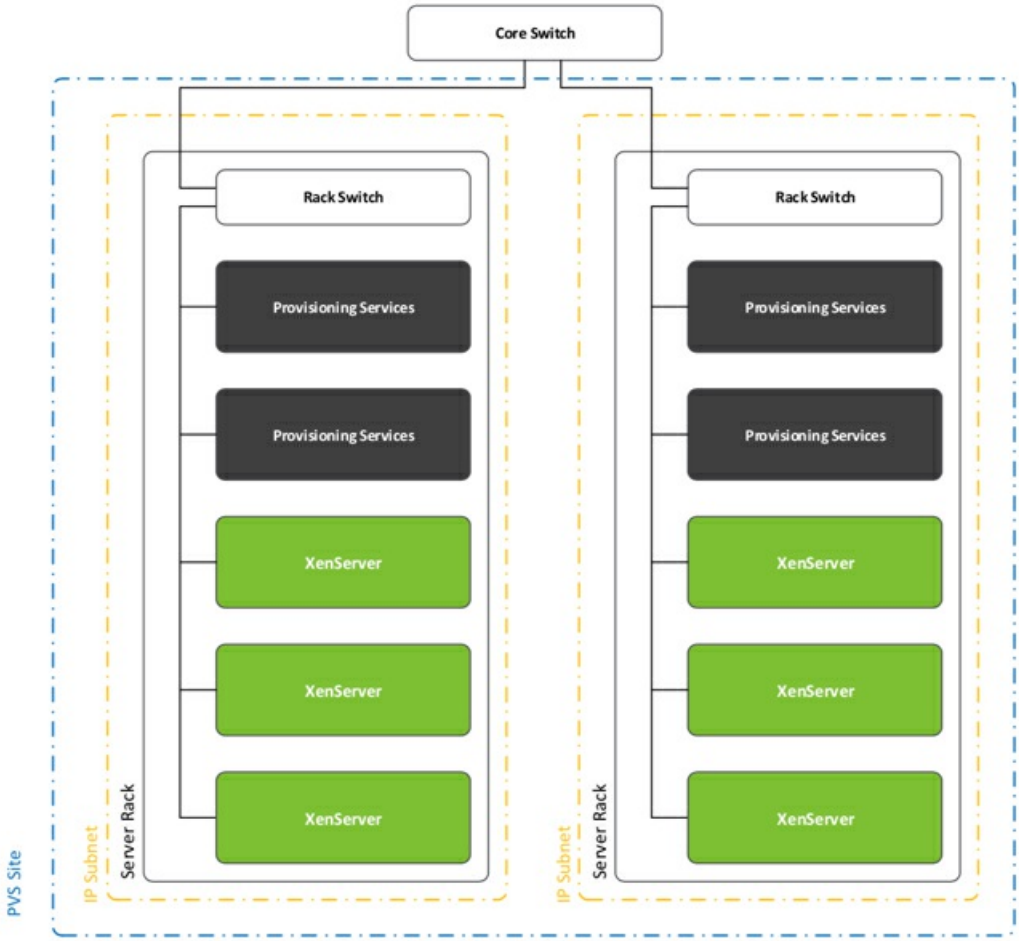


The “Best Effort” subnet affinity option is used to keep Provisioning Services traffic within the same chassis. Should the provisioning server become unavailable, the targets will failover to the second provisioning server in the second chassis, but same Provisioning Services site.

Rack Design

The second example is based on a rack design that uses rack switches to keep the provisioning traffic within the rack.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



As opposed to the blade chassis design, the subnet affinity feature is not used. Instead a Provisioning Services site with two provisioning servers will be configured per server rack. This will ensure that the target devices are streamed from provisioning servers within the same rack.

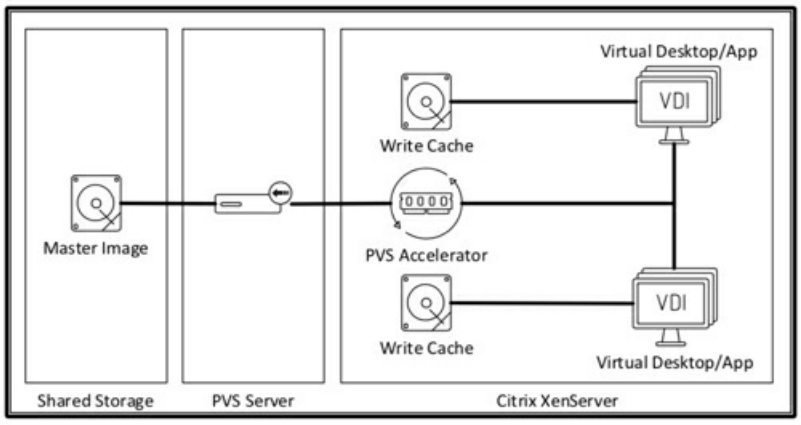
Experience from the Field

Manufacturing – A manufacturing company is designing a Provisioning Services solution to support five thousand virtual desktops. The company has concerns that Provisioning Services streaming traffic will create a bottleneck on the network affecting other applications. The company chose to build the environment on blade servers so that provisioning traffic is contained within the blade enclosure and will not impact other traffic on the network.

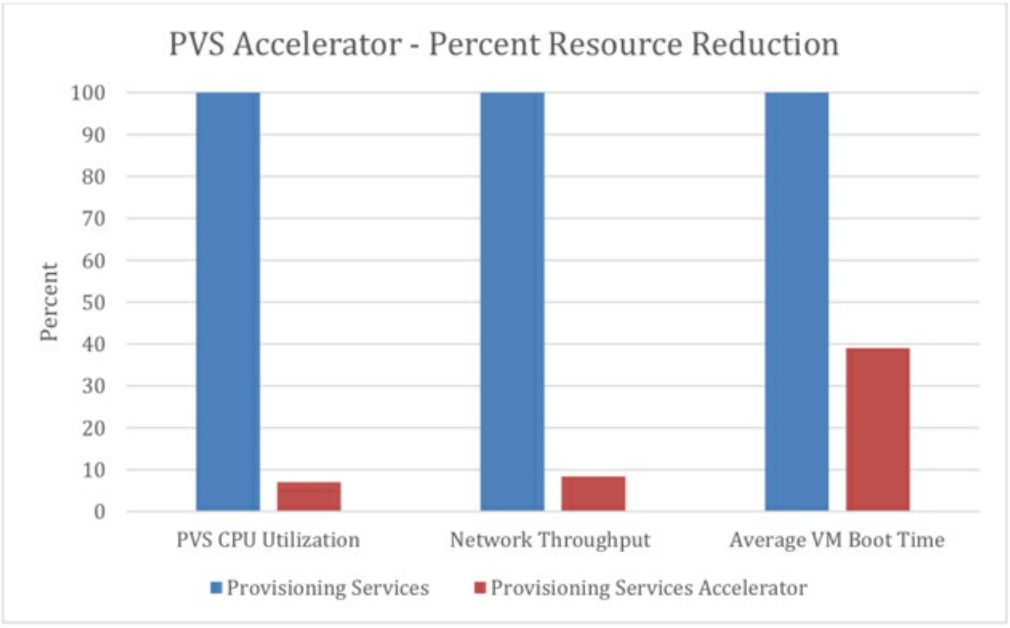
Decision: Read Cache

PVS Accelerator enables a PVS proxy to reside in the XenServer's Control Domain on a host where streaming of a Provisioning Services vDisk is cached at the proxy before being forwarded to the virtual machine. Using the cache, subsequent booting (or any I/O requests) of the virtual machine on the same host can be streamed from the proxy rather than streaming from the server over the network. PVS Accelerator requires more local resources on the XenServer host, but streaming from the server over the network saves resources, effectively improving performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Accelerator is a XenServer only capability. Utilizing this integrated technology reduces the load on the PVS server, reduces the overall network utilization and reduces the time it takes to boot a virtual machine.



For more information on the relationship among XenServer and Provisioning Services, see the blog XenServer and PVS: Better Together.

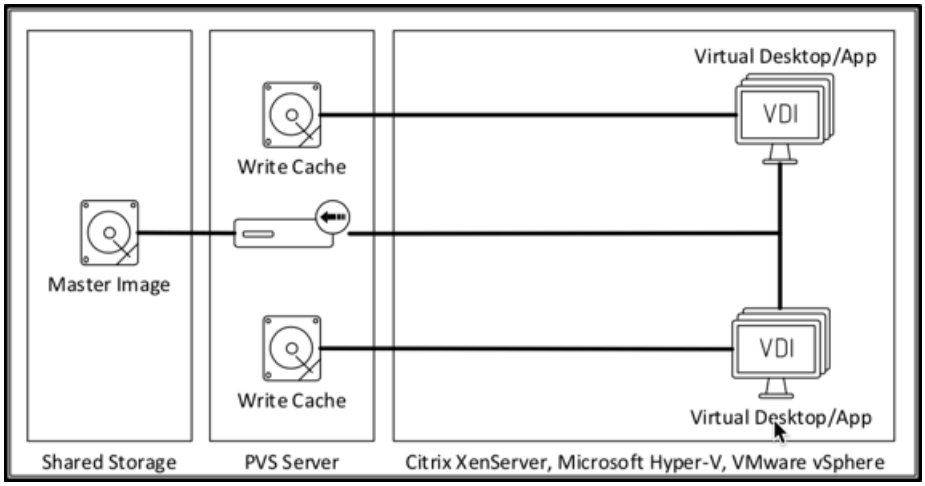
Decision: Write Cache

Because the master image is read-only, each virtual machine has a writable disk to store all changes. The administrator must decide where to store the write cache disk.

PVS Server – Local Storage

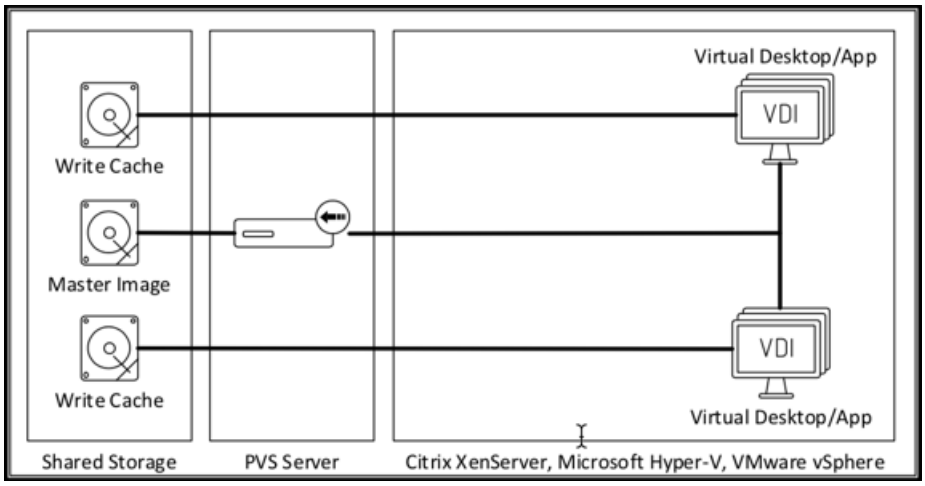
The Provisioning Services local storage holds the write cache drives for each target virtual machine. Although this is the default setting, it does increase network bandwidth requirements and increases the utilization of the Provisioning Services server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Server – Shared Storage

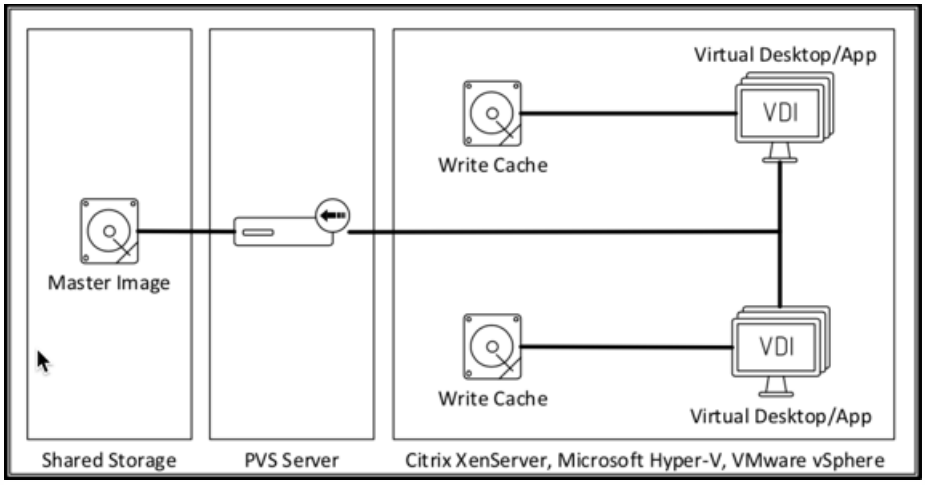
Shared storage associated with the Provisioning Services server holds the write cache drives for each target virtual machine. This option does increase network bandwidth requirements and increases the utilization of the Provisioning Services server. It also places temporary data (write cache) on expensive shared storage.



VM – Local Storage

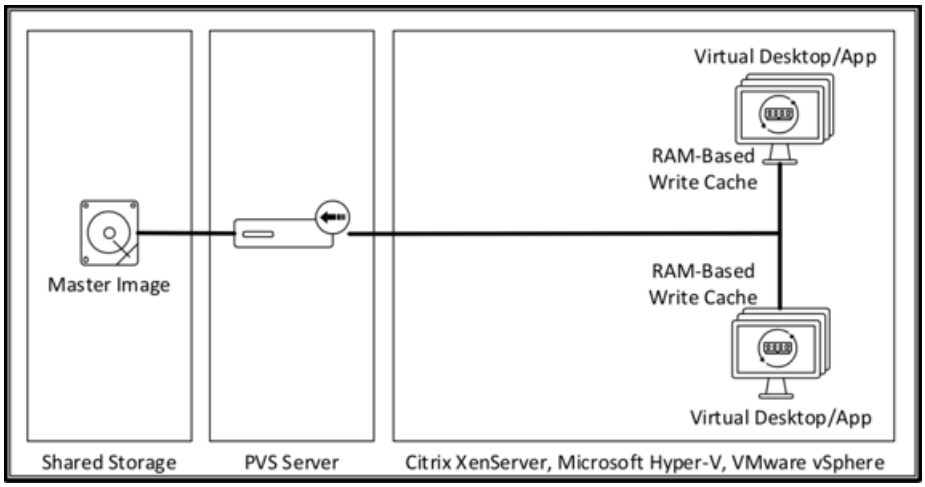
Local storage associated with the virtual machine holds the write cache drives for each target virtual machine. This option uses low cost local storage and does not consume additional resources on the Provisioning Services server. However, the local storage must be capable of support the IOPS of all virtual machines on the host.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



VM – Cache in RAM

RAM associated with the virtual machine holds the write cache drives for each target virtual machine. This option provides high performance due to the speed of RAM. However, if the RAM cache runs out of space, the virtual machine will become unusable. In order to use this option, significant amounts of RAM must be allocated to each virtual machine, increasing the overall cost.

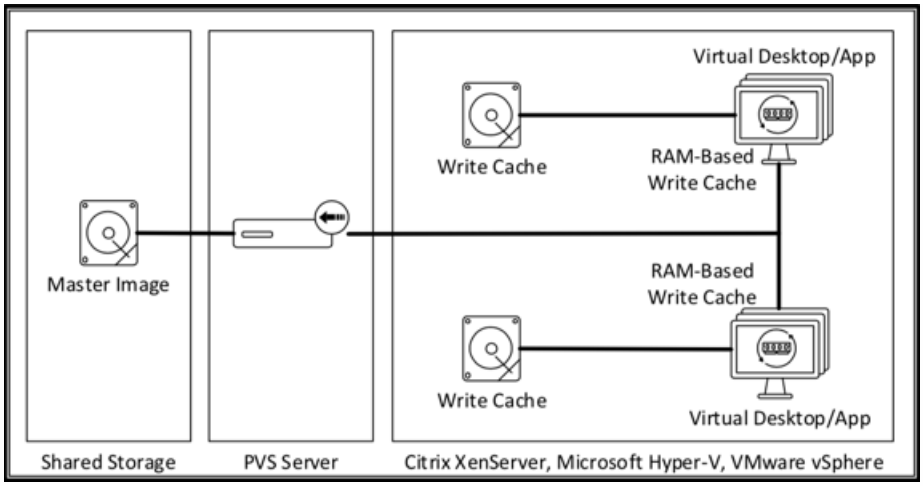


VM – Cache in RAM with Overflow to Disk

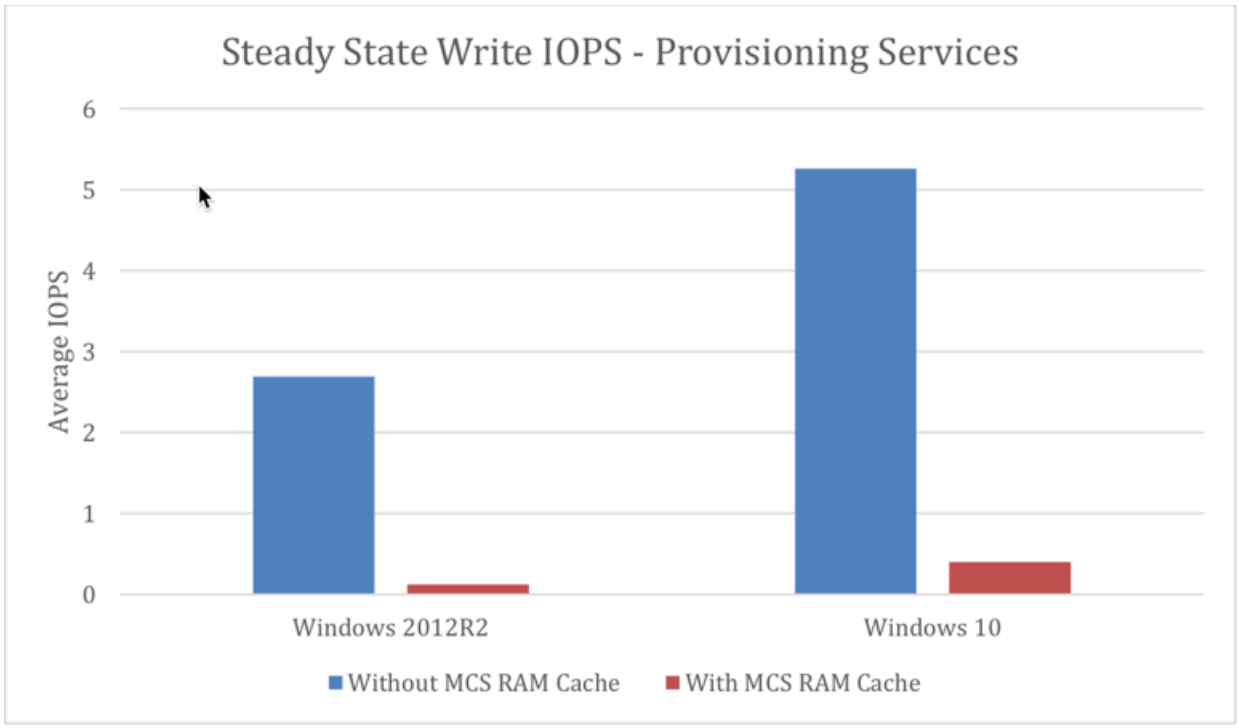
A combination of RAM and local storage is used for the write cache. First, writes are stored within the RAM cache, providing high performance. As the RAM cache is consumed, large blocks are removed from the RAM cache and placed onto the local storage write cache disk. This option provides high-levels of performance with the low cost of local storage.

Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cache in RAM with Overflow to Disk is the recommended option.



Decision: Antivirus

By default, most antivirus products scan all files and processes, which has a significant impact on Provisioning Services performance. For details on how antivirus software can be optimized for Provisioning Services, please refer to CTX124185 – Provisioning Services Antivirus Best Practices.

Antivirus software can cause file-locking issues on provisioning servers. The vDisk Store and write cache should be excluded from antivirus scans in order to prevent file contention issues.

When a virtual disk is running in standard mode and needs to be restarted, it downloads all of the previously loaded virus definitions. This can cause performance degradation when restarting several target devices at a time, often causing network congestion while the operation persists. In extreme cases, the target device and provisioning server can become

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sluggish and consume more resources than necessary. If the antivirus software supports it, definition files should be redirected to the write cache drive so that they are preserved between reboots.

Machine Creation Services

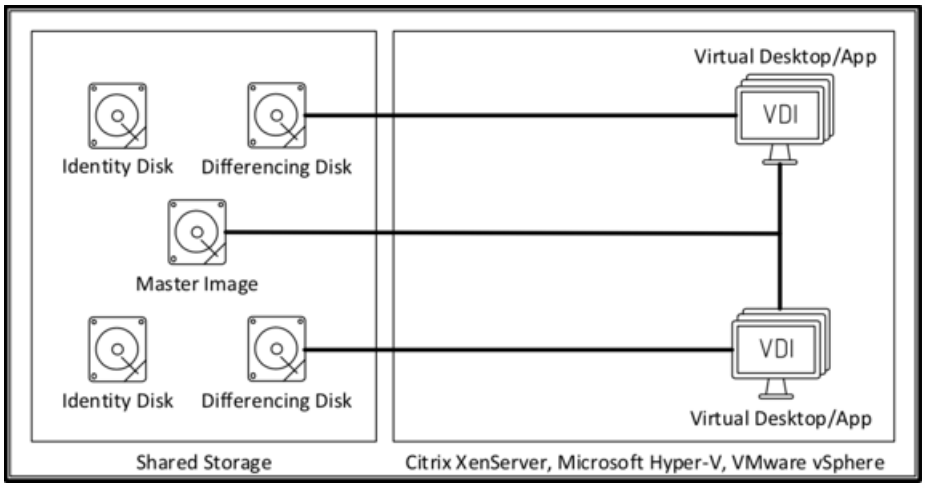
Machine Creation Services (MCS) uses disk-cloning technology to simplify the deployment of virtual machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can eliminate the need to manage and patch individual systems. Instead, administrators perform all image management on the master image.

Decision: Storage Location

Machine Creation Services allows administrators to break up a virtual desktop into multiple components and store those pieces on different storage arrays.

Shared Storage

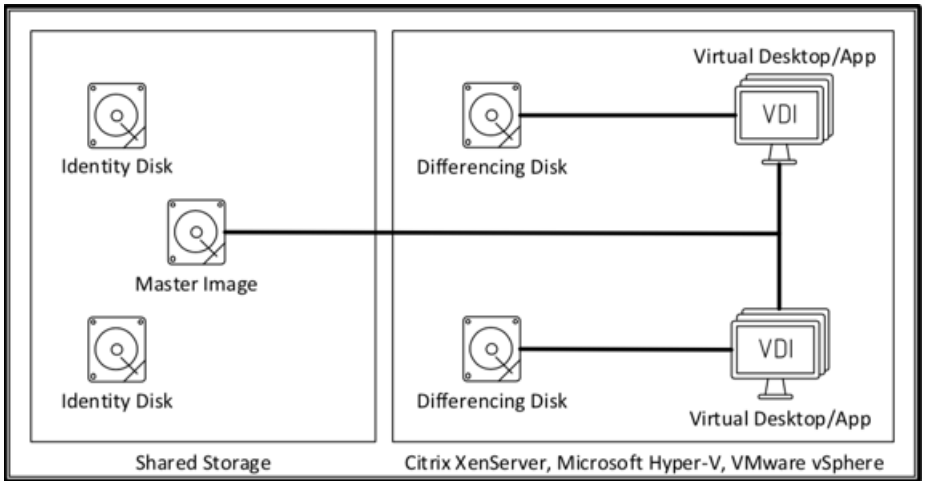
The first option utilizes shared storage for the operating system disk and the differencing disk.



Although this option allows the sharing of the master image across multiple hypervisor hosts, it puts more strain on the storage array because it must also host the differencing disk, which is temporary data.

Hybrid Storage

The second option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk.



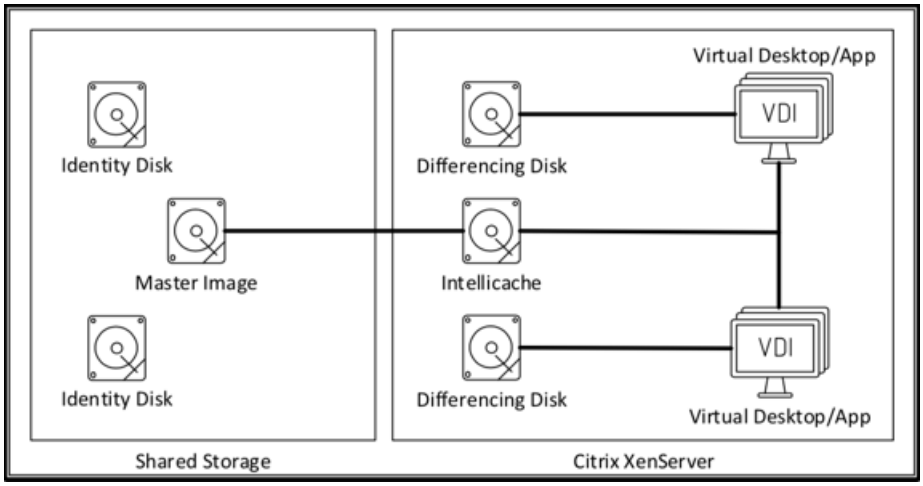
© 1999-2017 Citrix Systems, Inc. All rights reserved.

This is the most common option giving the administrator the benefits of sharing of the master image across multiple hypervisor hosts while offloading expensive, temporary write IOPS to cheap, local hypervisor storage.

XenServer IntelliCache Storage

The third option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk and local XenServer storage for a local cache of the operating system disk.

This is only an option for XenServer implementations. It provides the same value as the hybrid storage approach while also reducing read IOPS from shared storage. IntelliCache can coexist with the XenServer RAM-based read cache, if XenServer RAM is limited.



Decision: Cloning Type

Machine Creation Services incorporates two types of cloning techniques.

- **Thin** - Every VM within the catalog utilizes a single, read-only virtual disk for all reads. A second virtual disk, unique for each VM, captures all write IO activity.
- **Full** – Every VM within the catalog receives a full copy of the master disk image. Each VM fully owns the disk, allowing for read/write activity. Full cloning technology is only available for personal virtual desktops, where a dedicated virtual machine saves all changes to a local disk.

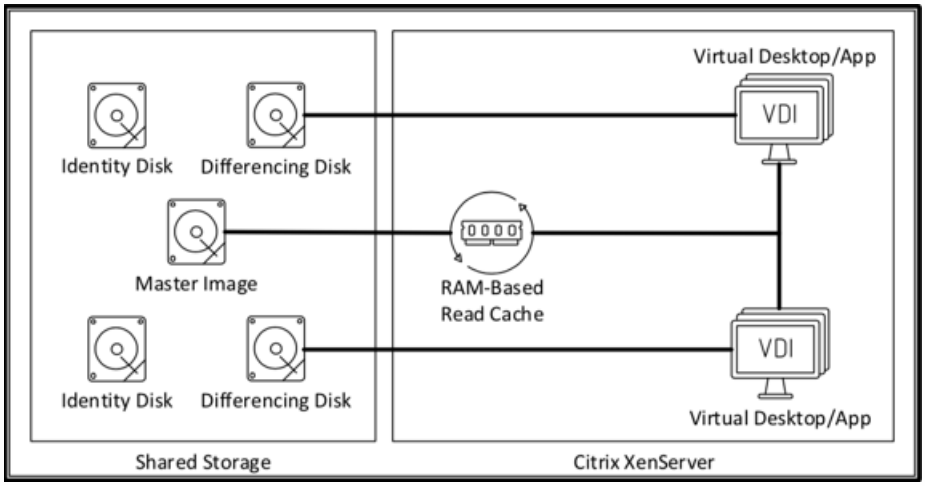
Administrators should consider the following when deciding between thin and full cloning technologies:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Thin Clone	Full Clone
Storage space requirements	Has greatest storage space savings. A single master disk image is shared across multiple VMs. Only the differencing disk (writes) consume space, which continues to grow until the VM reboots	High storage space requirements Each VM receives a full copy of the master image. The size continues to grow as changes are made to the VM.
Backup/Restore	Difficult Many 3rd party Backup/DR solutions do not support snapshot/delta disks, making thin provisioned VMs hard/impossible to backup or move to other storage arrays.	Easy The VM exists within a single virtual disk, making it easy to backup and restore.
Provisioning Speed	Fast Only requires a single disk image	Slow (can be mitigated) Each VM requires a full copy of the master image. Storage optimization technologies can help mitigate.
Performance	Slower A read I/O can occur twice, one for master disk and one for differencing disk, increasing read IOPS.	Faster All read/write direct to a single disk.
Boot Storm	High Impact In a boot storm, all differencing disks re- size to hold all writes from Windows start up; placing a high load on the storage as it happens all at once.	Low Impact

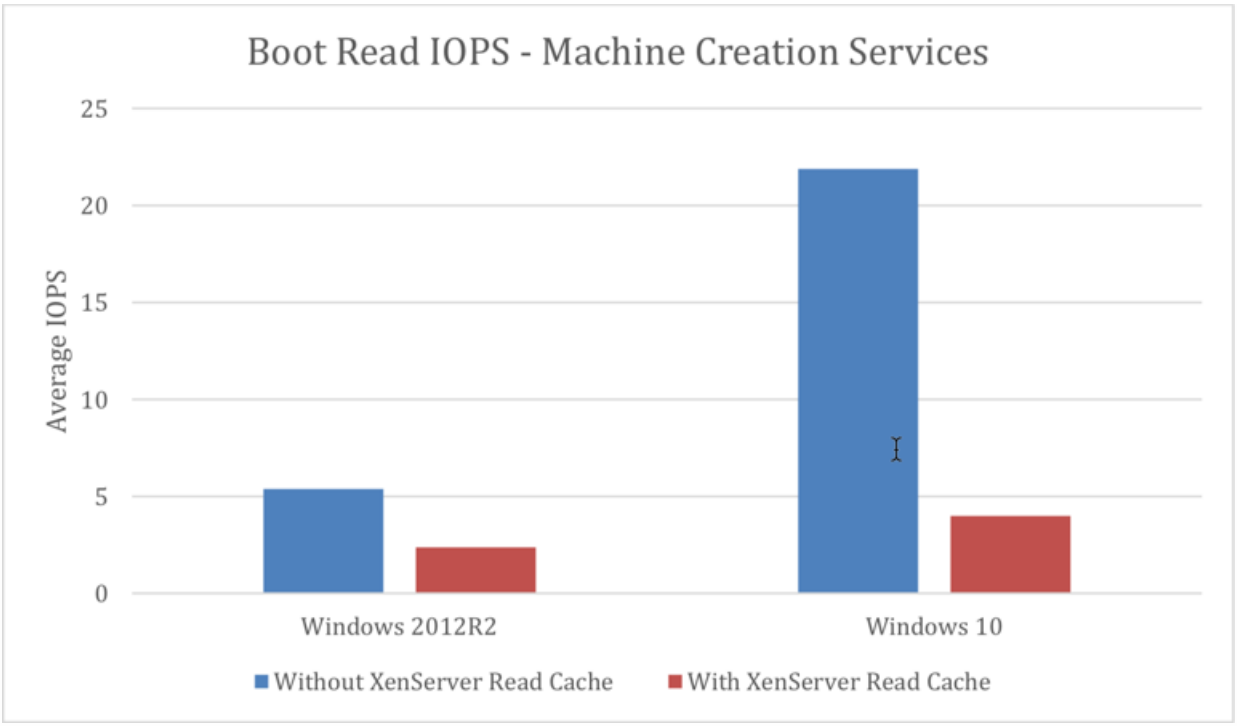
Decision: Read Cache

During boot and logon, virtual desktops incur high levels of storage read IOPS, which can put a strain on the underlying storage subsystem. When deployed on Citrix XenServer, Shared and Pooled VDI modes utilize a RAM-based read cache hosted on each XenServer.



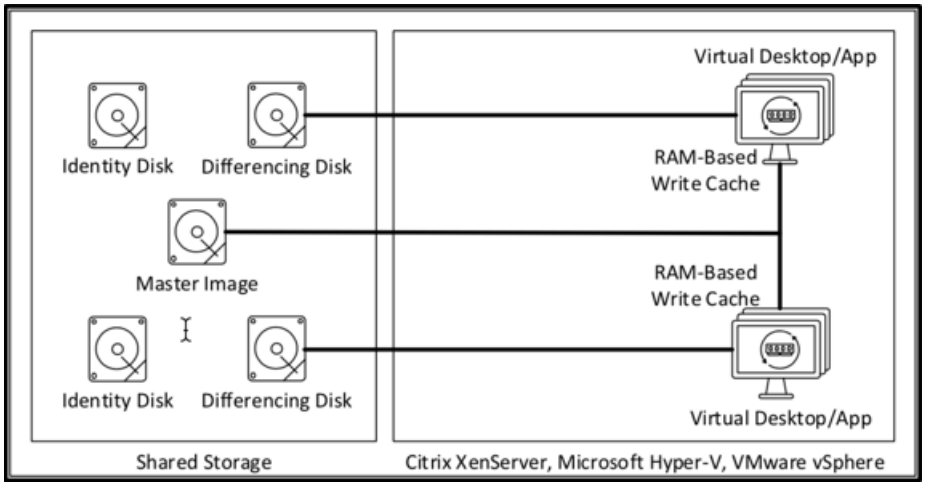
Utilizing this integrated technology reduces read IOPS by 50-80%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



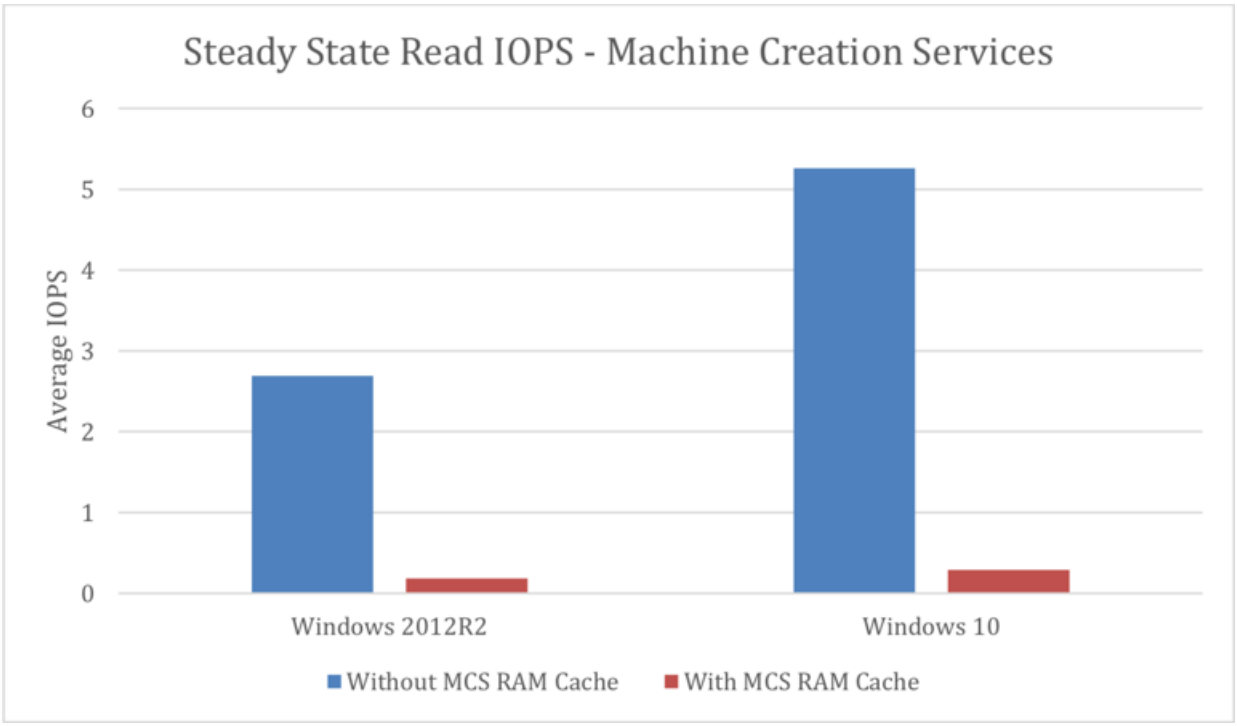
Decision: Write Cache

During steady state, virtual desktops incur high levels of storage write IOPS, which can put a strain on the underlying storage subsystem. Shared and Pooled VDI modes can utilize a RAMbased write cache by using non-paged pool RAM from the virtual machines operating system.



Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Security

Depending on the requirements of the organization, different security standards should be implemented within the solution. It is advisable refer to the following papers:

- Getting Started Guide for Security
- End-to-End Encryption
- System Hardening Guide
- Common Criteria
- Secure Browsing

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology hardware layer

May 07, 2018

This section covers hardware sizing for the virtual infrastructure servers, virtual desktops, and virtual application hosts. The sizing of these servers is typically done in two ways.

- The first and preferred way is to plan ahead and purchase hardware based on the workload requirements.
- The second way is to use existing hardware in the best configuration to support the different workload requirements.

This section will discuss decisions related to both methods.

Decision: Workload Separation

When implementing a XenApp and XenDesktop deployment, the workloads for the infrastructure, XenDesktop, and XenApp workloads can be separated into dedicated resource clusters or mixed on the same physical hosts. Citrix recommends using resource clusters to separate the workloads, especially in an enterprise deployment. This allows better host sizing as each workload has unique requirements such as overcommit ratios and memory usage.

In smaller environments where resource clusters are cost prohibitive, the workloads may be mixed in a manner which still allows for a highly available environment. Citrix leading practice is to separate the workloads however mixed workloads is a cost based business decision.
Decision: Physical Processor (pCPU)

The following table provides guidance on the number of virtual desktops that can be supported for light, medium and heavy workloads per physical core. Each desktop correlates to a single concurrent user, with the assumption that the operating system underwent optimization.

User Workload	Operating System	Users per Physical Core
Light	Windows 7	13
	Windows 8	12
	Windows 10	12
	Windows 2008R2	18
	Windows 2012R2	21
	Windows 2016	21
Medium	Windows 7	10
	Windows 8	9

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 10	9
	Windows 2008R2	12
	Windows 2012R2	14
	Windows 2016	14
Heavy	Windows 7	5
	Windows 8	4
	Windows 10	4
	Windows 2008R2	6
	Windows 2012R2	7
	Windows 2016	7

The estimate for "Users per Physical Core" is a baseline number running Microsoft Office 2010. The baseline number must be adjusted based on specific infrastructure requirements. As a general guideline, the following characteristics are baseline changes to server density.

Characteristic	Server Density Impact
Antivirus (not optimized)	25% decrease
Real-time Monitoring	15% decrease
Office 2013	20% decrease
Office 2016	25% decrease
Hyper-threading	20% increase

© 1999-2017 Citrix Systems, Inc. All rights reserved.

To estimate the total number of physical cores required for the XenApp and XenDesktop workload, use the following formula for each user group:

$$\text{Total XenDesktop pCPU} = \sum Usersi \,/ UsersPerCorei * (1 + (AV + Mon + Off13 + Off16 - HV))$$

$$\text{Total XenApp pCPU} = \sum Usersi \,/ UsersPerCoreii * (1 + (AV + Mon + Off13 + Off16 - HV))$$

∑ represents the sum of all user group combinations “i”.

Usersi = Number of concurrent users per user groups

UsersPerCorei = Number of users per physical core

AV = Antivirus impact (default = 0.25)

Mon = Monitoring tools impact (default = 0.15)

Off13 = Office 2013 impact (default = .2)

Off16 = Office 2016 impact (default = .25)

HT = Hyper-Threading impact (default = .2)

If workloads will be separated (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users in order

Decision: Physical Memory (pRAM)

The recommended method for sizing memory to a physical host is to size based on the total memory required to support the virtual machines and the CPU capacity of the host. In order to calculate the total memory required for XenApp and XenDesktop, simply multiply the number of virtual machines by the amount of memory allocated to the virtual machines. The sum of all of the machine catalogs will be the total RAM required for XenApp and XenDesktop hosts. This is shown in the formula below.

$$Total\ XenDesktop\ pRAM = \sum_i VM_i * vRAM_i$$

$$Total\ XenApp\ pRAM = \sum_i VM_i * vRAM_i$$

∑ represents the sum of all user group combinations “i”.

VMi = Number of concurrent users per user groups

vRAMi = Amount of RAM assigned to each virtual machine

If workloads will be separated onto different hosts (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Physical Host (pHost)

In most situations, the number of physical hosts (pHost) to support the XenApp and XenDesktop workloads will be limited on the number of processor cores available. The following formula provides an estimate for the number of hosts required for the user workloads. The formula is based on the best practice of separating the XenApp and XenDesktop workloads due to the different recommended CPU overcommit ratios for each.

[illegible] = ([illegible] [illegible] [illegible]/ [illegible] [illegible] [illegible] +1)

[illegible] = ([illegible] [illegible] [illegible]/ [illegible] [illegible] [illegible]+ 1)

Once the number of physical hosts has been determined based on processor cores, the amount of RAM for each host is calculated.

[illegible] [illegible] [illegible] [illegible] = [illegible] + ([illegible] [illegible] [illegible] /[illegible] [illegible] – 1)

[illegible] [illegible] [illegible] [illegible] = [illegible] + ([illegible] [illegible] [illegible]/[illegible] [illegible] – 1)

Decision: GPU

Hosts used to deliver graphical workloads require graphics processors to deliver a high end user experience. Specific hardware hosts and graphics cards are required to support high end graphics using HDX 3D Pro. An updated list of tested hardware is available in a knowledge base article. Sizing of the desktop and application hosts of high end graphics users should be based on the GPU requirements ensuring that the host then has adequate CPU and memory resource to support the workload.

NVIDIA GRID cards can be leveraged with vGPU profiles to support multiple users. Sizing guidelines are provided from NVIDIA in the table below.

In the table, **Y** indicates that application certificates are available.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NVIDIA GRID Graphics Board	Virtual GPU Profile	Application Certifications	Graphics Memory	Max Displays Per User	Max Resolution Per Display	Max vGPU Per Graphics Board	Use Case
GRID K2	K280Q	Y	4,096 MB	4	2560 x 1600	2	Designer
	K260Q	Y	2,048 MB	4	2560 X 1600	4	Designer / Power User
	K240Q	Y	1,024 MB	2	2560 x 1600	8	Designer / Power User
	K220Q	Y	512 MB	2	2560 x 1600	16	Knowledge Worker
	K200		256 MB	2	1900 x 1200	16	Power User
GRID K1	K180Q	Y	4,096 MB	4	2560 x 1600	4	Power User
	K160Q	Y	2,048 MB	4	2560 x 1600	8	Power User
	K140Q	Y	1,024 MB	2	2560 x 1600	16	Power User
	K120Q	Y	512 MB	2	2560 x 1600	32	Power User
	K100		256 MB	2	1900 x 1200	32	Knowledge Worker

Storage Sizing

Decision: Storage Architecture

The primary storage architectures are as follows:

- **Local Storage** - Uses hard disks directly attached to the computer system. The disks cannot be shared with other computer systems, but if the computer is hosting pooled or hosted shared desktops, a shared storage solution is not necessary. In many cases local storage can perform as well as shared storage. Scalability is limited to the number of drive bays available in the computer system. Many blade servers for example have just two drive bays, so using local storage to support a XenDesktop deployment may not be optimal.
- **DAS** - Storage sub-system directly attached to a server or workstation using a cable. It uses block-level storage and can be a hard disk local to the computer system or a disk shelf with multiple disks attached by means of external cabling. Unlike local disks, disk shelves require separate management. Storage shelves can be connected to multiple servers so the data or disks can be shared.
- **NAS** - Provides file-level storage to computer systems through network file shares. The NAS operates as a file server, and

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NAS systems are networked appliances which contain one or more hard drives, often arranged into logical, redundant storage containers or RAID arrays. Access is typically provided using standard Ethernet and network file sharing protocols such as NFS, SMB/CIFS, or AFP.

> **注意**
>
> NAS can become a single point of failure. If the network share becomes unavailable, all target devices streamed from the disk will be unavailable as well.

- **SAN** - Dedicated storage network that provides access to consolidated, block-level storage. SANs allow computers to connect to different storage devices, so no server has ownership of the storage subsystem enabling data to be shared among multiple computers. A SAN will typically have its own dedicated network of storage devices that are generally not accessible through the network by standard means. In order to connect a device to the SAN network a specialized adapter called the Host Bus Adapter (HBA) is required. SANs are highly scalable with no noticeable change in performance as more storage and devices are connected. SANs can be a costly investment both in terms of capital and the time required to learn, deploy and manage the technology.
- **Hybrid** - A NAS head refers to a NAS which does not have any on-board storage, but instead connects to a SAN. In effect, it acts as a translator between the file-level NAS protocols (NFS, CIFS, etc.) and the block-level SAN protocols (Fibre Channel and iSCSI). Thus it can combine the advantages of both technologies and allows computers without Host Bus Adapters (HBA) to connect to centralized storage.

The following table summarizes the storage options available and rates their suitability for XenDesktop deployments.

Storage Properties	Local	DAS	NAS	SAN
Implementation costs	Low	Medium	Medium	High
Administration	Low	Medium	Medium	High
Performance	High	Med - High	Med - High	High
Redundancy	Low - Med	Med - High	Med - High	High
Scalability	Low	Med - High	Med - High	High
Typical use case	Small to medium production and test environments	Small to medium production environments	Small to medium production environments	Medium to large production environments

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> Hyper-V 2008 R2 does not support NAS technology. Hyper-V 2012/2012 R2 only supports NAS solutions that support the SMB 3.0 protocol. For more information please refer to the HyperV 2008 R2 and Hyper-V 2012 R2 sections of the handbook.

Local storage is best suited for storing virtual machines which do not have high availability requirements or persistent data attached such as random (pooled) desktops or hosted shared desktops. Local and DAS is suited for storing user data and home directory files. If using Machine Creation Services, master images as well as any updates must be replicated to each server.

NAS and SAN storage is best suited for infrastructure servers supporting the XenDesktop environment, and virtual machines with persistent data such as static (dedicated) desktops.

Decision: RAID Level

To choose the optimal RAID level, it is necessary to consider the IOPS and read/write ratio generated by a given application or workload in combination with the individual capabilities of a RAID level. For hosting read intensive workloads, such as the Provisioning Services vDisk store, RAID levels that are optimized for read operations such as RAID 1, 5, 6, 10 are optimal. This is because these RAID levels allow read operations to be spread across all disks within the RAID set simultaneously.

For hosting write intensive workloads, such as Provisioning Services write cache and Machine Creation Services differencing disks, RAID levels such as RAID 1 or 10 are optimal, as these are optimized for writes and have a low write penalty.

The following table outlines the key quantitative attributes of the most commonly used RAID levels:

RAID	Capacity (%)	Fault Tolerance	Read Performance	Write Performance	Minimum number of disks
0	100	None	Very High	High (Write Penalty 1)	2
1	50	Single-drive failure	Very High	Medium (Write Penalty 2)	2
5	67 - 94	Single-drive failure	High	Low (Write Penalty 4)	3
6	50 - 88	Dual-drive failure	High	Low (Write Penalty 6)	4
10	50	Single-drive failure in each sub array	Very High	Medium (Write Penalty 2)	4

> **注意**
>
> The write penalty is inherent in RAID data protection techniques, which require multiple disk I/O requests for each application write request, and ranges from minimal (mirrored arrays) to substantial (RAID levels 5 and 6).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Number of Disks

To determine the number of disks required it is important to understand the performance characteristics of each disk, the characteristics of the RAID level and the performance requirements of the given workload. The basic calculation for determining the total number of disks needed is:

[illegible] # [illegible] =
([illegible] [illegible] [illegible] + ([illegible] [illegible] [illegible] ∗ [illegible] [illegible]))/[illegible] [illegible] [illegible]

For example, a disk manufacturer is reporting that a particular disk array which they have developed has a total workload IOPS of 2000. The raw IOPS per disk is 175. To determine how many disks are required to support a workload with 20% read operations and 80% write operations on RAID 10:

[illegible] # [illegible] =((20% ∗ 2000) + (80% ∗ 2000) ∗ 2) /175= 20.57 [illegible] 21 [illegible]

Based on the previous example, the following table shows how the disk count will vary based on the RAID level and the read/write ratio.

RAID	RAW IOPS (per disk)	Workload IOPS	Read %	Write %	Disk Count
0	175	2000	20	80	12
	175	2000	80	20	12
1 / 10	175	2000	20	80	21
	175	2000	80	20	14
5	175	2000	20	80	39
	175	2000	80	20	19

Decision: Disk Type

Hard disk drives (HDDs) are the traditional variation of disk drives. These kinds of disks consist of rotating platters on a motor-driven spindle within a protective enclosure. The data is magnetically written to and read from the platter by read/write heads.

Different implementations of this technology are available on the market, which differ in terms of performance, cost and reliability.

- Serial ATA (SATA) disk transmit data serially over two pairs of conductors. One pair is for differential transmission of data,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

and the other pair is for differential receiving of data. SATA drives are widely found in consumer desktop and laptop computers. Typical SATA drives have transfer speeds ranging from 1500 – 6000Mbps and support hot-swapping by design.

- Small Computer Systems Interface (SCSI) disks use a buffered, peer to peer interface that uses handshake signals between devices. Many SCSI devices require a SCSI initiator to initiate SCSI transactions between the host and SCSI target. SCSI disks are common in workstations and servers and have throughputs ranging from 40 – 5120Mbps. iSCSI (Internet Small Computer System Interface) is a mapping of the regular SCSI protocol over TCP/IP, more commonly over Gigabit Ethernet.
- Fibre Channel (FC) disk is the successor to the parallel SCSI disk and is common in SAN storage devices. Fibre Channel signals can run on an electrical interface or fibre-optic cables. Throughput can range from 1 – 20Gbps, and connections are hot-pluggable.
- Serial Attached SCSI (SAS) disk uses a new generation serial communication protocol to allow for higher speed data transfers than SATA disks. Throughput can range from 2400 – 9600Mbps.

In contrast to traditional hard disks, Solid State Disks (SSDs) use microchips to retain data in either NAND non-volatile memory chips (flash) or DRAM and contain no moving parts. SSDs are less susceptible to physical shock, have lower access times and latency and have higher I/O rates. SSDs have significantly higher random read performance. An SSD drive can attain anywhere from 5,000 to 20,000 random reads per second. SSDs are also more expensive per gigabyte (GB) and typically support a limited number of writes over the life of the disk.

Flash memory-based SSDs can be either based on multi-level cells (MLC) or single-level cells (SLC). SLC devices only store one bit of information in each cell. MLC devices can store multiple bits of information with each cell. Flash based SSDs cost lower than DRAM based SSDs but perform slower. DRAM based SSD devices are used primarily to accelerate applications that would otherwise be held back by the latency of flash SSDs or traditional HDDs.

SSDs were previously not viable for enterprise storage solutions because of the high cost, low capacity and fast wear of the drives. Improvements in SSD technology and lowering costs are making them more favorable over HDDs. Solid state hybrid drives (SSHD) combine the features of SSDs and HDDs, by containing a large HDD drive with an SSD cache to improve performance of frequently accessed data.

Comparing SSDs and HDDs is difficult since HDD benchmarks are focused on finding the performance aspects such as rotational latency time and seek time. As SSDs do not spin, or seek, they may show huge superiority in such tests. However, SSDs have challenges with mixed reads and writes and their performance may degrade over time.

The following table compares the transfer rates of some of the more common storage types available on the market today.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Technology	Rate (MBps)
iSCI over Fast Ethernet	100
Ultra-2 wide SCSI (16 bits/40 MHz)	640
iSCI over Gigabit Ethernet	1,000
SATA rev 3	6,000
SAS 3	9,600
FCoE over 10 GbE	10,000
SATA rev 3.2 - SATA Express	16,000
iSCI over Infiniband	32,000

SCSI and SATA disks are best suited for storing data that does not have high performance requirements like the PVS vDisk store. SAS, Fibre Channel, or SSD drives are best suited for storing data that have high performance requirements like the PVS write cache.

Decision: Storage Bandwidth

Storage bandwidth is the connectivity between servers and the storage subsystem. Understanding bandwidth requirements can help determine the proper hardware for delivering data and applications at speeds for a positive end user experience. For most datacenters 10Gbps Ethernet or 10Gbps FCoE is sufficient for storage connections. Smaller environments however may only need 1Gbps bandwidth. In virtualized environments it is not just important to look at the bandwidth requirements of the physical host and storage subsystem, but determining how much bandwidth is required for each virtual machine plays a factor too.

In order to plan for the required bandwidth, it is necessary to determine the throughputs for every individual system that uses a shared component or network path. For example, the following information is provided for an environment with 100 similar virtual machines (hosted on 10 virtualization hosts and connected to one NAS head).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Average	Peak
Throughput per VM	10 MBps	30 MBps
Throughput per host	100 MBps (10 VMs x 10 MBps)	300 MBps (10VMs x 30 MBps)
Throughput per storage	1 GBps (10 hosts x 100 MBps)	3 GBps (10 hosts x 300 MBps)

The NIC used for storage communication needs to be a 1Gbps adapter in order to handle the peak load. The NAS head as well as its network connection need to support 3Gbps worth of data traffic in order to support the peak load of all systems.

Decision: Tiered Storage

A one-size-fits-all storage solution is unlikely to meet the requirements of most virtual desktop implementations. The use of storage tiers provides an effective mechanism for offering a range of different storage options differentiated by performance, scalability, redundancy and cost. In this way, different virtual workloads with similar storage requirements can be grouped together and a similar cost model applied.

For example, a XenDesktop implementation using tiered storage may look like the following:

- **Tier 1 storage group** - Write intensive files such as the write cache and differencing disks are placed in a storage group consisting of SSDs.
- **Tier 2 storage group** - Mission critical data, or data that requires high availability, are placed in a storage group consisting of less expensive high performing drives.
- **Tier 3 storage group** - Seldom used data files, read-only files, or other non-mission critical data placed in a storage group consisting of low cost and lower performing drives.

Decision: Thin Provisioning

Thin provisioning allows more storage space to be presented to the virtual machines than is actually available on the storage repository. This lowers storage costs by allowing virtual machines access to disk space that is often unused. This is particularly beneficial to Machine Creation Services which uses a linked-clone approach to provisioning virtual machines. Thin provisioning minimizes the storage space required for the master image copies used to build virtual machines. Thin provisioning is possible at the physical storage layer, a feature usually available with most SAN solutions, and at the virtual layer. NFS based storage solutions will usually have thin provisioning enabled by default.

At the physical storage layer, it is important to ensure that sufficient storage is available to prevent the risk of virtual machines not being available in a storage “overcommit” scenario when available disk space is exhausted. Organizations should decide if the cost savings thin provisioning provides outweighs the associated risk and consider enabling if the storage solution supports it.

> **注意**
>
> Virtual machines may not function if disk space is exhausted so it is important to have a process in place, either through alerts or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

notifications that will give administrators enough time to add more disks to the storage solution so that the XenDesktop environment is not impacted.

Decision: Data De-Duplication

Data de-duplication is a data compression technique whereby duplicate data is replaced with pointers to a single copy of the original item. This reduces storage requirements and costs by improving storage utilization, however it can impact storage performance.

There are two implementations of de-duplication available:

- **Post-process de-duplication** – The de-duplication is performed after the data has been written to disk. Post-process de-duplication should be scheduled outside business hours to ensure that it does not impact system performance. Post Process de-duplication offers minimal advantages for random desktops as the write-cache/difference disk is typically reset on a daily basis.
- **In-line de-duplication** – Examines data before it is written to disk so that duplicate blocks are not stored. The additional checks performed before the data is written to disk can sometimes cause slow performance. If enabled, in-line duplication should be carefully monitored to ensure that it is not affecting the performance of the XenDesktop environment.

If the storage solution supports it, enabling post-process data de-duplication is recommended for minimal impact to XenDesktop performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Monitor

Jan 29, 2018

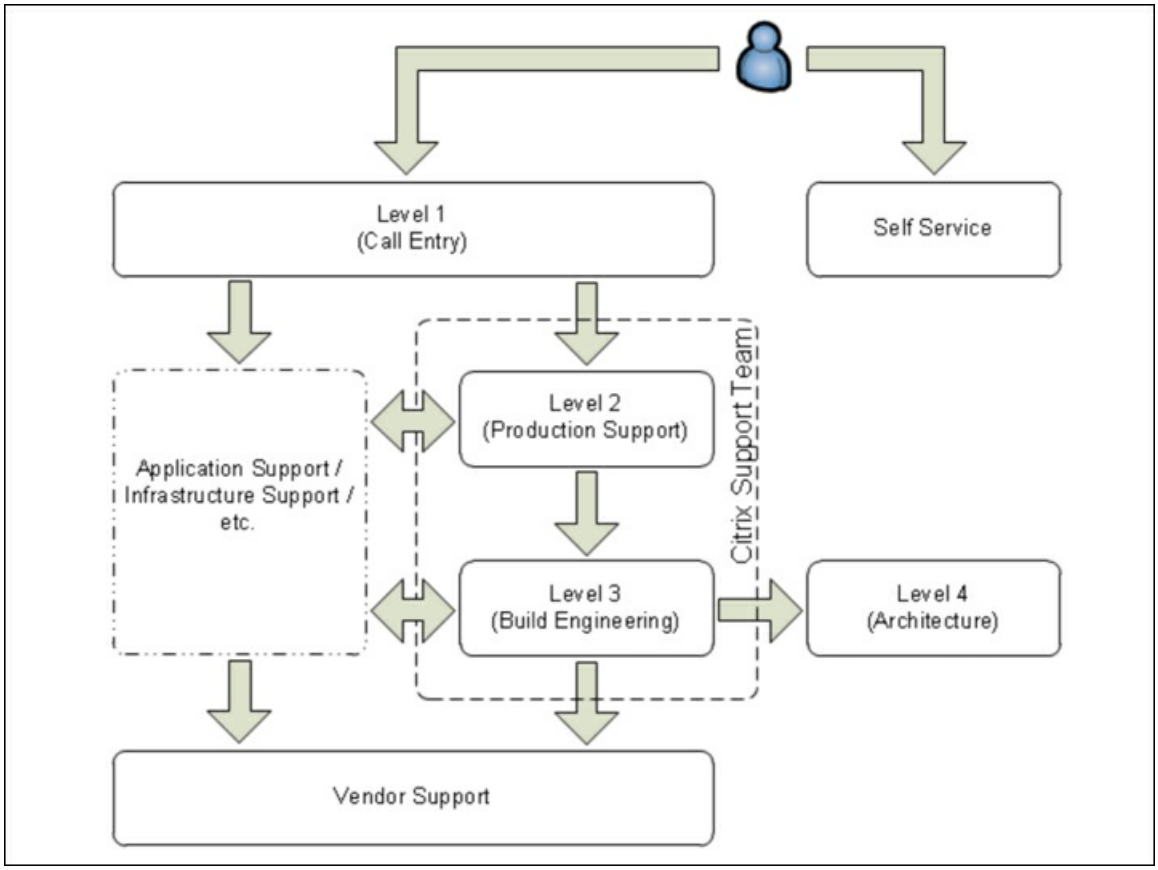
Like any integrated system, monitoring and maintenance is critical to the overall health of the solution. Without proper support, operations and health monitoring systems in place, the user experience will slowly start to degrade.

Process 1: Support

When problems arise, technical support is the first point of contact. This section addresses the proper staffing, organization, training, delegated administration and tools that should be used to maintain the Citrix deployment.

Decision: Support Structure

Multiple levels of support have been found to be the most effective ways of addressing support issues. Low criticality, low complexity or frequently occurring issues should be managed and resolved at the lower support levels. High criticality and complex issues are escalated to more experienced architects or infrastructure owners. The diagram below outlines a common multi-level support structure.



If a user encounters an issue, Level-1 support (help desk) is the entry point to the support system. Level-1 should resolve 75% of all issues encountered, of which a majority will be routine problems that only require a limited knowledge of the Citrix environment. At this level, issues are quickly resolved and some may be automated (self-service), for example password resets and resource provisioning.

Non-routine problems that exceed Level-1's abilities are escalated to Level-2 (Operators). This support level is generally

© 1999-2017 Citrix Systems, Inc. All rights reserved.

comprised of administrators supporting the production Citrix environment. Information on the end user's problem and attempted troubleshooting steps are documented at the first level allowing Level-2 technicians to immediately begin addressing the problem. Level-2 technicians should handle only 20% of the support tickets and are highly knowledgeable on the Citrix environment.

Complex issues that exceed Level-2's abilities should be escalated to Level-3 (Implementers). Level-2 and Level-3 support may often both be members of the Citrix Support Team, with Level-3 comprising the senior staff maintaining the Citrix environment. Level-3 issues are complicated and often mission critical requiring expert knowledge of the virtual desktop and application environment. Level-3 support tickets should amount to no more than 5% of all support issues.

The final level, Level-4 (Architects), is focused on the strategic improvements for the solution, testing new technologies, planning migrations, and other high level changes. Generally, Level-4 is not involved in active support of a production environment.

Should support discover an issue that is related to an application or underlying infrastructure, the ticket is handed to the appropriate team for troubleshooting. If a program bug is discovered, the issue is then re-escalated and a ticket is established with the appropriate vendor.

Decision: Support Responsibilities and Skill Set

The following table highlights the recommended characteristics of each support level.

Support level	Description	Responsibilities	Skill set
Level 1 - Help	Provide first-line support of reported issues. Initially, servicing support messages and phone calls. This level needs to perform	• Perform issue definition, initial analysis and basic issue resolution • Perform initial troubleshooting to determine the nature of the issue • Create ticket, collect user information, and log all troubleshooting steps performed • Resolve basic Citrix related issues, connectivity problems and application related issues using existing knowledge base articles • Escalate issue to Level-2 if advanced skills or elevated	• General Citrix XenApp/XenDesktop knowledge (CCA, CCA-V) • General Windows client OS/server OS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
	issue resolution. Often processes requests for application access or support with configuring plugins.	required • Ability to isolate the issue to be Citrix related, Microsoft related or third party Application related • If it affects the production environment or is potentially causing a system level outage, escalate directly to Level-3 • Generate requests for additional issue resolution guides as necessary • Follow up with end users when a support ticket is closed to ensure the problem has been satisfactorily resolved	• General Active Directory knowledge • General Networking knowledge (CCNA)
		• Perform intermediate issue analysis and resolution. • Identify root cause of issues. • Respond to server alerts and system outages. • Create weekly report on number of issues, close rate, open issues, etc. • Review vendor knowledge base articles. • Respond to out-of-hours helpdesk calls. • Respond to critical monitoring alerts. • Generate internal knowledge base articles and issue	Experience with Microsoft Windows Server including but not limited to: • Configuring operating system options • Understanding Remote Desktop Services policies and profiles • Using Active Directory • Creating users/managing permissions and administrator rights • Creating and modifying Active Directory group policies Basic administration

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-2 (Operators)	Primarily supporting day-to-day operations of the Citrix environment, may include proactive monitoring and management. In addition, this role should also perform intermediate level troubleshooting and utilize available monitoring or troubleshooting tools. Assist with resolving issues escalated by Level-1 support.	Level-1 troubleshooting workflows. • Perform basic server maintenance and operational procedures. • Manage user profiles and data. • Escalate ticket to Level-3 or appropriate technology owner if advanced skills or elevated permissions are required. • Generate requests for additional issue resolution scripts and knowledge base articles as necessary. • Able to read built-in event logs for Windows and Citrix to do basic troubleshooting following public information via Google/Bing.	protocols (TCP) • An understanding of firewall concepts • An understanding of email administration and account creation • An understanding of Remote Desktop Services policies and profiles • The ability to create shares and give access to shared folders/files Experience performing the following: • Managing, maintaining, monitoring and troubleshooting Citrix solutions • Backing up components in Citrix environments • Updating components in Citrix environments • Creating reports for trend analysis
		• Perform advanced issue analysis and resolution. • Perform maintenance and environment upgrades. • Addresses high severity issues and service outages. • Manage the Citrix environment. • Oversee and lead administrative tasks performed by Level-2. • Manage network and storage	Knowledge of how the following Windows components integrate with Citrix technologies: • Active Directory Domain Services • Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
		relates to the Citrix environment (depending on size	• Policies • Domain Name System (DNS)
Level-3 (Implementer)	Central point for implementing, administering and maintaining Citrix desktop and application virtualization infrastructure. This role focuses on deploying new use cases and leading lifecycle management initiatives. Generally, one Implementer could focus on one use-case at a time. For example, three new concurrent use cases would require three Implementers. Escalates issues to software vendor specific technical support and notifies Level-4 about this issue.	of company or Citrix environment). • Review periodic reports of server health, resource usage, user experience, and overall environment performance. • Review vendor knowledge base articles and newly released updates. • Perform policy-level changes and make Active Directory updates. • Review change control requests that impact the Citrix environment. • Perform advanced server and infrastructure maintenance. • Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility. • Create knowledge base articles and issue resolution scripts to address Level-2 requests. • Escalate ticket to vendor specific technical support, when necessary, and notify Level-4 of the issue.	• Dynamic Host Configuration Protocol (DHCP) • Group Policy Objects (GPOs) • NTFS Permissions • Authentication and Authorization • Knowledge of IIS • Microsoft Windows Operating Systems: Windows 10, Windows 8.1, Windows 7 Windows Server 2012 R2 Windows Server 2008 R2 • Roles and features of Windows Server • Knowledge of SQL 2008 R2 and newer • Knowledge of SQL Clustering, Mirroring and AlwaysOn Availability Groups. • General networking skills (i.e. routing, switching) • Knowledge of hypervisors. • Knowledge of shared storage configuration and management.
		• Provide technical leadership for	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-4 (Architect)	The Level-4 team has minimal exposure to administrative tasks but focuses on scoping, planning and executing Citrix-specific service and project requests. An architect translates business requirements into a technical design.	• Lead design updates and architecture revisions. • Address high severity issues and service outages. • Oversee technology integration workflows. • Review periodic reports of server health, resource usages, user experience, and overall environment performance to determine next steps and upgrade paths. • Initiate load testings to determine capacity of environment. • Review frequently recurring helpdesk issues. • Ensure technical specifications continue to meet business needs. • Update design documentation.	Advanced architectural assessment and design skills for: • Citrix XenApp • Citrix XenDesktop • Citrix XenServer, VMware vSphere, Microsoft Hyper-V • Citrix Provisioning Services • Citrix NetScaler • Citrix StoreFront • Active Directory • Storage solutions • Networking • Application delivery • Disaster recovery • Policies/policy structures and security restrictions • Licensing • Methodology Intermediate knowledge of: • General networking skills • Change control process • Project management • Risk assessment
Vendor support	Vendor assistance may be necessary should defects in a program be discovered. At this stage, Level-3 engineers need to establish a support ticket with the appropriate vendor to assist with finding a solution.		
Self-service	A self-service portal should be utilized for noncritical tasks, such as application access, permissions, password resets, etc. The portal can range from a simple FAQ page to a fully automated process requiring no human interaction. The purpose of the self-service portal is to add an additional touch point for end users to address basic issues, preventing the creation of new support tickets.		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Certifications and Training

The following table details the recommended training, certifications and experience for each support level.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Help Desk (Level 1)	Level-1 support personnel should be provided with basic training on Citrix XenApp, Citrix XenDesktop and supporting technologies. This can include internal training from subject matter experts or from a Citrix Authorized Learning Center. The training provided should focus on the following topics: • High level overview of the XenApp and XenDesktop implementation • Using Citrix Director to manage user sessions • Troubleshooting Citrix XenApp and XenDesktop sessions • Troubleshooting methodology In addition, regular training should be provided to the Tier-1 team members on the latest troubleshooting recommendations from the Level-2 and Level-3 teams as well as details on any relevant changes to the environment. This will help to ensure a good baseline knowledge level across the team and consistent customer service.	CXD-105: Citrix XenApp and XenDesktop Help Desk Support	N/A	1+ years (Entry level also acceptable)
Operator (Level 2)	Level-2 personnel should conduct regular team training sessions to refine administrative skills and ensure a baseline knowledge level across the team. Formalized trainings are also essential when there are architectural updates to the environment and the Level-2 team is working with unfamiliar technologies. All members of the Level-2 team should achieve the Citrix Certified Associate (CCA) certification for Citrix XenApp and XenDesktop. Advanced training on Windows concepts will also be essential for Level-2 team members who do not have desktop or server support experience. Finally, on-the-job training along with close integration with Level-3 administrators is essential as the Level-2 roles are formalized and responsibilities are handed over from Level-3 to Level-2.	CXD-210 XenApp and XenDesktop 7.1x Administration	Citrix Certified Associate - Virtualization	2-3 years
Implementer (Level-3)	Level-3 support team members hold a minimum of three years of enterprise experience implementing and supporting XenApp, XenDesktop, Provisioning Services and Windows operating systems. Level-3 staff should also complete the Citrix Certified Professional (CCP) certification track as this will prepare them to proactively manage the user community and implement Citrix solutions according to Citrix leading practices.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	3-4 years
	Experience is essential for Level-4 staff. A qualified Level-4			

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Architect (Level 4)	implementing, supporting, and serving in a technology architect role for a XenApp and/or XenDesktop environment as well as additional administrative experience with integrated technologies such as application and profile management solutions. The ideal candidate will have served in such a capacity at two or more environments for purposes of product exposure and in at least one environment of over 1,200 concurrent users. A Citrix Certified Expert (CCE) certification or comparable training and experience should be a prerequisite of the role.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	5+ years

Decision: Support Staffing

The following table provides guidance on the recommended number of support staff.

Role	Small Environment: Sites: 1; Users: <500; Images: 1-2	Mid-size Environment: Sites: 1-2; Users: 1000-5000; Images: 3-5	Large Environment: Sites: 2+; Users: >5000; Images: 5+
Help Desk (Level-1)	3	5-10	15-20
Operator (Level-2)	1-2	2-3	4-5
Implementer (Level-3)	1	1-2	2-3
Architect (Level-4)	1	1	1-2

> **注意**
>
> This table should only be used as a baseline. Support staffing decisions should be evaluated against the defined requirements, projected workloads, and operational procedures of an organization. Multiple levels can be combined, for example there may be insufficient design projects to have a dedicated architect role or a more senior member of the Citrix team can act as an Operator and Implementer.

Decision: Job Aids

General Support Tools: The following table details tools that should be made available to all support levels.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tools	Details
Ticket Management System	Used to document customer information and issues. A typical ticket management system provides the following functionality: • Monitoring the queue of tickets. • Setting a limit on the number of open tickets. • Establishing thresholds such as how long a certain type of ticket should take to be answered. • Identifying a group of users or individuals who require higher priority assistance. Informing the user when their ticket is open, updated, or closed. • Provide an internal knowledge base for the support professionals to search for known resolved issues.
Call Scripts	The first contact help desk personnel should have documented scripts to ensure that all relevant data is captured while the user is on the phone. This practice also assists in proper triage and allows the next support level to perform research prior to customer contact. A sample call script is provided for reference.
Remote Assistance Tools	Remote assistance tools are useful when troubleshooting user issues. Support technicians and administrators can remotely observe a user's actions.
Knowledge Base	Documentation should be created and maintained in a knowledge base or library of known issues. Articles should be searchable for quick recovery. Knowledge bases help support staff to quickly resolve known issues and reduce the need to perform time consuming research.

Citrix Support Tools

The following table provides recommendations on the Citrix support tools that should be made available to each support level.

Tool	Description	Products				Support Level			
		XenDesktop	XenApp	Provisioning Services Console	XenServer	L1	L2	L3	L4
Citrix Director	Citrix Director provides an overview of hosted desktops and application sessions. It enables support teams to monitor and troubleshoot issues.	X	X			X	X	X	X
Citrix Studio	Citrix Studio enables administrators to								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	perform configuration as well as maintenance tasks for a XenApp and XenDesktop site and associated virtual desktops or hosted applications.	X	X			X	X	X	X
Citrix Insights Services	Run from a single Citrix Delivery Controller to capture key data points and CDF traces for selected computers followed by a secure and reliable upload of the data package to Citrix Technical Support for escalation.	X	X	X	X			X	X
HDX Monitor	HDX Monitor is a tool to validate the operation of the Citrix ICA/HDX stack of a user session. HDX Monitor provides information about client capabilities, network performance/activity, session settings and many more items.	X	X			X	X	X	X
Provisioning Services Console	The Provisioning Services Console enables administrators to perform configuration and maintenance tasks for a Provisioning Services farm.			X				X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenCenter	XenCenter enables administrators to perform configuration and maintenance tasks for a XenServer Resource Pool.				X			X	X

Citrix Insight Services

Administrators can utilize Citrix Insight Services to simplify the support and troubleshooting of the Citrix environment. Citrix Insight Services is run locally to collect environment information. Online analysis capabilities analyze that information and provide administrators recommendations based on their Citrix environment and configuration. Additional information regarding Citrix Insight Services can be referenced in the Citrix Support article CTX131233 - FAQ: Citrix Insight Services.

A full list of the available tools provided by Citrix Support to assist with troubleshooting can be referenced in Citrix Supportability Pack.

Call Script

The following call script can be used as an initial baseline for a Citrix Help Desk team. Citrix Consulting recommends reviewing this sample call guide and adding any environment specific details that may need to be collected.

1. **What is the name and location of the user?**
   This question will identify if the user is accessing the environment from an external or internal network location.
2. **Is the problem always reproducible?**
   If it is a Yes, get the exact reproduce steps. This question is very important for the support team to troubleshooting an issue.
3. **Do any other users at the site/location experience the same issue? Can they have a colleague logon from same and/or different workstation?**
   These questions help to determine if this is a workstation issue or a user issue.
4. **What type of endpoint device is the user utilizing? (Corporate device, BYOD, thin client, pc, laptop, etc.)**
   This question will help determine if the issue is related to the user's endpoint.
5. **What is the Citrix Receiver version and connection information?**
   This question will verify if the user is using the right version of Receiver (the latest Receiver version or the version standardized by the company).
6. **Can the user see the StoreFront authentication page?**
   This question helps to identify network issues.
7. **What is the name of the application (or virtual desktop) the user is attempting to use? Does the user see the appropriate application or desktop icon on the StoreFront site?**
   These questions help to determine if there is an issue with user access and/or group membership.
8. **Does the application (or desktop) launch when the icon is selected? Does the application logon screen appear (if applicable)?**
   These questions help to determine if a connection is made into the Citrix XenDesktop infrastructure.
9. **Can the user authenticate into the application (if applicable)? Does the issue occur after the application is launched?**
   This question helps to determine if the issue is with the application rather than the application delivery infrastructure.
10. **What is the specific error seen (if applicable)?**
    This question identifies the specific error. The user should be requested to provide a screenshot, if available.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Delegated Administration

Each support level must be provided with sufficient rights to effectively perform their role. The following tables provide guidance on the recommended privileges per support level.

XenApp/XenDesktop Delegated Rights

Administrator role	Support Level
Help Desk Administrator	Level-1
Full Administrator	Level-2
Full Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenApp/XenDesktop Site, please refer to Citrix Product Documentation - XenApp and XenDesktop Delegated Administration.

Provisioning Services Delegated Rights

Administrator Role	Support Level
N/A	Level-1
Site Administrator	Level-2
Farm Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a Provisioning Services Site, please refer to Citrix eDocs - Provisioning Services Managing Administrative Roles.

StoreFront Delegated Rights

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Local Administrator on StoreFront Server	Level-3
Full Administrator	Level-4

Users with local administrator rights have access to view and manage all objects within StoreFront or Web Interface. These users can create new sites and modify existing ones.

Citrix License Server Delegated Rights

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Administrator	Level-3
Administrator	Level-4

By default, the account used during the installation of the license server becomes the administrator for the console. Often the accounts used for the installation are not the intended accounts for the regular administration tasks. For the steps on how to change the default administrator, please reference CTX135841 - How to Change the Default Administrator for the Citrix Licensing Server Version 11.10. All users created through this process are full administrators of the Citrix License Server.

XenServer Delegated Rights

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
Virtual Machine Operator	Level-2
Pool Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenServer Resource Pool, please refer to XenServer 7.0 Administrators Guide (see chapter Role Based Access Control).

Process 2: Operations

This section defines routine operations for the Citrix environment that help to improve stability and performance.

Decision: Administrative Tasks

The Citrix Support Team should perform regular operations and maintenance tasks to ensure a stable, scalable Citrix environment. Each operation is categorized by the associated component of the solution as well as the frequency of the operation (ongoing, daily, weekly and yearly). Tasks have been aligned to the roles described within Decision: Support Responsibilities and Skill Set.

If the administrators performing operations are the same the support team, then the designations are linked as follows:

- Level 2 Support = Operators
- Level 3 Support = Implementers

Daily Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a daily basis.

Component	Task	Description	Responsible
Generic	Review Citrix Director, Windows Performance Monitor, Event Log, and other monitoring software alerts	Check for warnings or alerts within Citrix Director, event logs, or other monitoring software. Investigate the root cause of the alert if any. **Note**: A computer and monitor can be set up to display the Citrix Director dashboard to create a Heads Up Display for the Citrix department. This ensures the status of the environment is clearly visible. Monitoring recommendations for XenDesktop and XenApp 7.x are included in the Monitoring section of the VDI Handbook.	Operators
		Verify all scheduled backups have been completed successfully.	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
		• User data (user profiles/home folders) • Application data	
Generic	Verify backups completed successfully	• Citrix databases • StoreFront configuration • Web Interface configuration • Provisioning Services vDisks (virtual desktops and application servers) • XenServer VM/Pool metadata (or equivalent for other hypervisors) • Dedicated virtual desktops • License files	Operators
Generic	Test environment access	Simulate a connection both internally and externally to ensure desktop and application resources are available before most users log on for the day. This should be tested throughout the day and may even be automated.	Operators
XenApp and XenDesktop	Virtual machine power checking	Verify that the appropriate number of idle desktops and application servers are powered on and registered with the Delivery Controllers to ensure availability for user workloads.	Operators
XenApp and XenDesktop	Perform incremental backup of Citrix related databases	Perform incremental-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check Citrix Provisioning Server utilization	Check the number of target devices connected to the Citrix Provisioning Servers and balance the load across servers, if required.	Operators
Provisioning Services	Perform incremental backup of Citrix PVS database	Incremental backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Operators, Database team (if Citrix environment is using a shared SQL)

Weekly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a weekly basis.

Component	Task	Description	Responsible
Generic	Review latest hotfixes and patches	Review, test, and deploy the latest Citrix hotfixes and ascertain whether the Delivery Controllers and Server-Based OS / Desktop-Based OS virtual machines require them. **Note**: Any required hotfixes should be tested using the recommended testing process prior to implementation in production.	Operators, Implementers (review process)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Generic	Create Citrix environment status report	Create report on overall environment performance (server health, resource usage, user experience) and number of Citrix issues (close rate, open issues, and so on).	Operators
Generic	Review status report	Review Citrix status report to identify any trends or common issues.	Implementers, Architect
Generic	Maintain internal support knowledge base	Create knowledge base articles and issue resolution scripts to address Level-1 and Level-2 support requests. Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility.	Operators (Level-2 requests), Implementers (Level-3 requests, and review process)
XenApp and XenDesktop	Check Configuration Logging report	Confirm that Citrix site-wide changes implemented during the previous week were approved through change control.	Auditors
XenApp and XenDesktop	Perform full backup of Citrix related databases	Perform full-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check storage capacity (only prior to updating a vDisk)	Review storage utilization, used and free storage space, for vDisk store and each vDisk. **Note**: Lack of space within the vDisk repository will be an issue only when the vDisks are updated using versioning or when a vDisk is placed in private mode during an update procedure. Storage utilization within vDisk should also be investigated. For example, a 20GB vDisk may only have 200MB of free storage. If the vDisk itself is limited for storage, then it needs to be extended. Citrix does not support resizing of a VHD file. Refer to the Microsoft link Resize-VHD for information on resizing a VHD file.	Operators
Provisioning Services	Perform vDisk updates (as necessary)	Perform a full backup of the vDisk before implementing any updates. Update the master vDisk image files and apply the following: • Windows software updates and patches • Operating system and application changes • Anti-virus pattern and definitions updates **Note**: Updates should be tested using the recommended testing process prior to implementation in production.	Auditors
Provisioning Services	Check auditing reports	Review the Citrix Provisioning Services auditing Logs. **Note**: Provisioning Server auditing is off by default and can be enabled to record configuration actions on components within the Provisioning Services farm. To enable auditing refer to the Citrix production documentation article, Enabling Auditing Information.	Operators, Database team (if Citrix environment is using a shared SQL)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Provisioning Services	Backup of Citrix PVS database	Backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Citrix Environment Administrator (or Shared SQL)

Monthly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a monthly basis.

Component	Task	Description	Responsible
Generic	Perform capacity assessment	Perform capacity assessment of the Citrix environment to determine environment utilization and any scalability requirements. **Note**: Recommendations for performing a capacity assessment are included in Decision: Capacity Management in the Monitoring section below.	Architect

Yearly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a yearly basis.

Component	Task	Description	Responsible
Generic	Conduct Citrix policy assessment	Review Citrix policies and determine whether new policies are required and existing policies need to be updated.	Implementers
Generic	Review software upgrades	Review and assess the requirement for new Citrix software releases or versions.	Implementers
Generic	Business Continuity Plan (BCP)/ Disaster Recovery (DR) test	Conduct functional BCP/DR test to confirm DR readiness. This plan should include a yearly restore test to validate the actual restore process from backup data is functioning correctly.	Architect
Generic	Perform application assessment	Review the usage of applications outside and within the Citrix environment. Assess the validity of adding additional applications to the Citrix site, removing applications that are no longer required, or upgrading the applications to the latest version.	Architect
Provisioning Services	Archive audit reports	Perform an archive of the Citrix Provisioning Server Audit Trail Information for compliance requirements.	Auditors

Decision: Backup Location

The location of backups directly effects the recovery time and reliability of the Citrix environment. It is recommended to store backups of critical data both onsite and at an offsite location. If offsite backups are not possible due to costs

© 1999-2017 Citrix Systems, Inc. All rights reserved.

associated or sensitivity of the data, backups should be placed at separate physical locations within the same datacenter.

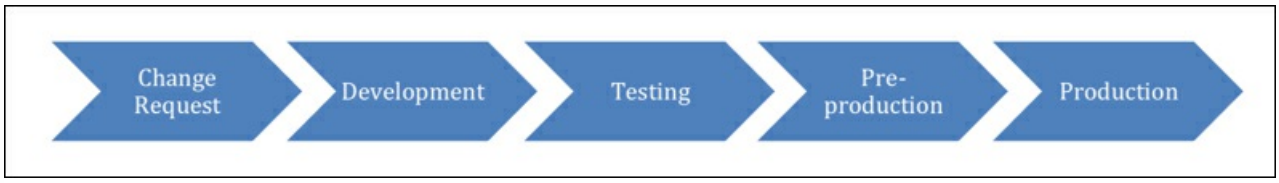
Each backup option is discussed further below.

- Onsite Backups – Onsite backups should be located on a storage device in the datacenter that will allow the data to be recovered quickly in the event of a failure. Onsite backups are ideal for issues that only affect a small subnet of hardware in the datacenter. Backups can also be stored on a cold storage solution such as tape. While this medium is slower to recover from, it provides additional protection since it is only active during the backup process.
- Offsite Backups – Although the time to recover is much higher, offsite backups provide additional protection in the event of a disaster. Offsite backups may require transferring data over the Internet to a third party provider or they are created onsite and then transported to a remote location on storage mediums such as tape. It is typical to put a limited number of backups offsite. For example, one backup a week or month.

Decision: Testing Process

Regular updates and maintenance are an everyday part of IT operations. Standard processes must be followed to ensure updates do not negatively impact the production environment. This includes maintaining a dedicated testing infrastructure where modifications can be validated prior to being implemented in production.

Since changes to Citrix infrastructure can impact thousands of virtual desktop and application users, multi-phase testing is critical for the reliability and performance of the environment. As such, the process for testing should resemble the following:



- Development - The development infrastructure exists outside of the production network. Typically, it consists of short-lived virtual machines whose configuration matches production as closely as possible. The purpose of the development phase is to provide change requestors a non-production environment to perform proof of concepts, determine integration requirements and perform iterative testing as part of a discovery phase. Proposed changes should be documented so they can be applied in the test phase.
- Testing - The test environment is a standalone 1:1 copy of the production infrastructure and is used to confirm that the proposed changes can be easily repeated prior to the preproduction staging environment. The changes made should follow documentation from the development stage. If testing fails within the testing stage, the architect must determine the severity of failure and determine whether minor updates to documentation is sufficient or a full development cycle is needed.
- Pre-production - The pre-production environment should mimic the current production environment. The goal of staging is to implement the proposed changes with little risk or uncertainty. It is expected that any changes made to the staging infrastructure have been tested and documented for repeatability. There should not be any iterations or adjustments required within this phase. During this phase and within this environment User Acceptance Testing (UAT) should be performed.
- Production - The production environment is a fully redundant and scalable solution designed for normal usage by end users. There should be minimal changes to the environment. If possible, all approved changes should be rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment.

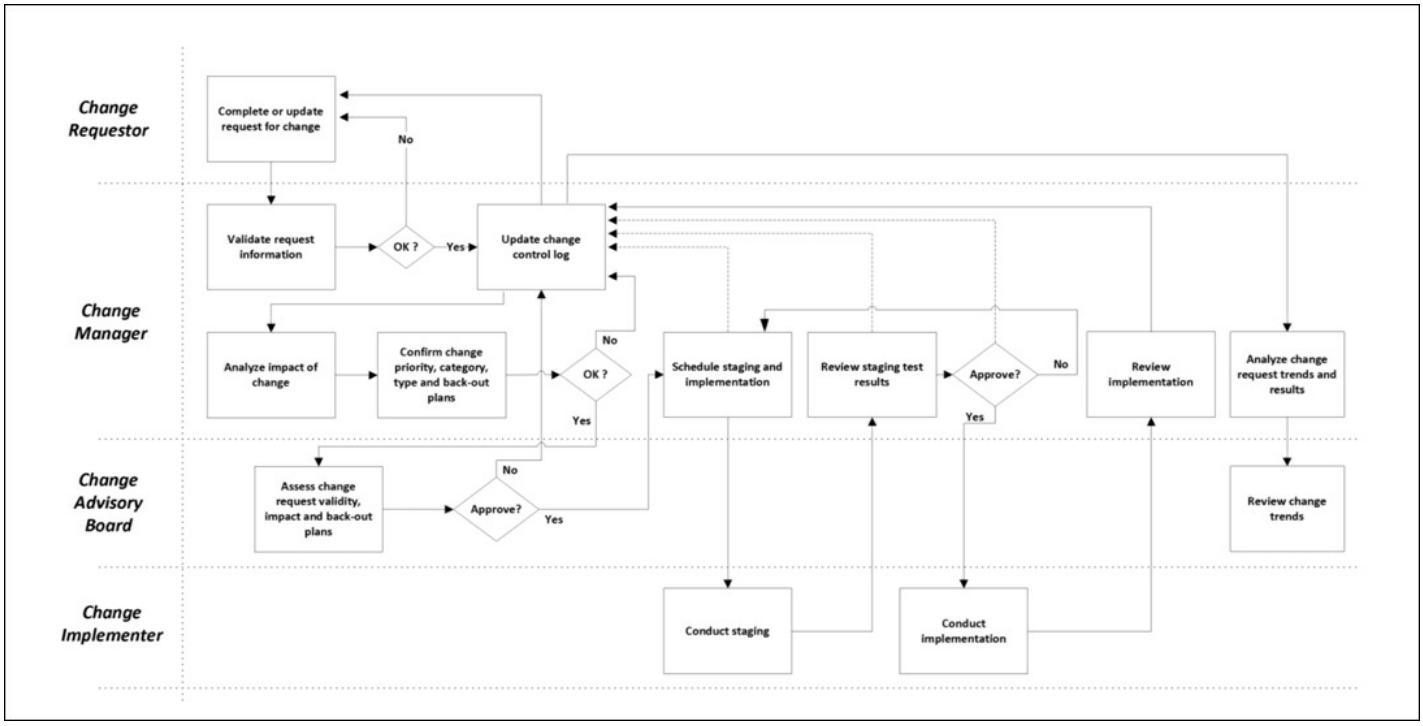
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Change Control

Standardized processes that manage changes throughout a system's lifecycle are necessary to ensure consistent and accountable performance. The following change control leading practices should be considered.

- Use a change control window so that all applicable parties know when there might be downtime. Make sure that all teams are represented in the Change Advisory Board (CAB).
- Every change should have a roll back plan.
- If a change fails have a "hot wash" to determine what went wrong.
- Always use an automated change control system so that support staff can quickly and easily identify changes.
- When available, ensure configuration logging is enabled to track any changes made to the Citrix environment.

The change control process should be closely followed starting with a change request. A change request form should be filled out detailing changes requested, reasons for the change, and intended timeframes for the action. This is then reviewed and edited if required by a Change Manager and advisory board. When the change request has gone through the entire change approval process it is given to a change implementer who stages the change for testing, and finally conducts the implementation in production. A sample change control process, including detailed steps, is provided in the diagram below:



The process is as follows:

1. The Change Request (CR) form is completed by any person requesting a change.

2. After appropriate manager approvals have been acquired, the CR is forwarded to the appropriate Change Manager(s).

3. The Change Manager validates the CR for completeness and logs the CR information into the Change Control Log for tracking. Incomplete change requests are returned to the requestor for update and re-submission.

4. The Change Manager assesses the impact of the change in conjunction with subject matter experts and/or managers of

© 1999-2017 Citrix Systems, Inc. All rights reserved.

the teams associated/affected by this change.

5. The Change Manager works with the associated/affected teams as well as the change requestor in order to confirm the priority, category and type of the change as well as the proposed rollback plan.

6. If the change is approved by the Change Manager, the CR is forwarded to the CAB for approval. If the change is rejected, the Change Control Log is updated with the current status as well as the reason of the rejection and the CR is send back to the requestor.

7. The CAB reviews and validates the change in detail, and discusses and evaluates purpose, reasons, impact, cost and benefits. Each board member represents their department and provides guidance on the change requests. The CAB also reviews multiple requests to coordinate implementations and "package" requests into a single release schedule.

8. Upon approval the change is sent back to the Change Manager to schedule the change for implementation into the staging environment.

9. The change is implemented and tests are conducted. The results are sent back to the Change Manager.

10. If the staging implementation and testing are successful, the change is scheduled for production implementation. In case the staging phase was not successful another staging iteration will be conducted.

11. If possible, the change is rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment. A rollback plan should be in place if there is an issue implementing a change in the production environment.

12. The Change Manager reviews the implementation and finally updates the Change Control Log.

13. On a periodic basis, the Change Manager reviews the Change Control Log to identify trends on type, frequency and size of changes and forwards the results to the CAB for review. In an emergency, the processes may be expedited. Should an issue be declared an emergency, a change request form is still filled out and delivered to the appropriate change management representative. When approved, the requested change is immediately implemented and the advisory board notified.

Decision: Availability Testing

Availability testing is focused on ensuring resources are still available in the instance of a component failure. These tests are essential to ensuring users always have access to business critical resources. The testing should be conducted during nonbusiness hours or during a scheduled maintenance weekend when appropriate notice has been given to end users to make them aware if any unforeseen issues arise.

The following is a list of the key components that should be tested on a regular basis.

- StoreFront – StoreFront should be load balanced and health checked by a NetScaler or other load balancing device. To validate its configuration, all but one of the StoreFront servers should be shutdown. This will validate that the load balancing device is detecting the failure and directing users to the functioning server.
- SQL – SQL Server should be in a high availability configuration. To validate the configuration, the primary SQL server should be taken offline and then the Citrix Studio console should be opened. Since Citrix Studio will not be accessible without a functioning SQL server, it will validate that the SQL server failover mechanisms are functioning properly.
- Delivery Controllers - Resources deployed should be configured with a list of multiple Delivery Controllers. If one is made unavailable, desktops and application hosts will automatically establish a connection to another server in the list. To validate this, shutdown one of the Delivery Controller hosts and determine if the resources initially connected to it

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

automatically register to another server. This can be determined by viewing the registration status of the resources inside Citrix Studio.

Sample Testing Workflow: Citrix Provisioning Services

Prerequisites and configuration requirements:

- Hypervisor, XenApp, and XenDesktop services are up and running.
- At least two PVS servers are installed and configured, providing the streamed disk image.
- Resilient networking and storage infrastructure with multiple links to each server.
- Test users are active on the XenApp or XenDesktop machines.

Steps	Expected Results
PVS Server Outage • Shutdown one of the Provisioning Servers. • Validate PVS continues to function. • Restart PVS Server. • Validate connections rebalance between PVS Servers. • Try the other(rest) PVS server(s) one by one.	• Existing XenApp/XenDesktop machines connect to another PVS server. • There is limited to no impact to the users utilizing that server. • New XenApp/XenDesktop machines can be booted and start correctly. • SCOM reports that the PVS server is down/not available. • Live connections are rebalanced between both PVS servers once both PVS servers are made available again.
PVS Bond Disruption: Disable / unplug a NIC in the PVS Streaming Bond on the PVS server.	Provisioning Server continues to stream over remaining NICS in PVS Streaming Bond.
SQL Server PVS Database Mirror Failover • Admin logs on to Principle SQL Server. • Initiate failover of PVS database. • Validate PVS continues to function. • Initiate failback of PVS database. • Validate PVS continues to function.	PVS continues to function.
SQL Service Outage • Admin reboots both Principle & Mirror SQL Servers simultaneously. • Validate PVS continues to function, but that administration is not possible. • Wait for the SQL Server to come back online. • Validate PVS administrative functions are once again possible.	• PVS continues to function. • PVS administrative functions are no longer available. • PVS administrative functions are available once the SQL services are restored.

Sample Testing Workflow: Citrix XenDesktop and XenApp Services

Prerequisites and configuration requirements:

- Hypervisor, XenDesktop, and StoreFront services are up and running.
- Network and storage services available.
- Provisioning Services is providing the streamed disk images.
- Test users are active on the virtual machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- SQL (Mirroring) and XenDesktop servers are up and running.
- Ensure multiple StoreFront servers are running.
- NetScaler load balancing services.

Steps	Expected Results
XenApp/XenDesktop 7.x Delivery Controller Citrix Broker Service Outage: • Stop the Citrix Broker Service on one of the Delivery Controller servers. • Validate virtual desktops or applications can still be enumerated and launched. • Start the Citrix Broker Service on the Delivery Controller server. • Shutdown one of the Desktop Controllers. • Validate virtual desktops or applications can still be enumerated and launched. • With a desktop launched, determine which Controller owns the host connection. Shut the Controller down and verify that another Controller takes over the session. **Note**: This should be done during the maintenance window. Once complete, the VDI resources should be rebooted so the VDAs are evenly distributed across all controllers.	• StoreFront correctly identifies service as being unavailable and redirects connections to remaining Delivery Controller. • Desktops continue to be enumerated and launch successfully. • Launched desktop can be supported if a hosting Controller goes down.
SQL Server Database Mirror Failover: • Admin logs on to principle SQL Server. • Initiate failover of XenApp/XenDesktop database. • Validate XenApp/XenDesktop continues to function.	• The database should failover and the Citrix Studio should pick up the failover database with no issues. • Existing sessions are not impacted. • New sessions are possible. • Administrative functions are possible.
SQL Service Outage: • Admin restarts both principle & mirror SQL Servers simultaneously. • Validate XenApp/XenDesktop continues to function, but that administration is not possible. Wait for the SQL Service to come back online. • Validate administrative functions are once again possible.	• Existing XenDesktop sessions are not impacted • Recently used applications, hosted shared desktops and assigned VDI can be accessed due to local host cache. • XenDesktop Administrative functions are not possible • XenDesktop Administrative functions are possible once SQL service is available.

Sample Testing Workflow: Citrix Licensing Services

Prerequisites and configuration requirements:

- Citrix Licensing Server up and running (with valid licenses installed).
- Hypervisor, XenApp/XenDesktop and StoreFront services are up and running.
- Users are active on the Server OS or Desktop OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Steps	Expected Results
Server: • Shutdown the Citrix Licensing server. • Reboot an existing Server OS machine. • Logon to the Citrix StoreFront and launch a published application. • Reboot an existing Desktop OS machine. • Logon to the Citrix StoreFront and launch a virtual desktop.	• License Server connectivity error posted in Event Log. • Provisioned Server OS boots successfully. • Users are able to launch published applications. • Provisioned Desktop OS boots successfully. • User is able to launch a virtual desktop. • Administrators will have 30 days grace to recover the Citrix Licensing Server.

Process 3: Monitoring

By having an in-depth understanding of current and expected behavior of the Citrix environment and its components, administrators are better equipped to discover an issue before it affects the user community. Furthermore, the data tracked during normal operations is beneficial for trending and capacity planning. This section defines the monitoring recommendations for a Citrix environment as well as some recommended tools.

Decision: Automated Monitoring

Depending on the size and scope of the XenApp and XenDesktop solution, it can take considerable time for an administrator to verify services, events, capacity and performance. It is advisable for administrators to investigate automation into their monitoring strategy.

Citrix includes a cloud-hosted monitoring solution called Smart Check (https://smart.cloud.com), which is a free service for any organization with active Citrix Customer Success Services: Select offering. Smart Check executes the following in a XenApp and XenDesktop environment:

- Site Health Checks – Evaluates all services with the XenApp and XenDesktop site
- Apps and Desktops Checks = Verifies delivery group availability
- Update Checks – Tracks and recommends patches and hotfixes for delivery controllers
- LTSR Checks – Verifies the delivery controllers and VDAs within the site comply with LTSR versions.
- Custom Checks – Allows administrators to import their own custom scripts to test across their XenApp and XenDesktop site.

A list of the current Smart Check capabilities, review the Smart Check documentation.

Decision: Performance Monitor Metrics

Monitoring the performance of the overall environment is crucial towards making sure all components are available and performing effectively to ensure users have a high quality experience.

Different components within the overall solution require monitoring of unique metrics with appropriately set thresholds. The metrics and thresholds presented are based on real world experience but may not apply to all environments. Organizations will need to perform their own baselining, validity testing and validation before implementing within a production environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> Some hypervisors, such as VMware vSphere and Hyper-V, provide specific performance counters for tracking CPU and Memory utilization within virtual machines (i.e. “VM Processor \ % Processor Time”). These performance counters should be used in addition to the general counters listed below.

General

These performance counters should be used to monitor the key performance metrics of the Citrix infrastructure, application servers, and virtual desktops.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Processor - % Processor Time	% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.	80% for 15 minutes	95% for 15 minutes	Identify the processes/services consuming processor time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of CPU consumption is an expected behavior it should be considered to add additional CPU resources to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
System - Processor Queue Length	Processor queue length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than ten threads per processor is normally acceptable, dependent of the workload.	5 (per core) for 5 minutes or 6 (per core) for 15 minutes	10 (per Core) for 10 minutes or 12 (per core) for 30 minutes	A long CPU queue is a clear symptom of a CPU bottleneck. Please follow the steps outlined for counter “Processor - % Processor Time”.
				Identify the processes/services consuming memory using Task

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Memory – Available Bytes	Available memory indicates the amount of memory that is left after nonpaged pool allocations, paged pool allocations, process' working sets, and the file system cache have all taken their piece.	<30% of total RAM or 20% of physical memory over 6 minutes	<15% of total RAM or 5% of physical memory over 6 minutes	all processes/services work within normal parameters and the level of memory consumption is an expected behavior it should be considered to add additional memory to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
Memory – Pages/sec	Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults.	>10	>20	A high value reported for this counter typically indicates a memory bottleneck, except if "Memory – Available Bytes" reports a high value at the same time. In this case most likely an application is sequentially reading a file from memory. Please refer to Microsoft Knowledge Base article KB139609 – High Number of Pages/Sec Not Necessarily Low Memory for further information.
Paging File - %Usage	This is the percentage amount of the Page File instance in use.	>40% or 80% over 60 minutes	>70% or 95% over 60 minutes	Review this value in conjunction with "Memory - Available Bytes" and "Memory - Pages/sec" to understand paging activity on the affected system.
LogicalDisk/PhysicalDisk - % Free Space	% Free Space is the percentage of total usable space on the selected logical disk drive that is free.	<20% of physical disk or 20% reported after 2 minutes	<10% of physical disk or 15% reported after 1 minute	Identify which files or folders consume disk space and delete obsolete files if possible. In case no files can be deleted, consider increasing the size of the affected partition or add additional disks.
LogicalDisk/PhysicalDisk - % Disk Time	% Disk Time marks how busy the disk is.	>70% consistently or 90% over 15 minutes (_Total)	>90% consistently or 95% over 15 minutes (_Total)	Identify the processes / services consuming disk time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of disk consumption is an expected behavior it should be considered to move the affected partition to a more capable disk subsystem in the future. If a process/service can be

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
				normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
LogicalDisk/PhysicalDisk – Current Disk Queue Length	Current disk queue length provides a primary measure of disk congestion. It is an indication of the number of transactions that are waiting to be processed.	>=1 (per spindle) consistently or 3 over 15 minutes (_Total)	>=2 (per spindle) consistently or 10 over 30 minutes (_Total)	A long disk queue length typically indicated a disk performance bottleneck. This can be caused by either processes/services causing a high number of I/Os or a shortage of physical memory. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time" and counter "Memory – Available Bytes"
LogicalDisk/PhysicalDisk – Avg. Disk Sec/Read – Avg. Disk Sec/Write – Avg. Disk Sec/Transfer	The Average Disk Second counters show the average time in seconds of a read/write/transfer from or to a disk.	>=15ms consistently	>=20ms consistently	High disk read or write latency indicates a disk performance bottleneck. Systems affected will become slow, unresponsive and application or services may fail. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time"
Network Interface – Bytes Total/sec	Bytes Total/sec shows the rate at which the network adaptor is processing data bytes. This counter includes all application and file data, in addition to protocol information, such as packet headers.	<8MB/sfor 100 Mbit/s adaptor <80 MB/s for 1000 Mbit/s adaptor or 60% of NIC speed inbound and outbound traffic for 1 min.	70% of NIC speed inbound and outbound traffic for 1 min.	Identify the processes / services consuming network using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of bandwidth consumption is an expected behavior it should be considered to move the respective process/service to a dedicated NIC (or team of NICs). If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.

XenApp/XenDesktop

These performance counters are specific to the Delivery Controllers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Database Avg. Transaction Time	The time on average, in seconds, taken to execute a database transaction. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	In case the reported values exceed the baseline response time constantly, a potential performance issue needs to be investigated at the SQL server level.
Database Connected	Indicates whether this service is in contact with its database. (1 is connected; 0 is not connected).	0	0 (for over 30 minutes)	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.
Database Transaction Errors/sec	The rate at which database transactions are failing.	None	> 0	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.

StoreFront

These performance counters are specific to the StoreFront servers.

Metric	Description	Warning (Yellow)	Critical (Red)
ASP.NET – Request Queued	The number of requests waiting to be processed by ASP. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values
ASP.NET – Requests Rejected	The number of requests rejected because the request queue was full.	None	> = 1
APP_POOL_WAS\Current Application Pool State\Citrix Receiver for Web	3		
APP_POOL_WAS\Current Application Pool State\Citrix Delivery Services Authentication	3		
APP_POOL_WAS\Cur rent Application Pool State\Citrix Delivery Services Resource	3		
Request response	Regardless it is authentication, enumerate or subscription) should be 3 to 5 seconds (http://www.perftestplus.com/resources/how_fast.pd f		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix License Server

These performance counters are specific to the Citrix License Server

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Citrix Licensing – Last Recorded License Check-Out Response Time	Displays the last recorded license check-out response time in milliseconds.	>2000 ms	> 5000 ms	If the reported values exceed the 5000 ms response time, a potential performance issue needs to be investigated in the Citrix License Server.
Citrix Licensing – License Server Connection Failure	Displays the number of minutes that XenDesktop has been disconnected from the License Server.	> 1 minute	> 1440 minutes	Both values report connectivity issues with the License Server. In case issues are reported, License Server and network availability needs to be verified.

Decision: Services Monitoring

Windows services that are critical to basic server functionality should be automatically monitored to ensure that they are running properly. The following table provides a list of the common Windows services that should be monitored. When any of these services are restarted or stopped a warning (Yellow) or critical (Red) alert should be assigned respectively. The recommended recovery actions for the services listed below are as follows:

- First failure: Restart the Service
- Second Failure: Restart the Service
- Subsequent Failures: Put the server in maintenance mode and investigate the root cause

XenApp/XenDesktop

Service	Functionality	Administration Risk
Citrix AD Identity Service	Manages Active Directory computer accounts. Dependencies: WMI Service	Machine Creation Service relies on this service to create virtual machines. Administrators will be unable to create new or modify existing Machine Catalogs. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Broker Service	Manages connections to virtual machines and applications.	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Any existing administrator connections to Citrix Studio can also be terminated. If this service is stopped existing user connections are not affected. No new connections can be established. Users logging into StoreFront will be unable to see any resources available for selection. Once the service is restarted users will need to re-login to StoreFront to establish connections.
Citrix Configuration Logging	Logs administrator activity and configuration changes	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Configuration Logging Database. Administrators will be unable make changes to the

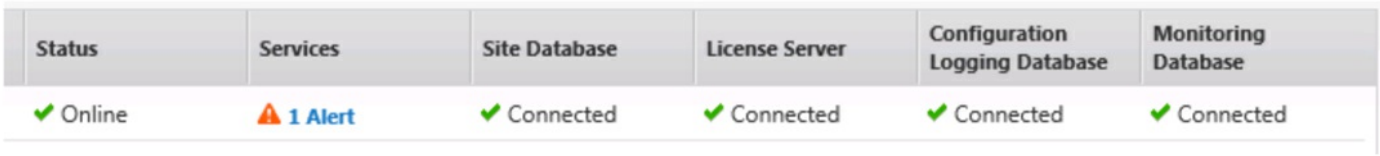
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Administration Risk
	deployment.	
Citrix Configuration Service	Stores service configuration information. Dependencies: WMI Service	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio.
Citrix Delegated Administration Service	Manages configuration of delegated administration permissions.	If this service is stopped XenApp/XenDesktop cannot assign administrative permissions. Administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Director and existing sessions within Citrix Director will be interrupted.
Citrix Diagnostic Facility COM Server Service	Manages and controls Citrix diagnostic trace sessions on the system. Dependencies: RPC Service	This service has no impact on the production environment. It is used to generate CDF trace files which aid in troubleshooting issues.
Citrix Environment Test Service	Manages tests for evaluating the state of a XenDesktop Site.	If this service is stopped administrators will be unable to establish new connections to Citrix Studio. Administrators will also be unable to check the status of the Citrix site configuration, machine catalogs, and delivery groups by running the tests under "Common Tasks" in the Citrix Studio administration console.
Citrix Host Services	Manages host and hypervisor connections. Dependencies: WMI Service	Administrators will be unable to create new Machine Catalogs or control virtual machine power settings via Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio. Users may experience issues connecting to virtual desktops when this service is not available. If this service is stopped existing connections are not affected.
Citrix Machine Creation Service	Creates new virtual machines. Dependencies: WMI Service	Administrators will be unable to create new or modify existing Machine Catalogs or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Monitor Service	Monitors the FlexCast system.	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Monitoring Database. Citrix Director will be unable to retrieve any data on the environment. Administrators will be unable to establish new connections to Citrix Studio.
Citrix StoreFront Service	Manages deployment of StoreFront.	Administrators will be unable to establish new connections to Citrix Studio.

Delivery Controller Services Monitoring in Citrix Director

The Infrastructure pane within the Citrix Director dashboard provides status of the services running on the Delivery Controllers and will provide warning indications if a service or Controller is unavailable. These alerts can be accessed by clicking the Alert hyperlink within the Infrastructure pane.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Status	Services	Site Database	License Server	Configuration Logging Database	Monitoring Database
✔ Online	⚠ 1 Alert	✔ Connected	✔ Connected	✔ Connected	✔ Connected

Provisioning Services

Service	Functionality	Risk
Citrix PVS PXE Service	Provides the PVS PXE Boot Server functionality. **Note**: Only applicable when PXE boot is used.	On failure of this service target devices may not be able to boot successfully if PXE booting is leveraged.
Citrix PVS Stream Service	Streams contents of the vDisk to the target device on demand.	If this service stopped it will not be possible to stream vDisk images.
Citrix PVS SOAP Service	Provides framework for external or existing solutions to interface with Provisioning services. **Note**: Only impacts console operations. User is unaffected	If this service fails PVS Server to PVS Server communication as well as PVS Console to PVS Server communication is not possible.
Citrix PVS TFTP Service	Provides the TFTP Server functionality. **Note**: Only applicable when TFTP is used.	On failure of this service target devices may not be able to boot if this server is used as TFTP server for the bootstrap.
Citrix PVS Two-Stage Boot Service	Provides the bootstrap functionality for devices booting by means of a BDM ISO file. **Note**: Only when BDM boot partitions are used.	On failure of this service target devices may not be able to boot if a BDM ISO file is used.

StoreFront

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
Citrix Cluster Join Service	Provides Server Group join services.	This service is started when adding additional StoreFront servers to a Server Group. If this service does not start or is interrupted when this process is initiated the additional server will be unable to join the indicated Server Group and the process will result in an error.
Citrix Configuration Replication	Provides access to Delivery Services configuration information.	This service only exists on the primary StoreFront server of a Server Group. If this service is stopped additional StoreFront servers will be unable to join the Server Group and any changes made to the primary StoreFront server will not be replicated to other servers. This can result in servers within the Server Group being out of sync.
Citrix Credential Wallet	Provides a secure store of credentials. Dependencies: Citrix Peer Resolution Service	If this service is stopped users will be unable to login to access their desktops or applications. Users logged into StoreFront will be unable to launch new application or desktop sessions. Existing application or desktop sessions are unaffected.
Citrix Default Domain Services	Provides authentication, change password, and other domain services.	If this service is stopped users will be unable to login to access their desktops or applications. Users currently logged in will not be affected.
Citrix Peer Resolution Service	Resolves peer names within peer-to-peer meshes.	On failure of this service both the Citrix Credential Wallet and Citrix Subscriptions store are stopped generating the risks associated with those services.
Citrix Storefront Privileged Administration Service	Manages privileged operations on Storefront	
Citrix Subscriptions Store	Provides a store and replication of user subscriptions. Dependencies: Citrix Peer Resolution Service	If this service is stopped Citrix Receiver cannot add, remove, and reposition applications within StoreFront. Users will need to re-add applications and all changes made to their selection of applications within the StoreFront store will not be saved or replicated to other sessions. Original user configuration will be restored once the service is restarted.
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through StoreFront. Users will be unable to resolve the Receiver for Web login page. Users logged into StoreFront will be unable to launch new application or desktop sessions and will need to reenter credentials when the service is restarted. Existing application or desktop sessions are unaffected.

Web Interface

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through Web Interface if the WWW service is not available.

Citrix License Server

Service	Functionality	Risk
Citrix Licensing Service	Provides licensing services for Citrix products.	Licensing mode changes to grace period when service is stopped or License Server cannot be contacted. If not monitored, functionality of Citrix products will cease after grace period expires.
Citrix Licensing Support Service	This account controls reading the license files and updating strings with license trailers (data dictionary functionality).	None
Citrix Licensing WMI	The Citrix License Management Console collects license data information using the WMI service.	None

Decision: Events Monitoring

Monitoring the Windows Event Log for unknown or critical events can help to proactively discover issues and allow administrators to understand event patterns:

- Licensing - Errors in the Event Log dealing with Remote Desktop licensing should be investigated. This might be a result of the installed Citrix product not being able to contact the Remote Desktop Licensing Server or the Citrix Licensing Server. If errors in the Event Log are not reviewed, users might eventually be denied access because they cannot acquire a valid license.
- Hardware Failure - Any event notification that relates to a hardware failure should be looked at immediately. Any device that has failed will have an impact on the performance of the system. At a minimum, a hardware failure will remove the redundancy of the component.
- Security Warnings - Customers should investigate security warnings or audit failure events regarding failed logons in the security log. This could be an indication that someone is attempting to compromise the servers.
- Disk Capacity - As the drives of a Windows system reach 90% of capacity, an event error message will be generated. To ensure continuous service, customers should poll these event errors. As the system runs out of hard disk space, the system is put at severe risk. The server might not have enough space left to service the requests of users for temporary file storage.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Application / Service errors - Any event notification that relates to application or services errors should be investigated.
- Citrix errors - All Citrix software components will leverage the Windows Event Log for error logging. A list of the known Event Log warnings and errors issued by Citrix components can be found at the following links:
  - Event Codes Generated by PVS
  - XenDesktop 7 - Event Log Messages

It is important to periodically check the Event Viewer for Citrix related warnings or errors. Warnings or errors that repeatedly appear in the logs should be investigated immediately, because it may indicate a problem that could severely impact the Citrix environment if not properly resolved.

In multi-server environments it becomes easier to administer the servers when logs can be collected and reviewed from a central location. Most enterprise grade monitoring solutions provide this functionality. More sophisticated monitoring solutions enable an administrator to correlate event information with other data points such as performance metrics or availability statistics. In case the selected monitoring solution does not provide this functionality the Windows Server 2008 R2 or Windows Server 2012/2012 R2 Event Log subscription feature can be used. This feature allows administrators to receive events from multiple servers and view them from a designated collector computer. Please see Microsoft TechNet article Manage Subscriptions for more information.

XenServer is also capable of sending its logs to a central syslog server. The administrator sets the IP address of the syslog daemon server in the properties of each XenServer in the pool. This configuration allows administrators to capture real-time activity across multiple XenServer hosts. Further information can be found within the XenServer Admin Guide.
Decision: Capacity Management

In addition to the day-to-day monitoring of system-level metrics, performance metrics should be tracked from a historical perspective to help plan for future growth as more users access the environment.

A baseline of the environment performance should be taken so that it can be compared against performance over time. For example, if a user complains of poor performance, this baseline can be used for comparison purposes to identify if the issues are related to the user load exceeding the capacity of the environment.

An example of baseline performance metrics for capacity management would include historical data for CPU, Memory, and network utilization on the Delivery Controller and application servers or desktops.

Citrix Director

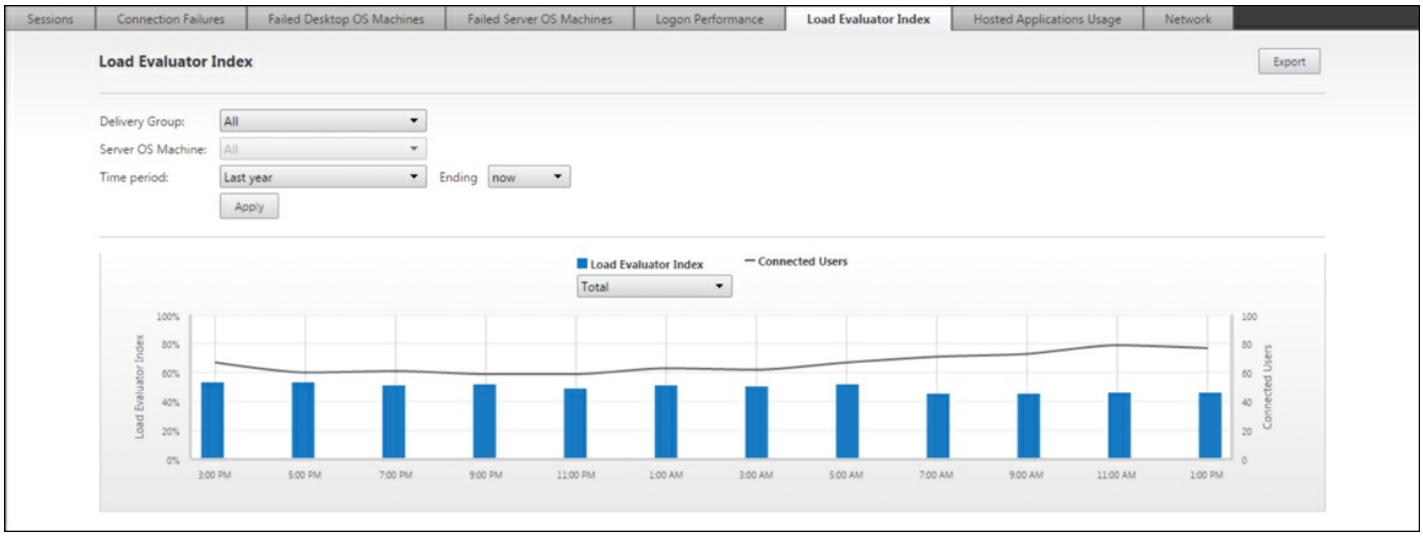
Administrators can utilize the Trends view within Citrix Director to track different parameters of the Citrix XenApp/XenDesktop deployment over time. These parameters can be leveraged for capacity planning of the Citrix environment.

From the Trends view, administrators can see historical data that is broken up into several categories including:

- **Sessions** - Provides the concurrent session usage over time enabling the ability to size the environment appropriately.
- **Connection Failures** - Gives an overview of the different types of connection failures that have occurred across different Delivery Groups.
- **Failed Desktop OS Machines** – Gives an overview of the different problems associated with failures in desktop machines.
- **Failed Server OS Machines** - Gives an overview of the different problems associated with failures in server machines.
- **Logon Performance** – Shows how long it takes for users to log on to their applications and desktops.
- **Load Evaluator Index** – Provides various performance counter-based metrics, including CPU, Memory, and Disk Usage for Server OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Capacity Management** – Shows utilization of published applications and desktops.
- **Resource Utilization** – Provides information on CPU, Memory and storage resource utilization.
- **Custom Reports** – Allows administrators to create custom historical reports on numerous metrics captured by the system.
- **Hosted Application Usage** – Details all applications published in the site and can provide usage information about each individual applications in detail (concurrent instances, launches, usage duration, and so on). **Note**: Requires XenApp or XenDesktop Platinum licensing
- **Network** – Network analytics provided through NetScaler HDX Insight.



For more information on Citrix Director Trends, please refer to the following.

- Citrix Blogs – Citrix Director: Trends Explained
- Citrix Support – CTX139382 - Best Practices for Citrix Director

The creation of the handbook is a time consuming process and requires real deployment experience across many scenarios. Citrix would like to thank the authors and subject matter experts who contributed to the Citrix VDI Handbook.

© 1999-2017 Citrix Systems, Inc. All rights reserved.