

XenAppおよびXenDesktop 7.9

Aug 26, 2016

新機能

[解決された問題](#)

[既知の問題](#)

[このリリースに含まれていない機能](#)

[サードパーティ製品についての通知](#)

システム要件

製品の技術概要

[概念およびコンポーネント](#)

[Active Directory](#)

[データベース](#)

[配信方法](#)

[リファレンスアーキテクチャ](#)

[設計ガイド](#)

[実装ガイド](#)

インストールと構成

[インストールの準備](#)

[グラフィカルインターフェイスを使ったインストール](#)

[コマンドラインを使ったインストール](#)

[スクリプトを使用したVDAのインストール](#)

[Red Hat Linux Virtual Delivery Agent \(VDA\) のインストール](#)

[SUSE Linux VDAのインストール](#)

[サイトの作成](#)

[マシンカタログの作成](#)

[マシンカタログの管理](#)

[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](#)

リモートPCアクセス

App-V

AppDisk

ローカルアプリケーションアクセスとURLリダイレクト

XenApp Secure Browser

サーバーVDI

Personal vDisk

コンポーネントの削除

アップグレードと移行

環境のアップグレード

XenApp 6.xからの移行

XenDesktop 4からの移行

セキュア

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

管理権限の委任

スマートカード

Transport Layer Security (TLS)

Federated Authentication Service

印刷

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

HDX

Thinwire互換モード

Framehawk仮想チャネル

HDX 3D Pro

Flashリダイレクト

WindowsデスクトップOSのためのGPUアクセラレーション

WindowsサーバーOSのためのGPUアクセラレーション

OpenGLソフトウェアアクセラレータ
オーディオ機能
ネットワークトラフィックの優先度
USBとクライアント側ドライブの考慮事項

Policies

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

アプリケーションの

ライセンス管理
アプリケーション
ゾーン
接続とリソース
接続リース
仮想IPおよび仮想ループバック
Delivery Controller
Sessions
Studioでの検索の使用
タグ
IPv4/IPv6サポート
クライアントフォルダーのリダイレクト
ユーザープロファイル
Citrix Insight Services

監視

Session Recording
構成ログ
Personal vDiskの監視

Director

詳細構成

展開環境の監視

アラートおよび通知

管理権限の委任とDirector

Director展開環境の保護

XenDesktop 7 よりも前のVDAに対する権限の構成

HDX Insightの構成

ユーザーの問題のトラブルシューティング

SDKおよびAPI

Monitor Service OData API

FIPS展開の例

Citrix SCOM Management Pack for XenApp and XenDesktop

ライセンスサーバー用Citrix SCOM Management Pack

新機能

Jul 07, 2016

ここでは次のことについて説明します。

[このリリースについて](#)

[XenApp/XenDesktop 7.9](#)

[Virtual Delivery Agent \(VDA\) 7.9](#)

[StoreFront 3.6](#)

[Provisioning Services 7.9](#)

[AppDNA 7.9](#)

このリリースについて

XenAppおよびXenDesktopの7.9リリースは、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で構成されています。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。これにより、以下に示すすべての最新機能を使用できます。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。

- **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。これは、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。VDAの新機能と更新された機能は以下の通りです。手順については、以下の記事を参照してください。

[スタンドアロンVDAインストーラーのグラフィックインターフェイスを使用してVDAをインストールまたはアップグレードする](#)

[スタンドアロンVDAインストーラーのコマンドラインインターフェイスからVDAをインストールまたはアップグレードする](#)

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](#)

[Provisioning Services](#)

[AppDNA](#)

XenApp/XenDesktop 7.9

この製品リリースでの新機能、および強化された機能は以下のとおりです。

インストールと構成

このセクションでは、XenAppおよびXenDesktopのインストールと構成におけるこのリリースでの変更点の概要を示します。

- コンポーネントをインストールすると、分析情報が収集されてローカルに保存されます。
- VDAのインストール時にControllerのアドレスを指定しない場合、Controllerのアドレスを入力しない限りVDAを登録できないことを示すメッセージが表示されます。
- VDAをインストールするときにControllerアドレスを指定すると、VDAとController間で接続を確立できるかどうかがインストーラーによって検証され、結果が報告されます。
- インストールウィザードでは、Citrixのカスタマーエクスペリエンス向上プログラムに参加しているものとみなされ、登録は促されなくなりました。
- コアコンポーネントおよびVDAのインストールウィザードでは、Call Homeへの登録が促されるようになりました。
- 全製品インストーラーのグラフィックインターフェイスから、Federated Authentication Serviceをインストールできるようになりました。

今後のリリースでの使用に備えて、以下の変更が実装されました。

- Delivery Controllerのインストール時に、Microsoft SQL Express LocalDB 2014が自動的にインストールされます。このソフトウェアは、サイト、監視、データベースの記録には使用されません。このデータベースでの管理者による操作はありません。このインストールを禁止するには、Controllerのインストール時にXenDesktopServerSetup.exeコマンドで「/exclude 'Microsoft SQL Server 2014 Express LocalDB'」オプションを使用します。
- サイトを作成するときに、サイトのデータベースとして使用する目的でSQL Server Expressデータベース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）、データベース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。

アップグレード

アップグレードの実行中、インストーラーにより、Citrix Receiver for Windows Enterprise、Offline Plug-in for Windows、またはXenApp Plugin for Streamed Appsの検出やアップグレードが行われることはなくなりました。詳しくは、「[展開のアップグレード](#)」を参照してください。

プロビジョニング：MCS I/Oストレージの最適化

Machine Creation Services (MCS) で作成されたマシンのホストに使用されるハイパーバイザーやクラウドサービスプロバイダーへの接続を作成するときに、データの種類に応じてストレージの場所を指定できるようになりました。

- マスターイメージを含むオペレーティングシステムデータ。
- 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、ユーザープロフィールファイルデータ、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。

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、一時マシンデータ用に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。この接続を使用するマシンカタログを作成する場合、各仮想マシンのキャッシュディスクサイズおよびメモリサイズに対し、デフォルトでない値を有効化および構成できます。

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する場合、Personal vDiskの共有ストレージを使用するかどうかを選択できます（Personal vDiskを使用している場合）。

詳しくは、「[接続およびリソース](#)」および「[マシンカタログの作成](#)」を参照してください。

プロビジョニング：StudioでのNutanix統合

プロビジョニングされた仮想マシンをホストするのにNutanix Acropolisを使用する場合は、Delivery ControllerにNutanixプラグインをインストールして、StudioでNutanix接続の構成を有効にします。

Nutanixへの接続およびNutanixイメージを使用するマシンカタログへの接続の作成にStudioを使用する場合、ウィザードで標準およびNutanix固有の構成情報を指定できます。

詳しくは、「[Nutanix仮想化環境](#)」を参照してください。

公開：アプリケーショングループ

アプリケーショングループを使用すると、アプリケーションをまとめて管理できます。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す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。

アプリケーショングループはオプションであり、複数のデリバリーグループへの同じアプリケーションの追加に代わる方法になります。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ます。また、同じアプリケーショングループを複数のデリバリーグループに関連付けることもできます。

詳しくは、「[アプリケーショングループの作成](#)」および「[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導入は、その他の複数のStudio領域に影響します。たとえば、あるアプリケーションのプロパティを編集する場合、そのアプリケーションのグループメンバーシップにデリバリーグループやアプリケーショングループを含めることができます。これまでは、アプリケーションは1つ以上のデリバリーグループに関連付ける必要がありましたが、今後は、1つ以上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。アプリケーションの管理については、「[アプリケーション](#)」を参照してください。

セキュリティおよびアクセス：Federated Authentication Service

Citrix Federated Authentication Serviceは、Microsoft証明機関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Citrix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。

詳しくは、「[Federated Authentication Service](#)」を参照してください。

Citrix Insight Services

参加方法など、利用統計情報機能について詳しくは、「[Citrix Insight Services](#)」を参照してください。

インストーラーの分析

全製品インストーラーを使用する場合、XenAppおよびXenDesktopコンポーネントをインストールすると、分析データが収集されてローカルに保存されます。インストールで問題が発生した場合は、分析用にこのデータのアップロードを求められることがあります。

Call Home

全製品インストーラーでは、（常時トレースを含む）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。PowerShellコマンドレットを使用して、登録の変更、カスタムのアップロードスケジュールの作成、およびパッケージの手動アップロードを行うこともできます。

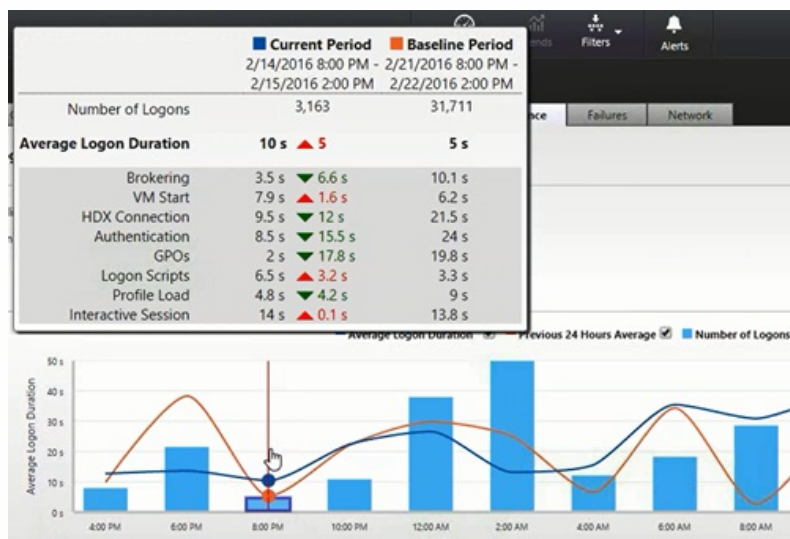
Citrixカスタマーエクスペリエンス向上プログラム (CEIP)

Citrixのカスタマーエクスペリエンス向上プログラムへの参加は、サイトの作成時に自動で有効化されるようになりました。サイトの作成ウィザードで登録する必要はありません。サイトを作成した後で、参加状態を変更することができます。

Director

Directorの新機能、および強化された機能は以下のとおりです。

- **ログオン処理時間の改善。** [ログオンパフォーマンス] グラフでデータポイントを選択すると、「ヒント」データがより明快に表示されるようになり、理解しやすくなりました。さらに、[ログオン数] が棒グラフで表示されるようになりました（以前は折れ線グラフでした）。[ログオン数] および以前の基準期間は、グラフ上の表示で切り替えることができます。選択した期間の [ユーザーセッションごとのサインイン処理時間] を表示する新しい表が、[ログオンパフォーマンス] グラフの下に表示されるようになりました。管理者は、ユーザーを検索したり、列を選択して表示順序をソートしたりできます。詳しくは、「[展開環境の監視](#)」を参照してください。



Virtual Delivery Agent (VDA) 7.9

VDA for Server OSおよびVDA for Desktop OSのバージョン7.9での印刷、HDXテクノロジー、およびプラットフォームのサポートについて強化された機能は以下のとおりです。

- **Citrix Universal Print Server (UPS) の負荷分散。** 管理者は、新しい2つのポリシー設定である「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」を使用して、複数の負分散されたプリントサーバーを追加できます。これらの設定により、VDAでのXenAppおよびXenDesktopセッションで、ログオン時にセッションプリンターを他のプリントサーバーにシームレスにマップできます。詳しくは、「[Universal Print Serverのポリシー設定](#)」、および「[印刷環境の保守](#)」の「Universal Print Serverの負荷分散」を参照してください。
- **Citrix XPSユニバーサルプリンタードライバでのホチキス留めおよび給紙方法の選択** Citrix XPSユニバーサルプリンタードライバは、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。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。

- **Universal Print ServerとCEIP**。CEIPへの参加は、Universal Print Serverのインストール時に自動で行われます。最初の7日間は、データの収集は行われません。この期間中、またはそれ以降のいつでも、レジストリ設定によりUPSのCEIPへの参加を無効にすることができます。詳しくは、「[プリンターのプロビジョニング](#)」および「[Citrix Insight Services](#)」を参照してください。
- **StudioでのLPTおよびCOMポートリダイレクトのポリシー設定** LPTおよびCOMのポート設定をStudioで構成できるようになりました。VDA7.0~7.8では、これらの設定はレジストリでのみ構成できました。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。
- **Intel Iris Pro Graphics内蔵Intel CPU向けのHDX 3D Proサポートの拡張**。Intel Iris Pro Graphicsを搭載した第5世代または第6世代のIntel CPUでは、HDX 3D Proグラフィックアクセラレーションテクノロジーを使用します。このリリースでは、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。VDAインストーラーには、この機能をサポートするための新しいファイルGfxDisplayTool.exeが含まれます。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。
- **HDX 3D Pro VDAでのWindows 10 のサポート**。このリリースでは、VDA for Windows Desktop OSのHDX 3D ProバージョンにおけるWindows 10のサポートが追加されました。
- **Windows 10でのリモートPCアクセス向けセキュアブートのサポート**。Virtual Delivery Agent (VDA) for Desktop OSでは、Windows 10および8.1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。
- **「圧縮にビデオコーデックを使用する」の新しいデフォルト設定** 「選択された場合ビデオコーデックを使用する」が、グラフィックポリシー設定「圧縮にビデオコーデックを使用する」の新しいデフォルト設定になりました。これは、VDAによるThinwire互換モードの使用をサポートするための変更です。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。
- **Red HatおよびSUSE向けLinux VDAの拡張と改善** VC CDMおよびCentOS（バージョン6.7、7.2）のサポートが、お客様からご報告いただいた問題を解決する多数の改善とともに追加されました。詳しくは、「[Red Hat/CentOS](#)」および「[SUSE](#)」を参照してください。
- **XenApp上のマストストレージデバイスの汎用USBリダイレクト** マストストレージデバイスの汎用USBリダイレクト（USBプラグアンドプレイ）がXenAppおよびXenDesktopでサポートされるようになりました。XenAppユーザーはXenAppセッションで、マストストレージデバイスが物理的に接続されているかのように操作できます。この機能を使用するには、MicrosoftのセキュリティアップデートKB3155784をインストールする必要があります。このリリースでは、この機能はデフォルトでXenAppに対して無効化されており、レジストリキーで有効になります。

USBストレージデバイスをXenAppの汎用USBリダイレクトに対して有効にするには、レジストリキーHKLM\SOFTWARE\Citrix\Portica\GenericUSBで値の名前UsbStorageEnabledを作成し、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。

StoreFront 3.6

StoreFrontには次の新機能があります。

- **異なるファーム間での負荷分散**。以前のStoreFrontバージョンでは、マルチサイト構成を使用して同等のファームセットを作成するときに、負荷分散を正常に行うにはすべてのリソースを各Delivery Controllerで公開する必要がありました。StoreFrontが使用可能なリソースの一覧を取得するリソースの列挙プロセスでは、同等のファームセット内のDelivery Controllerのうち1つだけにアクセスされていました。StoreFront 3.6では、各リソースを、同等のファームセットのすべてのDelivery Controllerに共通としたり、特定のDelivery Controllerのみで公開したりできます。これらすべてのリソースから列挙されるように、StoreFrontを設定できるようになりました。

- **単一サーバー展開に対するActive Directoryドメイン要件の解消。**さまざまな理由により、サーバーをActive Directoryドメインに追加しない場合があります。このバージョンでは単一サーバーの展開に対する要件が解消され、ドメイン不参加サーバーにStoreFrontをインストールできるようになりました。
- **StoreFront REST API。**NetScaler GatewayでStoreFrontクラスターの現在のゲートウェイ構成を特定するために照会できる、StoreFront REST APIが作成されました。NetScaler管理コンソールにより、StoreFrontおよびNetScaler設定を組み合わせたゲートウェイ構成ファイルが作成されます。StoreFront管理コンソールまたはPowerShellを使用して、構成ファイルをStoreFrontにインポートできます。

詳しくは、[StoreFront 3.6](#)のドキュメントを参照してください。

Provisioning Services 7.9

Provisioning Servicesには次の新機能があります。

- **Citrixカスタマーエクスペリエンス向上プログラム (CEIP)** CEIPでは、Provisioning Servicesからの構成および使用に関するデータが匿名で収集され、そのデータがCitrixに自動的に送信されます。このデータは、Provisioning Servicesの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。
- **XenDesktopセットアップウィザードからのUEFI向けBDMサポート。**UEFI BDMサポートに、ターゲットUEFIファームウェアにBDM起動オプションを設定できるXenDesktopセットアップウィザードとの統合が含まれています。このサポートにより、PVSは以下からの起動をサポートします。
 - ISO
 - USB
 - 起動パーティション
- **BDMパーティションの更新。**Provisioning Services 7.9では、ユーザーが接続されているPVSサーバーのブートストラップにおけるサーバーIPアドレスに基づいてBDMパーティションをアップグレードできる機能が導入されます。BDMパーティションは次の3つの方法でアップグレードできます。
 - コレクション別
 - 強調表示されたデバイスのグループ別
 - 個別のデバイス別

詳しくは、「[Provisioning Services 7.9](#)」を参照してください。

AppDNA 7.9

AppDNAには次の新機能があります。

- **アプリケーションワークフローのインポート機能の強化** アプリケーションワークフローのインポート機能が向上し、サーバー側の処理の進行状況に関するフィードバックやインポート対象を追加やキャンセルできる柔軟性が導入されました。
- **Compliance Managerモジュール。**Compliance Managerモジュールによって、ITインフラに展開する予定のアプリケーションにセキュリティリスクの可能性があるかどうかを確認するのに役立ちます。このモジュールには、アルゴリズムおよびレポートの初期のセットが含まれます。これは今後拡張される予定です。これは、このリリースの評価用の機能で、実稼働環境でのアプリケーションの展開を決定するために使用すべきではありません。
- **アプリケーション属性フォームへのWebクライアントアクセス** このリリースでは、AppDNA Webクライアントからアプリケーション属性フォームへのアクセスを追加します。Webクライアントで [Applications] を選択してアプリケーションを強調表示し、[Properties] を選択します。

詳しくは、[AppDNA 7.9のドキュメント](#)を参照してください。

解決された問題

Jul 15, 2016

バージョン7.8では、次の問題が解決されています。

AppDNA	Provisioning Services
Citrix Director	StoreFront
Citrixポリシー	Universal Print Server
Citrix Studio	VDA for Desktop OS
Controller	VDA for Server OS
HDX MediaStream Flashリダイレクト	仮想デスクトップコンポーネント - その他

AppDNA

Citrix Director

- PDF形式で大量のデータをエクスポートしようとする、サーバーのCPUおよびメモリ消費が100%に到達しそうになり、次のエラーメッセージが表示されます。

「操作に失敗しました。データソースが応答しないか、エラーを報告しました。詳しくは、サーバーのイベントログを参照してください。」

この修正を適用すると、PDFのエクスポートの制限を構成できるようになり、少なくともレポートの一部を取得できます。

この修正のインストール後、wwwroot\Directorフォルダーでweb.configファイルを次のように構成する必要があります。

[appSettings] セクションで次の行を追加します。

この制限は、値がPDFレポートの行の数を指定するメモリサイズなど、サーバーの機能に応じて異なります。

[#LC4108]

- 任意のファイル形式でレポートをエクスポートしようとする、次のエラーメッセージが表示されることがあります。

「操作に失敗しました。予期されないサーバーエラーです。詳しくは、サーバーのイベントログを参照してください。」

[#LC4281]

- XenAppサーバーに2つのIPアドレスがあり、DNSサーバーが最初のIPアドレスを解決できない場合、管理者によるCitrix Directorへのログオンの試行が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。

「現在、システムを使用できません。後で再試行するか、管理者に問い合わせてください。」

[#LC4411]

- CSV形式で大量のデータをエクスポートしようとする、タイムアウトが発生してエクスポートが失敗し、次のエラーメッセージが表示されることがあります。

「操作に失敗しました。データソースが応答しないか、エラーを報告しました。詳しくは、Directorサーバーのイベントログを参照してください。」

この修正により、データエクスポートのタイムアウト値を構成できるようになります。

この修正のインストール後、wwwroot\Directorフォルダーでweb.configファイルを次のように構成する必要があります。

[appSettings] セクションで次の行を追加します。

値は秒単位でタイムアウトを指定します。

[#LC4467]

- ユーザーを選択してこのユーザーのセッション詳細を表示しようとする、画面の左上隅のユーザー名が「NULL」と表示されることがあります。

[#LC4589]

- NetBiosドメイン名にアンパサンド (&) が含まれている場合、Citrix Directorコンソールからのシャドウが失敗することがあります。この問題は、アンパサンドがXMLの予約文字であるために発生し、これにより現在のログオンの解析が失敗する可能性があります。

[#LC4633]

- 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ポリシー

- Citrix Director管理者がセッション詳細でCitrixポリシーを表示できないことがあります。

[#LC3941]

- 複数のセッションプリンターを [プリンター割り当て] ウィンドウでユーザーデバイスのグループに追加しようとする、拡張とスクロールバーの表示が失敗します。その結果、ユーザーデバイスのグループへの複数のセッションプリンターの追加が失敗することがあります。

[#LC4658]

- Citrix Director管理者がセッション詳細でCitrixポリシーを表示できないことがあります。

[#LC4956]

Citrix Studio

- Machine Creation Serviceを使用してServer OSのVDAを列挙すると、Personal vDiskストレージを使用できないことによりカタログの [CleanOnBoot] プロパティが [False] に設定されることがあり、これは正しくありません。その結果、カタ

ログのアップデートが失敗することがあります。

[#LC2959]

- Citrix Studioのデリバリーグループにおいて複数のフォルダーで複数のアプリケーションを作成すると、フォルダー構造が大きくなることがあります。初めてCitrix Studioを開いてフォルダーまたはアプリケーションをクリックしたときに、フォルダーやアプリケーションが選択されずにドラッグされることがあります。これにより、選択したオブジェクトがドラッグされ、フォルダーやアプリケーションの構造が変更されます。

[#LC3705]

- データベース管理者グループのメンバーではないユーザーがCitrix Studioを開こうとすると、SQL Serverで権限エラーが発生することがあります。

[#LC4127]

- 追加リソースをApp Orchestration 2.6のマルチテナントオフリングにプロビジョニングしようとする、オフリングに既に2つ以上のテナントが含まれている場合は失敗する可能性があります。

[#LC4170]

- 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。

[#LC4481]

- Citrix StudioからマシンをMachine Catalogに追加しようとする、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]

Controller

- VMware Vsphere Hypervisorに接続されたVDA for Server OSのスケジュールによる再起動を実行すると、サーバーがシャットダウンし、電源オフの状態になることがあります。

- 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\DesktopServer Client\RebootSchedule
値の名前：ShutdownTimeoutRecovery
種類：REG_DWORD
値のデータ：1

- この修正を無効にするには、以下のレジストリキーを設定します。
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer Client\RebootSchedule
値の名前：ShutdownTimeoutRecovery
種類：REG_DWORD
値のデータ：0

値を設定した後で、Broker Serviceを再起動する必要があります。

[#LC3807]

- データベース管理者ユーザーグループのメンバーでないユーザーがCitrix Studioを開こうとすると、SQL Server上で権限エラーが発生することがあります。

[#LC4127]

- Controllerで、「SupportMultipleForest」設定でNTLM認証が許可されている場合、Windows Communication Foundation (WCF) のEndpointReferenceにそのサービスプリンシパル名 (Service Principal Name : SPN) が設定されていないことが原因で、Linux VDAでの登録プロセスが失敗することがあります。

[#LC4235]

- Delivery Controllerがオフラインまたは使用不可になると、Citrix Studioの動作が遅くなるがありました。

[#LC4481]

- WaitForTask応答により、マシンカタログの更新を許可しない例外VmApi.MissingPropertyが発生します。

[#LC4573]

- 夏時間との切り替えが行われる時間範囲内にPowerShellコマンド「Get-LogSummary」を実行すると、次のエラーメッセージが表示されます。

「同一のキーを含む項目が既に追加されています。」

この問題は、夏時間により、ローカルの日付または時刻があいまいになる場合に発生します。結果的に、HashMapに重複するエントリが作成され、例外が発生します。

この修正では、夏時間の開始時刻と終了時刻をそれぞれ含む期間に分割するように通知するメッセージを導入されました。

[#LC4612]

- アマゾンウェブサービス (AWS) 環境でマシンカタログを更新しようとすると、断続的に失敗することがあります。修正を有効化するには、マシンカタログの更新時にイメージ準備段階がスキップされるように、コマンド「Set-ProvServiceConfigurationData -Name ImageManagementPrep_DoImagePreparation -Value \$false」を実行する必要があります。

[#LC4709]

- 多数のアプリおよびVDAプロセスが実行されている場合、Controllerとデータベースの接続が切断されることがあります。接続が切断された場合、VDAは初期化状態になり、アプリケーションを利用できなくなります。

[#LC4848]

- 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]

- この修正により、コントローラーがWebプロキシ経由でAmazonのパブリックAPIエンドポイントから孤立するとMachine Creation ServicesのプロビジョニングがAmazon Web Servicesで機能しなくなるという問題が解消されます。

[#LC5109]

HDX MediaStream Flash リダイレクト

- HDX MediaStream for Flashを有効にすると、FlashコンテンツのあるInternet Explorerで複数のタブを開いたり閉じたりすることによってInternet Explorerが予期せず終了することがあります。

[#LA3065]

- HDX MediaStream for Flashを有効にすると、Internet Explorerで複数のタブを開いたり閉じたりすることによってInternet Explorerが予期せず終了することがあります。

[#LC1141]

- HDX MediaStream Flashリダイレクトを有効にすると、pseudoserverinproc2.dllの実行中にMicrosoft Internet Explorerが予期せず終了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作成します。

- *Windows 32ビットシステムの場合:*
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
値の名前: AllowCOMObjectTrack
種類: REG_DWORD
値のデータ: 0
- *Windows 64ビットシステムの場合:*
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
値の名前: AllowCOMObjectTrack
種類: REG_DWORD
値のデータ: 0

[#LC1885]

- HDX MediaStream Flashリダイレクトが有効な状態でWebサイトを閲覧する場合に、
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\ApplInit_DLLsのレジストリ値が
「mfaphook.dll」または「mfaphook64.dll」へのフルパスではなく「mfaphook.dll」または「mfaphook64.dll」に設定されていると、Flashリダイレクト機能でエラーが発生します。

[#LC4388]

Provisioning Services 7.9

StoreFront 3.6

Universal Print Server

クライアント

サーバー

クライアント

- Universal Print Serverに印刷しようとする、NextGenアプリケーションでエラーが発生することがありました。

[#LC4246]

サーバー

- Microsoft GDI Print APIを使用した一括印刷が失敗して最後のページが印刷されず、次のエラーメッセージが表示されるこ

とがありました。

「Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check Printer」

[#LC3920]

- この修正により、Universal Print Server 7.6.300向けのCitrix UPSプリンタードライバー証明ツールがサポートされます。詳しくは、Knowledge Centerの[CTX142119](#)を参照してください。

[#LC4265]

VDA for Desktop OS

スマートカード

HDX MediaStream Windows Mediaリダイレクト

システムの例外

印刷

ユーザーエクスペリエンス

セッション/接続

ユーザーインターフェイス

HDX MediaStream Windows Mediaリダイレクト

- ICAセッション（または公開デスクトップセッション）内でWindows Media Playerを使用して.aviファイルを再生し、最初に再生した.aviファイルを停止せずに別の.aviファイルを再生すると、ビデオのフレームがユーザーデバイスで適切に配置されないことがありました。これにより、mmvdhost.exeプロセスのCPU使用率が通常より高くなり、ビデオがユーザーデバイスで適切にレンダリングされなくなる可能性があります。

[#LC4260]

- HDX MediaStream Windows Mediaリダイレクトが有効な状態で、Windows 10で実行中のVDAでファイルをレンダリングすると、特定のサードパーティ製プレーヤーが異常終了するという問題がありました。

[#LC5110]

印刷

- Citrix印刷スプーラーサービスが異常終了することがありました。

[#LC4180]

- 公開アプリケーションで「自動作成クライアントプリンター」ポリシーがデフォルトのプリンターを正しく設定できず、Microsoft XPSドキュメントライターがデフォルトのプリンターとして設定されるという問題がありました。

[#LC4696]

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

入力した文字が1002文字を超過すると発生します。

[#LC1144]

- 複数のWebカメラやビデオキャプチャーデバイスがエンドポイントにインストールされると、インストールされたデバイスのうち1つだけがクライアントセッションにマップされます。さらに、このデバイスはCitrix HDX Webカメラとしてマップされ、どのデバイスがマップされているかの手掛かりがありません。

[#LC1919]

- 特定のサードパーティ公開アプリケーションをXenAppサーバーで起動できないことがありました。これにより、wfshell.exeプロセスが予期せず終了します。このエラーが発生すると、ユーザーデバイスではセッションが開始されたというメッセージが表示されないか、エラーメッセージが表示されます。

[#LC3766]

- マルチモニターセッションでThomson Reuters Eikonツールバーのドックを解除した後、ツールバーが占有していたスペースはセッションに回復されません。

プライマリモニターがアレイの左上隅に配置されていないモニター構成では、Receiver for Windows 4.4以降に含まれる修正#LC1599もインストールする必要があります。

[#LC3773]

- App-V構成設定「EnablePublishingRefreshUI」がセッションホストで有効であり、「セッションの残留」も有効な場合、iOSデバイスでアプリケーションを終了しようとするデバイスの画面が黒い画面のままになります。

[#LC3800]

- ICAセッション中にリモートPCの電源をオフにするか強制的に再起動すると、リモートPCの再起動が完了したときに、すべてのオーディオドライバーが無効になっていることがありました。

[#LC4071]

- Hotfix ICAWS760WX6403をインストールしてSSLを有効にすると、VDAへの再接続が断続的に失敗するという問題がありました。この問題は、Citrix ICA Serviceが異常終了したり、SSLリスナーのエラーにより応答不能となったりした場合に発生します。

[#LC4438]

- VDAとCitrix Receiver間のネットワーク中断後、Windows Media Playerで.aviファイルを再生できなくなります。

[#LC4670]

- 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]

- この修正により、DirectShowベースのアプリケーションのクライアント側での取得が失敗し、ビデオをレンダリングできないという問題が解決されます。

[#LC5098]

スマートカード

- Microsoft Internet Explorerで、特定のWebサイトに対するスマートカードログオンのユーザーインターフェイスが断続的に使用できなくなるという問題がありました。

[#LC3988]

- Windows 10 Build 10586以降で実行されているバージョン7.6.300以降のVDAでサインインオプションが表示されないという問題がありました。その結果、スマートカードログオンを実行できません。

[#LC4778]

システムの例外

- サーバーのctxad.sysで、バグチェックコード0xD1によるブルースクリーンエラーが発生することがありました。

[#LC4007]

- Windows Media Playerで.aviファイルを繰り返し再生すると、wfica32.exeプロセスのメモリ消費が増加し続けてプロセスが異常終了するという問題がありました。

[#LC4335]

- レジストリキーHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcessesが定義されている場合、VDAを再起動して公開デスクトップを開始するとブルースクリーンエラーが発生することがありました。

[#LC4597]

- MobileDesktopHook64.dllで発生する例外「c000041d」により、公開アプリケーションプロセスが異常終了することがありました。

[#LC4821]

ユーザーエクスペリエンス

- タッチパネルでの操作に最適化された公開デスクトップから通常の公開デスクトップに切り替えると、スタートボタンで次の問題が発生することがありました。

- マウスを合わせても強調表示されない
- 公開デスクトップではなくローカルデスクトップが表示される

[#LC3466]

ユーザーインターフェイス

- シームレスなアプリケーションを公開した後、タスクバーに公開アプリケーションのアイコンではなく一般的なCitrix Receiverアイコンが表示されるという問題がありました。

[#LC4757]

VDA for Server OS

[HDX MediaStream Windows Media リダイレクト](#)

[スマートカード](#)

[印刷](#)

[システムの例外](#)

HDX MediaStream Windows Mediaリダイレクト

- ICAセッション（または公開デスクトップセッション）内でWindows Media Playerを使用して.aviファイルを再生し、最初に再生した.aviファイルを停止せずに別の.aviファイルを再生すると、ビデオのフレームがユーザーデバイスで適切に配置されないことがありました。これにより、mmvdhost.exeプロセスのCPU使用率が通常より高くなり、ビデオがユーザーデバイスで適切にレンダリングされなくなる可能性があります。

[#LC4260]

- HDX MediaStream Windows Mediaリダイレクトが有効な状態で、Windows 10で実行中のVDAでファイルをレンダリングすると、特定のサードパーティ製プレーヤーが異常終了するという問題がありました。

[#LC5110]

印刷

- Citrix印刷スプーラーサービスが異常終了することがありました。

[#LC4180]

- 従来のプリンター名が有効な状態で、同一ユーザーに対して1つのサーバーで複数のセッションが確立されると自動作成されたプリンターが公開アプリケーションで使用できないということがありました。

[#LC4517]

- プリンターリダイレクトで断続的にエラーが発生することがあります。

[#LC4584]

- 公開アプリケーションで「自動作成クライアントプリンター」ポリシーがデフォルトのプリンターを正しく設定できず、Microsoft XPSドキュメントライターがデフォルトのプリンターとして設定されるという問題がありました。

[#LC4696]

サーバー/サイトの管理

- 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]

- 個別のユーザーデバイスがVDAに対して複数のリモートデスクトップ（RDP）接続を同時に試行すると、VDAが登録解除されるという問題がありました。

[#LC4014]

セッション/接続

- クライアントオーディオリダイレクトまたはWindows Mediaリダイレクトが無効の状態で、公開デスクトップセッション

の通知領域のボリュームコントロール（スピーカー）アイコンに、正しくないオーディオステータスが表示されることがありました。

[#LC2538]

- デフォルトで、以前手動で削除したWindowsクイックアクセスの「デスクトップ」および「ダウンロード」のショートカットが、ログオン時に%userprofile%\Linksで再び作成されるという問題がありました。この動作が望ましくないシナリオもあります。この修正により、以下のレジストリキーを0（ゼロ）に設定すると、これら2つのショートカットが自動的に再作成されなくなります。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell

値の名前：CreateShortcutLinks

種類：REG_DWORD

値のデータ：0

[#LC3274]

- この修正により、マップされたクライアントデバイスに書き込み中のファイルが破損するという問題が解決されます。

[#LC3684]

- 特定のサードパーティ公開アプリケーションをXenAppサーバーで起動できないことがありました。これにより、wfshell.exeプロセスが予期せず終了します。このエラーが発生すると、ユーザーデバイスではセッションが開始されたというメッセージが表示されないか、エラーメッセージが表示されます。

[#LC3766]

- マルチモニターセッションでThomson Reuters Eikonツールバーのドックを解除した後、ツールバーが占有していたスペースはセッションに回復されません。

プライマリモニターがアレイの左上隅に配置されていないモニター構成では、Receiver for Windows 4.4以降に含まれる修正#LC1599もインストールする必要があります。

[#LC3773]

- Excelhookを有効にして、複数のExcelワークブックを開いて最小化すると、いずれかのワークブックを選択して画面に表示することができなくなるという問題がありました。

[#LC3799]

- App-V構成設定「EnablePublishingRefreshUI」がセッションホストで有効であり、「セッションの残留」も有効な場合、iOSデバイスでアプリケーションを終了しようとするときデバイスの画面が黒い画面のままになります。

[#LC3800]

- クライアントオーディオリダイレクトポリシーを有効にしても、オーディオ（.wav）ファイルの再生に失敗することがありました。この問題は、セッションIDが再利用されており、クライアントオーディオリダイレクトのポリシーが以前のセッションに対して無効になっていた場合に発生します。

[#LC3882]

- （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]

- Microsoft Internet Explorerの公開インスタンスを使用してWebサイトからファイルをダウンロードしてそのファイルをマップされたクライアントドライブに保存（[名前を付けて保存]）しようとすると、失敗することがありました。

[#LC4300]

- icaendpoint.dllファイルによってWindowsオーディオサービスが異常終了することがありました。

[#LC4356]

- 別のプロセスによってpicadms.sysと同じロックが保持されている場合、ユーザーはセッションからログオフできず、セッションは切断された状態のままとなります。

[#LC4415]

- 修正#LC0615がインストールされているシステムで、セッションのログオフに想定よりも時間がかかることがありました。

[#LC4674]

- 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
値の名前: 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
値の名前: 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]

- この修正により、DirectShowベースのアプリケーションのクライアント側での取得が失敗し、ビデオをレンダリングできないという問題が解決されます。

[#LC5098]

スマートカード

- Microsoft Internet Explorerで、特定のWebサイトに対するスマートカードログオンのユーザーインターフェイスが断続的

に使用できなくなるという問題がありました。

[#LC3988]

- Windows 10 Build 10586以降で実行されているバージョン7.6.300以降のVDAでサインインオプションが表示されないという問題がありました。その結果、スマートカードログオンを実行できません。

[#LC4778]

システムの例外

- Windows Media Playerで.aviファイルを繰り返し再生すると、wfica32.exeプロセスのメモリ消費が増加し続けてプロセスが異常終了するという問題がありました。

[#LC4335]

- レジストリキーHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcessesが定義されている場合、VDAを再起動して公開デスクトップを開始するとブルースクリーンエラーが発生することがありました。

[#LC4597]

- MobileDesktopHook64.dllで発生する例外「c000041d」により、公開アプリケーションプロセスが異常終了することがありました。

[#LC4821]

ユーザーエクスペリエンス

- タッチパネルでの操作に最適化された公開デスクトップから通常の公開デスクトップに切り替えると、スタートボタンで次の問題が発生することがありました。
 - マウスを合わせても強調表示されない
 - 公開デスクトップではなくローカルデスクトップが表示される

[#LC3466]

- Microsoft Excelウィンドウをシームレスなデュアルモニターセッション内で移動しようとする、新しい場所でのウィンドウの再表示に時間がかかることがありました。

[#LC4441]

ユーザーインターフェイス

- シームレスなアプリケーションを公開した後、タスクバーに公開アプリケーションのアイコンではなく一般的なCitrix Receiverアイコンが表示されるという問題がありました。

[#LC4757]

仮想デスクトップコンポーネント - その他

- 構成済みの作業ディレクトリが存在しない場合、App-Vの統合機能を使用するアプリケーションが起動できないことがありました。

既知の問題

Aug 26, 2016

レジストリエントリの変更を伴う回避策については、次の点に注意してください。

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ます、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。

XenAppおよびXenDesktop

XenAppおよびXenDesktop 7.9のリリースには、以下の問題が含まれます。

- エンドポイントでUSBリダイレクトポリシーを有効にした状態でUSB大容量記憶装置デバイスを使用すると、デバイスをイジェクトしようとしたときに「Device in use」というエラーメッセージが表示されることがあります。
 - リモートPCアクセス環境では、コマンドラインからVDAを再インストールします。これにより、このエラーは発生しなくなります。
 - 他の環境でこの問題を回避するには、以下のいずれかを行います。
 - 汎用の代わりに最適化された仮想チャネルリダイレクトを使用します。これにより、USBデバイスをクライアントマシンからイジェクトできるようになります。CTX137939と「[USBデバイスリダイレクト](#)」を参照してください。
 - USBデバイスで、Windowsを使用してキャッシュの書き込みを無効にし、デバイスを迅速に削除できるように最適化します。詳しくは、Microsoft社のドキュメントを参照してください。[#628442]
- Delivery Controllerをインストールしたサーバーに、既にSQL Server Express 2008 R2（サービスパックなし）がインストールされていた場合、サイトの作成中にStudioでエラーが発生します。（この問題は、サイト、ログ、監視データベースにこのデータベースを使用していない場合にも発生します。）この問題を回避するには、Controllerをインストールする前に、SQL Server Express 2008 R2サービスパックをインストールするか、SQL Server Express 2008 R2をアンインストールします。[#632483]
- AppDiskの作成に使用するマシンに現在のListOfDDCs（Delivery Controllerの一覧）がない場合、ControllerからのAppDisk作成要求が、認識されないことがあり、この要求が失敗します。このようなマシンでは、通常の自動更新機能は動作しません。ポリシー設定またはレジストリを使用してListOfDDCsを手動で更新する必要があります（「Delivery Controller」を参照してください）。[#63341]
- サイトを作成するときに、サイトのデータベースとして使用する目的でSQL Server Expressデータベース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）、データベース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。[#634316]
- マシンに最新のWindows更新プログラムがインストールされていない場合、Windows Server OSへのVDAインストールが失敗することがあります。（Windows Server 2008R2マシンの更新プログラムに、KB2685811の更新プログラムが含まれている必要があります。それより新しいサポート対象OSにはこれらの更新プログラムは含まれています。）[#635456]
- Studioのナビゲーションパネルで「構成」>「ライセンス」を選択して「操作」ペインで[ログオン]をクリックすると、権限がない場合はStudioのスナップインがクラッシュします。修復するには、Studioを再起動します。（ライセンスサーバーは、ライセンス管理コンソールから直接管理できます。）[#640925]
- App-VサーバーがStudio内に構成されている場合、Studioを閉じるとMicrosoft管理コンソール（MMC）がクラッシュする場合があります。[#652949]
- OSとライトバックキャッシュの両方にローカルストレージを使用している場合は、両方で同じストレージを使用していることを確認してください。ライトバックキャッシュ用ストレージの一覧に、OSストレージには使用できないストレージが含まれている場合は、カタログの作成中にエラー「ファイル<データストア>が見つかりません」が表示される可能性があります。[#637430]
- Windows 10マシンを使用してAppDiskを作成すると、封印プロセスが正常に終了しないことがあります。これを回避するには、（PowerShell Remove-AppLibAppDiskコマンドレットを使用して）AppDiskを削除し、再びAppDiskを作成します。[#633998]
- XenAppおよびXenDesktopの全製品インストーラーを使用したStoreFrontのアップグレードが正常に完了しないことがあります。この現象が繰り返されないようにするには、StoreFrontサーバーを再起動して潜在的なファイルのロックを取り除いてから、Citrix管理コンソールやPowerShellセッションを開かずにインストーラーを実行します。[#641242]
- バージョン7.5（または7.5からアップグレードした7.6）からアップグレードすると、Studioまたは高レベルのSDKの起動に失敗することがあります。回避策：Studio MSI（[XDInstallerRoot]\x64\DesktopStudio\DesktopStudio_x64.msi）または高レベルのSDK MSI（[XDInstallerRoot]\x64\Citrix Desktop Delivery Controller\XDPoshSnapin.msi）の修復インストールを実行します。[#617897]
- 大規模なサイトでは、期限切れのSQL統計や断片化されたインデックスにより、StudioおよびDirectorでパフォーマンスの問題が発生することがあります。これら回避するには、データベース管理者が、オフピーク時間帯にSQL Serverメンテナンスプランを実行する必要があります。保守プランには、サイト、監視、および成ログデータベースでの、インデックスと統計の再構築を含める必要があります。詳しくは、SQL Serverバージョンのメンテナンスプランのドキュメントを参照してください。[#641889]
- デリバリーグループが削除済みで、そのデリバリーグループが選択されている場合、削除されたデリバリーグループのロ

グオン処理時間がグラフで「n/a」と表示され、表に行が表示されません。 [#615106]

- [傾向] > [容量管理] > [ホストされたアプリケーションの使用量] で使用期間またはユーザー別にソートするとエラーが発生します。この問題を解決するには、Directorを再起動する必要がありました。 [#640508]
- マウスホイールを使用してFramehawkセッションの内側をクリックした場合、予想した結果が得られないことがあります。 [#625408]
- Intel Iris Pro Graphics内蔵Intel CPUを使用するリモートPCアクセスの展開でHDX 3D Pro VDAを切断すると、コンソールモニターの明るさが低下します。これはサードパーティ製品の問題です。これを回避するにはリモートPCアクセスデバイスを再起動して、モニターの明るさを復元します。 [#633101]
- HDX 3D Pro VDAによるWindows 10 (32ビットのみ) リモートPCアクセス展開で、Intelドライバーバージョン20.19.15.9999をインストールするとリモートPCアクセスデバイスが起動しなくなります。これはサードパーティ製品の問題です。この問題を回避するには、Windows更新プログラムからのドライバーを使用します。 [#637294] 注：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。標準またはHDX 3D ProモードでのVDAの構成について詳しくは、「[インストールの準備](#)」を参照してください。
- .NET 4.5.2のインストール後、XenAppおよびXenDesktopがインストールを続行しません。この問題は、Windows Server 2008 R2で確認されています。回避策としては、手動で.NET 4.5.2をインストールしてからインストールを再試行します。 [#633721]
- (マウスとキーボードを除く) タッチパッドなどのUSBヒューマンインターフェイスデバイス (HID) が複数接続されているリモートPCセッションの実行中にUSB HIDをアンプラグし、セッションを切断して再接続してからプラグインし直すと、USB HIDが無効のままとなります。この問題を解決するには、デバイスマネージャーでHIDを有効にしてください。 [#638766]
- Thinwire互換モードでビデオを複数のモニター間ドラッグすると、一部のグラフィックが破損することがあります (この問題は3つ以上のマルチモニターセッションで確認されます)。 [#640437]
- ユーザーがSurface Proをシャットダウンすると、電源を再びオンにしたときにリモートPCアクセスを使用したHDX接続が機能しないことがあります。この問題を解決するには、マシンを再起動してください。 [#634830]
- Windows 8.1でSurface Proデバイスへの接続を確立する場合に、セキュアブートが有効になるとセッションの速度が最初の数分間低下することがあります。 [#634382]
- グラフィックインターフェイスの全製品インストーラーを使用してVDAをインストールするときにリモートPCアクセスを有効にすると、追加のコンポーネント (Machine Creation ServicesおよびProfile Management) がインストールされます。 [#637741] このリリースでは、コマンドラインをリモートPCアクセスのみに使用し、/componentsと/remotepcの構文の順序を変更しないでください。次に例を示します。

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE  
"AppDisks VDA Plug-in" /enable_hdx_ports /noreboot /quiet
```

/remotepcが/componentより前に使われると、/remotepcオプションは無視されます。コマンドラインオプションについて詳しくは、「[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。

Windows Server 2016 Tech Preview

このXenAppおよびXenDesktopのリリースをWindows Server 2016 Tech Previewで使用したときに発生することが確認されている問題の一覧については、「[Windows Server 2016 Tech Previewフォーラム](#)」を参照してください (Citrixアカウントへのログインが必要です)。

その他のコンポーネント

XenAppおよびXenDesktopのダウンロードページから個別に入手できるコンポーネントには、以下の問題があることが確認

れています。

Session Recording

- 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グループ] > [グループ] > [ユーザー] の順に選択して、ユーザーにこのフォルダーへの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。 [#611487]
- Session RecordingではFramehawkの表示モードがサポートされないため、Framehawkの表示モードのセッションは正しく録画および巻き戻しされません。 この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ていない可能性があります。 [#622085]
- 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。 回避策：グループポリシーオブジェクトをCitrix Receiver for Windowsをインストールしたマシンに展開することで、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の無効化について詳しくは、<http://support.citrix.com/article/CTX123169>および<http://docs.citrix.com/en-us/receiver/windows/4-4/ica-overview-receiver-config/ica-import-icaclient-template-v2.html>を参照してください。 [#618237]
- ロールオーバーの設定は、XenDesktop 7.8、XenDesktop 7.9、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。 [#584890]
- Machine Creation Services (MCS) またはProvisioning Services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、それらのVDAのQMIDは同じになります。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 Serverによって受信されず、セッションが常にライブステータスになってしまう可能性があります。 [#528678]

VDAごとに固有の永続的なQMIDを作成するための解決策は、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またはそれ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。

MCSまたはPVSによって作成されたサーバーOSのVDA、またはMCSによって静的デスクトップモードで作成された専用デスクトップOSのVDA（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された専用デスクトップOSのVDA）では、スクリプト（GenQMID.ps1）を使用してシステムの起動時にQMIDを変更します。

MCSまたはPVSによって作成され、ユーザーがログオフするとすべての変更が削除されるように構成されたデスクトップOSのVDAでは、別のスクリプト（GenRandomQMID.ps1）を使用してシステムの起動時に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。

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。

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At system startupに設定して、Provisioning Services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:\GenQMID.ps1

または

powershell .exe -file C:\GenRandomQMID.ps1

GenQMID.ps1の概要：

1. マシンのUUIDのハッシュ値に基づいてQMIDを生成します。
2. CitrixSmAudAgentやMSMQなどの関連サービスを停止します。
3. 以前に停止したサービスを開始して、QMIDの変更を適用します。

GENQMID.PS1（参照用）：

コピー

```
function ConvertHexStringToByte($theString)

{

    $bytes = New-Object Byte[] ($theString.Length / 2)

    for ($i = 0; $i -lt $theString.Length; $i += 2) {

        $bytes[$i / 2] = [System.Convert]::ToByte($theString.Substring($i, 2), 16)

    }

    return $bytes

}

Try {

    # Get UUID of machine

    $strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Property UUID).UUID

    # Remove "-"

    $strUUID = $strUUID.ToString().Replace("-", "")

}
```



```

# Convert string to bytes

$UUID = ConvertHexStringToByte($strUUID)


# Set UUID as QMId

$new_QMID = $UUID

}

Catch {

# IF exception occurred, just use MD5 digest of FQDN as QMID


# Get FQDN

$fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName


# Calculate MD5 hash of FQDN

$md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider


# Set md5 digest as QMID

$utf8 = new-object -TypeName System.Text.UTF8Encoding

$new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))

}


# Write new_QMID into registry

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name "QMId" -Value $new_QMID


# Restart MSMQ to adopt new QMId

```

```
# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

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

        }

    }

}
```

GenRandomQMID.ps1の概要：

1. レジストリから現在のQMIDを削除します。
2. HKLM\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. 以前に停止したサービスを開始して、ランダムなQMIDを生成します。

GENRANDOMQMID.PS1（参照用）：

コピー

```
# 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

        }

    }

}

}
```

- 4096 x 4096以上の解像度でセッションを録画すると、録画にフラグメントが表示される場合があります。[#524973]
- XenAppまたはXenDesktopのライセンスの種類を変更しても、その変更がSession Recordingにすぐに反映されません。 解決策：VDAマシンを再起動します。[#532393]
- Session Recordingにおける事前起動されたアプリケーションセッションのサポート制限[#561109]
 - 問題点：
 - 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に、事前起動されたセッションで起動されたアプリケー

セッションは照合されないため、セッションは録画されません。

- 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Windows Receiver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、空のセッションと、後にそのセッションで起動されたすべてのアプリケーションが録画されます。
- 回避方法：
 - 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を使用しないでください。このようにすることで、事前起動セッションが録画されるようになります。ただし、通知は表示されます。

このリリースに含まれていない機能

Jul 07, 2016

ヒント：最後に使用したXenAppがリリース6.5以前である場合は、[こちらの説明](#)を参照して、アーキテクチャ、用語、要素の差異も確認してください。

以下の機能は、このリリースでは提供されません（サポートされない機能など）。

- **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Windows 10マシンでは無効になっています。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。
- **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。
 - 従来のクライアントプリンター名を使用する機能を含む、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。サーバー上のユーザープロファイルに保存されます。
- **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。
- **電源能力管理** - 7.xより前のリリースでは、電源の消費を減らし、サーバーの能力を管理するために、電源能力管理機能を使用できました。このリリースでは、Microsoft Configuration Managerを使用してこれを行います。
- **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。
- **Smart Auditor** - 7.xより前のリリースでは、Smart Auditorを使用してユーザーセッションの画面上のアクティビティを記録できました。7.6 Feature Pack 1以降、この機能はSession Recordingにより提供されます。
- **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およびWindows Server 2012環境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。CitrixダウンロードWebサイト (<http://citrix.com/downloads>) で見つけることができます
- **Oracleデータベースのサポート** - このリリースでは、SQL Server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** - このリリースでは、SCOMを使ってサーバーファームのアクティビティを監視する管理パックはサポートされていません。
- **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、ポリシーを作成することにより無効にできます。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Studioでは、この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PowerShellスクリプト** - リモートPCは、StudioおよびControllerに統合されました。
- **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ック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。
- **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。
- **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。

Citrix Receiverに含まれていない機能またはデフォルト値が異なる機能

- **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** - 以下のプロキシはサポートされなくなりました。
 - 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)。

サードパーティ製品についての通知

Jul 07, 2016

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。

- [XenApp 7.9 and XenDesktop 7.9 Third Party Notices](#)
- [FLEXnet Publisher Documentation Supplement Third Party](#)およびFlexNet Publisher 11.13.1で使用されるオープンソースソフトウェア
- [Linux Virtual Desktop Version 1.2のサードパーティ製品についての通知](#)

システム要件

Aug 26, 2016

ここでは次のことについて説明します。

- [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
- Other

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。

インストールに必要なディスクスペースの値は参考値であり、製品イメージ、オペレーティングシステム、およびその他のソフトウェア用の容量は含まれていません。

すべてのコアコンポーネント（ControllerとSQL Server Express、Studio、Director、StoreFront、およびライセンス）を単一のサーバーにインストールする場合、製品評価のため最低4 GBのRAMが必要です。ユーザー用の環境を実行する場合は、より多くのRAMが推奨されます。性能は、ユーザー、アプリケーション、デスクトップ、およびその他の要因の数など、実際の構成により異なります。

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。

Delivery Controller

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の現在のTechnology Preview：このリリースでは、このオペレーティングシステムを評価目的でのみサポートしていますが、実稼働環境での使用についてはサポートしていません。
- 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もサポートされます)。
- Windows PowerShell 2.0 (Windows Server 2008 R2に付属) または3.0 (Windows Server 2016 TechnologyPreview、Windows Server 2012 R2、およびWindows Server 2012に付属)。
- Visual C++ 2008 SP1再頒布可能パッケージ
- 100MBの空きディスク容量。

オプションの機能を使用すると、必要なディスクスペースが増加します。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。

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 2016のExpress、Standard、およびEnterprise Edition。
- SQL Server 2014のSP2、Express、Standard、およびEnterprise Edition。
- SQL Server 2012のSP3、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 2012 SP2 Expressがインストールされます。
- 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機能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クラスター化インスタンス
- SQL Serverミラーリング
- SQL Server 2012 AlwaysOn可用性グループ

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

詳しくは、「[データベース](#)」の記事および[CTX114501](#)を参照してください。

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。

- Windows 10、Professional、Enterprise、およびEducationalエディション。

- Windows 8.1、Professional、およびEnterpriseエディション。
- Windows 8、Professional、およびEnterpriseエディション。
- Windows 7 Professional、Enterprise、およびUltimateエディション。
- Windows Server 2016の現在のTechnology Preview：このリリースでは、このオペレーティングシステムを評価目的でのみサポートしていますが、実稼働環境での使用についてはサポートしていません。
- 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：

- 75 MBの空きディスク容量。
- Microsoft .NET Framework 4.5.2（4.6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（Windows 7およびWindows Server 2008 R2に付属）または3.0（Windows 10、Windows 8.1、Windows 8、Windows Server 2016 Technology Preview、Windows Server 2012 R2、およびWindows Server 2012に付属）。

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の現在のTechnology Preview：このリリースでは、このオペレーティングシステムを評価目的でのみサポートしていますが、実稼働環境での使用についてはサポートしていません。
- 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：

- 140MBの空きディスク容量。
- Microsoft .NET Framework 4.5.2（4.6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サーバーの役割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。

- Internet Explorer 11以降。Internet Explorer 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。Internet Explorerの互換モードはサポートしていません。Directorを表示するには、Webブラウザ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ときに、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を表示するための推奨画面解像度は1366×1024です。

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、Professional、Enterprise、およびEducationalエディション Windows 10では、標準モードで構成されたVDAのGPUアクセラレーション、デスクトップコンポジションのリダイレクト、従来のグラフィックモード、セキュアブート（リモートPCアクセスでのみサポートされます）、VM Hosted Appを使用したユニバーサルなWindowsアプリケーションの公開はサポートされません。
- Windows 8.1、Professional、およびEnterpriseエディション。
- Windows 8、Professional、およびEnterpriseエディション。
- Windows 7 SP1、Professional、Enterprise、およびUltimateエディション。

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。手順については、「[サーバーVDI](#)」を参照してください。

- Windows Server 2016の現在のTechnology Preview：このリリースでは、このオペレーティングシステムを評価目的でのみサポートしていますが、実稼働環境での使用についてはサポートしていません。
- 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もサポートされます）。
- Microsoft .NET Framework 3.5.1（Windows 7のみ）
- Microsoft Visual C++ 2008 SP1、2010 SP1、および2013のRuntime（32ビットおよび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Virtual Delivery Agent (VDA) では、Windows 10および8.1でのXenDesktopリモートPCアクセス向けのセキュアブートをサポートされます。

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。

VDAをインストールするときに、VDA for Windows Desktop OSのHDX 3D Proバージョンのインストールを選択できます。このバージョンは、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。

Windows XPまたはWindows Vistaが動作するマシン上にこのバージョンのVDAをインストールすることはできません。これらのオペレーティングシステムが必要な場合は、以前のバージョンのVirtual Desktop Agentをインストールできます。詳しくは、[CTX140941](#)を参照してください。このリリースのリモートPCアクセスは、Windows Vistaをサポートしません。

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の現在のTechnology Preview：このリリースでは、このオペレーティングシステムを評価目的でのみサポートしていますが、実稼働環境での使用についてはサポートしていません。
- 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もサポートされます）。
- Microsoft .NET Framework 3.5.1（Windows Server 2008 R2のみ）
- Microsoft Visual C++ 2008 SP1、2010 SP1、および2013のRuntime（32ビットおよび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なくなります。Windows Server 2012 R2、Windows Server 2012、およびWindows Server 2008 R2のほとんどのエディションでは、サーバーマネージャーによりMedia Foundation機能がインストールされます（Windows Server 2012 R2およびWindows Server 2012の場合はServerMediaFoundation、Windows Server 2008 R2の場合はDesktopExperience）。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。

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とVMware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。

[CTX131239](#)に、ハイパーバイザーバージョンの追加のサポート情報が記載されています。

サポートされるホストプラットフォームは、以下のとおりです。

XenServer

- 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。vSphere vCenterのリンクモードはサポートされません。

- VMware vSphere 6.0およびUpdate 1および2
- VMware vSphere 5.5およびUpdate 1～3
- VMware vSphere 5.1 Update 2および3
- VMware vSphere 5.0 Update 2および3
- VMware vCenter 5.5 / 6アプライアンス

System Center Virtual Machine Manager - これらのSystem Center Virtual Machine ManagerをサポートするHyper-Vのバージョンを含みます。

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

Nutanix Acropolis 4.5。このプラットフォームを使用している場合は、複数のXenAppおよびXenDesktop機能を実行できません。詳しくは、[CTX202032](#)を参照してください。Acropolisがある製品の使用について詳しくは、<https://portal.nutanix.com/#/page/docs>を参照してください。

サポートされるクラウド環境は、以下のとおりです。

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。
- AWSでは、SQL Server 2012 Enterprise Editionを使用できません。
- AWSでは、デスクトップOSのインスタンスは提供されていません。
- 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。

Citrix 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

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が必要です。

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 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）

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せん。

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リダイレクト機能では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)。

- 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)。

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ときに、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パススルー機能は、Citrix XenServerで使用できます。また、VMware vSphereおよびVMware ESXでも、同様の仮想Direct Graphics Acceleration (vDGA) 機能を使用できます。
- vGPU機能は、Citrix XenServerおよびVMware vSphereで使用できます。www.citrix.com/go/vGPUを参照してください (CitrixのMy Account資格情報が必要です)。

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。
- サポートされるNVIDIA GRIDカードとHDX 3D Proを併用すると、NVIDIA GRID APIを使用してGPUフレームバッファアクセスを最適化できます (「[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。
- サポートされるIntelハードウェアプラットフォームおよびIntel Iris Pro GraphicsとHDX 3D Proを併用すると、Intel Media SDKを使用してGPUフレームバッファアクセスを最適化できます。サポートされるIntelプロセッサは、[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](#)です。
- HDX 3D ProでXenServerのvGPU機能を使用するための要件には、NVIDIA GRID K1およびK2カードが含まれています (「[NVIDIA GRID](#)」参照)。

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 2013および2010
- 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

その他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

このセクションでは、以下に対するシステム要件について説明します。

[Session Recording Administration](#)コンポーネント

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、同一サーバー上にインストールしたり、個別のサーバー上にインストールしたりできます。

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。

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

要件：.NET Framework Version 3.5 SP1（Windows Server 2008 R2のみ）、もしくは.NET Framework Version 4.5.2または4.6。

Session Recording Server

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。

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Session Recording Serverをインストールする前に、前提条件をインストールする必要があります。サーバーマネージャーから、IISロールを追加し、次のオプションを選択します。

- [Application Development] > [ASP.NET 4.5]（Server 2012およびServer 2012 R2の場合）、[ASP.NET]（Server 2008 R2の場合）その他のコンポーネントは自動的に選択されます。[追加]をクリックして、必須ロールに同意します。
- セキュリティ>Windows認証
- [管理ツール] > [IIS 6管理互換]（[IIS 6メタベース互換]、[IIS 6 WMI互換]、[IIS 6スクリプトツール]、および[IIS 6管理コンソール]）

その他の要件：

- .NET Framework Version 3.5 SP1（Windows Server 2008 R2のみ）、もしくは.NET Framework Version 4.5.2または4.6。
- 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)。

Session Recording Policy Console

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。

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

要件：.NET Framework Version 3.5 SP1（Windows Server 2008 R2のみ）、もしくは.NET Framework Version 4.5.2または4.6。

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。

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

要件：

- PlatinumライセンスのXenApp 7.8またはXenDesktop 7.8
- .NET Framework Version 4.5.2または4.6
- 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。

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

要件：.NET Framework Version 3.5 SP1（Windows 7のみ）、4.5.2、または4.6。

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
- 1GB 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 2012 R2および2012。
- Windows Server 2008 R2 SP1
- Windows Server 2008 32ビット

要件：Microsoft Visual C++ 2013ランタイム

Windows Server OS対応VDS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。

詳しくは、「[プリンターのプロビジョニング](#)」の記事を参照してください。

Other

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。すべてのコンポーネントをこの製品リリースのインストールメディアに収録されているバージョンにアップグレードすることをお勧めします。

- StoreFrontには2GBのメモリが必要です。システム要件については、StoreFrontのドキュメントを参照してください。この製品では、StoreFront 2.6以降がサポートされます。
- Provisioning Servicesを併用する場合、Provisioning Services 7.0以降がサポートされます。
- Citrixライセンスサーバーには40MBのディスク領域が必要です。システム要件については、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。Citrix License Server for Windowsのみサポートされます。必要な最小バージョンは11.13.1です。

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。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。

ローカルアプリケーションアクセス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。

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。

製品の技術概要

Aug 26, 2016

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提供したり制限したりできます。
- 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。

FMAの主要コンポーネント

一般的なXenApp/XenDesktop環境は、いくつかの主要コンポーネントで構成されます。これらのコンポーネントは、ユーザーがアプリケーションやデスクトップにアクセスすると連係して動作し、サイトでのアクティビティデータをログとして記録します。

Citrix Receiver : ユーザーデバイス上にインストールされるクライアントソフトウェアで、TCPポート80または443経由で仮想マシンに接続し、StoreFront Service APIを使用してStoreFrontと通信します。

Citrix StoreFront : ユーザーを認証するインターフェイスであり、アプリケーションやデスクトップを管理してアプリケーションストアをホストします。StoreFrontは、XMLを使用してDelivery Controllerと通信します。

Delivery Controller : XenAppおよびXenDesktopサイトの中心的管理コンポーネントで、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の負荷を最適化および分散したりするためのいくつかのサービスで構成されています。

Virtual Delivery Agent (VDA) : Windowsの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 (OS) のマシン上にインストールされるエージェントで、マシンやそのマシンでホストされるリソースをユーザーに提供します。WindowsサーバーOS上にインストールされたVDAは、複数ユーザーに対して複数の接続を提供します。これらの接続では、以下のいずれかのポートが使用されます。

- TCPポート80 (またはTLSが有効な場合は443)
- セッション画面の保持機能のためのCitrix Gateway Protocol (CGP) が有効な場合はTCPポート2598
- CGPが無効な場合、または従来のクライアントソフトウェアから接続する場合はTCPポート1494

Broker Service : Delivery Controllerのサービスの1つで、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・監視します。Broker Serviceは、PowerShellコマンドを実行し、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。

Broker agent : いくつかのプラグインをホストするエージェントで、リアルタイムデータを収集します。Broker AgentはVDA上で動作して、TCPポート80でControllerに接続します。TCPポート443を使用するオプションはありません。

Monitor Service : Delivery Controllerのサービスの1つで、履歴データを収集してサイトのデータベース上に格納します。

Monitor ServiceはTCPポート80または443で通信します。

ICA File/Stack : VDAへの接続に必要なユーザー情報が格納されています。

サイトデータベース : サイトのポリシー、マシンカタログ、デリバリーグループなど、Delivery Controllerのデータを格納するMicrosoft SQL Serverデータベースです。

NetScaler Gateway : 追加の資格情報によりLANのファイアウォール内外からのアクセスを保護するデータアクセスソリューションです。

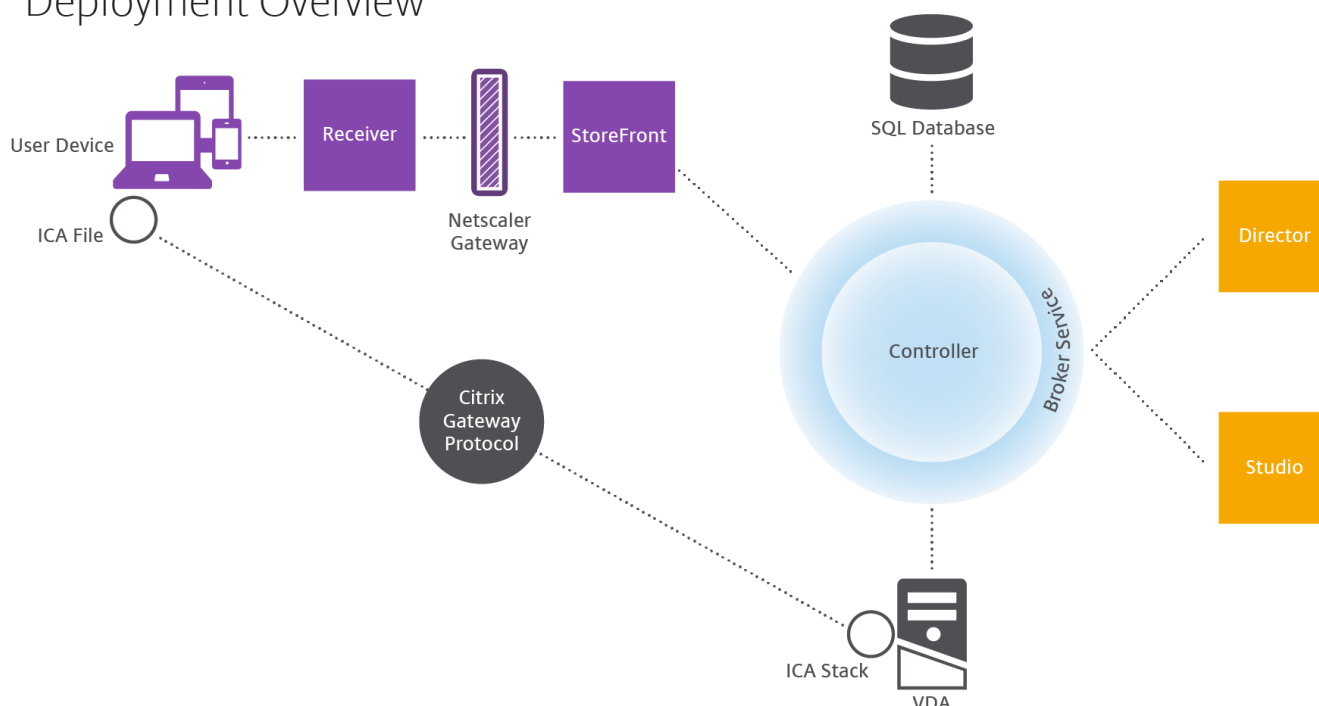
Citrix Director : 管理者およびヘルプデスク担当者がBroker Agentからのリアルタイムデータ、サイトデータベースからの履歴データ、およびNetScalerからのHDXデータにアクセスしてトラブルシューティングやサポート業務に使用するWebベースのツールです。Directorは、TCPポート80または443でControllerと通信します。

Citrix Studio : 管理者がサイトの構成および管理を行うための管理コンソールで、Broker Agentからのリアルタイムデータにアクセスすることもできます。Studioは、TCPポート80でControllerと通信します。

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。

Deployment Overview



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インすると、ユーザーの資格情報が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。

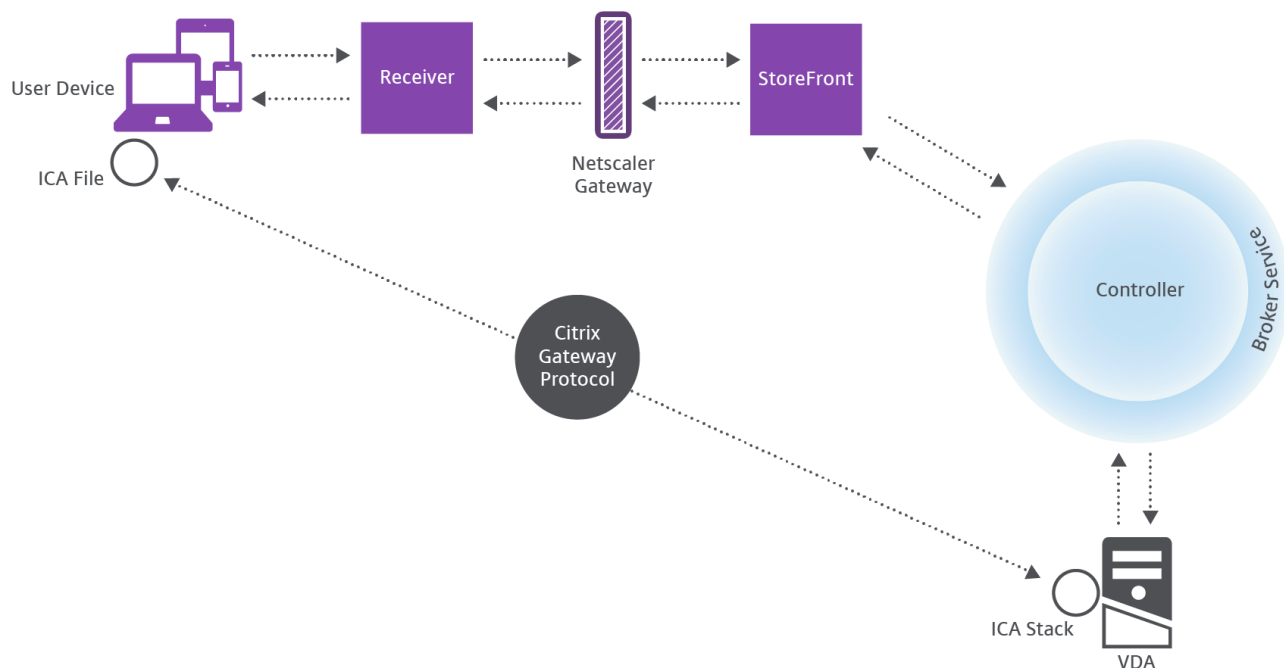
ユーザー接続を処理するしくみ

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WebベースのCitrix Receiver for Web (RFW) 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Citrix Receiverで選択します。

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。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。

User connections



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。Citrix Receiverがセッションで生成されたすべての情報を集めてIndependent Computing Architecture (ICA) ファイルを作成します。ICAファイルは、Citrix Receiverがローカルにインストールされている場合はユーザーデバイス上で作成され、Webブラウザでアクセスしている場合はCitrix RFW上で作成されます。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って暗号

化されたまま転送されます。

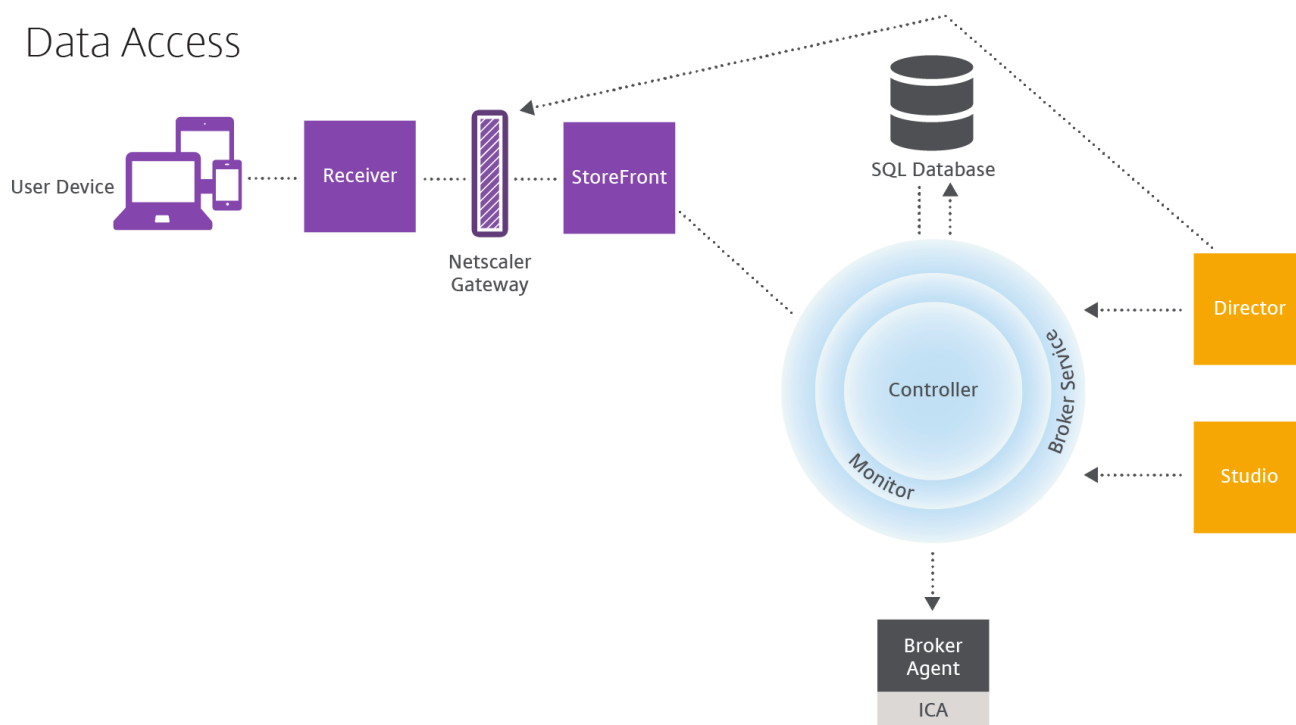
ICAファイルがユーザーデバイスにコピーされ、VDA上で実行されるICAスタックとの直接接続が確立されます。この接続により、管理インフラストラクチャ（Citrix Receiver、StoreFront、およびController）がバイパスされます。

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/無効の設定はStudio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。Studioでは、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仮想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。

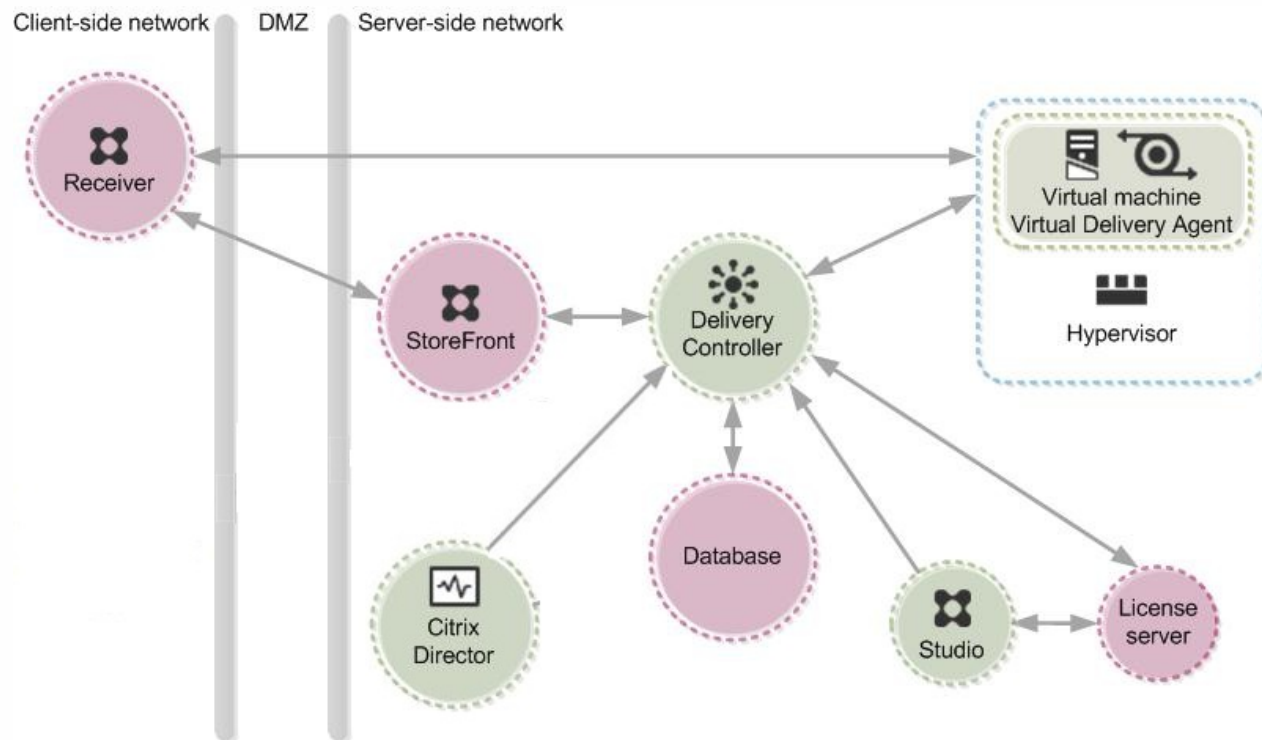
関連トピック

- 概念およびコンポーネント
- 配信方法

概念およびコンポーネント

Jul 07, 2016

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。



以下のコンポーネントで構成されます。

- **Delivery Controller** : Delivery Controllerは、あらゆる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。各サービス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、すべての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。
- **Virtual Delivery Agent (VDA)** : サイトからユーザーに提供する各物理マシンおよび仮想マシン上にVDAをインストールします。これにより、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

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。

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。

- **Citrix StoreFront** : 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、およびその他のデータが維持・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** : 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には、Controller上のBroker Serviceからの情報が表示されます。
- **Citrix Director** : ITサポート担当者やヘルプデスクのスタッフは、このWebベースのツールを使ってシステムの状態を監視して、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ことができます。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、以下のサービスからのセッション情報およびサイト情報が表示されます。
 - 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** : Citrix製品のライセンスの管理サーバーです。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** : 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にはハイパーバイザーとしてCitrix XenServerが付属しています。適切なバージョンのMicrosoft Hyper-VまたはVMware vSphereを使用することもできます。

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。

一般的な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。

- **Provisioning Services** : 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、Provisioning Services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。Provisioning Services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Provisioning Services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、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。
- **Citrix CloudBridge** : 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 CloudBridge (旧称「Citrix 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。CloudBridge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 Optimization with CloudBridge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。詳しくは、Citrix CloudBridgeのドキュメントを参照してください。

リソースのセットアップと割り当て：マシンカタログとデリバリーグループ

ユーザーに提供するリソースを「マシンカタログ」でセットアップし、そのリソースへのアクセスを「デリバリーグループ」で特定のユーザーに付与します。

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。マシン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それらのマシン上で使用可能になっている必要があります。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。管理者は、マシンカタログを作成するときにマシンの種類とプロビジョニング方法を指定します。

- **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 Apps」 (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** : ホワイトリストに含まれている、オフィスにあるユーザーのコンピューターで、そのコンピューター上のリソースへのアクセスを、Citrix Receiverが動作するあらゆるデバイスに提供します。リモートPCアクセスでは、ユーザーの物理PCへのアクセスをXenDesktop展開で管理できます。

プロビジョニング方法

- **Machine Creation Services (MCS)** : マスターイメージから仮想サーバーや仮想デスクトップをオンデマンドで作成する一連のサービスで、ストレージ使用を最適化したり、ユーザーのログオン時に仮想マシンを提供したりすることができます。MCSは、Citrix Studioに完全に統合され管理されます。
- **Provisioning Services** : 単一の共有ディスクイメージからリアルタイムでコンピューターをプロビジョニングしたり再プロビジョニングしたりすることができます。Provisioning Servicesでは、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。デスクトップおよびアプリケーションは、マスターターゲットデバイスから作成されたProvisioning ServicesのvDiskで配信されます。これにより、物理ハードウェアまたは仮想マシンの処理能力を活かすことができます。Provisioning Servicesの管理は、Provisioning Servicesコンソールで行います。
- **既存のイメージ** : データセンター内の仮想マシンに移行済みのデスクトップやアプリケーションがこれにあたります。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散的に管理します。

デリバリーグループ

デリバリーグループとは、共通のリソースへのアクセスが付与されたユーザーのグループを指します。デリバリーグループは、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つのマシン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、アプリケーション、デスクトップ、またはその両方を配信するデリバリーグループを作成できます。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。

XenApp/XenDesktop 7.xとXenApp 6.5やそれ以前のバージョンとの違い

XenApp 6.5やそれ以前のバージョンのXenAppの運用経験がある場合は、これらのバージョンとXenApp/XenDesktop 7.xとの違いについて理解しておくくと便利です。

注 : このセクションを通じて、7.xはXenApp Version 7.5以降、およびXenDesktop Version 7以降を指します。

以前のバージョンとXenApp/XenDesktop 7.x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。

XenApp 6.5以前の機能	対応するXenApp/XenDesktop 7.x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

	Delivery Group
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
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 Scope

XenApp/XenDesktop 7.x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テクノロジー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。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、マシンカタログとデリバリー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 (Virtual Delivery Agent)** : 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はありませんが、7.xでのゾーン機能を使用して、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。
- **Citrix StudioとCitrix 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することができます。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。
- **データベース** : XenApp/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。
- **委任管理** : 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環境全体を監視して、システム全体の問題を解決できます。

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。
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。	接続リリースにより、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。接続リリースは、SQL Server高可用性ベストプラクティスを補完する機能です。「 接続リリース 」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	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。
SmartAuditor	Session Recordingを使用します。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。

Active Directory

Jul 07, 2016

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。ポリシーの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でWindows Server 2003～Windows Server 2012 R2が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、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。

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	いいえ

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。

データベース

Jul 15, 2016

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。ただし、接続リースが構成されている場合を除き、データベースサーバーが使用できなければ、新しい接続は確立できません。

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数秒で実行され、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なります。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ではノードへのControllerのインストールはサポートされていません。

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。詳しくは、「[接続リース](#)」の記事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。

こ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ー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。

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、必要に応じて、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。こ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。これにより、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で使用されます。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

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で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

- 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。

配信方法

Jul 07, 2016

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テクノロジーにより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

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。

XenAppの公開アプリケーションと公開デスクトップ

Jul 07, 2016

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員など。
- 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。

- 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。ユーザーのログオン時に、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に関する記事を参照してください。

VM Hosted Apps

Jul 07, 2016

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。

Windows XPやWindows Vistaなど以前のバージョンのオペレーティングシステムや、32ビットや16ビットの古いアーキテクチャで動作するアプリケーション。各アプリケーションを専用の仮想マシン上で分離して、1つの仮想マシンに障害が発生してもほかのユーザーに影響しないようにします。

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ncatalogを作成するか、既存のマシncatalogをこのマスターイメージで更新します。
3. マシncatalog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続するか同じ仮想マシンに接続するのを指定します。
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。

VDIデスクトップ

Jul 07, 2016

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、VDI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接続するのと同じ仮想マシンに接続するのかを指定し、さらにデスクトップに対する変更内容の保持方法を指定します。
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。

インストールと構成

Jul 15, 2016

個々の展開手順を開始する前に、参考記事を確認してください。これにより、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できます。

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](#)」の記事を確認し、必要なタスクをすべて完了します。これには以下のタスクが含まれます。

- XenAppとXenDesktopの理解。この記事には、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、データベースに関する情報をどこで入手できるかが記載されています。
- 仮想化環境、ホスト環境、またはサポート環境を使用する場合は、そのセットアップ。
- コンポーネントのインストール先マシンのセットアップ。
- Active Directory環境のセットアップ。

この記事では、コンポーネントのインストールおよび機能の有効化で選択または指定する必要がある情報についても説明します。

Linux VDAをインストールする場合は、インストールを始める前に、[Red Hat Linux VDA](#) および [SUSE Linux VDAs](#) を必ず確認してください。

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。ウィザードベースの[グラフィックインターフェイス](#)を使うこともできますし、[コマンドラインインターフェイス](#)で、スクリプトを使ったインストールを行うこともできます。どちらの方法でも、この製品の実行に必要なサードパーティ製ソフトウェアの多くが自動的にインストールされます。

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ウィザードを使った[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、仮想マシンの作成に使用するマスターイメージにインストールすることもできますし、各マシン上に直接インストールすることもできます。[グラフィックインターフェイス](#)、または[コマンドインターフェイス](#)を使用可能です。Active Directory経由でVDAをインストール

する場合の[スクリプト](#)例も用意されています。

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、[Red Hat Linux VDA](#)または[SUSE Linux VDA](#)のインストール手順に従います。

リモートPCアクセス展開では、オフィスPCそれぞれにVDA for Desktop OSをインストールします。[スタンドアロンVDAインストーラーのコマンドラインインターフェイス](#)や既存の電子ソフトウェア配信（ESD）方法を使用すると効率的です。

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。[グラフィックインターフェイス](#)、または[コマンドインターフェイス](#)を使用可能です。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。

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。可能であれば、ほかのCitrixコンポーネントが含まれないサーバー上にインストールしてください。

必要に応じて、追加のCitrixコンポーネントをXenApp/XenDesktop展開に統合します。次に例を示します。

- 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。Provisioning Servicesのドキュメントを参照してください。
- 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 Gatewayのドキュメントを参照してください。
- Citrix CloudBridge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。Citrix CloudBridgeのドキュメントを参照してください。

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、およびテクノロジー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、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を使用している場合は、まず、そのオストにマスターイメージを作成する必要があります。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われます。

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、選択されたマシン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す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。

インストールの準備

Jul 15, 2016

ここでは次のことについて説明します。

- [一般的なインストールのガイダンス](#)
- [コアコンポーネントのインストール時に指定する事項](#)
- [VDAインストールガイダンス](#)
- [VDAのインストール時に指定する事項](#)

一般的なインストールのガイダンス

- 「[Technical overview](#)」を参照して、製品およびコンポーネントについて理解を深めてください。現在XenApp 6.x以前をお使いの場合、XenAppおよびXenDesktopの7.xバージョンでの違いについては「[概念およびコンポーネント](#)」を参照してください。
- 導入を計画する場合は、[セキュリティ](#)の記事を参照してください。
- 「[既知の問題](#)」を参照して、インストールに関する既知の問題について確認してください。
- アプリケーションおよびデスクトップへの仮想マシンの構築に、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を使用している場合、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、そのホストに対して最初の接続を設定します。ただし、仮想化環境はそれより前にいつでも設定できます。[ここに](#)記載されている情報ソースを参照してください。
- アプリケーションおよびデスクトップへのアクセスの管理にMicrosoft System Center Configuration Managerを使用している場合は、[この記事](#)を参照してください。
- コンポーネントに.NETの前提条件がある場合、必要な.NETのバージョンが存在し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。.NETがインストールされると、マシンの再起動が必要となる可能性があります。
- 「[データベース](#)」の記事を参照して、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のインストール中に、同じサーバー上にMicrosoft SQL Server 2012 Expressをインストールするかどうかを選択できます。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。
- Citrixライセンスサーバーをインストールする管理者は、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管理者として設定されます。詳しくは、「[委任管理](#)」を参照してください。
- 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（ネットワーク、マシンカタログ、デリバリーグループ、リソースなど）には、重複しない名前を指定してください。
- 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、処理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、インストールし直す必要はありません。
- Citrix Studioは、インストールの完了時に自動的に起動します。グラフィックインターフェイスを使用するときは、ウィザードの最終ページでこのアクションを無効にすることができます。
- 製品ISOに含まれているインストーラーを使用して、コアコンポーネントおよびVirtual Delivery Agent (VDA) をインストールできます。このインストーラーは「全製品インストーラー」と呼ばれます。VDAのインストールには、この全製品インストーラー、または製品ダウンロードサイトで提供されているスタンドアロンVDAインストーラーのどちらも使用できます。どちらのインストーラーでも、[グラフィック](#)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。
- この製品のインストールメディアには、Active Directory環境のマシンのグループで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、このスクリプトを個々のマシンに適用して、それらを使って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。詳しくは、「[スクリプトを使用したVDAのインストール](#)」の記事を参照してください。
- 全製品インストーラーを使用して、お使いの印刷サーバーにUniversal Print Serverのサーバーコンポーネント (UpsServer)

を、グラフィックまたはコマンドラインインターフェイスのどちらを使用してもインストールできます。製品ダウンロードページで、UpsServerダウンロードパッケージも提供されている可能性があります。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。

- 全製品インストーラーを使用して、[Federated Authentication Service](#)をインストールできます。
- コンポーネントをインストールすると、分析情報が自動的に収集されます。さらに、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ControllerまたはVDAをインストールする場合、Citrix Call Home機能に参加するかどうかを指定することができます。両方の機能について詳しくは、「[Citrix Insight Services](#)」を参照してください。
- 製品ISOには、Citrix Receiver for MacとCitrix Receiver for Linuxのバージョンは含まれなくなりました。管理者（またはユーザー）が、Citrix ReceiverをCitrix Webサイトからダウンロードできます。また、Citrix ReceiverをStoreFrontサーバーから入手できるようにすることもできます（StoreFront 3.0.xドキュメントの「[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](#)」セクションか、または使用しているStoreFrontバージョンでの対応するコンテンツを参照）。

権限

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、管理者権限でインストールを開始するか、**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](#)」の記事には、サポートされるActive Directoryの機能レベルが一覧にされています。 [Active Directory](#)」の記事には、そのほかのサポート情報も記載されています。
- 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として動作するコンピューター上にはいずれのコンポーネントも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。
- Active Directoryの構成手順については、Microsoft社のドキュメントを参照してください。

コンポーネントのインストール先

各コンポーネントをどこにインストールするか決定し、次にマシンおよびオペレーティングシステムを準備します。

- Controller、Studio、Director、仮想化リソース、Virtual Delivery Agentでサポートされるオペレーティングシステムおよびその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。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。例外については、「システム要件」を確認してください。サポートされるプラットフォームについては、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。たとえば小規模な展開をリモートで管理する場合、Controllerをインストールしたサーバーとは異なるマシン上にStudioをインストールできます。将来的にサイトを拡張する計画がある場合は、各コンポーネントを個別のサーバー上にインストールします。たとえば、ライセンスサーバーとDirectorを別のサーバー上にインストールします。
- Delivery ControllerとVirtual Delivery Agent for Windows 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Delivery Controller（およびインストールするその他のコアコンポーネント）をインストールし、インストーラーを再度起動してVirtual Delivery Agent for Windows Server OSをインストールします。
- 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。
- 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。

- 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。これは、Kerberosでマシン間の通信を保護するために必要です。

コアコンポーネントのインストール時に指定する事項

以下のセクションでは、インストール中に確認および指定する事項について説明します。この説明は、[グラフィックインターフェイスウィザード](#)の順序に従っています。また、対応する[コマンドラインオプション](#)も提供されています。インストールの記事には、ウィザードの開始方法およびオプションのあるコマンドの実行方法に関する詳細が記載されています。

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。[コアコンポーネント] ページで別の場所を指定することもできますが、ネットワークサービスの実行権限が必要となります。（デフォルトではないディレクトリを指定するためのコマンドラインオプション：/installdir）

コアコンポーネントで使用される機能

Microsoft SQL Server Expressをインストールするかどうかを選択または指定します。[「データベース」](#)の記事を参照し、データベースについての理解を深めてください。（インストールを阻止するためのコマンドラインオプション：/nosql）

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、およびTCPポート3389を開放するかどうかを選択できます。デフォルトで、この機能は有効になっています。（コマンドラインオプション：/no_remote_assistance）

コアコンポーネントに対するファイアウォールのポート

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これらの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やファイアウォールを使用していない場合、またはインストール完了後に手作業でポートを開放する場合は、このデフォルトの動作を無効にすることができます。このCitrix製品またはその他のCitrix製品に関するポート情報について詳しくは、[CTX101810](#)を参照してください。（コマンドラインオプション：/configure_firewall）

- Controller : TCP 80、443
- Director : TCP 80、443
- ライセンスサーバー : TCP 7279、8082、8083、27000
- StoreFront : TCP 80、443

VDAインストールガイド

- VDAインストーラーでは、[グラフィック](#)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。
- サポートされるオペレーティングシステムおよびVDAの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。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。例外については、「システム要件」を確認してください。VDA for Windows Server OSをインストールすると、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。
- Windows 7またはWindows Server 2008 R2のマシンにVDAをインストールしている場合は、VDAのインストールを開始する前に、.NET 3.5.1がインストールされていることを確認してください。後述の「[再起動](#)」セクションには、その他のインストールの前提条件および注意事項が記載されています。
- 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することができないため、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。

- Profile managementがVDAのインストール時に自動的にインストールされます。コマンドラインインターフェイスを使用している場合はProfile managementを除外できますが、除外すると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。
- 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。このユーザーグループは、VDA for Windows Desktop OSではRDP接続でのみ使用され、VDA for Windows Server OSではICA接続およびRDP接続で使用されます。
- リモートPCアクセス構成の場合は、ユーザーがリモートでアクセスする社内の物理PC上にVDA for Windows Desktop OSをインストールします。最適化機能を有効にしないでください。
- サポートされるLinuxオペレーティングシステム上にVDAをインストールしている場合、基本情報について [Red Hat Linux VDAs](#) または [SUSE Linux VDAs](#) を参照してください。
- 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が、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。詳しくは、下記の「[Delivery Controllerのアドレス](#)」セクションを参照してください。
- Windows Server 2012 R2システムにVDA for Server OSをインストールしたら、Kerberos Enable Tool (XASsonKerb.exe) を使用してCitrix Kerberos認証が正しく行われるようにしてください。このツールは、インストールメディアのSupport > Tools > XASsonKerbフォルダーに収録されています。このツールを使用するには、ローカルの管理者権限が必要です。サーバー上のコマンドプロンプトで**xassonkerb.exe -install**を実行します。その後のアップデートなどでレジストリHKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\OSConfigが変更された場合は、このコマンドを再度実行してください。このコマンドで利用できるオプションについての情報を表示するには、-helpパラメーターを指定してコマンドを実行します。

使用できるVDAインストーラー：全製品およびスタンドアロン

全製品インストーラーまたはスタンドアロンインストールパッケージを使用して、VDAをインストールできます。どちらをイ
用しても、グラフィック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。

インストール時にオペレーティングシステムが自動的に認識されるため、適切なVDA (VDA for Windows Server OSまたは
VDA for Windows Desktop OS) がインストールされます。

スタンドアロンVDAインストールパッケージ

スタンドアロンパッケージはサイズが小さいため、電子ソフトウェア配信 (ESD) ツールを使用してVDAをローカルにステー
ジングまたはコピーしたり、物理マシンやリモートオフィスに展開したりする場合に便利です。スタンドアロンパッケージ
主にコマンドラインでのサイレント (無人) インストールで使用し、全製品インストーラーと同じコマンドラインパラメ
ーターを指定できます。このパッケージには、全製品インストーラーに相当するグラフィックインターフェイスも用意されて
います。

スタンドアロンVDAインストーラーに対するグラフィックインストーラーの使用方法

スタンドアロンVDAインストーラーに対するコマンドラインインターフェイスの使用方法

VDAの自己展開型スタンドアロンパッケージには、サーバーOSマシン用とワークステーション (デスクトップ) OSマシン用
の2つがあります。

デフォルトでは、パッケージ内のファイルは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。Tempフォルダーに抽出されたファイルは自動的に
削除されません。インストールが完了したら、これらのファイルをC:\Windows\Temp\Ctx-* (ここで「*」はランダムなグ
ローバル一意識別子) から手作業で削除することができます。もしくは、絶対パスと/extractコマンドを使用できます。

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。

VDAのインストール時の再起動

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。

インストールシーケンスで再起動する回数を最小化するには、

- 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。

通常、ほかの必須条件のインストールでは再起動が不要なため、インストーラーでこれらのソフトウェアを自動的にインストールできます。

VDAをインストールする前に必須条件をインストールせず、コマンドラインで/norebootオプションを指定してインストールする場合は、必要に応じてマシンを再起動してください。たとえば、必須条件を自動的にインストールする場合は、RDSのインストール後にインストーラーがいったん停止して再起動を確認するメッセージが表示されます。VDAのインストールを続けるには、マシンを再起動した後でインストールコマンドを再実行してください。

サポートされていないWindowsシステム上のVDA

最新のVDAはWindows XPまたはWindows Vistaシステムではサポートされていません。また、新しい機能の一部もこれらのオペレーティングシステムではサポートされません。これらのシステムを、現在サポートされているWindowsデスクトップOSバージョンで置き換えてから、このリリースからVDAをインストールすることをお勧めします。Windows XPまたはWindows Vistaを実行しているマシンを引き続き使用する必要がある場合は、古いバージョンのVirtual Desktop Agent (5.6 FP1およびいくつかのHotfix) をインストールできます。詳しくは、[CTX140941](#)を参照してください。次の点に注意してください。

- Windows XPまたはWindows Vistaシステムには、コアコンポーネント (Controller、Studio、Director、StoreFront、ライセンスサーバー) をインストールできません。
- Windows XPまたはWindows Vistaを使用してこれらのマシンを含むマシンカタログを作成する場合、[マスターイメージ] ページの [インストールされているVDAのバージョンを選択...] ボックスで「5.6 FP1」を選択してください。
- リモートPCアクセスは、Windows Vistaをサポートしません。
- CitrixでのWindows XPのサポートは、Microsoft社によるサポートが終了した2014年4月8日に終了しました。
- 古いバージョンのVDAを継続使用すると、新しい機能やControllerへのVDA登録で問題が発生することがあります。詳しくは、「混在環境の考慮事項」を参照してください。

VDAのインストール時に指定する事項

以下のセクションでは、インストール中に指定する事項について説明します。この説明は、グラフィックインターフェイスウィザードの順序に従っています。また、対応するコマンドラインオプションも提供されています。インストールの記事には、ウィザードの開始方法およびオプションのあるコマンドの実行方法に関する詳細が記載されています。

VDAのインストール後に必要な作業については、「[VDAインストールガイド](#)」を参照してください。

環境

VDA環境によって、VDAの使用方法が指定されます。

- デフォルトの [マスターイメージ] オプションは、Machine Creation Services (MCS) またはProvisioning Servicesを使用して、ハイパーバイザーまたはクラウドサービスで作成されたマスターイメージに基づいた仮想マシンを作成することを示しています。マスターイメージ上にVDAをインストールします。(コマンドラインオプション: /masterimage)
- [リモートPCアクセス] オプションは、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をインストールすることを示しています。

Important

XenAppおよびXenDesktop7.9では、リモートPCアクセス展開にのみコマンドラインを使用してください。詳しくは、[コマンドラインを使ったインストール](#) および「[既知の問題](#)」[#637741]を参照してください。

HDX 3D Pro (VDA for Windows Desktop OSのバージョン)

グラフィックインターフェイスを使用してVDAをインストールする場合、VDAを(サーバーOSマシンでなく)デスクトップOSマシンにインストールするときのみ次のページが表示されます。標準モードまたはHDX 3D ProモードのVDAの構成を選択します。

- 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VDAモードの使用をお勧めします。このモードはデフォルトの構成です。
- VDA for HDX 3D Proモードでは、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。これは、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。(デスクトップOSマシン上でのみ有効なコマンドラインオプション: /enable_hdx_3d_pro)

XenDesktop 7.9

✓ Environment

HDX 3D Pro

Core Components

Delivery Controller

Features

Firewall

Summary

Install

Call Home

Finish

HDX 3D Pro

HDX 3D Pro optimizes the performance of graphics-intensive programs and media-rich applications.

Configuration

Install the Virtual Delivery Agent (VDA) for HDX 3D Pro?

- ☒ No, install the standard VDA
Recommended for most desktops, including those enabled with Microsoft RemoteFX.
- ☐ Yes, install the VDA for HDX 3D Pro
Recommended if the machine will access a graphics processor for 3D rendering.

標準VDA

- 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。
- あらゆるGPUによるGPUアクセラレーションがサポートされます（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では、GPUアクセラレーションはウィンドウ表示の（全画面ではない）DirectX 10、11、12アプリケーションに制限されます。DirectX 9および全画面アプリケーションはソフトウェアでレンダリングされます（WARP）。
 - 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）。
- 任意のモニター解像度（最大4K）および最大8つのモニターがサポートされるCitrix WDDMディスプレイドライバーを使用します。
- Windows 7および8.x Aeroデスクトップへのブロードバンドアクセス用デスクトップコンポジションリダイレクトオプション
 - ユーザーデバイス（WindowsまたはMac）に開放されたWindowsデスクトップコンポジション

VDA for HDX 3D Pro

- 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。
- 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またはIntel Iris Pro graphics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）およびNVIDIA GRID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）。
- 最大で4つのモニターをサポートします。

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。

コアコンポーネント（インストール先およびCitrix Receiverのインストール）

デフォルトでは、C:\Program Files\Citrixに各VDAがインストールされます。インストール時に別の場所を指定することもできますが、Network Serviceアカウントでの実行権限が必要です。（デフォルトではないディレクトリを指定するためのコマンドラインオプション：/installdir）

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。このデフォルトの動作は無効にできます。（コマンドラインオプション：Citrix Receiverのインストールを阻止するには「/components vda」を使用）

Delivery Controller

VDAのインストール時（推奨）または後から、インストールされたControllerのアドレス（FQDN）を指定できます。VDAをインストールするときにControllerアドレスを指定する必要はありませんが、この情報なしでVDAをControllerとともに登録することはできない点に注意してください。VDAを登録できないと、マシン上でこれらのVDAを含むユーザーが、VDAのアプリケーションおよびデスクトップにアクセスできなくなります。（コマンドラインオプション：/controllers）

- VDAをインストールするときにController FQDNを指定すると、インストーラーによって、指定されたアドレスへの接続が試行されます。接続が失敗すると、情報メッセージが表示されます。
- Controllerアドレスの指定を後で指定するようにすると、指定するようリマインドされます。Controllerアドレスを指定せずにVDAをインストールする場合は、インストーラーを後で再実行するか、またはCitrixグループポリシーを使用することができます。

VDAのインストールおよびグループポリシーの両方でController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もあることに注意してください。

（VDAのインストール時またはその後）Controllerのロケーションを指定すると、追加でControllerがインストールされた場合に、自動更新機能によってVDAが更新されます。

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は、[Delivery Controller](#)の記事を参照してください。

機能

VDAで使用される以下の機能を有効または無効にすることができます。

- **パフォーマンスの最適化**：（デフォルト＝有効）この機能を有効にすると、ハイパーバイザー上の仮想マシンで実行される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。リモートPCアクセスを使用する場合は、このオプションを有効にしないでください。（コマンドラインオプション：/optimize）
- **Microsoft Remote Assistanceの使用**：（デフォルト＝有効）この機能を有効にすると、Directorのユーザーシャドウ機能でMicrosoft Remote Assistanceが使用されます。また、ファイアウォールのTCPポート3389が自動的に開放されます（ファイアウォールポートを手動で開放することを選択した場合も開放されます）。（コマンドラインオプション：/enable_remote_assistance）

- **リアルタイムオーディオ転送**：（デフォルト = 有効）この機能を有効にすると、オーディオパケットにUDPが使用され、オーディオパフォーマンスが向上します。（コマンドラインオプション：/enable_real_time_transport）
- **Framehawk**：（デフォルト = 有効）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（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。変更した場合、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VDAからNetScaler Gateway）および外部のファイアウォール（NetScaler GatewayからCitrix Receiver）で解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）。
- **Citrix App-V公開コンポーネントのインストール**：（デフォルト = 有効）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、この機能を有効にします。詳しくは、「[App-V](#)」を参照してください。（コンポーネントのインストールを禁止するコマンドラインオプション：/no_appv）
- **Personal vDisk**：（デフォルトは無効。仮想マシンにVDA for Desktop OSをインストールする場合にのみ選択可能）。この機能を有効にすると、マスターイメージでPersonal vDiskが使用されます。詳しくは、「[Personal vDisk](#)」の記事を参照してください。（コマンドラインオプション：/baseimage）

ファイアウォール

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これらの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やファイアウォールを使用していない場合、またはインストール完了後に手作業でポートを開放する場合は、このデフォルトの動作を無効にすることができます。Citrix製品で使用するポートについて詳しくは、[CTX102112](#)を参照してください。（コマンドラインオプション：/enable_hdx_ports）

- **Controllerの通信**：TCP 80、1494、2598、8008。ユーザーデバイスと仮想デスクトップ間の通信については、ポート1494と2598上の受信TCPトラフィックをポート例外として構成します。セキュリティ上の理由から、これらの登録ポートをICPプロトコルとCommon Gateway Protocol以外の用途で使用しないことをお勧めします。Controllerと仮想デスクトップ間の通信については、ポート80上の受信トラフィックをポート例外として構成します。
- **リモートアシスタンス**：TCP 3389。前のページでMicrosoft Remote Assistance機能を有効にすると、このポートはWindowsにより自動的に開放されます（ポートを手動で開放することを選択した場合も開放されます）。
- **リアルタイムオーディオ**：UDP 16500～16509
- **Framehawk**：UDP 3224～3324

概要

表示された内容を確認して「インストール」をクリックすると、インストールの進行状況が表示されます。インストールの完了後、VDAを使用するにはマシンを再起動する必要があります。

VMware仮想化環境

Jul 07, 2016

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。

ハイパーバイザーのインストールおよび構成

手順1: 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）。

手順2: 次の権限があるVMwareユーザーアカウントを、DataCenterまたはそれ以上のレベルで作成します。このアカウントは、vCenterとの通信で使用されます。また、新しい仮想マシンを作成するための権限が必要です。

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]
System.Anonymous、System.Read、および System.View	自動的に追加されます。
Task.Create	[タスク] > [タスクの作成]
VirtualMachine.Config.AddRemoveDevice	[仮想マシン] > [構成] > [デバイスの追加または削除]
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.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.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Config.Resource	[仮想マシン] > [構成] > [リソースの変更]
VirtualMachine.Config.Settings	[仮想マシン] > [構成] > [設定]
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]
VirtualMachine.Inventory.Create	[仮想マシン] > [インベントリ] > [新規作成]
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.Delete	[仮想マシン] > [インベントリ] > [削除]
VirtualMachine.Inventory.Register	[仮想マシン] > [インベントリ] > [登録]
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.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.DiskRandomAccess	[仮想マシン] > [プロビジョニング] > [ディスクアクセスの許可]
VirtualMachine.Provisioning.GetVmFiles	[仮想マシン] > [プロビジョニング] > [仮想マシンのダウンロードの許可]
VirtualMachine.Provisioning.PutVmFiles	[仮想マシン] > [プロビジョニング] > [仮想マシンファイルのアップロードの許可]
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]
VirtualMachine.Provisioning.MarkAsVM	[仮想マシン] > [プロビジョニング] > [仮想マシンとしてマーク]

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]
VirtualMachine.State.RemoveSnapshot	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削除] 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削除]
VirtualMachine.State.RevertToSnapshot	vSphere 5.0, Update 2およびvSphere 5.1, Update 1 : [仮想マシン] > [状態] > [スナップショットまで戻る] vSphere 5.5 : [仮想マシン] > [スナップショット管理] > [スナップショットまで戻る]

手順3 : 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。

手順4 : AppDiskを作成するには、ユーザーアカウントに次の追加の権限が必要です。

- SDK : VirtualMachine.Config.EditDevice
- ユーザーインターフェイス : [仮想マシン] > [構成] > [デバイス設定の変更]

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またはWindows Server 2012 R2の場合：
 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。

マスター仮想マシンの作成

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。

仮想デスクトップの作成

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「」形式で指定します。

VMware SSLの拇印機能

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。

Microsoft System Center Virtual Machine Manager仮想化環境

Jul 15, 2016

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。

このリリースでは、以下のVMMがサポートされています。

- VMM 2012 - 管理機能が向上し、仮想マシンだけでなく仮想化されたデータセンター全体を管理できます。このリリースには、Windows Server Update Servicesとの統合に加えて、クラスターホストへの修正プログラムの適用をオーケストレーションする機能も用意されており、各ホストに必要な修正プログラムのレベルを定義できます。
- VMM 2012 SP1 - クラスター化された共有ボリュームおよびStorage Area Network (SAN) のファイルサーバー上でServer Message Block (SMB) 3.0を使用する場合のMachine Creation Services (MCS) のパフォーマンスが向上しました。これらのファイル共有では低コストのキャッシュ機能が提供され、SANストレージ上のI/Oが減少してパフォーマンスが向上します。
- VMM 2012 R2 - 実行中の仮想マシンのスナップショット作成、VHDXの動的なサイズ変更、および記憶域など、Windows Server 2012 R2の主要な機能をスケーラブルに管理できます。

このリリースは、VMM 2012 R2の第1世代の仮想マシンのみをサポートします。MCSを使って仮想マシンを作成する場合、マスター仮想マシンの一覧に第2世代の仮想マシンが表示されません。第2世代の仮想マシンはデフォルトでセキュアブートが有効になっているため、VDAが正しく機能しません。

VMMのアップグレード

- 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 5.6をXenDesktop 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 2012をVMM 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 SP1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）。

インストールと構成の概要

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。
 - 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MCS

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との依存関係を削除）します。

root\virtualization\v2名前空間でConvertVirtualHardDiskを実行します。

例：

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2"; $result = $ims.ConvertVirtualHardDisk($diskName, $vhdaText) $result
```

- **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 = $ims.CreateVirtualHardDisk($vhdaText); $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Controller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、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。

Microsoft Azure仮想化環境

Jul 07, 2016

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長くなります）。

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdfklsdjfl;akjsdfl;akjsdfl;sdjfklsdflaskjdfkluqweiopruaiopdfaklsdjfjsdflfaskdflfjerioup" />
```

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>
- Virtual Machines 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。

Standard層 : Standard層のVMには、A、D、DS、Gの4シリーズがあります。

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。

VMインスタンスの種類とコストおよびパフォーマンス

米国での、各仮想マシンインスタンスタイプの1時間あたりの料金については、以下を参照してください。

<http://azure.microsoft.com/en-us/pricing/details/virtual-machines/>。

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、コスト削減のために、性能の低い仮想マシンを使いたくなることもあるでしょう。 次善の策は、タスクに適切な仮想マシンを使用することです。 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。

スケーラビリティ

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。

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、<https://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。

Microsoft System Center Configuration Manager環境

Jul 07, 2016

System Center Configuration Manager (Configuration Manager) 2012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** — Citrix Connectorを使用するかどうかにかかわらず、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。

プロパティ

Microsoft System Center Configuration Manager 2012および2012 R2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 2012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。 ● ClientIP ● 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	説明 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。
PersonalDiskDriveLetter	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。以下のタスクについて詳しくは、<http://support.citrix.com/article/ctx140905>を参照してください。

- 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。

Configuration ManagerとリモートPCアクセスのWake on LAN

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。

- 組織内にConfiguration Manager 2012を構成してからリモートPCアクセス用のすべてのマシンにConfiguration Manager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、自動で強制的に実行することもできます）。StudioでConfiguration Manager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。
- Configuration Manager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。
 - Configuration Managerのウェイクアッププロキシの場合は、Configuration Manager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Configuration Manager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、Configuration Managerのウェイクアッププロキシやマジックパケットの使用を構成したり、パケットの転送方法を変更したりすることができます。

詳しくは、「[リモートPCアクセス](#)」を参照してください。

Nutanix仮想化環境

Aug 26, 2016

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 (<https://portal.nutanix.com>) にあるNutanix Acropolis MCSプラグインのインストールガイド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\RegisterPlugin.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

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。

【仮想マシン】ページで、仮想CPUの数と各仮想CPUのコア数を指定します。

【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。

グラフィカルインターフェイスを使ったインストール

Jul 07, 2016

注：このアティクルは、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れます。LinuxオペレーティングシステムのVDAについては、「[Red Hat Linux VDA](#)」および「[SUSE Linux VDA](#)」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。

- [はじめに](#)
- [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](#)
- [VDAのカスタマイズ](#)

はじめに

重要：どのようなインストールであっても、開始する前にまず、「[インストールの準備](#)」の記事を確認してください。そこには、インストーラーなど、インストールの前に確認しておくべき内容が記載されています。また、グラフィカルインターフェイス形式のウィザードに表示されたり、そこで指定したりする項目もひとつと説明しています。この記事では、製品インストーラーでグラフィックインターフェイスを起動する方法について説明します。

グラフィックインターフェイスは、以下の目的で使用できます。

- Delivery Controller、Citrix Studio、Citrix Director、ライセンスサーバー、StoreFrontの1つまたは複数のコンポーネントをインストールする。
- マスターイメージ、仮想マシン、または物理マシン上にVirtual Delivery Agent (VDA) をインストールする。また、メディアに収録されているスクリプトをカスタマイズして、Active DirectoryでVDAをインストールしたり削除したりできます。
- インストール済みのVDAをカスタマイズする。
- Universal Print Serverコンポーネントをインストールする。ControllerにはUniversal Print Serverクライアントの機能が既に統合されているため、必要なのは、印刷サーバーへのUpsServerコンポーネントのインストールだけです。コンポーネントのインストール後、「プリンターの構成」に記載されている構成手順に従って操作します。
- コンポーネントをアップグレードする。「[展開のアップグレード](#)」の記事を参照してください。

全製品インストーラーとスタンドアロンVDAインストーラーの両方にグラフィックインターフェイスが付属しています。

全製品インストーラーの使用

全製品インストーラーを使用して、コアコンポーネント、VDA、Universal Print Serverのサーバーコンポーネントをインストールできます。

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。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。
5. XenAppとXenDesktopのどちらをインストールするかを選択します。
6. インストールするコンポーネントを選択します。

- 製品を初めてインストールする場合は、左側の列から **[Delivery Controller]** をクリックします。ウィザードに従って、インストーラーを実行しているマシンにインストールするコンポーネント (Delivery Controller、Studio、Director、License Server、StoreFront) を選択します。
- いくつかのコンポーネントがインストール済みの環境で展開を拡張する場合は、インストールするコンポーネントを **[拡張展開]** セクションで個別にクリックできます。この列では、コアコンポーネントと Universal Print Server を選択できます。
- VDA をインストールするには、中央の列から VDA エントリをクリックします。実行しているオペレーティングシステムに合ったエントリのみが選択可能になっています。

ウィザードの指示に従って操作します。「[インストールの準備](#)」の記事には、ウィザードに表示されたり、そこで指定したりする情報に関する説明が記載されていますので、ご利用ください。VDA をインストールしている場合、インストールが完了すると、デフォルトで自動的に再起動されます。サイトで VDA を使用できるようにするには、再起動は必須です。

スタンドアロンVDAインストーラーの使用

重要：「[インストールの準備](#)」の記事には、スタンドアロンVDAインストーラーを使用していたインストール中に表示されたり、その時に指定したりする情報、特に再起動と抽出スペースの処理に関する説明が記載されています。

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。インストールの前に管理者権限を設定するか、または **[管理者として実行]** を使用する必要があります。ユーザーアカウント制御 (UAC) を無効にしてください。

1. Citrix から該当するパッケージ、**VDA Server Setup.exe** (サーバー OS マシン用)、または **VDA Workstation Setup.exe** (デスクトップ OS マシン用) をダウンロードします。単一ユーザー、単一サーバー OS マシン展開 (たとえば Windows Server 2012 マシンを Web サイト開発者などの単一ユーザーに配信する場合など) では、VDA Workstation Setup.exe パッケージを使用します。詳しくは、「[サーバー VDI](#)」の記事を参照してください。
2. 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。
3. ウィザードの指示に従って操作します。インストールが完了すると、デフォルトで自動的に再起動されます。サイトで VDA を使用できるようにするには、再起動は必須です。

VDAのカスタマイズ

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 <version>]** を右クリックして、**[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て、Controller のアドレスや Controller への登録時の TCP/IP ポート (デフォルトは 80) を変更したり、Windows ファイアウォールで自動的にポートを開くかどうかを変更したりできます。

コマンドラインを使ったインストール

Jul 15, 2016

注：このアーティクルは、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れます。LinuxオペレーティングシステムのVDAについては、「[Red Hat Linux VDA](#)」および「[SUSE Linux VDA](#)」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。

- [はじめに](#)
- [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](#)
- [コマンドラインを使ったVDAのカスタマイズ](#)
- [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](#)
- [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](#)
- [コマンドラインを使ったUniversal Print Serverのインストール](#)

はじめに

重要：どのようなインストールであっても、開始する前にまず、「[インストールの準備](#)」の記事を確認してください。そこには、インストーラーなど、インストールの前に確認しておくべき内容が記載されています。さらに、コマンドに含めることができるオプションについても説明されています。この記事では、製品インストーラーでコマンドラインインターフェイスを起動する方法について説明します。

コマンドラインインターフェイスを使用して、以下の操作を実行できます。

- Delivery Controller、Citrix Studio、Citrix Director、ライセンスサーバー、StoreFrontの1つまたは複数のコンポーネントをインストールする。
- マスターイメージ、仮想マシン、または物理マシン上にVirtual Delivery Agent (VDA) をインストールする。また、メディアに収録されているスクリプトをカスタマイズして、Active DirectoryでVDAをインストールしたり削除したりできます。
- インストール済みのVDAをカスタマイズする。
- ネットワークセッションプリンターをプロビジョニングするUniversal Print Serverをインストールする。ControllerにはUniversal Print Serverの機能が既に統合されているため、印刷サーバー上にのみインストールします。
- コンポーネントをアップグレードする。「[展開のアップグレード](#)」の記事を参照してください。

また、インストール済みのコンポーネントを削除することもできます。これを行うには、/removeオプションまたは/removeallオプションを使用します。詳しくは、「[コンポーネントの削除](#)」の記事を参照してください。

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。

全製品インストーラーとスタンドアロンVDAインストーラーの両方にコマンドラインインターフェイスが付属しています。

用意されているスクリプト例を、Active DirectoryにあるVDAマシンのインストール、アップグレード、または削除に使用する場合は、後述の「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」にリストされているVDA構成オプションを指定できます。スクリプト例についての詳細は、「[スクリプトを使用したVDAのインストール](#)」の記事を参照してください。

全製品インストーラーの使用

コアコンポーネントとVDAをインストールするには、全製品インストーラーを使用します。

- 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。
- 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、インストール先のサーバーにログオンします。
- 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。
- 製品メディアの\x64\XenDesktop Setupディレクトリから、次の操作を実行します。

コアコンポーネントをインストールするには、**XenDesktopServerSetup.exe**コマンドを実行します。後述の「[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](#)」セクションにリストされているオプションを使用してください。

VDAをインストールするには、**XenDesktopVDASetup.exe**コマンドを実行します。後述の「[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](#)」セクションにリストされているオプションを使用してください。

全製品インストーラーを使用したコアコンポーネントのインストール例

例1：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ポートは自動的に開放されます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver
/configure_firewall
```

例2：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
```

全製品インストーラーを使用したVDAのインストール例

例1：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 Windows 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-
Main.mydomain.local" /enable_hdx_ports /optimize /masterimage /baseimage /enable_remote_assistance
```

例2：次のコマンドを実行すると、リモートPCアクセスで使用される社内のPC上のデフォルトの場所にVDA for Windows Desktop OSおよびCitrix Receiverがインストールされます。インストールの完了後にマシンは再起動されませんが、VDAを使用するには再起動が必要です。VDAは、まず「mydomain」ドメインの「Contr-East」サーバー上で動作するControllerに登録され、オーディオパケットにUDPが使用されます。Windowsファイアウォールサービスが検出された場合は、HDXポートが開放されます。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-
East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboot
```

スタンドアロンVDAインストーラーの使用

重要：「[インストールの準備](#)」の記事には、スタンドアロンVDAインストーラーを使用していたインストール中に表示されたり、その時に指定したりする情報、特に再起動と抽出スペースの処理に関する説明が記載されています。

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。インストールの前に管理者権限を設定するか、または【管理者として実行】を使用する必要があります。

1. Citrixから該当するパッケージ、**VDAServerSetup.exe**（サーバーOSマシン用）、または**VDAGWorkstationSetup.exe**（デスクトップOSマシン用）をダウンロードします。単一ユーザー、単一サーバーOSマシン展開（たとえばWindows Server 2012マシンをWebサイト開発者などの単一ユーザーに配信する場合など）では、VDAGWorkstationSetup.exeパッケージを使用します。詳しくは、「[サーバーVDI](#)」の記事を参照してください。
2. まず、パッケージから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、「`.\VDAGWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia`」のように絶対パスと**/extract**を使います。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。後述の「[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](#)」セクションにリストされている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ただ実行するだけの場合は、**VDAServerSetup.exe**または**VDAGWorkstationSetup.exe**を実行します。後述の「[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](#)」セクションにリストされている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、ダウンロードしたスタンドアロンパッケージは名前以外、XenDesktopのVdaSetup.exeコマンドと同じですので、同様に実行してください）。

スタンドアロンのVDAインストーラーを使用したVDAのインストール例

以下のインストールコマンドは、リモートPCアクセスでよく使用されます。これは物理的なオフィスPCにVDAをインストールしますが、Citrix ReceiverやCitrix Profile Managerはインストールしません。以下の例でインストール後にマシンは再起動されませんが、VDAを使用するには再起動が必要です。VDAは「Contr-East」という名前のControllerに登録されます。インストール時にWindowsファイアウォールサービスが検出された場合は、適切なポートが開放されます。

```
VDAGWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

注意

インストールからCitrix User Profile Manager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。

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後述の「[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](#)」のセク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

次の表は、**XenDesktopServerSetup.exe**コマンドで有効なオプションをまとめたものです。

オプション	説明
/components [...]...	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に必要な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。
/helpまたは/h	コマンドのヘルプを表示します。
/installdir	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	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（自動的に作成されません）。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）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がインストールされます。
/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。
/tempdir	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。

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

次の表は、**XenDesktopVDASetup.exe**コマンドで有効なオプションをまとめたものです。

リモートPCアクセス用のVirtual Delivery Agentをインストールする場合は、物理マシン用のオプションと、VDA for Windows Desktop OSをインストールするためのオプションを指定します。仮想マシンやマスターイメージ用のオプションは指定できません。

特に明記されている場合を除き、各オプションは物理マシンおよび仮想マシン、VDA for Windows Desktop OSおよびVDA for Windows Server OSに適用されます。

Important

XenAppおよびXenDesktop 7.9では、コマンドラインをリモートPCアクセスのみに使用し、/componentsと/remotepcの構文の順序を変更しないでください。次に例を示します。

```
VDAWorkstationSetup.exe /components vda /controllers "example.delivery.controller.net" /remotepc /EXCLUDE "AppDisks VDA Plug-in" /enable_hdx_ports /noreboot/quiet
```

/remotepcが/componentより前に使われると、/remotepcオプションは無視されます。

オプション	説明
/baseimage	(仮想マシン上にVDA for Windows Desktop OSをインストールする場合にのみ有効) 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 」の記事を参照してください。
/components []	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をインストールします • PLUGINS — Citrix Receiver for Windows (CitrixReceiver.exe) をインストールします 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。
/controllers "[]"	VDAが通信するControllerの完全修飾ドメイン名 (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。
/enable_framehawk_port	Framehawkで使用するUDPポートを開放します。デフォルト値: false
/enable_hdx_3d_pro	VDA for HDX 3D Proをインストールします。詳しくは、「 HDX 3D Pro 」の記事を参照してください。
/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および指定する機能 (Windowsリモートアシスタンス、リアルタイムオーディオトランスポート、および最適化) 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。
/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、/enable_hdx_portsオプションを指定しなくても、WindowsファイアウォールでTCPポート3389が開放されます。
/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、Machine Creation Services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 VDAのインストールからCitrix User Profile Manager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。
/hまたは/help	コマンドのヘルプを表示します。

/installdir	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	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（自動的には作成されません）。（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）。デフォルト値 = "%TEMP%\Citrix\XenDesktop Installer"
/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）VDAをマスターイメージとしてセットアップします。
/no_appv	Citrix App-Vコンポーネントのインストールを無効にします。詳しくは、 App-V 」の記事を参照してください。
/nocitrixwddm	（WDDMドライバーを含まないWindows 7マシン上でのみ有効）Citrix WDDMドライバーのインストールを無効にします。
/nodesktopexperience	（仮想マシン上にVDA for Windows Server OSをインストールする場合にのみ有効）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 Virtual Delivery Agentを使用するには、再起動が必要です。
/optimize	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アクセスでは、このオプションを指定しないでください。最適化ツールについては、 CTX125875 を参照してください。
/portnumber	（/reconfigオプションを指定する場合にのみ有効）Virtual Delivery AgentとController間の通信で使用す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以外は無効になりません）。
/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ックインターフェイスが開きます。
/remotepc	デスクトップ（ワークステーション）OSで次のコンポーネントのインストールを無効にします。 • App V Component - Citrix Personalization for App-V - VDA • UpmComponent - Citrix User Profile Manager • UpmVdaPlugin Component - Citrix User Profile Manager WMI Plugin • Mps Component - Machine Identity Service • VDisk Component - Personal vDisk アップグレード中、これらのコンポーネントがインストールされるとインストーラーが検出してアップグレードします。
/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。

/servervdi	Windowsサーバー上にVDA for Windows Desktop OSをインストールします。VDA for Windows 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 」の記事を参照してください。（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	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	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（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）。デフォルト値：c:\Windows\Temp
/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）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。
/xa_server_location	アプリケーションを配信するWindowsサーバーのURLです。

コマンドラインを使ったUniversal Print Serverのインストール

注：32ビットのWindows 2008サーバーにUpsServerコンポーネントをインストールする場合は、[32ビット Windows 2008サーバーにUniversal Print Serverをインストールする前に](#)」の手順に従ってください。

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。

- サポートされる32ビットオペレーティングシステム上：Citrixインストールメディアの\x86\Universal Print Server\ディレクトリで、**UpsServer_x86.msi**を実行します。
- サポートされる64ビットオペレーティングシステム上：Citrixインストールメディアの\x64\Universal Print Server\ディレクトリで、**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](#)」の記事にある説明に従って、このコンポーネントを構成します。

32ビット Windows 2008サーバーにUniversal Print Serverをインストールする前に

32ビットのWindows 2008マシンにUpsServer_x86.msiを展開する前に、Visual Basicスクリプト、またはOrcaなどのツールを使って、cdf_x86.msiとUpsServer_x86.msiで使用するWindowsインストーラーの最小バージョンを調節する必要があります。

- CDFおよびUPS MSIファイル（cdf_x86.msiおよびUpsServer_x86.msi）の32ビットバージョンを一時フォルダーにコピーします。
- WiSumInf.vbsスクリプトまたはOrcaツールをインストールします。これらは、[Windows SDK Components for Windows Installer Developers](#)パッケージに収録されています。スクリプトについて詳しくは、MSDNの技術文書 [Manage Summary Information](#)」を参照してください。
- 次のいずれかの方法で、Windowsインストーラーの最小バージョンを変更できます。

WiSumInf.vbsスクリプトを使用する：WiSumInf.vbsを2つのCitrix msiと同じ一時フォルダーにコピーします。次に、パラメータ **WiSumInf.vbs cdf_x86.msi Pages=405**および**WiSumInf.vbs UpsServer_x86.msi Pages=405**を指定して、それぞれのパッケージでスクリプトを実行します。

Orcaを使用する：cdf_x86.msiおよびUpsServer_x86.msiパッケージをそれぞれ開き、[View menu]、[Summary Information] の順に選択して、**[Schema]** テキストボックスの値を**405**に変更します。

前述の手順を完了したら、プリントサーバーにUniversal Print Serverをインストールします。

スクリプトを使用したVDAのインストール

Jul 07, 2016

注：このアーティクルは、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れます。LinuxオペレーティングシステムのVDAについては、「[Red Hat Linux VDA](#)」および「[SUSE Linux VDA](#)」を参照してください。

インストールメディアには、Active Directory環境のマシンのグループで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、このスクリプトを個々のマシンに適用して、それらを使って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、操作が成功した場合にはプレフィックスとしてPASSが付き、そのほかの場合はFAILが付きます。失敗したインストールまたは削除処理をすばやく検索できるように、ターゲットマシンのローカルドライブではなく、ネットワーク共有を使用します。

重要：インストールを開始する前に、「[インストールの準備](#)」を読み、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には

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、「SET DESIREDVERSION」により指定します。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](#)」で説明されているとおりにVDA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Active Directoryの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。

スクリプトを使ってVDAを削除するには

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Active Directoryの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、マシンへの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、ターゲットマシンのローカルドライブを調べることでトラブルシューティングを実行できます。初期トラブルシューティングのため、各マシン上の%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

これらのログの内容から、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。

Red Hat Linux Virtual Delivery Agent (VDA) のインストール

Jul 07, 2016

Red Hat/CentOSディストリビューションをベースとしたLinux仮想デスクトップを作成できます。Linux仮想マシンを準備して新しいソフトウェアをインストールし、Delivery Controllerを構成したらStudioを使ってユーザーがデスクトップを使用できるようにします。

詳しくは、この記事に記載されている情報を参照してください。

注意

このドキュメントで使用するLinuxシェルコマンドは、GNU Bashシェルで動作することが確認されています。

この記事は、次のセクションで構成されています。

- [システム要件](#)
- [Delivery Controllerの構成](#)
- [VDAをインストールするLinuxマシンの準備](#)
- [Linuxマシンカタログおよびデリバリーグループの構成](#)
- [Linux VDAソフトウェアのインストール](#)
- [VDAソフトウェアの実行](#)
- [Linux VDAソフトウェアのアンインストール](#)
- [トラブルシューティング](#)
- [既知の問題](#)
- [用語集](#)

システム要件

Linuxディストリビューション

Linux Virtual Desktop製品では、次のLinuxディストリビューションがサポートされます。

- SUSE Linux Enterprise
 - Desktop 11 Service Pack 4
 - Desktop 12 Service Pack 1
 - Server 11 Service Pack 4
 - Server 12 Service Pack 1
- Red Hat Enterprise Linux
 - Workstation 6.7
 - Workstation 7.2
 - Server 6.7
 - Server 7.2
- CentOS Linux

- CentOS 6.7
- CentOS 7.2

注意

すべての場合で、サポートされるプロセッサアーキテクチャはx86-64です。

ヒント

CentOS Linuxはバージョン1.3以降でサポートされます。この記事に記載されているインストールに関する情報は、CentOSにも適用できます。

XenDesktop

Linux VDAでは、次のバージョンのXenDesktopがサポートされます。

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Linux VDAの構成手順はWindows VDAの場合と多少異なります。ただし、Delivery ControllerファームはWindowsデスクトップとLinuxデスクトップを両方とも仲介できます。

注意

Linux VDAは、XenDesktop Version 7.0以前には対応していません。

Citrix Receiver

次のバージョンのCitrix Receiverがサポートされます。

- Citrix Receiver for Windows Version 4.4以降 (wfica32.exeのv14.4と同じ)
- Citrix Receiver for Linux Version 13.3以降
- Citrix Receiver for Mac OSX Version 12.1以降
- Citrix Receiver for Android Version 3.8以降
- Citrix Receiver for iOS Version 6.1.4以降
- Citrix Receiver for Chrome/HTML5 Version 2.0 (Access Gateway経由でのみサポート)

ハイパーバイザー

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

- XenServer

- VMware ESXおよびESXi
- Microsoft Hyper-V

ベアメタルホスティングもサポートされます。

ヒント

サポートされるプラットフォームの一覧については、ハイパーバイザーのベンダーのドキュメントを参照してください。

Active Directory統合パッケージ

Linux VDAでは、次のActive Directory統合パッケージまたは製品がサポートされます。

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

ヒント

サポートされるプラットフォームの一覧については、Active Directory統合パッケージのベンダーのドキュメントを参照してください。

HDX 3D Pro

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

ハイパーバイザー

以下のハイパーバイザーがサポートされます。

- XenServer
- VMware ESXおよびESXi

Linuxディストリビューション

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

- Red Hat Enterprise Linux - Workstation 7.2

GPU

以下のGPUがサポートされます。

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

Delivery Controllerの構成

XenDesktop 7.7以降には、Linux Virtual Desktopをサポートするための必要な変更が含まれていますが、以前のバージョンの場合は、Hotfixまたは更新スクリプトが必要です。これらのインストールと確認について、このセクションで説明しています。

Delivery Controller構成の更新

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

- [CTX142438](#) : Hotfixes Update 2 - Delivery Controller 7.6 (32ビット) 用 – 英語
- [CTX142439](#) : Hotfixes Update 2 - Delivery Controller 7.6 (64ビット) 用 – 英語

XenDesktopの以前のバージョンに対しては、ブローカーサービスの構成を更新するUpdate-BrokerServiceConfig.ps1という名前のPowerShellスクリプトが提供されています。これは次のパッケージから入手できます。

- citrix-linuxvda-scripts-1.3.0.zip

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

1. Update-BrokerServiceConfig.ps1スクリプトをDelivery Controllerマシンにコピーします。
2. ローカル管理者のコンテキストでWindows PowerShellコンソールを開きます。
3. スクリプトを含むフォルダーを参照します。
4. 次のスクリプトを実行します。

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

注意

デフォルトでは、PowerShellはPowerShellスクリプトを実行できないように構成されています。スクリプトの実行に失敗する場合は、再試行する前にPowerShell実行ポリシーの変更が必要な場合があります。

```
Set-ExecutionPolicy Unrestricted
```

Update-BrokerServiceConfig.ps1スクリプトを実行すると、Linux VDAに必要とされる新しいWCFエンドポイントでブローカーサービス構成ファイルが更新され、ブローカーサービスが再起動します。このスクリプトでは、自動的にブローカーサービス構成ファイルの場所が特定されます。元の構成ファイルのバックアップが、**.prelinux**という拡張子で同じディレクトリに作成されます。

これらの変更は、同じDelivery Controllerファームを使用するように構成されたWindows VDAの仲介には影響しません。このことにより、単一のControllerファームがWindows VDAおよびLinux VDAの両方とのセッションをシームレスに管理し、仲介できます。

Delivery Controller構成の確認

必要な構成変更がDelivery Controllerに適用されているかどうかを確認するには、次のファイル中に文字列**EndpointLinux**が5回出現していることを確認します。

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

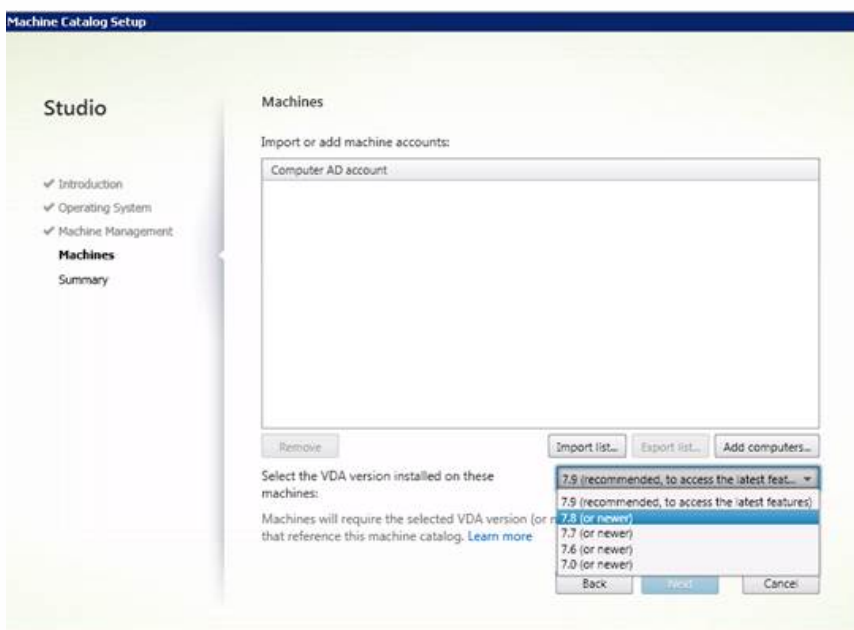
Windowsコマンドプロンプトで、ローカル管理者としてログオンし、次の操作を行います。

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

```
findstr EndpointLinux BrokerService.exe.config
```

Important

バージョン1.3では、Linux VDAのBroker AgentはXenApp 7.8およびXenDesktop 7.8に設定されます。ただし、Studioの「マシンカタログのセットアップ」画面でマシンカタログを追加する場合、デフォルト値は自動的にバージョン7.9に設定されます。インストールするVDAのバージョンを、**7.8（またはそれより新しい）**バージョンに明示的に設定する必要があります。下の図を参照してください。



VDAをインストールするLinuxマシンの準備

ネットワーク構成の確認

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

RHEL 6のみ：ホスト名の設定

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

```
HOSTNAME=hostname
```

RHEL 7のみ：ホスト名の設定

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

ホスト名へのループバックアドレスの割り当て

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

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

次に例を示します。

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

ファイルのほかのエントリから、**hostname-fqdn**または**hostname**に対するその他の参照を削除します。

注意

Linux VDAでは、現在、NetBIOS名の切り捨てをサポートしていません。したがって、ホスト名は15文字以下にしてください。

ヒント

a~z、0~9、およびハイフン (-) の文字のみ使用してください。アンダースコア (_)、スペース、およびその他の記号は使用しないでください。ホスト名を数字で開始したり、ハイフンで終了したりしないでください。

ホスト名の確認

次のコマンドで、ホスト名が正しく設定されていることを確認します。

```
hostname
```

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

次のコマンドで、完全修飾ドメイン名が正しく設定されていることを確認します。

```
hostname -f
```

これにより、そのマシンの完全修飾ドメイン名が返されます。

名前解決とサービス到達可能性の確認

次のコマンドで、完全修飾ドメイン名が解決できることと、ドメインコントローラーとXenDesktop Delivery Controllerからpingに応答があることを確認します。

```
nslookup domain-controller-fqdn
```

```
ping domain-controller-fqdn
```

```
nslookup delivery-controller-fqdn
```

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

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

時刻同期の構成（NTP）

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

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

RHEL 6のみ：NTPサービスの構成

rootとして**/etc/ntp.conf**を編集し、次のように各リモートタイムサーバーに対応するサーバーエントリを追加します。

```
server peer1-fqdn-or-ip-address iburst
```

```
server peer2-fqdn-or-ip-address iburst
```

一般的な環境では、時間はローカルドメインコントローラーから同期する必要があり、公開NTPプールサーバーから直接は同期しません。ドメインの各Active Directoryドメインコントローラーに対応するサーバーエントリを追加します。

ループバックIPアドレス、localhost、パブリックサーバーの***.pool.ntp.org**エントリなど、一覧にあるその他の**server**エントリを削除します。

変更を保存してから、次のコマンドでNTPデーモンを再起動します。

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

RHEL 7のみ：Chronyサービス

rootとして**/etc/chrony.conf**を編集し、次のように各リモートタイムサーバーに対応するサーバーエントリを追加します。

```
server peer1-fqdn-or-ip-address iburst
```

```
server peer2-fqdn-or-ip-address iburst
```

一般的な環境では、時間はローカルドメインコントローラーから同期する必要があり、公開NTPプールサーバーから直接は同期しません。ドメインの各Active Directoryドメインコントローラーに対応するサーバーエントリを追加します。

ループバックIPアドレス、localhost、パブリックサーバーの***.pool.ntp.org**エントリなど、一覧にあるその他の**server**エントリを削除します。

変更を保存してから、次のコマンドでChronyデーモンを再起動します。

```
sudo /sbin/service chronyd restart
```

ネットワークプロキシ認証ポップアップを無効にする

RHEL 6の特定の問題が原因となって、ログオン後、ユーザーにルートパスワードの入力を求めるポップアップが表示されません。

この問題を解決するには、rootとしてテキストエディターで**/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla**ファイルを作成し、次の内容を追加します。

```
[No Show Proxy Dialog]
```

```
Identity=unix-user:*
```

```
Action=org.freedesktop.packagekit.system-network-proxy-configure
```

```
ResultAny=no
```

```
ResultInactive=no
```

```
ResultActive=no
```

ヒント

この問題について詳しくは、[こちら](#)にあるRedHatソリューションのページを参照してください。コメントセクションに適切な回避策が説明されています。

OpenJDKのインストール

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

RHEL 6のみ : OpenJDK 1.7

次のコマンドで正しいバージョンを確認します。

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

事前にパッケージされたOpenJDKは、以前のバージョンである可能性があります。必要に応じて、次のコマンドで最新バージョンに更新します。

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

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

```
export JAVA_HOME=/usr/lib/jvm/java
```

新しいシェルを開き、次のコマンドでJavaのバージョンを確認します。

```
java -version
```

RHEL 7.0のみ : OpenJDK 1.8

次のコマンドで正しいバージョンを確認します。

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

事前にパッケージされたOpenJDKは、以前のバージョンである可能性があります。必要に応じて、次のコマンドで最新バージョンに更新します。

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

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

```
export JAVA_HOME=/usr/lib/jvm/java
```

新しいシェルを開き、次のコマンドでJavaのバージョンを確認します。

```
java -version
```

ヒント

問題を回避するには、必ずOpenJDK Version 1.7.0または1.8.0のいずれかのみをインストールしておきます。その他のバージョンのJavaは、システムからすべて削除します。

PostgreSQLのインストール

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

次のパッケージをインストールします。

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

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

RHEL 6のみ：PostgreSQL 8

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

RHEL 7のみ：PostgreSQL 9

```
sudo postgresql-setup initdb
```

PostgreSQLの起動

いずれのバージョンのPostgreSQLでも、次のコマンドで、起動時にサービスを開始する構成と、直ちにサービスを開始する構成を行います。

```
sudo /sbin/chkconfig postgresql on
```

```
sudo /sbin/service postgresql start
```

次のコマンドを使用して、PostgreSQLのバージョンを確認します。

```
psql --version
```

次のように**psql**コマンドラインユーティリティを使用して、データディレクトリが設定されていることを確認します。

```
sudo -u postgres psql -c 'show data_directory'
```

Motifのインストール

Linux VDAには、ディストリビューションに応じて、motifパッケージまたはopenmotifパッケージが必要です。

RHEL 6のみ : Open Motif

```
sudo yum -y install openmotif
```

RHEL 7のみ : Motif

```
sudo yum -y install motif
```

印刷サポートのインストール

Linux VDAには、CUPSフィルターとFoomaticフィルターの両方が必要です。

RHEL 6のみ : 印刷サポート

```
sudo yum -y install cups
```

```
sudo yum -y install foomatic
```

RHEL 7のみ : 印刷サポート

```
sudo yum -y install cups
```

```
sudo yum -y install foomatic-filters
```

ほかのパッケージのインストール

次のコマンドで、ほかの必要なパッケージをインストールします。

```
sudo yum -y install redhat-lsb-core
```

```
sudo yum -y install ImageMagick
```

ハイパーバイザー用Linux仮想マシンの準備

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

Citrix XenServerでの時間同期の修正

XenServerの時間同期機能が有効な場合、それぞれの準仮想化Linux仮想マシンで、NTPとXenServerの両方がシステムの時刻を管理しようとするのが原因となり問題が発生します。システムの時刻とほかのサーバーの時刻との同期が失われるのを防ぐには、各Linuxゲストのシステムの時刻がNTPと同期する必要があります。この状態にするには、ホストの時間同期を無効にする必要があります。HVMモードでは、変更は必要ありません。

一部のLinuxディストリビューションでは、XenServer Toolsをインストールした状態で準仮想化Linuxカーネルを実行すると、XenServerの時間同期機能が存在し有効になっているかどうかをLinux仮想マシンから次のようにして確認できます。

```
su -
```

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

これにより、次のいずれかが返されます。

- 0 - 時間同期機能が有効となっていて、無効にする必要があります。
- 1 - 時間同期機能が無効となっていて、これ以上の操作は必要ありません。

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

時間同期機能が有効な場合は、次のようにしてファイルに1を書き込んで無効にします。

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

この変更を永続化し、再起動後も保持するには、/etc/sysctl.confファイルを編集して、次の行を追加します。

```
xen.independent_wallclock = 1
```

これらの変更を確認するため、次のようにしてシステムを再起動します。

```
reboot
```

再起動後、次のようにしてこの変更が正しく設定されているかどうか確認します。

```
su -
```

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

これにより、値1が返されます。

Microsoft Hyper-Vでの時間同期の修正

Hyper-V Linux統合サービスがインストールされたLinux仮想ホストでは、Hyper-Vの時間同期機能を活用してホストオペレーティングシステムの時間を利用できます。システムの時刻を正確な状態で維持するには、NTPサービスと共にこの機能を有効にする必要があります。

管理オペレーティングシステムで、次の操作を行います。

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

注意

この方法はVMwareおよびXenServerの場合とは異なります。VMwareおよびXenServerでは、NTPとの競合を避けるためにホストの時間同期を無効にします。Hyper-Vの時間同期は、NTPと共存し、NTPの時間同期を補完することができます。

ESXおよびESXiでの時間同期の修正

VMwareの時間同期機能が有効な場合、それぞれの準仮想化Linux仮想マシンで、NTPとハイパーバイザーの両方がシステムの時刻を同期しようとするのが原因となり問題が発生します。システムの時刻とほかのサーバーの時刻との同期が失われるのを防ぐには、各Linuxゲストのシステムの時刻がNTPと同期する必要があります。この状態にするには、ホストの時間同期を無効にする必要があります。

VMware Toolsをインストールした状態で準仮想化Linuxカーネルを実行している場合は、次の操作を行います。

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

Windows ドメインへのLinuxマシンの追加

Linux用のXenDesktopでサポートされるLinuxマシンをActive Directoryドメインに追加する方法は、以下のように複数あります。

- Samba Winbind
- Quest Authentication Services
- Centrify DirectControl

選択した方法に応じて、以下の手順に従います。

Samba Winbind

必要なパッケージのインストールまたは更新

次のようにして、必要なパッケージをインストールまたは更新します。

```
sudo yum -y install samba-winbind \
    samba-winbind-clients \
    krb5-workstation \
    authconfig \
    oddjob-mkhomedir
```

起動時にWinbindデーモンが開始するようにする

次のコマンドで、起動時にWinbindデーモンが開始するように構成する必要があります。

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

Winbind認証の構成

次のようにして、Winbindを使用したKerberos認証用にマシンを構成します。

```
sudo authconfig \
    --disablecache \
    --disablesd \
    --disablesdauth \
    --enablewinbind \
    --enablewinbindauth \
```

```
--disablewinbindoffline \  
  
--smbsecurity=ads \  
  
--smbworkgroup=domain \  
  
--smbrealm=REALM \  
  
--krb5realm=REALM \  
  
--krb5kdc=fqdn-of-domain-controller \  
  
--winbindtemplateshell=/bin/bash \  
  
--enablemkhomedir --updateall
```

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

KDCサーバーおよびレルム名をDNSベースで参照する必要がある場合は、次の2つのオプションを上記のコマンドに追加します。

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

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

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

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

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

Windowsドメインへの参加

これには、ドメインコントローラーに到達できることと、コンピューターをドメインに追加する権限を持つActive Directoryユーザーアカウントが必要です。

```
sudo net ads join REALM -U user
```

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

Winbind用のPAMの構成

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

```
krb5_auth = yes
```

```
krb5_ccache_type = FILE
```

```
mkhomedir = yes
```

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

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

ヒント

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

/etc/krb5.confを開いて、[libdefaults]セクションで次の設定をKEYRINGからFILEタイプに変更します。

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

ドメインメンバーシップの確認

XenDesktopのコントローラーを使用するには、WindowsまたはLinuxに関係なく、すべてのVDAマシンでActive Directoryにコンピューターオブジェクトが必要です。

次のように、Sambaの**net ads**コマンドを使用して、マシンがドメインに参加していることを確認します。

```
sudo net ads testjoin
```

次のコマンドで、追加のドメインおよびコンピューターオブジェクトの情報を確認できます。

```
sudo net ads info
```

Kerberos構成の確認

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

```
sudo klist -ke
```

これにより、プリンシパル名と暗号スイートのさまざまな組み合わせに対して使用できるキーの一覧が表示されます。Kerberosの**kinit**コマンドを実行し、これらのキーを使用して、マシンをドメインコントローラーに対して認証します。

```
sudo kinit -k MACHINE\${@REALM}
```

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

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

```
sudo klist
```

次のコマンドを使用して、マシンのアカウントの詳細を調査します。

```
sudo net ads status
```

ユーザー認証の確認

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

```
wbinfo --krb5auth=domain\\username%password
```

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

Winbind PAMモジュールが正しく構成されていることを確認するには、次のように、以前にマシンにログオンしたことがないドメインユーザーアカウントを使用してローカルでログオンします。

```
ssh localhost -l domain\\username
```

```
id -u
```

次のコマンドで、**id -u**コマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

次のコマンドで、セッションを終了します。

```
diskpart.exeを終了します
```

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

Quest Authentication Services

ドメインコントローラーでのQuestの構成

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

Linux VDAマシンにドメインユーザーがログオンできるようにする

Linux VDAマシンでHDXセッションを確立する必要がある各ドメインユーザーに対して、次の操作を行います。

1. [Active Directoryユーザーとコンピューター] 管理コンソールで、目的のユーザーアカウントのActive Directoryユーザーのプロパティを開きます。
2. [Unix Account] タブを選択します。
3. [Unix-enabled] チェックボックスをオンにします。
4. [Primary GID Number] のプライマリGID番号を、実際のドメインユーザーグループのグループIDに設定します。

注意

この手順は、ドメインユーザーがコンソール、RDP、SSH、またはその他のリモート処理プロトコルを使用してログオンできるように設定する場合も同じです。

Linux VDAでのQuestの構成

SELinuxポリシー適用の回避策

デフォルトのRHEL環境では、SELinuxが完全に適用されています。これは、Questが使用するUnixドメインソケットのIPCのメカニズムに干渉し、ドメインユーザーのログオンを妨げます。

ヒント

回避策はいくつかあり、その概要は[こちら](#)で説明されています。

最も簡単な方法は、SELinuxを無効にすることです。rootとして、/etc/selinux/configを編集し、SELinux設定を次のとおりに変更します。

```
SELINUX=disabled
```

この変更を行うには、次のコマンドで再起動する必要があります。

```
reboot
```

Important

この設定は注意して使用してください。SELinuxポリシーの適用を無効にした後に再度有効にすると、ルートユーザーやその他のローカルユーザーであっても、完全にロックアウトされてしまう可能性があります。

VASデーモンの構成

次のようにKerberosチケットの自動更新を有効にして、切断する必要があります。また、認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd \  
    auto-ticket-renew-interval 32400  
sudo /opt/quest/bin/vastool configure vas vas_auth \  
    allow-disconnected-auth false
```

これにより、更新間隔が9時間（32400秒）に設定されます。すなわち、チケットのデフォルトの有効期間である10時間よりも1時間短くなります。チケットの有効期間がさらに短いシステムでは、より小さい値をこのパラメーターに設定します。

PAMおよびNSSの構成

Questでは、HDXや、su、ssh、RDPなどのその他のサービスを介したドメインユーザーのログインを可能にするには、PAMとNSSを手動で構成する必要があります。PAMおよびNSSを構成するには、次のコマンドを実行します。

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

Windowsドメインへの参加

次のように、Questのvastoolコマンドを使用して、LinuxマシンをActive Directoryドメインに追加します。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

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

ドメインメンバーシップの確認

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

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合は、ドメイン名が返されます。 参加していない場合は、次のエラーが表示されます。

```
ERROR: No domain could be found.
```

```
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
```

```
default_realm not configured in vas.conf. Computer may not be joined to domain
```

ユーザー認証の確認

QuestがPAMを使用してドメインユーザーを認証できることを確認するには、次のように、以前にマシンにログオンしたことがないドメインユーザーアカウントを使用してログオンします。

```
ssh localhost -l domain\\username
```

```
id -u
```

次のコマンドで、**id -u**コマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

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

```
/opt/quest/bin/vastool klist
```

次のコマンドで、セッションを終了します。

```
diskpart.exeを終了します
```

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

Centrify DirectControl

Windowsドメインへの参加

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


```
su -
```

```
adjoin -w -V -u user domain-name
```

userパラメーターは、コンピューターをActive Directoryドメインに追加する権限を持つ任意のActive Directoryドメインユーザーです。 **domain-name**パラメーターは、Linuxマシンを追加するドメインの名前です。

ドメインメンバーシップの確認

XenDesktopのコントローラーを使用するには、WindowsまたはLinuxに関係なく、すべてのVDAマシンでActive Directoryにコンピューターオブジェクトが必要です。Centrifyにより追加されたLinuxマシンがドメインに存在することを確認するには、次のコマンドを実行します。

```
su -
```

```
adinfo
```

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

次を使用すると、より包括的なシステム情報と診断情報を取得できます。

```
adinfo --sysinfo all
```

```
adinfo --diag
```

さまざまなActive DirectoryおよびKerberosサービスとの接続をテストするには、次のコマンドを実行します。

```
adinfo --test
```

NVIDIA GRIDドライバーのインストール

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

次のオプションを構成します。

1. Citrix XenServer
2. VMware ESX

選択したハイパーバイザーに対応する手順に従います。

Citrix XenServer

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

VMware ESX

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

VDAマシン

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

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

NVIDIA GRIDドライバー用にマシンを準備するには、次の手順が必要です。

```
# yum install gcc

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

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

完了したら、[Red Hat Enterprise Linuxのドキュメント](#)の手順に従って、NVIDIA GRIDドライバーをインストールします。

注意

GPUドライバーのインストール時は、すべての質問でデフォルト（「いいえ」）を選択してください。

Important

GPUパススルーが有効になると、XenCenterを介してLinux VMにアクセスできなくなります。したがって、接続するにはSSHを使用する必要があります。

NVIDIA GRID™グラフィックドライバーが正しくインストールされているかどうかを確認するには、「nvidia-smi」を実行します。次の内容に似た結果が出力されます。

nvidia-smi

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

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

次のコマンドで、カードに適切な構成を設定します。

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

高い解像度やマルチモニター機能を利用するには、有効なNVIDIAライセンスが必要です。このライセンスを適用するには、『GRID Licensing Guide.pdf - DU-07757-001 September 2015』の製品ドキュメントに従ってください。

Linuxマシンカタログおよびデリバリーグループの構成

マシンカタログへのLinuxマシンの追加

マシンカタログを作成し、Linux VDAマシンを追加する手順は、従来のWindows VDAでの方法とほとんど同じです。このタスクを完了する方法のより総合的な説明については、オンラインのCitrix製品ドキュメントを参照してください。

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

- オペレーティングシステムには、次を選択します。
 - ホストされる共有デスクトップ配信モデルの場合、[WindowsサーバーOS] オプションまたは[サーバーOS] オプション
 - VDI専用デスクトップ配信モデルの場合、[WindowsデスクトップOS] オプションまたは[デスクトップOS] オプション
- マシンが電源管理を行わない設定になっていることを確認します。
- PVSおよびMCSはLinux VDAではサポートされないため、ほかのサービスまたはテクノロジー (既存のイメージ) の展開方法を選択してください。
- 同じマシンカタログで、Linux VDAマシンとWindows VDAマシンを混在させないでください。

注意

以前のバージョンのCitrix Studioでは、「Linux OS」という概念に対応していませんでした。ただし、[WindowsサーバーOS] オプションまたは[サーバーOS] オプションを選択すると、同等のホストされる共有デスクトップ配信モデルが暗黙的に選択されます。[WindowsデスクトップOS] オプションまたは[デスクトップOS] オプションを選択すると、XenDesktopのマシンごとに単一ユーザーの配信モデルが暗黙的に選択されます。

マシンカタログを作成するためのCitrixドキュメントは、以下を参照してください。

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)
- [XenDesktop 7.9](#)

上記より前のバージョンのXenDesktopはサポートされません。

ヒント

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

デリバリーグループの追加

デリバリーグループを作成し、Linux VDAマシンを含むマシンカタログを追加する手順は、Windows VDAマシンの場合とほとんど同じです。このタスクを完了する方法のより総合的な説明については、オンラインのCitrix製品ドキュメントを参照してください。

Linux VDAマシンカタログを含むデリバリーグループを作成する場合は、次の制約があります。

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

デリバリーグループを作成するためのCitrixドキュメントは、以下を参照してください。

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)
- [XenDesktop 7.9](#)

上記より前のバージョンのXenDesktopはサポートされません。

Linux VDAソフトウェアのインストール

古いバージョンのアンインストール

Version 1.0よりも古いバージョンのLinux VDAがインストールされている場合は、それをアンインストールしてから新しいバージョンをインストールします。

次のコマンドで、Linux VDAサービスを停止します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

次のコマンドで、パッケージをアンインストールします。

```
sudo rpm -e XenDesktopVDA
```

Important

テクニカルプレビューリリースからバージョン1.0、1.1、1.2、または1.3へのアップグレードはサポートされません。

Red Hat Enterprise Linux 6.0については、Xorg-x11-server-Xorg Version 1.15の取得をお勧めします。このパッケージはアップグレードしないでください。

注意

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

コマンドを実行するには、フルパスが必要です。代わりに、システムパス`/opt/Citrix/VDA/sbin`と`/opt/Citrix/VDA/bin`を追加することもできます。

Linux VDAのインストール

次のように、RPM Package Managerを使用して、Linux VDAソフトウェアをインストールします。

RHEL 6の場合：

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm
```

RHEL 7.2の場合：

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm
```

Linux VDAのアップグレード

Linux VDA Version 1.1またはVersion 1.2をインストールしている場合は、RPM Package Managerを使用して、Linux VDAソフトウェアをアップグレードします。

RHEL 6の場合：

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.el6.x86_64.rpm
```

RHEL 7.2の場合：

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.el7.x86_64.rpm
```

Important

アップグレード後は、Linux VDAマシンを再起動してください。

Linux VDAの構成

パッケージのインストール後、ctxsetup.sh スクリプトを実行して、Linux VDAを構成する必要があります。パッケージをアップグレードした場合、ctxsetup.shスクリプトを実行してアップグレードを完了する必要があります。変更を行う前に、このスクリプトでは、環境を確認し、すべての依存コンポーネントがインストールされていることが確認されます。必要に応じて、いつでもこのスクリプトを再実行して設定を変更できます。

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

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

質問に回答する構成

次のようにして、質問に回答する手動構成を実行します。

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

自動化された構成

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

サポートされる環境変数には次のようなものがあります。

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Virtual Delivery Agentでは、DNS CNAMEレコードを使用して、Delivery Controller名を指定することができます。通常は、Nに設定します。
- CTX_XDL_DDC_LIST = list-ddc-fqdns - Virtual Delivery Agentには、配信の登録に使用するDelivery Controllerの完全修飾ドメイン名
- (FQDN) のスペース区切りの一覧が必要です。1つ以上の完全修飾ドメイン名またはCNAMEエイリアスを指定する必要があります。
- CTX_XDL_VDA_PORT = port-number - Virtual Delivery Agentは、TCP/IPポートを使用してDelivery Controllerと通信します。通常は、ポート80です。
- CTX_XDL_REGISTER_SERVICE = Y | N - Linux Virtual Desktopサービスは、起動時の開始をサポートします。通常は、Yに設定します。
- CTX_XDL_ADD_FIREWALL_RULES = Y | N - Linux Virtual Desktopサービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop用に、システムのファイアウォールの必要なポート（デフォルトではポート80およびポート1494）を自動で開放できます。通常は、Yに設定します。
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 - Virtual Delivery Agentには、Delivery Controllerに対して認証するためにKerberos構成設定が必要です。Kerberos構成は、システムにインストールおよび構成済みのActive Directory統合ツールから指定します。次に示す、サポートされているActive Directory統合方法のうち、使用するものを指定します。
 - 1 - Samba Winbind
 - 2 - Quest Authentication Services
 - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO = Y | N - Linux Virtual Desktopでは、HDX 3D Proがサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連のグラフィックアクセラレーションテクノロジーです。HDX 3D Proをサポートするには、対応するNVIDIA GRIDグラフィックカードをインストールする必要があります。HDX 3D Proを選択した場合、Virtual Delivery AgentはVDIデスクトップ（単一セッション）モード用に構成されます（すなわち、CTX_XDL_VDI_MODE=Yとなります）。これは、SUSEではサポートされていません。必ずこの値をNに設定してください。
- CTX_XDL_VDI_MODE = Y | N - 専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro環境の場合は、Yに設定する必要があります。通常は、Nに設定します。
- CTX_XDL_SITE_NAME = dns-name - Virtual Delivery Agentは、DNSを使用してLDAPサーバーを検出し、LDAPサービスレコードを照会します。DNSの検索結果をローカルサイトに制限するには、DNSサイト名を指定します。通常は、空（none）です。
- CTX_XDL_LDAP_LIST = list-ldap-servers - Virtual Delivery Agentは、デフォルトではDNSを照会してLDAPサーバーを検出します。ただし、DNSがLDAPサービスレコードを提供できない場合は、LDAPの完全修飾ドメイン名（FQDN）およびLDAPポートのスペース区切りの一覧（例：ad1.mycompany.com:389）を指定することができます。通常は、空（none）です。
- CTX_XDL_SEARCH_BASE = search-base - Virtual Delivery Agentは、デフォルトではActive Directoryドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを使用してLDAPを照会します。ただし、検索のパフォーマンスを改善するために検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。通常は、空（none）です。
- CTX_XDL_START_SERVICE = Y | N - Linux VDA構成の完了時にLinux VDAサービスが開始されるようにするかどうかを指定します。通常は、Yに設定します。

次のようにして、環境変数を設定し、構成スクリプトを実行します。

```

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

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

```

sudoに-Eオプションを指定し、作成する新しいシェルに既存の環境変数を渡す必要があります。 Citrixは、最初の行に#!/bin/bashを記述し、上記のコマンドからなるシェルスクリプトファイルを作成することをお勧めします。

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

```

sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
CTX_XDL_DDC_LIST=list-ddc-fqdns \
CTX_XDL_VDA_PORT=port-number \
CTX_XDL_REGISTER_SERVICE=Y|N \
CTX_XDL_ADD_FIREWALL_RULES=Y|N \
CTX_XDL_AD_INTEGRATION=1|2|3 \
CTX_XDL_HDX_3D_PRO=Y|N \
CTX_XDL_VDI_MODE=Y|N \
CTX_XDL_SITE_NAME=dns-name \
CTX_XDL_LDAP_LIST=list-ldap-servers \
CTX_XDL_SEARCH_BASE=search-base \
CTX_XDL_START_SERVICE=Y|N \
/opt/Citrix/VDA/sbin/ctxsetup.sh

```


構成変更の削除

シナリオによっては、Linux VDAパッケージをアンインストールしないで、ctxsetup.shスクリプトによって行われた構成変更を削除することが必要となる場合があります。

続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します。

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

構成変更を削除するには、次のコマンドを実行します。

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

Important

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

構成ログ

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

```
/tmp/xdl.configure.log
```

Linux VDAサービスを再起動し、変更を反映させます。

VDAソフトウェアの実行

ctxsetup.shスクリプトを使用してLinux VDAを構成したら、次のコマンドを使用してLinux VDAを制御します。

Linux VDAの起動

Linux VDAサービスを起動するには、次のコマンドを実行します。

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

Linux VDAの停止

Linux VDAサービスを停止するには、次のコマンドを実行します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Linux VDAの再起動

Linux VDAサービスを再起動するには、次のコマンドを実行します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

Linux VDAの状態の確認

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

```
sudo /sbin/service ctxvda status
```

```
sudo /sbin/service ctxhdx status
```

Linux VDAソフトウェアのアンインストール

Linux VDAのインストール状態の照会

Linux VDAがインストールされているかどうかを確認したり、インストールされているパッケージのバージョンを表示したりするには、次のコマンドを実行します。

```
rpm -q XenDesktopVDA
```

詳細を表示するには、次のコマンドを実行します。

```
rpm -qi XenDesktopVDA
```

注意

Linux VDAソフトウェアをアンインストールすると、関連付けられたPostgreSQLおよびその他の構成データが削除されます。ただし、Linux VDAのインストールより前にセットアップされた、PostgreSQLパッケージおよびその他の依存するパッケージは削除されません。

依存するパッケージの削除

この記事では、PostgreSQLなど、依存するパッケージの削除方法については説明していません。

トラブルシューティング

H.264エンコーディングが使用中であるかどうかの確認

Linux VDA v1.3によってH264およびHardwareEncodingの値がレジストリパスHKLM\Software\Citrix\Ica\Session\<セッションID>\Graphicsに追加され、VDAで発生するグラフィックの問題のトラブルシューティングに役立ちます。

セッションを起動するには、次のコマンドを実行して、H.264エンコーディングをLinux VDAでアドバタイズします。

```
/opt/Citrix/VDA/bin/ctxreg create -k
```

```
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
```

```
"AdvertiseH264" -d "0x00000001" --force
```

セッションを開始して、キーH264がレジストリパスで作成されていることを確認します。作成されている場合、H.264エンコーディングが使用中であることを意味します。

```
/opt/Citrix/VDA/bin/ctxreg list -k  
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

3D Proのハードウェアエンコーディングが使用中であるかどうかの確認

3D Proハードウェアエンコーディング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、次のコマンドを使用します。

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

セッションを開始して、レジストリパスの"HardwareEncoding"の値を確認します。この値が「0」の場合は使用されておらず、「1」はハードウェアエンコーディングが使用中であることを意味します。

```
/opt/Citrix/VDA/bin/ctxreg list -k  
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

以下のコマンドを使用して、セッションIDをクエリします。

```
/opt/Citrix/VDA/bin/ctxqsession
```

各ユーザーのデスクトップ環境のカスタマイズ

現在、Linux VDAではユーザーがログイン時にデスクトップ環境を選択することを許可していません。この問題の回避策として、ユーザーはLinuxディストリビューション用にファイル（.xsessionなど）を構成して、各ユーザーにデフォルトのデスクトップ環境を設定することができます。詳しくは、Linuxディストリビューションに付属のドキュメントを参照してください。

KDEをデフォルトの環境として設定する場合：

```
#!/usr/bin/env bash  
  
exec startkde
```

GNOMEをデフォルトのデスクトップ環境として設定する場合：

```
#!/usr/bin/env bash  
  
exec gnome-session
```

Linuxマシンが正しく準備されているかどうかの確認

最も一般的な問題は、主にネットワーク、NTPタイムサーバー構成、またはActive Directoryドメインのメンバーシップに関連する、Linuxマシンの誤った構成から直接引き起こされます。多くの場合、Linuxマシンの構成を修正すると、VDAソフトウェアの問題は解決します。

ログとトレースの構成

Broker AgentとHDXサービスでは、syslogにログを記録します。Citrixサポートには、サポートへの連絡時に追加のトレースを有効にできるツールのセットがあります。

HDXサービスログ

HDXサービスは、設定することなくsyslogにログを記録するよう構成されているため、追加の構成は不要です。

Broker Agent ログ

Broker Agent (ctxvdaサービスとも呼ばれます) は、ネットワークソケットを介してログデータをsyslogに書き込みます。この機能は、初期状態では構成されていない場合があります。syslogへのBroker Agentログの記録を有効にするには、次の構成が必要です。

/etc/rsyslog.confファイルを編集して、次の行を追加します。

```
$ModLoad imudp
$UDPServerRun 514
```

rsyslog.confファイルを保存して閉じます。次のコマンドで、rsyslogサービスを再起動して変更を反映させます。

```
sudo /sbin/service rsyslog restart
```

HDXセッションが起動しないときの対応策

次のコマンドで、新しいセッションの起動を妨げている可能性がある、孤立したプロセスがないことを確認します。

```
sudo pkill -9 ctxhdx
sudo pkill -9 ctxgfx
sudo pkill -9 ctxlogin
sudo pkill -9 ctxvfb
```

Linux VDAサービスを再起動し、接続を再試行します。

重要なディレクトリおよびファイルの所有者および権限の確認

次のディレクトリおよびファイルのファイル所有者および権限を確認します。

- /var - 所有者 : root、グループ : root、権限 : 0755
- /var/xdl - 所有者 : ctxsrvr、グループ : ctxadm、権限 : 0755
- /var/xdl/.isacagent - 所有者 : root、グループ : root、権限 : 0666
- /var/xdl/.winsta - 所有者 : ctxsrvr、グループ : ctxadm、権限 : 0777
- /var/xdl/vda - 所有者 : root、グループ : root、権限 : 0755

HDX 3D Proマルチモニターでの再描画の問題

プライマリモニター以外の画面で再描画の問題が発生している場合は、NVIDIA GRIDライセンスが利用可能であることを確認してください。

オーディオが聞こえない

Citrix ReceiverおよびLinuxデスクトップを実行しているデバイスのボリュームコントロールがミュートまたは低いレベルに設

定されていないことを確認します。

Linux VDAでオーディオが有効になっていることを確認します。次のように、ctxregツールを使用して、構成項目fDisableCamの値を照会します。

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

値が0x1である場合は、オーディオが無効になっています。有効にするには、次のようにしてfDisableCamを0x0に設定します。

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

それでもオーディオが聞こえない場合は、Citrixオーディオシンクがpulseaudioによってロードされていることを確認します。このPulseAudioモジュールは、セッションの起動時にpulseaudioデーモンにロードされます。次のように、pacmdツールを使用して、Citrixオーディオシンクがロードされていることを確認します。

```
pacmd list-sinks
```

Citrixオーディオシンクがロードされている場合、出力は次のようになります。

```
name:
```

```
driver:
```

Citrixオーディオシンクがロードされていない場合は、ctxaudioプロセスを強制終了してから再起動します。

オーディオが録音されない

Linux VDAでオーディオが有効になっていることと、ICAクライアントでオーディオ録音が有効になっていることを確認します。それでもオーディオが録音されない場合は、Citrixオーディオソースがpulseaudioによってロードされていることを確認します。ICAクライアントでオーディオ録音が有効になっている場合は、セッションの起動時に、このPulseAudioモジュールがpulseaudioデーモンにロードされます。次のように、pacmdツールを使用して、Citrixオーディオソースがロードされていることを確認します。

```
pacmd list-sources
```

Citrixオーディオソースがロードされている場合、出力は次のようになります。

```
name:
```

```
driver:
```

Citrixオーディオソースがロードされていない場合は、ctxaudioプロセスを強制終了してから再起動します。

印刷できない

印刷が正しく機能しない場合に確認する項目はいくつかあります。印刷デーモンはセッションごとのプロセスで、実行されるのはセッションの期間中です。次のコマンドで、印刷デーモンが実行中であることを確認します。

```
ps -ef | grep ctxlpmngt
```

ctxlpmngtプロセスが実行中でない場合は、コマンドラインから手動でctxlpmngtを起動します。

それでも印刷が機能しない場合は、次にCUPSフレームワークを確認します。ctxcupsサービスはプリンター管理用であり、

Linux CUPSフレームワークと通信します。これはマシンごとの単一プロセスとなっていて、次のコマンドで確認できます。

```
service ctxcups status
```

サービスが実行中でない場合は、次のようにして手動で起動します。

```
service ctxcups start
```

CUPS印刷の追加ログ

Linux VDAのコンポーネントの1つとして、印刷コンポーネントのログの取得方法はその他のコンポーネントと同様です。

Red Hatの場合、CUPSサービスファイルの構成には追加の手順が必要です。追加の手順を実行しないと、一部のログがhdx.logで記録されません。

```
sudo service cups stop
```

```
sudo vi /etc/systemd/system/printer.target.wants/cups.service
```

```
PrivateTmp=false
```

```
sudo service cups start
```

```
sudo systemctl daemon-reload
```

この構成は、問題が発生した場合に完全な印刷ログを収集することのみを目的としています。通常は、CUPSのセキュリティが破られるため、この構成はお勧めしません。

印刷出力が文字化けする

出力が文字化けする場合、対応していないプリンタードライバーが原因となっている可能性があります。ユーザーごとのドライバー構成を使用できるため、~/CtXlpProfile構成ファイルを編集して構成できます。

```
[DEFAULT_PRINTER]
```

```
printername=
```

```
model=
```

```
ppdpath=
```

```
drivertype=
```

printernameは、現在クライアント側で通常使うプリンターの名前が指定されているフィールドです。これは読み取り専用の値となっており、編集できません。

Important

ppdpath、**model**、および**drivertype**の各フィールドは、マップされたプリンターに対していずれか1つのフィールドしか有効にならないため、同時には設定できません。

ユニバーサルプリンタードライバーがクライアントプリンターに対応していない場合、model=オプションを使用してネイティブプリンタードライバーのモデルを構成できます。プリンターの現在のモデル名は、lpinfoコマンドを使用して表示でき

ます。

```
lpinfo -m
```

...

```
xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

...

次のようにして、プリンターに一致するようにモデルを設定できます。

```
Model=xerox/ph3115.ppd.gz
```

ユニバーサルプリンタードライバーがクライアントプリンターに対応していない場合、ネイティブプリンタードライバーのppdファイルのパスを構成できます。ppdpathの値は、ネイティブプリンタードライバーファイルの絶対パスです。

たとえば、ppdドライバーが/home/tester/NATIVE_PRINTER_DRIVER.ppdにある場合は、次のようになります。

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

Citrixが提供するユニバーサルプリンタードライバーは3種類（Postscript、pcl5、およびpcl6）です。ネイティブプリンタードライバーが使用できない場合は、これらをドライバーの種類として構成できます。

たとえば、クライアントが通常使うプリンターのドライバーの種類がPCL5である場合は、次のようになります。

```
drivertype=pcl5
```

注意

Citrix Receiver for MacおよびCitrix Receiver for Linuxでは、サポートされるのがPostscriptプリンターのみであるため、PCL5およびPCL6ユニバーサルプリンタードライバーは適用できません。この状況では、ネイティブプリンタードライバーのppdpathまたはモデルをPostscript以外のプリンターに設定する必要があります。

CDMが機能しない

CDM機能にはデーモンプロセス（ctxcdmd）が含まれます。CDM機能でエラーが発生した場合は、Linux VDAマシンを再起動して、デーモンが正しく起動されたかどうかを確認します。

```
Ps -lef | grep ctxcdmd
```

マップされたドライブでのファイルの名前付けは、VDAとReceiver OSの名前付け規則に従う必要があります。

既知の問題

セッションのローミング時、Citrix Receiver for AndroidでCaps Lock状態が反対になる場合がある

Citrix Receiver for Androidへの既存の接続をローミングすると、Caps Lock状態が失われる場合があります。回避策として、拡張キーボードのShiftキーを使用して大文字と小文字を切り替えます。

Citrix Receiver for Macを使用して**Linux VDA**に接続している場合、**alt**キーを使用するショートカットキーが常に機能するとは限らない

Citrix Receiver for Macでは、左右どちらのoption/altキーを押しても、デフォルトではAltGrが送信されます。Citrix Receiverの設定でこれを変更することはできますが、結果はアプリケーションによって変わります。

SuSE Linux Enterprise Desktop 11で新しいXクライアントライブラリがキーボードマッピングの問題を引き起こす可能性がある

SuSE Linux Enterprise Desktop 11のxorg-x11-libX11パッケージの新しいバージョンでは、キーボードマッピングの変更を処理する際に問題が発生する場合があります。これが原因で、HDXセッション内でキーボード機能の問題が生じる可能性があります。この問題は、インストールしたパッケージのバージョンが7.4-5.11.11.1~7.4-5.11.15.1の範囲である場合に、発生する可能性があります。

回避策として、ストックバージョンのxorg-x11-libX11 SP3パッケージにロールバックすると、キーボードマッピングの変更が正常に機能します。次に例を示します。

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1
```

```
rpm -i --force xorg-x11-libX11-32bit-7.4-5.9.1
```

```
rpm -e xorg-x11-libX11-7.4-5.11.15.1
```

```
rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

この回避策は、ユーザーがマシンにログオンする前に実施する必要があります。セッションがアクティブなときに行うと、ユーザーが次回ログインするまで上記の設定は有効になりません。

ストックバージョンのSP3からアップグレードすると、上記のxorg-x11-libX11パッケージを現在インストールされているバージョンにロックできるため、アップグレード中に変更されることはありません。アップグレードする前に以下を実行し、その後は通常どおりのアップグレードを続行します。

```
zypper al xorg-x11-libX11
```

```
zypper al xorg-x11-libX11-32bit
```

XenDesktop Version 7.1の**Delivery Controller**と共に**Linux VDA**を使用すると、セッションの起動に時間がかかる場合がある

起動が遅くなる原因は、Version 7.1のDelivery Controllerによって生成されたICAファイルにCommon Gateway Protocol設定が存在するためです。この設定が存在すると、Citrix ReceiverはTCPポート2598で接続を確立しようとします。SLED 12など一部のLinuxディストリビューションでは、デフォルトのファイアウォール設定でTCP SYNパケットをドロップするため、タイムアウトが発生してセッションの起動に時間がかかります。回避策として、TCPポート2598でTCP SYNを拒否するように、Linux VDAでファイアウォールを構成します。この問題は、新しいバージョンのDelivery Controllerでは解決済みです。

Linux VDAをドメインに再度追加するときに、登録に失敗する

特定の状況で、Linux VDAがドメインに再度追加されて、Kerberosキーの新しいセットが生成されると、ブローカーがVDAとのセキュリティコンテキストの確立に失敗します。多くの場合、この問題は、Kerberosキーの以前のセットに基づいた期限切れのVDAサービスチケットがキャッシュに存在し、それをブローカーが使用することが原因で発生します。この問題に

よって、VDAがブローカーへの接続を停止することはありませんが、ブローカーはVDAに返すセキュリティコンテキストを再立できません。通常見られる現象は、VDA登録の失敗です。

この問題は、VDAサービスチケットが最終的に期限切れとなって更新されると自動的に解決しますが、サービスチケットは通常、長時間有効です。何時間も有効である可能性があります。

解決策として、ブローカーのチケットキャッシュをクリアします。ブローカーを再起動するか、管理者としてコマンドプロンプトからブローカーで次のコマンドを実行します。

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

このコマンドにより、Citrix Broker Serviceを実行するNetwork ServiceプリンシパルがLSAキャッシュに保持するサービスチケットはすべて削除されます。これにより、ほかのVDAのサービスチケットが削除されます。また、その他のサービスのサービスチケットも削除される可能性があります。ただし、この処理は悪影響を及ぼしません。これらのサービスチケットは、再度必要になったときにKDCから再取得されます。

HDX 3D ProをGNOMEと共に使用すると、ロック画面のアイコンが見つからない

NVIDIA GRIDドライバーが有効なとき、Gnomeデスクトップマネージャー（GDM）は無効となりGDMのロック画面機能は使用できません。

オーディオプラグアンドプレイがサポートされない

ICAセッションでオーディオの録音を開始する前に、オーディオキャプチャデバイスをクライアントマシンに接続することをお勧めします。オーディオ録音アプリケーションの開始後にデバイスを接続した場合は、アプリケーションが応答しなくなる可能性があります。この問題が発生した場合は、アプリケーションを再起動してください。録音中にキャプチャデバイスが取り外されると、同様の問題が発生する可能性があります。

オーディオの歪み

Windows 10 Receiverでは、オーディオ録音中にオーディオが歪む場合があります。

CTXPSドライバーが一部のPLCプリンターに対応しない

印刷出力が適切でない場合は、プリンタードライバーを、製造元から提供されたネイティブプリンタードライバーに設定してください。

サイズの大きな文書の印刷が遅い

ローカルのクライアントプリンターでサイズの大きな文書を印刷すると、印刷ファイルはサーバーとの接続を介して転送されます。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。

別のセッションからプリンター通知と印刷ジョブ通知が表示される

Linuxでのセッションの考え方は、Windowsオペレーティングシステムとは異なります。したがって、すべてのユーザーがシステム全体の通知を受け取ります。管理者は、CUPS構成ファイル/etc/cups/cupsd.confを変更して、これらの通知を無効にすることができます。

次のように、構成されている現在のポリシー名がこのファイルに記述されています。

```
DefaultPolicy default
```

ポリシー名がdefaultである場合は、次の行をデフォルトポリシーのXMLブロックに追加します。

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ..

Require user @OWNER

Order deny,allow

Order deny,allow
```

用語集

ブローカー - XenDesktop環境で、異なるVDAに対するHDXセッションを仲介するXenDesktopコンポーネントです。DDCまたはXenDesktopのコントローラーとも呼ばれます。

Broker Agent - 配信するデスクトップを提供する、Linux VDAマシン上のコンポーネントです。Broker Agentは、ブローカーと通信してセッションを仲介できるようにします。Broker Agentは、VDAサービスとHDXサービスという2つの主要コンポーネントで構成されます。

Citrix Director - Citrixヘルプデスク/サポートがXenDesktop VDAを監視および制御するために使用するコンソールです。

Citrix Studio - XenDesktopを構成するために使用するCitrix管理コンソールです。

DDC - XenDesktop Desktop Delivery Controllerです。ブローカーまたはDelivery Controllerとも呼ばれます。

FQDN - 完全修飾ドメイン名です。

HDX - High Definition Experience（高品位なユーザーエクスペリエンス）プロトコルです。以前はCitrix ICAプロトコルと呼ばれていました。

HDXサービス - HDXプロトコルを介して仮想Linuxデスクトップをリモート処理するLinuxサービス（ctxhdx）です。VDAサービスと通信してセッションを仲介できるようにします。

RHEL - Red Hat Enterprise Linuxです。Red Hatが提供する商用のLinuxディストリビューションです。

SLED - SUSE Linux Enterprise Desktopです。Novellが提供する商用のLinuxディストリビューションです。

SLES - SUSE Linux Enterprise Serverです。Novellが提供する商用のLinuxディストリビューションです。

VDA - Virtual Delivery Agentです。

VDAサービス - ブローカーと通信してセッションを仲介できるようにするLinuxサービス（ctxvda）です。HDXサービスとも通信してリモートセッションを配信します。

SUSE Linux VDAのインストール

Jul 07, 2016

SUSEディストリビューションをベースとしたLinux仮想デスクトップを作成できます。Linux仮想マシンを準備して新しいLinux VDAソフトウェアをインストールし、Delivery Controllerを構成したらStudioを使ってユーザーがデスクトップを使用できるようにします。

詳しくは、この記事に記載されている情報を参照してください。

注意

この記事で説明するLinuxシェルコマンドは、GNU Bashシェルで動作することが確認されています。

この記事は、次のセクションで構成されています。

- [システム要件](#)
- [Delivery Controllerの構成](#)
- [VDAをインストールするLinuxマシンの準備](#)
- [Linuxマシンカタログおよびデリバリーグループの構成](#)
- [Linux VDAソフトウェアのインストール](#)
- [VDAソフトウェアの実行](#)
- [Linux VDAソフトウェアのアンインストール](#)
- [トラブルシューティング](#)
- [既知の問題](#)
- [用語集](#)

システム要件

Linuxディストリビューション

Linux Virtual Desktop製品では、次のLinuxディストリビューションがサポートされます。

- SUSE Linux Enterprise
 - Desktop 11 Service Pack 4
 - Desktop 12 Service Pack 1
 - Server 11 Service Pack 4
 - Server 12 Service Pack 1
- Red Hat Enterprise Linux
 - Workstation 6.7
 - Workstation 7.2
 - Server 6.7
 - Server 7.2
- CentOS Linux
 - CentOS 6.7
 - CentOS 7.2

注意

すべての場合で、サポートされるプロセッサアーキテクチャはx86-64です。

XenDesktop

Linux VDAでは、次のバージョンのXenDesktopがサポートされます。

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8
- XenDesktop 7.9

Linux VDAの構成手順はWindows VDAの場合と多少異なります。ただし、Delivery ControllerファームはWindowsデスクトップとLinuxデスクトップを両方とも仲介できます。

注意

Linux VDAは、XenDesktop Version 7.0以前には対応していません。

Citrix Receiver

次のバージョンのCitrix Receiverがサポートされます。

- Citrix Receiver for Windows Version 4.4以降 (wfica32.exeのv14.4と同じ)
- Citrix Receiver for Linux Version 13.3以降
- Citrix Receiver for Mac OSX Version 12.1以降
- Citrix Receiver for Android Version 3.8以降
- Citrix Receiver for iOS Version 6.1.4以降
- Citrix Receiver for Chrome/HTML5 Version 2.0 (Access Gateway経由でのみサポート)

ハイパーバイザー

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

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

ベアメタルホスティングもサポートされます。

ヒント

サポートされるプラットフォームの一覧については、ハイパーバイザーのベンダーのドキュメントを参照してください。

Active Directory統合パッケージ

Linux VDAでは、次のActive Directory統合パッケージまたは製品がサポートされます。

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

ヒント

サポートされるプラットフォームの一覧については、Active Directory統合パッケージのベンダーのドキュメントを参照してください。

Delivery Controllerの構成

XenDesktop 7.7以降には、Linux Virtual Desktopをサポートするための必要な変更が含まれていますが、以前のバージョンの場合は、Hotfixまたは更新スクリプトが必要です。これらのインストールと確認について、このセクションで説明しています。

Delivery Controller構成の更新

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

- [CTX142438](#) : Hotfixes Update 2 - Delivery Controller 7.6 (32ビット) 用 – 英語
- [CTX142439](#) : Hotfixes Update 2 - Delivery Controller 7.6 (64ビット) 用 – 英語

XenDesktopの以前のバージョンに対しては、ブローカーサービスの構成を更新する**Update-BrokerServiceConfig.ps1**という名前のPowerShellスクリプトが提供されています。これは次のパッケージから入手できます。

- citrix-linuxvda-scripts-1.3.0.zip

次の手順をファーム内の各Delivery Controllerで繰り返します。

1. **Update-BrokerServiceConfig.ps1**スクリプトをDelivery Controllerマシンにコピーします。
2. ローカル管理者のコンテキストでWindows PowerShellコンソールを開きます。
3. スクリプトを含むフォルダーを参照します。
4. 次のスクリプトを実行します。

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

注意

デフォルトでは、PowerShellはPowerShellスクリプトを実行できないように構成されています。スクリプトの実行に失敗する場合は、再試行する前にPowerShell実行ポリシーの変更が必要な場合があります。

```
Set-ExecutionPolicy Unrestricted
```

Update-BrokerServiceConfig.ps1スクリプトを実行すると、Linux VDAに必要とされる新しいWCFエンドポイントでブローカーサービス構成ファイルが更新され、ブローカーサービスが再起動します。このスクリプトでは、自動的にブローカーサービス構成ファイルの場所が特定されます。元の構成ファイルのバックアップが、**.prelinux**という拡張子で同じディレクトリに作成されます。

これらの変更は、同じDelivery Controllerファームを使用するように構成されたWindows VDAの仲介には影響しません。このことにより、単一のControllerファームがWindows VDAおよびLinux VDAの両方とのセッションをシームレスに管理し、仲介できます。

Delivery Controller構成の確認

必要な構成変更がDelivery Controllerに適用されているかどうかを確認するには、次のファイル中に文字列**EndpointLinux**が5回出現していることを確認します。

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

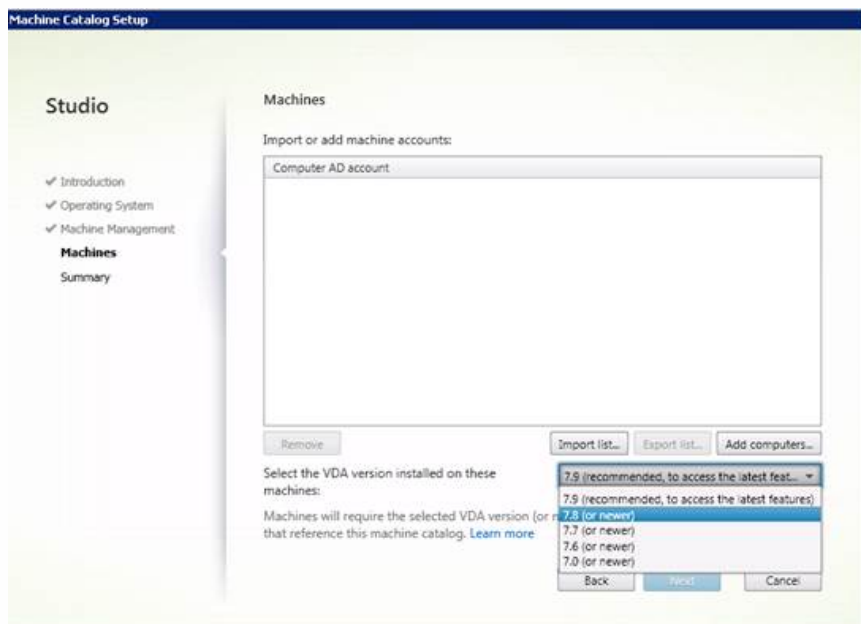
Windowsコマンドプロンプトで、ローカル管理者としてログオンし、次の操作を行います。

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

```
findstr EndpointLinux BrokerService.exe.config
```

Important

バージョン1.3では、Linux VDAのBroker AgentはXenApp 7.8およびXenDesktop 7.8に設定されます。ただし、Studioの「マシンカタログのセットアップ」画面でマシンカタログを追加する場合、デフォルト値は自動的にバージョン7.9に設定されます。インストールするVDAのバージョンを、**7.8**（またはそれより新しい）バージョンに明示的に設定する必要があります。下の図を参照してください。



VDAをインストールするLinuxマシンの準備

YaSTツールの起動

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

テキストベースのYaSTツールを起動する方法

```
su -
```

```
yast
```

代わりに、UIベースのYaSTツールを起動する方法

```
su -
```

```
yast2 &
```

ネットワークの構成

以降のセクションでは、Linux VDAで使用するさまざまなネットワーク設定およびサービスの構成方法に関する情報について説明します。ネットワークの構成は、Network Managerなどのほかの方法ではなく、YaSTツールで実行する必要があります。次の手順は、UIベースのYaSTツールの使用が前提となっています。テキストベースのYaSTツールも使用できますが、ナビゲーション方法が異なり、ここでは説明していません。

ホスト名とDNSの構成

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

- ホスト名 – マシンのDNSホスト名を追加します。
- ドメイン名 – マシンのDNSドメイン名を追加します。
- ネームサーバー – DNSサーバーのIPアドレスを追加します。通常はADドメインコントローラーのIPアドレスです。
- [ドメイン検索] 一覧 – DNSドメイン名を追加します。

注意

Linux VDAでは、現在、NetBIOS名の切り捨てをサポートしていません。したがって、ホスト名は15文字以下にしてください。

ヒント

a~z、0~9、およびハイフン (-) の文字のみ使用してください。アンダースコア (_)、スペース、およびその他の記号は使用しないでください。ホスト名を数字で開始したり、ハイフンで終了したりしないでください。

マルチキャストDNSの無効化

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

合があります。SLESの場合、mDNSはデフォルトでは有効化されていないため、特に操作を行う必要はありません。

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

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

目的：

```
hosts: files dns
```

ホスト名の確認

次のコマンドで、ホスト名が正しく設定されていることを確認します。

```
hostname
```

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

次のコマンドで、完全修飾ドメイン名が正しく設定されていることを確認します。

```
hostname -f
```

これにより、そのマシンの完全修飾ドメイン名が返されます。

名前解決とサービス到達可能性の確認

次のコマンドで、完全修飾ドメイン名が解決できることと、ドメインコントローラーとXenDesktop Delivery Controllerからpingに応答があることを確認します。

```
nslookup domain-controller-fqdn
```

```
ping domain-controller-fqdn
```

```
nslookup delivery-controller-fqdn
```

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

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

NTPサービスの構成

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

1. YaSTの [NTP環境設定] を開いて、[一般的な設定] タブをクリックします。
2. [NTPデーモンを起動する] セクションで、[今すぐ開始し、システム起動時に開始するよう設定] をクリックします。
3. 表示されている場合は、[Undisciplined Local Clock (LOCAL)] 項目を選択し、[削除] をクリックします。
4. [追加] をクリックして、NTPサーバーのエントリを追加します。
5. [Server Type] を選択して、[次へ] をクリックします。
6. [アドレス] フィールドに、NTPサーバーのDNS名を入力します。このサービスは、通常Active Directoryドメインコントローラーでホストされます。

- 7. [オプション] フィールドは変更しません。
- 8. [テスト] をクリックして、NTPサービスに到達できるかどうかを確認します。
- 9. 一連のウィンドウで [OK] をクリックして、変更を保存します。

注意

SLES 12の実装でNTPデーモンが起動に失敗する場合は、AppArmorポリシーに関するSUSEの既知の問題が原因となっている可能性があります。詳しくは、[こちら](#)を参照し、掲載されている解決方法に従ってください。

Linux VDAに依存するパッケージのインストール

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

- PostgreSQL
 - SLED/SLES 11 : Version 9.1以降
 - SLED/SLES 12 : Version 9.3以降
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1以降
- CUPS
 - SLED/SLES 11 : Version 1.3.7以降
 - SLED/SLES 12 : Version 1.6.0以降
- Foomaticフィルター
 - SLED/SLES 11 : Version 3.0.0以降
 - SLED/SLES 12 : Version 1.0.0以降
- ImageMagick
 - SLED/SLES 11 : Version 6.4.3.6以降
 - SLED/SLES 12 : Version 6.8以降

リポジトリの追加

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

- SLED 11 : PostgreSQLは、SLES 11では入手できますが、SLED 11では入手できません。
- SLES 11 : OpenJDKとOpenMotifは、SLED 11では入手できますが、SLES 11では入手できません。
- SLED 12 : PostgreSQLは、SLES 12では入手できますが、SLED 12では入手できません。 ImageMagickは、SLE 12 SDK ISOまたはオンラインリポジトリから入手できます。
- SLES 12 : 問題はありません。すべてのパッケージを入手できます。 ImageMagickは、SLE 12 SDK ISOまたはオンラインリポジトリから入手できます。

この解決策として推奨されるのは、インストール元となるSLEの代替エディションのメディアから、不足しているパッケージを取得する方法です。すなわち、SLEDで不足しているパッケージをSLESメディアからインストールし、SLESで不足しているパッケージをSLEDメディアからインストールします。次に説明する方法では、SLEDおよびSLESのISOメディアファイルを両方ともマウントして、リポジトリを追加します。

SLED 11	<pre>sudo mkdir -p /mnt/sles sudo mount -t iso9660 \</pre>

	<pre>path-to-iso/SLES-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles</pre>
SLES 11	<pre>sudo mkdir -p /mnt/sled sudo mount -t iso9660 \ path-to-iso/SLED-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sled sudo zypper ar -f /mnt/sled sled</pre>
SLED 12	<pre>sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-12-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles</pre>
SLED/SLES 12	<pre>sudo mkdir -p /mnt/sdk sudo mount -t iso9660 \ path-to-iso/SLE-12-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk sudo zypper ar -f /mnt/sdk sdk</pre>

Kerberosクライアントのインストール

次のコマンドで、Linux VDAとXenDesktopのコントローラー間の相互認証用にKerberosクライアントをインストールします。

```
sudo zypper install krb5-client
```

Kerberosクライアントの構成は、使用するActive Directory統合の方法によって異なります。この点については後で説明します。

OpenJDKのインストール

OpenJDK 1.7.0に依存するLinux VDA

ヒント

問題を回避するには、必ずOpenJDK Version 1.7.0のみをインストールしておきます。その他のバージョンのJavaは、システムからすべて削除します。

SLEDでは、Java Runtime Environmentはオペレーティングシステムと共にインストールされています。次のコマンドで、このことを確認します。

SLED	<pre>sudo zypper info java-1_7_0-openjdk</pre> ステータスがout-of-dateであると報告された場合は、次のようにして最新バージョンに更新します。 <pre>sudo zypper update java-1_7_0-openjdk</pre> 次のコマンドで、Javaのバージョンを確認します。 <pre>java -version</pre>
SLES	SLESでは、次のようにしてJava Runtime Environmentをインストールする必要があります。 <pre>sudo zypper install java-1_7_0-openjdk</pre> 次のコマンドで、Javaのバージョンを確認します。 <pre>java -version</pre>

PostgreSQLのインストール

SLED/SLES 11	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install libecpg6</pre> <pre>sudo zypper install postgresql?init</pre> <pre>sudo zypper install postgresql91</pre> <pre>sudo zypper install postgresql91?server</pre> <pre>sudo zypper install postgresql?jdbc</pre> データベースサービスを初期化し、起動時にPostgreSQLが確実に開始するようにするには、次に示すインストール後の手順がいくつか必要です。 <pre>sudo /sbin/insserv postgresql</pre> <pre>sudo /etc/init.d/postgresql restart</pre>
SLED/SLES 12	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install postgresql-init</pre> <pre>sudo zypper install postgresql93-server</pre> <pre>sudo zypper install postgresql-jdbc</pre> データベースサービスを初期化し、起動時にPostgreSQLが確実に開始するようにするには、次に示すインストール後の手順が必要です。 <pre>sudo systemctl enable postgresql</pre>

	<pre>sudo systemctl restart postgresql</pre> データベースファイルは、/var/lib/pgsql/dataに配置されます。

OpenMotiff Runtime Environmentのインストール

Linux VDAには、ディストリビューションに応じて、motifパッケージまたはopenmotifパッケージが必要です。

SLED/SLES 11	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install openmotif-libs</pre>
SLED/SLES 12	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install motif</pre>

印刷サポートのインストール

Linux VDAには、CUPSフィルターとFoomaticフィルターの両方が必要です。

SLED/SLES 11	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install cups</pre> <pre>sudo zypper install foomatic-filters</pre>
SLED/SLES 12	次のコマンドで、パッケージをインストールします。 <pre>sudo zypper install cups</pre> <pre>sudo zypper install cups-filters-foomatic-rip</pre>

ImageMagickのインストール

次のコマンドで、ImageMagickパッケージをインストールします。

```
sudo zypper install ImageMagick
```

リポジトリの削除

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

SLED 11	次のパッケージを削除します。 <pre>sudo zypper rr sles</pre> <pre>sudo umount /mnt/sles</pre>

	<pre>sudo rmdir /mnt/sles</pre>
SLES 11	次のパッケージを削除します。 <pre>sudo zypper rr sled</pre> <pre>sudo umount /mnt/sled</pre> <pre>sudo rmdir /mnt/sled</pre>
SLED 12	次のパッケージを削除します。 <pre>sudo zypper rr sles</pre> <pre>sudo umount /mnt/sles</pre> <pre>sudo rmdir /mnt/sles</pre>
SLED/SLES 12	次のパッケージを削除します。 <pre>sudo zypper rr sdk</pre> <pre>sudo umount /mnt/sdk</pre> <pre>sudo rmdir /mnt/sdk</pre>

ハイパーバイザー用Linux仮想マシンの準備

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

Citrix XenServerでの時間同期の修正

XenServerの時間同期機能が有効な場合、それぞれの準仮想化Linux仮想マシンで、NTPとXenServerの両方がシステムの時刻を管理しようとするのが原因となり問題が発生します。システムの時刻とほかのサーバーの時刻との同期が失われるのを防ぐには、各Linuxゲストのシステムの時刻がNTPと同期する必要があります。この状態にするには、ホストの時間同期を無効にする必要があります。HVMモードでは、変更は必要ありません。

一部のLinuxディストリビューションでは、XenServer Toolsをインストールした状態で準仮想化Linuxカーネルを実行すると、XenServerの時間同期機能が存在し有効になっているかどうかをLinux仮想マシンから次のようにして確認できます。

```
su -
```

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

これにより、次のいずれかが返されます。

- 0 - 時間同期機能が有効となっていて、無効にする必要があります。
- 1 - 時間同期機能が無効となっていて、これ以上の操作は必要ありません。

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

時間同期機能が有効な場合は、次のようにしてファイルに1を書き込んで無効にします。

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

この変更を永続化し、再起動後も保持するには、/etc/sysctl.conf ファイルを編集して、次の行を追加します。

```
xen.independent_wallclock = 1
```

これらの変更を確認するため、次のようにしてシステムを再起動します。

```
reboot
```

再起動後、次のようにしてこの変更が正しく設定されているかどうか確認します。

```
su -
```

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

これにより、値1が返されます。

Microsoft Hyper-Vでの時間同期の修正

Hyper-V Linux統合サービスがインストールされたLinux仮想ホストでは、Hyper-Vの時間同期機能を活用してホストオペレーティングシステムの時間を利用できます。システムの時刻を正確な状態で維持するには、NTPサービスと共にこの機能を有効にする必要があります。

管理オペレーティングシステムで、次の操作を行います。

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

注意

この方法はVMwareおよびXenServerの場合とは異なります。VMwareおよびXenServerでは、NTPとの競合を避けるためにホストの時間同期を無効にします。Hyper-Vの時間同期は、NTPと共存し、NTPの時間同期を補完することができます。

ESXおよびESXiでの時間同期の修正

VMwareの時間同期機能が有効な場合、それぞれの準仮想化Linux仮想マシンで、NTPとハイパーバイザーの両方がシステムの時刻を同期しようとするのが原因となり問題が発生します。システムの時刻とほかのサーバーの時刻との同期が失われるのを防ぐには、各Linuxゲストのシステムの時刻がNTPと同期する必要があります。この状態にするには、ホストの時間同期を無効にする必要があります。

VMware Toolsをインストールした状態で準仮想化Linuxカーネルを実行している場合は、次の操作を行います。

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

Windows ドメインへのLinuxマシンの追加

Linux用のXenDesktopでサポートされるLinuxマシンをActive Directoryドメインに追加する方法は、以下のように複数あります。

- Samba Winbind
- Quest Authentication Services
- Centrify DirectControl

選択した方法に応じて、以下の手順に従います。

Samba Winbind

Windows ドメインへの参加

これには、ドメインコントローラーに到達できることと、マシンをドメインに追加する権限を持つActive Directoryユーザー・アカウントが必要です。

1. YaSTの [Windows ドメインメンバーシップ] を開きます。
2. 以下の変更を行います。
 - [ドメイン/ワークグループ] にActive Directoryドメインの名前またはドメインコントローラーのIPアドレスを設定します。ドメインは必ず大文字で入力します。
 - [Linuxの認証にもSMBの情報を使用する] チェックボックスをオンにします。
 - [ログイン時にホームディレクトリを作成する] チェックボックスをオンにします。
 - [SSH向けのシングルサインオン] チェックボックスをオンにします。
 - [オフライン認証] チェックボックスがオフになっていることを確認します。Linux VDAは、このオプションに対応していません。
3. [OK] をクリックします。いくつかのパッケージのインストールを促すメッセージが表示された場合は、[インストール] をクリックします。
4. ドメインコントローラーが見つかり、ドメインに参加するかどうかを確認するメッセージが表示されます。[はい] をクリックします。
5. メッセージが表示されたら、コンピューターをドメインに追加する権限を持つドメインユーザーの資格情報を入力し、[OK] をクリックします。
6. 成功を示すメッセージが表示されます。
7. いくつかのSambaおよびkrb5パッケージのインストールを促すメッセージが表示されたら、[インストール] をクリックします。

YaSTにより、これらの変更には一部のサービスの再起動またはマシンの再起動が必要であることが示される場合があります。以下のようにして、マシンの再起動をお勧めします。

```
su -
```

```
reboot
```

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

SLED/SLES 12では、デフォルトのKerberos資格情報キャッシュ名の指定方法が、従来のFILE:/tmp/krb5cc_%{uid}からDIR:/run/user/%{uid}/krb5ccに変更されました。Linux VDAはこの新しいDIRによるキャッシュ方法に対応していないため、手動で変更する必要があります。次の設定がない場合は、rootとして/etc/krb5.confを編集して、[libdefaults]セクションに追加します。

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

ドメインメンバーシップの確認

XenDesktopのコントローラーを使用するには、WindowsまたはLinuxに関係なく、すべてのVDAマシンでActive Directoryにコンピューターオブジェクトが必要です。

次のように、Sambaのnet adsコマンドを使用して、マシンがドメインに参加していることを確認します。

```
sudo net ads testjoin
```

次のコマンドで、追加のドメインおよびコンピューターオブジェクトの情報を確認します。

```
sudo net ads info
```

Kerberos構成の確認

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

```
sudo klist -ke
```

これにより、プリンシパル名と暗号スイートのさまざまな組み合わせに対して使用できるキーの一覧が表示されます。Kerberosのkinitコマンドを実行し、これらのキーを使用して、マシンをドメインコントローラーに対して認証します。

```
sudo kinit -k MACHINE\${@REALM}
```

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

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

```
sudo klist
```

次のコマンドを使用して、マシンアカウントの詳細を調査します。

```
sudo net ads status
```

ユーザー認証の確認

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

```
wbinfo --krb5auth=domain\username%password
```

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

Winbind PAMモジュールが正しく構成されていることを確認するには、次のように、以前にマシンにログオンしたことがない

ドメインユーザーアカウントを使用してローカルでログオンします。

```
ssh localhost -l domain\\username
```

```
id -u
```

次のコマンドで、id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

次のコマンドで、セッションを終了します。

```
diskpart.exeを終了します
```

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

Quest Authentication Services

ドメインコントローラーでのQuestの構成

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

Linux VDAマシンにドメインユーザーがログオンできるようにする

Linux VDAマシンでHDXセッションを確立する必要がある各ドメインユーザーに対して、次の操作を行います。

1. [Active Directoryユーザーとコンピューター] 管理コンソールで、目的のユーザーアカウントのActive Directoryユーザーのプロパティを開きます。
2. [Unix Account] タブを選択します。
3. [Unix-enabled] チェックボックスをオンにします。
4. [Primary GID Number] のプライマリGID番号を、実際のドメインユーザーグループのグループIDに設定します。

注意

この手順は、ドメインユーザーがコンソール、RDP、SSH、またはその他のリモート処理プロトコルを使用してログオンできるように設定する場合も同じです。

Linux VDAでのQuestの構成

VASデーモンの構成

次のようにKerberosチケットの自動更新を有効にして、切断する必要があります。また、認証（オフラインログオン）は無効にする必要があります。

```
sudo /opt/quest/bin/vastool configure vas vasd \
```

```
auto-ticket-renew-interval 32400
```

```
sudo /opt/quest/bin/vastool configure vas vas_auth \
```

```
allow-disconnected-auth false
```

これにより、更新間隔が9時間（32400秒）に設定されます。すなわち、チケットのデフォルトの有効期間である10時間よりも1時間短くなります。Kerberosチケットの有効期間がさらに短いシステムでは、より小さい値をこのパラメーターに設定します。

PAMおよびNSSの構成

Questでは、HDXや、su、ssh、RDPなどのその他のサービスを介したドメインユーザーのログインを可能にするには、PAMとNSSを手動で構成する必要があります。PAMおよびNSSを構成するには、次のコマンドを実行します。

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

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

Windowsドメインへの参加

次のように、Questのvastoolコマンドを使用して、LinuxマシンをActive Directoryドメインに追加します。

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

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

ドメインメンバーシップの確認

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

```
sudo /opt/quest/bin/vastool info domain
```

マシンがドメインに参加している場合は、ドメイン名が返されます。参加していない場合は、次のエラーが表示されます。

```
ERROR: No domain could be found.
```

```
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
```

```
default_realm not configured in vas.conf. Computer may not be joined to domain
```

ユーザー認証の確認

QuestがPAMを使用してドメインユーザーを認証できることを確認するには、次のように、以前にマシンにログオンしたことがないドメインユーザーアカウントを使用してログオンします。

```
ssh localhost -l domain\\username
```

```
id -u
```

次のコマンドで、id -uコマンドによって返されたUIDに対応するKerberos資格情報キャッシュファイルが作成されたことを確認します。

```
ls /tmp/krb5cc_uid
```

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

```
/opt/quest/bin/vastool klist
```

次のコマンドで、セッションを終了します。

```
diskpart.exeを終了します
```

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

Centrify DirectControl

Windowsドメインへの参加

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

```
su -
```

```
adjoin -w -V -u user domain-name
```

userパラメーターは、コンピューターをActive Directoryドメインに追加する権限を持つ任意のActive Directoryドメインユーザーです。 **domain-name**パラメーターは、Linuxマシンを追加するドメインの名前です。

ドメインメンバーシップの確認

XenDesktopのコントローラーを使用するには、WindowsまたはLinuxに関係なく、すべてのVDAマシンでActive Directoryにコンピューターオブジェクトが必要です。 Centrifyにより追加されたLinuxマシンがドメインに存在することを確認するには、次のコマンドを実行します。

```
su -
```

```
adinfo
```

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

次を使用すると、より包括的なシステム情報と診断情報を取得できます。

```
adinfo --sysinfo all
```

```
adinfo -diag
```

さまざまなActive DirectoryおよびKerberosサービスとの接続をテストするには、次のコマンドを実行します。

```
adinfo --test
```

Linuxマシンカタログおよびデリバリーグループの構成

マシンカタログへのLinuxマシンの追加

マシンカタログを作成し、Linux VDAマシンを追加する手順は、従来のWindows VDAでの方法とほとんど同じです。このタスクを完了する方法のより総合的な説明については、[Citrix製品ドキュメント](#)を参照してください。

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

- オペレーティングシステムには、次を選択します。
 - ホストされる共有デスクトップ配信モデルの場合、[WindowsサーバーOS] オプションまたは[サーバーOS] オプション
 - VDI専用デスクトップ配信モデルの場合、[WindowsデスクトップOS] オプションまたは[デスクトップOS] オプション
- マシンが電源管理を行わない設定になっていることを確認します。
- PVSとMCSはLinux VDAではサポートされないため、ほかのサービスまたはテクノロジー (既存のイメージ) の展開方法を選択してください。
- 同じマシンカタログで、Linux VDAマシンとWindows VDAマシンを混在させないでください。

注意

以前のバージョンのCitrix Studioでは、「Linux OS」という概念に対応していませんでした。ただし、[WindowsサーバーOS] オプションまたは[サーバーOS] オプションを選択すると、同等のホストされる共有デスクトップ配信モデルが暗黙的に選択されます。[WindowsデスクトップOS] オプションまたは[デスクトップOS] オプションを選択すると、XenDesktopのマシンごとに単一ユーザーの配信モデルが暗黙的に選択されます。

マシンカタログを作成するためのCitrixドキュメントは、以下を参照してください。

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)
- [XenDesktop 7.9](#)

上記より前のバージョンのXenDesktopはサポートされません。

ヒント

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

デリバリーグループの追加

デリバリーグループを作成し、Linux VDAマシンを含むマシンカタログを追加する手順は、Windows VDAマシンの場合とほとんど同じです。このタスクを完了する方法のより総合的な説明については、オンラインのCitrix製品ドキュメントを参照してください。

Linux VDAマシンカタログを含むデリバリーグループを作成する場合は、次の制約があります。

- 配信の種類には、デスクトップを選択します。Linux VDAマシンでは、アプリケーション配信はサポートされていません。

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

デリバリーグループを作成するためのCitrixドキュメントは、以下を参照してください。

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)
- [XenDesktop 7.9](#)

上記より前のバージョンのXenDesktopはサポートされません。

Linux VDAソフトウェアのインストール

古いバージョンのアンインストール

Version 1.0よりも古いバージョンのLinux VDAがインストールされている場合は、それをアンインストールしてから新しいバージョンをインストールします。

次のコマンドで、Linux VDAサービスを停止します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

次のコマンドで、パッケージをアンインストールします。

```
sudo rpm -e XenDesktopVDA
```

Important

テクニカルプレビューリリースからバージョン1.0、1.1、1.2、または1.3へのアップグレードはサポートされません。

注意

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

コマンドを実行するには、フルパスが必要です。代わりに、システムパス **/opt/Citrix/VDA/sbin** と **/opt/Citrix/VDA/bin** を追加することもできます。

Linux VDAのインストール

次のように、RPM Package Managerを使用して、Linux VDAソフトウェアをインストールします。

SuSE 11の場合：

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

SuSE 12の場合：

```
sudo rpm -i XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

Linux VDAのアップグレード

Linux VDA Version 1.1をインストールしている場合は、RPM Package Managerを使用して、Linux VDAソフトウェアをアップグレードします。

SuSE 11の場合：

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

SuSE 12の場合：

```
sudo rpm -U XenDesktopVDA-1.3.0.312-1.x86_64.rpm
```

Important

アップグレード後は、Linux VDAマシンを再起動してください。

Linux VDAの構成

パッケージのインストール後、**ctxsetup.sh**スクリプトを実行して、Linux VDAを構成する必要があります。パッケージをアップグレードした場合、ctxsetup.shスクリプトを実行してアップグレードを完了する必要があります。変更を行う前に、このスクリプトでは、環境を確認し、すべての依存コンポーネントがインストールされていることが確認されます。必要に応じて、いつでもこのスクリプトを再実行して設定を変更できます。

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

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

質問に回答する構成

次のようにして、質問に回答する手動構成を実行します。

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

自動化された構成

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

サポートされる環境変数には次のようなものがあります。

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Virtual Delivery Agentでは、DNS CNAMEレコードを使用して、Delivery

Controller名を指定することができます。通常は、Nに設定します。

- CTX_XDL_DDC_LIST = list-ddc-fqdns – Virtual Delivery Agentには、配信の登録に使用するDelivery Controllerの完全修飾ドメイン名
- (FQDN)のスペース区切りの一覧が必要です。1つ以上の完全修飾ドメイン名またはCNAMEエイリアスを指定する必要があります。
- CTX_XDL_VDA_PORT = port-number – Virtual Delivery Agentは、TCP/IPポートを使用してDelivery Controllerと通信します。通常は、ポート80です。
- CTX_XDL_REGISTER_SERVICE = Y | N – Linux Virtual Desktopサービスは、起動時の開始をサポートします。通常は、Yに設定します。
- CTX_XDL_ADD_FIREWALL_RULES = Y | N – Linux Virtual Desktopサービスでは、ネットワーク受信接続がシステムのファイアウォールの通過を許可されている必要があります。Linux Virtual Desktop用に、システムのファイアウォールの必要ポート（デフォルトではポート80およびポート1494）を自動で開放できます。通常は、Yに設定します。
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 – Virtual Delivery Agentには、Delivery Controllerに対して認証するためにKerberos構成設定が必要です。Kerberos構成は、システムにインストールおよび構成済みのActive Directory統合ツールから指定します。次に示す、サポートされているActive Directory統合方法のうち、使用するものを指定します。
 - 1 - Samba Winbind
 - 2 - Quest Authentication Services
 - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO = Y | N – Linux Virtual Desktopでは、HDX 3D Proがサポートされます。これは、強力なグラフィックアプリケーションの仮想化を最適にするための一連のグラフィックアクセラレーションテクノロジーです。HDX 3D Proをサポートするには、対応するNVIDIA GRIDグラフィックカードをインストールする必要があります。HDX 3D Proを選択した場合、Virtual Delivery AgentはVDIデスクトップ（単一セッション）モード用に構成されます（すなわち、CTX_XDL_VDI_MODE=Yとなります）。これは、SUSEではサポートされていません。必ずこの値をNに設定してください。
- CTX_XDL_VDI_MODE = Y | N – 専用デスクトップ配信モデル（VDI）またはホストされる共有デスクトップ配信モデルのどちらとしてマシンを構成するかを決定します。HDX 3D Pro環境の場合は、Yに設定する必要があります。通常は、Nに設定します。
- CTX_XDL_SITE_NAME = dns-name – Virtual Delivery Agentは、DNSを使用してLDAPサーバーを検出し、LDAPサービスレコードを照会します。DNSの検索結果をローカルサイトに制限するには、DNSサイト名を指定します。通常は、空（none）です。
- CTX_XDL_LDAP_LIST = list-ldap-servers – Virtual Delivery Agentは、デフォルトではDNSを照会してLDAPサーバーを検出します。ただし、DNSがLDAPサービスレコードを提供できない場合は、LDAPの完全修飾ドメイン名（FQDN）およびLDAPポートのスペース区切りの一覧（例：ad1.mycompany.com:389）を指定することができます。通常は、空（none）です。
- CTX_XDL_SEARCH_BASE = search-base – Virtual Delivery Agentは、デフォルトではActive Directoryドメインのルート（例：DC=mycompany,DC=com）に設定された検索ベースを使用してLDAPを照会します。ただし、検索のパフォーマンスを改善するために検索ベースを指定できます（例：OU=VDI,DC=mycompany,DC=com）。通常は、空（none）です。
- CTX_XDL_START_SERVICE = Y | N – Linux VDA構成の完了時にLinux VDAサービスが開始されるようにするかどうかを指定します。通常は、Yに設定します。

注意

現在、HDX 3D ProはSUSEでは使用できません。

次のようにして、環境変数を設定し、構成スクリプトを実行します。

```

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

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

```

sudoに**-E**オプションを指定し、作成する新しいシェルに既存の環境変数を渡す必要があります。Citrixは、最初の行に**#!/bin/bash**を記述し、上記のコマンドからなるシェルスクリプトファイルを作成することをお勧めします。

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

```

sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
    CTX_XDL_DDC_LIST=list-ddc-fqdns \
    CTX_XDL_VDA_PORT=port-number \
    CTX_XDL_REGISTER_SERVICE=Y|N \
    CTX_XDL_ADD_FIREWALL_RULES=Y|N \
    CTX_XDL_AD_INTEGRATION=1|2|3 \
    CTX_XDL_HDX_3D_PRO=Y|N \
    CTX_XDL_VDI_MODE=Y|N \
    CTX_XDL_SITE_NAME=dns-name \
    CTX_XDL_LDAP_LIST=list-ldap-servers \
    CTX_XDL_SEARCH_BASE=search-base \
    CTX_XDL_START_SERVICE=Y|N \
    /opt/Citrix/VDA/sbin/ctxsetup.sh

```

構成変更の削除

シナリオによっては、Linux VDAパッケージをアンインストールしないで、**ctxsetup.sh**スクリプトによって行われた構成変更を削除することが必要となる場合があります。

続行する前に、次のコマンドを使用してこのスクリプトのヘルプを確認します。

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

構成変更を削除するには、次のコマンドを実行します。

```
sudo /usr/local/sbin/ctxcleanup.sh
```

Important

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

構成ログ

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

```
/tmp/xdl.configure.log
```

Linux VDAサービスを再起動し、変更を反映させます。

VDAソフトウェアの実行

ctxsetup.shスクリプトを使用してLinux VDAを構成したら、次のコマンドを使用してLinux VDAを制御します。

Linux VDAの起動

Linux VDAサービスを起動するには、次のコマンドを実行します。

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

Linux VDAの停止

Linux VDAサービスを停止するには、次のコマンドを実行します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Linux VDAの再起動

Linux VDAサービスを再起動するには、次のコマンドを実行します。

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

Linux VDAの状態の確認

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

```
sudo /sbin/service ctxvda status
```

```
sudo /sbin/service ctxhdx status
```

Linux VDAソフトウェアのアンインストール

Linux VDAのインストール状態の照会

Linux VDAがインストールされているかどうかを確認したり、インストールされているパッケージのバージョンを表示したりするには、次のコマンドを実行します。

```
rpm -q XenDesktopVDA
```

詳細を表示するには、次のコマンドを実行します。

```
rpm -qi XenDesktopVDA
```

Linux VDAのアンインストール

Linux VDAパッケージ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。

```
sudo rpm -e XenDesktopVDA
```

注意

Linux VDAソフトウェアをアンインストールすると、関連付けられたPostgreSQLおよびその他の構成データが削除されます。ただし、Linux VDAのインストールより前にセットアップされた、PostgreSQLパッケージおよびその他の依存するパッケージは削除されません。

依存するパッケージの削除

この記事では、PostgreSQLなど、依存するパッケージの削除方法については説明していません。

トラブルシューティング

H.264エンコーディングが使用中であるかどうかの確認

Linux VDA v1.3によってH264およびHardwareEncodingの値がレジストリパスHKLM\Software\Citrix\Ica\Session\<セッションID>\Graphicsに追加され、VDAで発生するグラフィックの問題のトラブルシューティングに役立ちます。

セッションを起動するには、次のコマンドを実行して、H.264エンコーディングをLinux VDAでアドバタイズします。

```
/opt/Citrix/VDA/bin/ctxreg create -k
```

```
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
```

```
"AdvertiseH264" -d "0x00000001" --force
```

セッションを開始して、キーH264がレジストリパスで作成されていることを確認します。作成されている場合、H.264エンコーディングが使用中であることを意味します。

```
/opt/Citrix/VDA/bin/ctxreg list -k
```

```
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

3D Proのハードウェアエンコーディングが使用中であるかどうかの確認

3D Proハードウェアエンコーディング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、次のコマンドを使用します。

```
/opt/Citrix/VDA/bin/ctxreg create -k
```

```
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
```

```
"HardwareEncoding" -d "0x00000001" --force
```

セッションを開始して、レジストリパスの"HardwareEncoding"の値を確認します。この値が「0」の場合は使用されておらず、「1」はハードウェアエンコーディングが使用中であることを意味します。

```
/opt/Citrix/VDA/bin/ctxreg list -k
```

```
"HKLM\Software\Citrix\Ica\Session\{SESSION_ID}\Graphics"
```

以下のコマンドを使用して、セッションIDをクエリします。

```
/opt/Citrix/VDA/bin/ctxqsession
```

ユーザーごとのデスクトップ環境のカスタマイズ

現在、Linux VDAではユーザーがログイン時にデスクトップ環境を選択することを許可していません。この問題の回避策として、ユーザーはLinuxディストリビューション用にファイル（.xsessionなど）を構成して、各ユーザーにデフォルトのデスクトップ環境を設定することができます。詳しくは、Linuxディストリビューションに付属のドキュメントを参照してください。

KDEをデフォルトの環境として設定する場合：

```
#!/usr/bin/env bash
```

```
exec startkde
```

GNOMEをデフォルトのデスクトップ環境として設定する場合：

```
#!/usr/bin/env bash
```

```
exec gnome-session
```

Linuxマシンが正しく準備されているかどうかの確認

最も一般的な問題は、主にネットワーク、NTPタイムサーバー構成、またはActive Directoryドメインのメンバーシップに関連する、Linuxマシンの誤った構成から直接引き起こされます。多くの場合、Linuxマシンの構成を修正すると、VDAソフトウェアの問題は解決します。

ログとトレースの構成

Broker AgentとHDXサービスでは、syslogにログを記録します。Citrixサポートでは、サポートへの連絡時に追加のトレースを有効にできるツールのセットを提供しています。

HDXサービスログ

HDXサービスは、設定が不要なsyslogメッセージをログに記録するように構成されているため、追加の構成は不要です。

Broker Agent ログ

Broker Agent (ctxvdaサービスとも呼ばれます) は、ネットワークソケットを介してログデータをsyslogに書き込みます。この機能は、初期状態では構成されていない場合があります。syslogへのBroker Agent ログの記録を有効にするには、次の構成が必要です。

SLED/SLES 11

/etc/syslog-ng/syslog-ng.conf ファイルを編集し、s_sys セクションに次の行を追加します。

```
udp(ip(127.0.0.1) port(514));
```

syslog-ng.conf ファイルを保存して閉じます。次のコマンドで、syslog-ng サービスを再起動して変更を適用します。

```
sudo service syslog-ng restart
```

SLED/SLES 12

/etc/rsyslog.conf ファイルを編集して、次の行を追加します。

```
$ModLoad imudp
```

```
$UDPServerRun 514
```

rsyslog.conf ファイルを保存して閉じます。次のコマンドで、rsyslog サービスを再起動して変更を適用します。

```
sudo service rsyslog restart
```

HDXセッションが起動しないときの対応策

次のコマンドで、新しいセッションの起動を妨げている可能性がある、孤立したプロセスがないことを確認します。

```
sudo pkill -9 ctxhdx
```

```
sudo pkill -9 ctxgfx
```

```
sudo pkill -9 ctxlogin
```

```
sudo pkill -9 ctxvfb
```

Linux VDA サービスを再起動し、接続を再試行します。

重要なディレクトリおよびファイルの所有者および権限の確認

次のディレクトリおよびファイルのファイル所有者および権限を確認します。

- /var - 所有者 : root、グループ : root、権限 : 0755

- /var/xdl - 所有者 : ctxsrvr、グループ : ctxadm、権限 : 0755
- /var/xdl/.isacagent - 所有者 : root、グループ : root、権限 : 0666
- /var/xdl/.winsta - 所有者 : ctxsrvr、グループ : ctxadm、権限 : 0777
- /var/xdl/vda - 所有者 : root、グループ : root、権限 : 0755

オーディオが聞こえない

Citrix ReceiverおよびLinuxデスクトップを実行しているデバイスのボリュームコントロールがミュートまたは低いレベルに設定されていないことを確認します。

Linux VDAでオーディオが有効になっていることを確認します。次のように、ctxregツールを使用して、構成項目fDisableCamの値を照会します。

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

値が0x1である場合は、オーディオが無効になっています。有効にするには、次のようにしてfDisableCamを0x0に設定します。

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

それでもオーディオが聞こえない場合は、Citrixオーディオシンクがpulseaudioによってロードされていることを確認します。このPulseAudioモジュールは、セッションの起動時にpulseaudioデーモンにロードされます。次のように、pacmdツールを使用して、Citrixオーディオシンクがロードされていることを確認します。

```
pacmd list-sinks
```

Citrixオーディオシンクがロードされている場合、出力は次のようになります。

```
name:
```

```
driver:
```

Citrixオーディオシンクがロードされていない場合は、ctxaudioプロセスを強制終了してから再起動します。

オーディオが録音されない

Linux VDAでオーディオが有効になっていることと、ICAクライアントでオーディオ録音が有効になっていることを確認します。それでもオーディオが録音されない場合は、Citrixオーディオソースがpulseaudioによってロードされていることを確認します。ICAクライアントでオーディオ録音が有効になっている場合は、セッションの起動時に、このPulseAudioモジュールがpulseaudioデーモンにロードされます。次のように、pacmdツールを使用して、Citrixオーディオソースがロードされていることを確認します。

```
pacmd list-sources
```

Citrixオーディオソースがロードされている場合、出力は次のようになります。

```
name:
```

```
driver:
```

Citrixオーディオソースがロードされていない場合は、ctxaudioプロセスを強制終了してから再起動します。

印刷できない

印刷が正しく機能しない場合に確認する項目はいくつかあります。印刷デーモンはセッションごとのプロセスで、実行されるのはセッションの期間中です。次のコマンドで、印刷デーモンが実行中であることを確認します。

```
ps -ef | grep ctxlpmngt
```

ctxlpmngt プロセスが実行中でない場合は、コマンドラインから手動でctxlpmngtを起動します。

それでも印刷が機能しない場合は、次にCUPSフレームワークを確認します。ctxcupsサービスはプリンター管理用であり、Linux CUPSフレームワークと通信します。これはマシンごとの単一プロセスとなっていて、次のコマンドで確認できます。

```
service ctxcups status
```

サービスが実行中でない場合は、次のようにして手動で起動します。

```
service ctxcups start
```

印刷出力が文字化けする

出力が文字化けする場合、対応していないプリンタードライバが原因となっている可能性があります。ユーザーごとのドライバ構成を使用できるため、~/CtulpProfile構成ファイルを編集して構成できます。

```
[DEFAULT_PRINTER]
```

```
printername=
```

```
model=
```

```
ppdpath=
```

```
drivertype=
```

printernameは、現在クライアント側で通常使うプリンターの名前が指定されているフィールドです。これは読み取り専用の値となっており、編集できません。

Important

ppdpath、**model**、および**drivertype**の各フィールドは、マップされたプリンターに対していずれか1つのフィールドしか有効にならないため、同時には設定できません。

ユニバーサルプリンタードライバがクライアントプリンターに対応していない場合、model=オプションを使用してネイティブプリンタードライバのモデルを構成できます。プリンターの現在のモデル名は、lpinfoコマンドを使用して表示できます。

```
lpinfo -m
```

```
...
```

```
xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

...

次のようにして、プリンターに一致するようにモデルを設定できます。

```
Model=xerox/ph3115.ppd.gz
```

ユニバーサルプリンタードライバーがクライアントプリンターに対応していない場合、ネイティブプリンタードライバーのppdファイルのパスを構成できます。ppdpathの値は、ネイティブプリンタードライバーファイルの絶対パスです。

たとえば、ppdドライバーが/home/tester/NATIVE_PRINTER_DRIVER.ppdにある場合は、次のようになります。

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

Citrixが提供するユニバーサルプリンタードライバーは3種類（Postscript、pcl5、およびpcl6）です。ネイティブプリンタードライバーが使用できない場合は、これらをドライバーの種類として構成できます。

たとえば、クライアントが通常使うプリンターのドライバーの種類がPCL5である場合は、次のようになります。

```
drivertype=pcl5
```

注意

Citrix Receiver for MacおよびCitrix Receiver for Linuxでは、サポートされるのがPostscriptプリンターのみであるため、PCL5およびPCL6ユニバーサルプリンタードライバーは適用できません。この状況では、ネイティブプリンタードライバーのppdpathまたはモデルをPostscript以外のプリンターに設定する必要があります。

CDMが機能しない

CDM機能にはデーモンプロセス（ctxcdmd）が含まれます。CDM機能でエラーが発生した場合は、Linux VDAマシンを再起動して、デーモンが正しく起動されたかどうかを確認します。

```
Ps -lef | grep ctxcdmd
```

マップされたドライブでのファイルの名前付けは、VDAとReceiver OSの名前付け規則に従う必要があります。

既知の問題

セッションのローミング時、Citrix Receiver for AndroidでCaps Lock状態が反対になる場合がある

Citrix Receiver for Androidへの既存の接続をローミングすると、Caps Lock状態が失われる場合があります。回避策として、拡張キーボードのShiftキーを使用して大文字と小文字を切り替えます。

Citrix Receiver for Macを使用して**Linux VDA**に接続している場合、**alt**キーを使用するショートカットキーが常に機能するとは限らない

Citrix Receiver for Macでは、左右どちらのoption/altキーを押しても、デフォルトではAltGrが送信されます。Citrix Receiverの設定でこれを変更することはできますが、結果はアプリケーションによって変わります。

SuSE Linux Enterprise Desktop 11で新しいXクライアントライブラリがキーボードの問題を引き起こす可能性がある

SuSE Linux Enterprise Desktop 11のxorg-x11-libX11パッケージの新しいバージョンでは、キーボードマッピングの変更を処理する際に問題が発生する場合があります。これが原因で、HDXセッション内でキーボード機能の問題が生じる可能性があります。この問題は、インストールしたパッケージのバージョンが7.4-5.11.11.1~7.4-5.11.15.1の範囲である場合に、発生する可能性があります。

回避策として、ストックバージョンのxorg-x11-libX11 SP3パッケージにロールバックすると、キーボードマッピングの変更が正常に機能します。次に例を示します。

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1

rpm -i --force xorg-x11-libX11-32bit-7.4-5.9.1

rpm -e xorg-x11-libX11-7.4-5.11.15.1

rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

この回避策は、ユーザーがマシンにログオンする前に実施する必要があります。セッションがアクティブなときに行うと、ユーザーが次回ログインするまで上記の設定は有効になりません。

ストックバージョンのSP3からアップグレードすると、上記のxorg-x11-libX11パッケージを現在インストールされているバージョンにロックできるため、アップグレード中に変更されることはありません。アップグレードする前に以下を実行し、その後は通常どおりのアップグレードを続行します。

```
zypper al xorg-x11-libX11

zypper al xorg-x11-libX11-32bit
```

XenDesktop Version 7.1のDelivery Controllerと共にLinux VDAを使用すると、セッションの起動に時間がかかる場合がある

起動が遅くなる原因は、Version 7.1のDelivery Controllerによって生成されたICAファイルにCommon Gateway Protocol設定が存在するためです。この設定が存在すると、Citrix ReceiverはTCPポート2598で接続を確立しようとします。SLED 12など一部のLinuxディストリビューションでは、デフォルトのファイアウォール設定でTCP SYNパケットをドロップするため、タイムアウトが発生してセッションの起動に時間がかかります。回避策として、TCPポート2598でTCP SYNを拒否するように、Linux VDAでファイアウォールを構成します。この問題は、新しいバージョンのDelivery Controllerでは解決済みです。

Linux VDAをドメインに再度追加するときに、登録に失敗する

特定の状況で、Linux VDAがドメインに再度追加されて、Kerberosキーの新しいセットが生成されると、ブローカーがVDAとのセキュリティコンテキストの確立に失敗します。多くの場合、この問題は、Kerberosキーの以前のセットに基づいた期限切れのVDAサービスチケットがキャッシュに存在し、それをブローカーが使用することが原因で発生します。この問題によって、VDAがブローカーへの接続を停止することはありませんが、ブローカーはVDAに返すセキュリティコンテキストを確立できません。通常見られる現象は、VDA登録の失敗です。

この問題は、VDAサービスチケットが最終的に期限切れとなって更新されると自動的に解決しますが、サービスチケットは通常、長時間有効です。期限切れとなるまで、非常に長い時間が必要となる可能性があります。

解決策として、ブローカーのチケットキャッシュをクリアします。ブローカーを再起動するか、管理者としてコマンドプロンプトからブローカーで次のコマンドを実行します。

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

このコマンドにより、Citrix Broker Serviceを実行するNetwork ServiceプリンシパルがLSAキャッシュに保持するサービスチ

チケットはすべて削除されます。これにより、ほかのVDAのサービスチケットが削除されます。また、その他のサービスのサービスチケットも削除される可能性があります。ただし、この処理は悪影響を及ぼしません。これらのサービスチケットは、再度必要になったときにKDCから再取得されます。

オーディオプラグアンドプレイがサポートされない

ICAセッションでオーディオの録音を開始する前に、オーディオキャプチャデバイスをクライアントマシンに接続することをお勧めします。オーディオ録音アプリケーションの開始後にデバイスを接続した場合は、アプリケーションが応答なくなる可能性があります。この問題が発生した場合は、アプリケーションを再起動してください。録音中にキャプチャデバイスが取り外されると、同様の問題が発生する可能性があります。

オーディオの歪み

Windows 10 Receiverでは、オーディオ録音中にオーディオが歪む場合があります。

CTXPSドライバーが一部のPLCプリンターに対応しない

印刷出力が適切でない場合は、プリンタードライバーを、製造元から提供されたネイティブプリンタードライバーに設定してください。

サイズの大きな文書の印刷が遅い

ローカルのクライアントプリンターでサイズの大きな文書を印刷すると、印刷ファイルはサーバーとの接続を介して転送されます。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。

別のセッションからプリンター通知と印刷ジョブ通知が表示される

Linuxでのセッションの考え方は、Windowsオペレーティングシステムとは異なります。したがって、すべてのユーザーがシステム全体の通知を受け取ります。管理者は、CUPS構成ファイル/etc/cups/cupsd.confを変更して、これらの通知を無効にすることができます。

次のように、構成されている現在のポリシー名がこのファイルに記述されています。

DefaultPolicy default

ポリシー名がdefaultである場合は、次の行をデフォルトポリシーのXMLブロックに追加します。

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ..

Require user @OWNER

Order deny,allow
```

用語集

ブローカー - XenDesktop環境で、異なるVDAに対するHDXセッションを仲介するXenDesktopコンポーネントです。DDCまたはXenDesktopのコントローラーとも呼ばれます。

Broker Agent - 配信するデスクトップを提供する、Linux VDAマシン上のコンポーネントです。Broker Agentは、ブローカーと通信してセッションを仲介できるようにします。Broker Agentは、VDAサービスとHDXサービスという2つの主要コンポーネントで構成されます。

Citrix Director - Citrixヘルプデスク/サポートがXenDesktop VDAを監視および制御するために使用するコンソールです。

Citrix Studio - XenDesktopを構成するために使用するCitrix管理コンソールです。

DDC - XenDesktop Desktop Delivery Controllerです。ブローカーまたはDelivery Controllerとも呼ばれます。

FQDN - 完全修飾ドメイン名です。

HDX - High Definition Experience（高品位なユーザーエクスペリエンス）プロトコルです。以前はCitrix ICAプロトコルと呼ばれていました。

HDXサービス - HDXプロトコルを介して仮想Linuxデスクトップをリモート処理するLinuxサービス（ctxhdx）です。VDAサービスと通信してセッションを仲介できるようにします。

RHEL - Red Hat Enterprise Linuxです。Red Hatが提供する商用のLinuxディストリビューションです。

SLED - SUSE Linux Enterprise Desktopです。Novellが提供する商用のLinuxディストリビューションです。

SLES - SUSE Linux Enterprise Serverです。Novellが提供する商用のLinuxディストリビューションです。

VDA - Virtual Delivery Agentです。

VDAサービス - ブローカーと通信してセッションを仲介できるようにするLinuxサービス（ctxvda）です。HDXサービスとも通信してリモートセッションを配信します。

サイトの作成

Jul 07, 2016

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（使用している場合）、およびそのサイトで作成された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、最初マシンカタログ・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。このプログラムへの登録の有無の変更はサイト作成後いつでも自由に行えます。登録の有無を変更するには、Studioのナビゲーションペインで **【構成】**、**【製品サポート】** タブの順に選択し、表示される手順に従ってください。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、このアートを確認してください。これには、サイトを実際に作成する前に完了しておく必要があるタスクと、考慮する必要がある決定事項が含まれています。

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。

サイトの種類と名前

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（<サイト名>）】**）の上部に表示されます。

データベース

【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。

サイトを作成するときに、サイトデータベースとして使用する目的でのSQL Server Expressデータベースのインストールを選択すると（デフォルトの設定）、データベースソフトウェアがインストールされた後に再起動されます。サイトデータベースとして使用する目的でSQL Server Expressをインストールしなかった場合は、再起動されません。

デフォルトのSQL Server Express Editionインストールを使用しない場合、サイトを作成する前に、SQL Serverソフトウェアが

マシンにインストールされていることを確認してください。「システム要件」には、サポートされているバージョンが一覧表示されています。

サイトにDelivery Controllerを追加する必要があり、既に別のサーバーでControllerソフトウェアをインストールしている場合、サイトの作成ウィザードのこのページからサイトにDelivery Controllerを追加することができます。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、スクリプトを生成する前にControllerを追加します。

ライセンス管理

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ライセンス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、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、`<name>[:<port>]`の形式で指定します。名前 () は、完全修飾ドメイン名 (FQDN)、NetBIOS、またはIPアドレスにする必要があります。FQDNが推奨されます。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。

電源管理 (リモートPCアクセスのみ)

後述の「[リモートPCアクセス](#)」セクションを参照してください。

ホスト接続、ネットワーク、およびストレージ

ホスト (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、サイトを作成するときにホストへの最初の接続を作成 (構成) 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。この接続やリソースは後で変更でき、追加の接続を作成することもできます。

重要: サイト作成ウィザードで接続やリソースの情報を構成するときには、ガイダンスとして [接続とリソース](#) を参照してください。

- 「[接続の種類の情報ソース](#)」では、サポートされる各接続の種類に関する情報の参照先を示します。
- 「[ホストストレージ](#)」では、ストレージの種類とストレージの管理手法について説明します。
- 「[ストレージの管理](#)」および「[ストレージの選択](#)」では、接続作成時にストレージ情報を構成する方法を説明します。

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やデスクトップを提供しない場合、つまり専用ブレードPC上でホストされるユーザーデスクトップをStudioで管理する場合は、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、ホストの種類として[**Microsoft System Center Configuration Manager**]を選択します。

【[接続](#)】ページで、ホスト上の仮想マシンを作成するツールとして、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](#)】ページで、上述の情報ソースリンクのガイダンスに従って、必要な情報を構成します。

リマインダー: 詳細なガイダンスは「[接続とリソース](#)」に記載されています。

追加の機能

追加の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

今後AppDiskを使用する予定であり、AppDNAを既にインストール済みの場合、この機能を選択すると、AppDiskのアプリケーションを分析し、互換性問題を確認し、修復操作を実行してそれらの問題を解決できます。詳しくは、[「AppDisks」](#)を参照してください。

App-V公開

App-Vサーバーにある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。このチェックボックスをオンにすると、App-V Management serverのURLと、App-V公開サーバーのURLおよびポート番号の入力を求められます。

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

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の構成手順を完了します。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。自動的にすべてのユーザーを追加するデフォルトの機能はありません。また、ウィザードの[\[マシンアカウント\]](#)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、[\[マシンアカウントの追加\]](#)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。

注：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。これには、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。これには、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。

概要

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、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。

マシンカタログの作成

Aug 26, 2016

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。マシン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。

サイトの作成後、Studioでは最初の実マシンカタログを作成する手順が表示されます。最初の実マシン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

仮想マシンを含むカタログを作成する場合、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。MCS (Machine Creations Services) やProvisioning Servicesなど、Studioでサポートされているツールを使用するか、独自のツールを使用してマシンを提供することができます。マシンが既に提供されており、マスターイメージを使用する必要がない場合でも、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します。

- Provisioning Services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による仮想マシンのプロビジョニングを選択した場合、カタログで同一の仮想マシンを作成するためのガイドとして、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上またはクラウドサービス上でツールを使用し、マスターイメージを作成して構成します。これには、イメージへのVDA (Virtual Delivery Agent) のインストールが含まれます。その後、Studioでのマシンカタログの作成時に、そのイメージ（またはそ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、追加情報を構成します。

MCSまたはPVS (Provisioning Services) を使用して最初の実マシン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（最初の実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。

マシンカタログの作成ウィザードを完了した後、テストが自動的に実行されて正しく構成されているかどうか検証されます。テストが完了したら、テストレポートを表示できます。後で、Studioのナビゲーションペインの[Citrix Studio<サイト名>]において、これらのテストをいつでも実行できます。

ヒント：Studioではなく、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 (VM Templates) を指定できます。

Windows XPまたはWindows Vistaマシンでは以前のバージョンのVDAを使用する必要があるため、最新の機能を使用することはできません。それらのマシンのWindowsオペレーティングシステムバージョンをアップグレードできない場合は、それらを個別の実マシンカタログで管理することをお勧めします。

MCSカタログ作成の概要

以下は、マシンカタログの作成ウィザードに情報を入力した後のMCS操作の簡単な概要です。

- ウィザードで（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によって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によってデスクトップが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。2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。このディスクに、セッション中に加えられた変更が保存されます。これは、専用デスクトップでは恒久的に保持されます。プールデスクトップでは、再起動のたびに削除され、新しいディスクが作成されます。

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、およびその他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。
- Provisioning Services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。Provisioning Services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、関連ドキュメントを参照してください。
- 作成するマシンの数に応じて十分なプロセッサ、メモリ、ストレージがハイパーバイザーホスト上にあることを確認してください。
- デスクトップやアプリケーションの実行に必要な正確なハードディスク容量を指定します。この値は後から変更できません。
- リモートPCアクセスのマシンのカタログでは、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。アプリケーションを仮想化して配信することで、ユーザーのデスクトップに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、デスクトップの管理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：Provisioning Services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、新しい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。vCPUの数を指定します（この値は、マシンのカタログを作成するときに指定することもできますが、PowerShellを使用する場合だけです。カタログの作成時にStudioのユーザーインターフェイスでvCPUの数を指定することはできません）。デスクトップやアプリケーションの実行に必要なハードディスク容量をこの時点で指定しておく必要があります。この値は後から変更できません。
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. Provisioning Services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. マスターイメージを、そのマスターイメージで提供するアプリケーションやデスクトップのドメインに追加して、仮想マシンを作成するハイパーバイザーホスト上でこのマスターイメージを使用できることを確認します。MCSを使用している場合、ドメインにマスターイメージを追加する必要はありません。プロビジョニングされたマシンは、マシンカタログのウィザードで指定したドメインに追加されます。
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。マシン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。

XenServerでのGPU対応マシン用マスターイメージの準備

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では、GPUをサポートするビデオカードドライバーをインストールして、グラフィックソフトウェアでGPUを使用できるように構成しておく必要があります。

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でのマシンカタログの作成

マシン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。このウィザードで選択する項目によっては、後述のページの一部が表示されなかったり、タイトルが異なったりする場合があります。

重要：マスターイメージを使用している場合、マシンカタログを作成する前に、イメージにVDAをインストールし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。

- サイトを作成した後でマシンカタログを作成していない場合は、マシン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、[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。

オペレーティングシステム

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、複数のユーザーが共有可能なデスクトップや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。
- **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られる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。

マシン管理

[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、マシンの展開に使用するツールを選択します。

- **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。
- **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Provisioning Services 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。

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ー** 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を一貫させることをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

【デスクトップエクスペリエンス】ページ（デスクトップOSマシンを含むカタログの作成時のみに表示）では、作成されるデスクトップの種類が決定されます。デスクトップがユーザーに割り当てられるかどうか、およびユーザーが加えた変更がマシンの再起動時にどのように処理されるかによって種類が異なります。

次の3つの種類があります。

- **プール、ランダム**：デスクトップがランダムに割り当てられます。ユーザーがログオンするたびに、新しい（ランダム）デスクトップに接続されます。ユーザーがログオフすると、別のユーザーがデスクトップを利用できるようになります。デスクトップが再起動されると、行った変更はすべて破棄されます。
- **プール、静的**：デスクトップが恒久的に割り当てられます。ユーザーがログオンするたびに、同じ（静的）デスクトップに接続されます。ユーザーがログオフしても、そのユーザーのみがデスクトップを利用できます。デスクトップが再起動されると、行った変更はすべて破棄されます。
- **専用**：デスクトップが、恒久的に1人のユーザーに割り当てられます。ユーザーがログオフしても、そのユーザーのみがデスクトップを利用できます。デスクトップが再起動されても、行った変更はすべて保持されます。変更は、ローカル仮想マシンディスクか、専用のPersonal vDiskの指定したドライブ文字に保存することができます。

マスターイメージ

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。最初のマシン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：

- Provisioning Services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。
- 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。

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。ウィザードページにおいてデフォルトで選択されている、【インストールされているVDAのバージョンを選択します】は変更しないでください。

ウィザードで過去に選択したマシン管理テクノロジー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。

セキュリティ（クラウドサービス環境）

仮想マシンの1つまたは複数のセキュリティグループを選択します。これらはアベイラビリティゾーンでセキュリティグループがサポートされる場合にのみ表示されます。

マシンで使用するハードウェアとして、共有のハードウェアまたはアカウント専用のハードウェアを選択します。

仮想マシン、デバイスコレクション、または仮想マシンとユーザー

このページのタイトルは、【マシン管理】ページで選択した展開方法によって変わります。

- MCSを選択した場合、このページのタイトルは[仮想マシン]です。
- Provisioning Servicesを選択した場合、このページのタイトルは[デバイスコレクション]です。
- そのほかのツールを選択した場合、このページのタイトルは[仮想マシンとユーザー]です。

ページ名

- 作成する仮想マシンの数を指定します。
- 各マシンのメモリ量 (MB単位) を選択します。
- [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専用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。
- MCSを使用してマシンを展開し、Personal vDiskを使用しないプールされたランダムな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。詳しくは、次のセクションを参照してください。

重要：各仮想マシンはハードディスクを持ちます。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。

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。

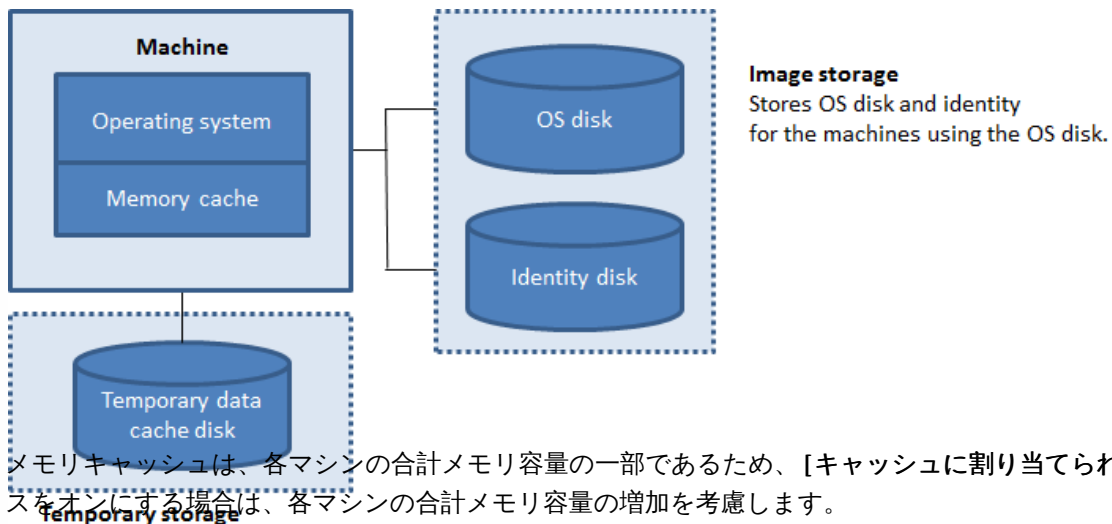
一時データのキャッシュを有効にするには、カタログの各マシンのVDAをバージョン7.9以上にする必要があります。

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。



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。

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。

ネットワークインターフェイスカード（NIC）

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。

マシンアカウント

（リモートPCアクセスカタログのみで有効）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。

コンピューターアカウント

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。

- 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。

Provisioning Services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。

名前と説明

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。

マシンカタログの管理

Jul 07, 2016

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）マシンが含まれるマシンカタログの場合は、カタログで使用す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。

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。

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

サイト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

マシン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。
- 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。

マシン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マシンカタログおよびサーバーOSマシンカタログから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。
- 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。

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

ヒント：接続の管理について詳しくは、「[接続およびリソース](#)」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. オペレーティングシステムの最適化ガイド（『[Windows 7最適化ガイド](#)』および『[Windows 8/8.1仮想デスクトップ最適化ガイド](#)』）を確認し、環境に対して最適化を適用します。
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われます。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。

カタログの更新

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。

更新のロールバック

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なことがあります。ロールバックした場合、カタログ内のマシンは前回起動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

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。

注：Windows XPまたはWindows Vistaマシンでは以前のバージョンのVDAを使用する必要があるため、最新の機能を使用することはできません。 それらのマシンのWindowsオペレーティングシステムをアップグレードできない場合は、それらを個別のカタログで管理することをお勧めします。

デリバリーグループの作成

Aug 26, 2016

デリバリーグループは、いくつかのマシNCatalog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NCatalog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NCatalog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

マシNCatalogを選択して、そのマシNCatalogから使用するマシNCの数を選択します。

ヒント：

- マシNCatalogに未使用のマシンが残っていない場合、そのCatalogを選択することはできません。
- 同じマシNCatalog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NCatalogのマシンを使用できますが、これらのマシNCatalog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NCのCatalogとLinuxマシNCのCatalog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NC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NCatalog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NC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NC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NCatalog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NCatalog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。

配信の種類

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

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。

Users

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。

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、すでにユーザーデータ（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は一意的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	いいえ
認証が不要なユーザーのみ	いいえ	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

アプリケーション

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。
- 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、[次へ] 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。

デスクトップ (またはデスクトップ割り当て規則)

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。
- 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。

- (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。

概要

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。

デリバリーグループの管理

Jul 07, 2016

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。

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。
ユーザーごとのデスクトップ数	(割り当てられたデスクトップOSマシンのみ) ユーザーが同時にアクティブにできる共有デスクトップの最大数です。初回使用時割り当てのデスクトップグループでは、この値によってユーザーが自分に割り当てることのできるデスクトップ数が指定されます。
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。
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。

ユーザー一覧のインポートまたはエクスポート

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**【構成】** > **【StoreFront】** の順に選択します。

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、そのマシンカタログに関連付けられ、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せんが、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：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」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、電源状態タイマーを設定することはできませんが、プールまたはバッファ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は制御できません。

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] ページで、[マシンの電源管理] ボックスから[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。

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

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. [再起動の開始]で、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。

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

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. [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

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。そのため、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。

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。

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いない場合）。
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。

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。

使用されない事前起動セッションや残留セッションがアクティブのまま保持される時間

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

つ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。

セッションの事前起動を有効にするには、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. 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。

Edit Delivery Group

Studio

Users
Delivery Type
Application Prelaunch
Application Linging
Basic settings
Access Policy
Restart Schedule

Prelaunch Sessions for Applications

With prelaunch, sessions launch when users log on to Receiver, so applications are available sooner.

When do you want sessions to launch?

☐ Launch when users start an application (no prelaunch)

☒ Prelaunch when any user in the Delivery Group logs on to Receiver for Windows

☐ Prelaunch when any of the following users log on to Receiver for Windows:

Add... Remove

If no application is started, when do you want prelaunched sessions to end?

After a specified time: Hours 2 - +

☒ When average load on all machines exceeds (%): 80 - +

☒ When load on any machine exceeds (%): 85 - +

OK Cancel Apply

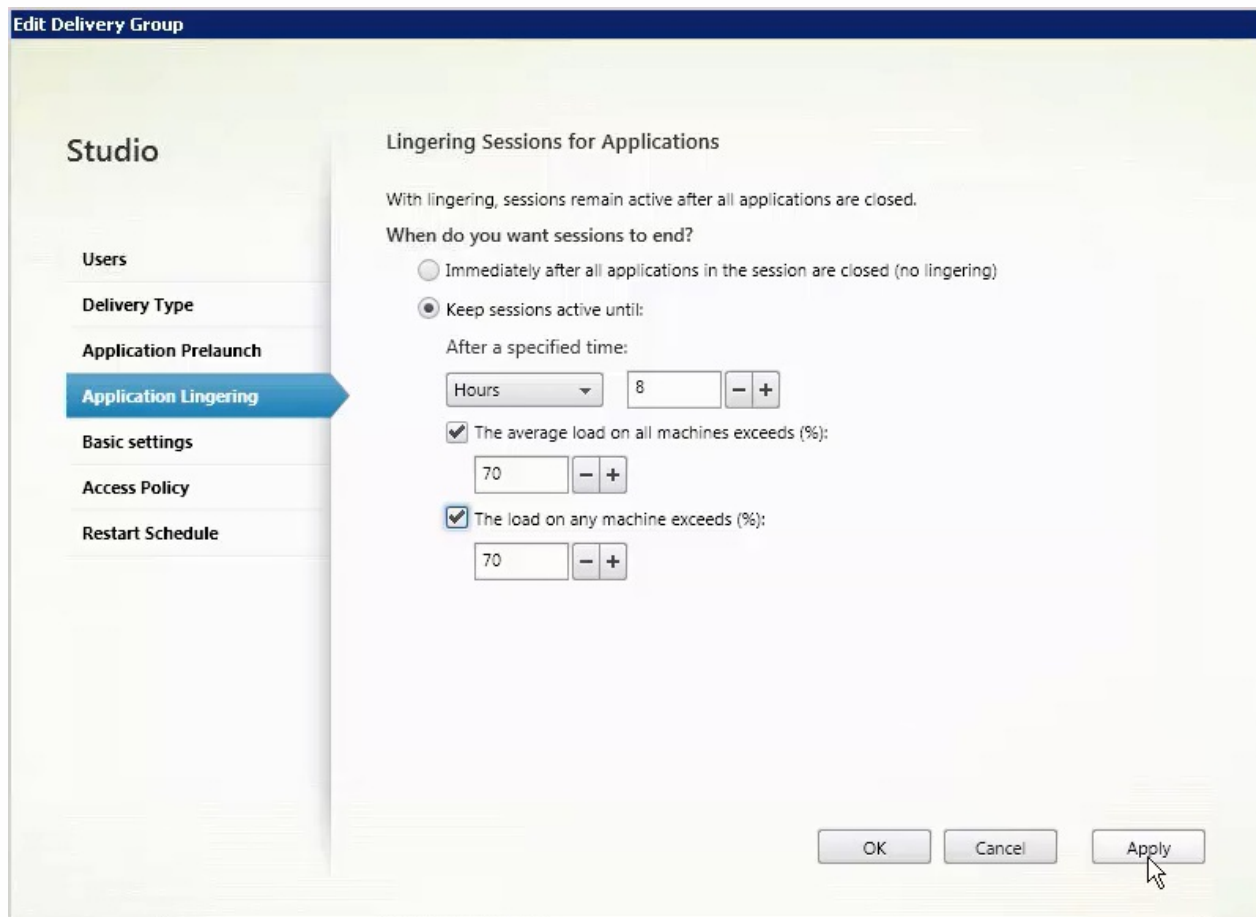
4. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。
 - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を1～99日間、1～2,376時間、または1～142,560分で指定します。
 - デリバリーグループ内のすべてのマシンの平均負荷が上限値（1～99%）を超えたときに終了する。

- 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。

セッション残留を有効にするには、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. 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。

アプリケーショングループの作成

Jul 07, 2016

はじめに

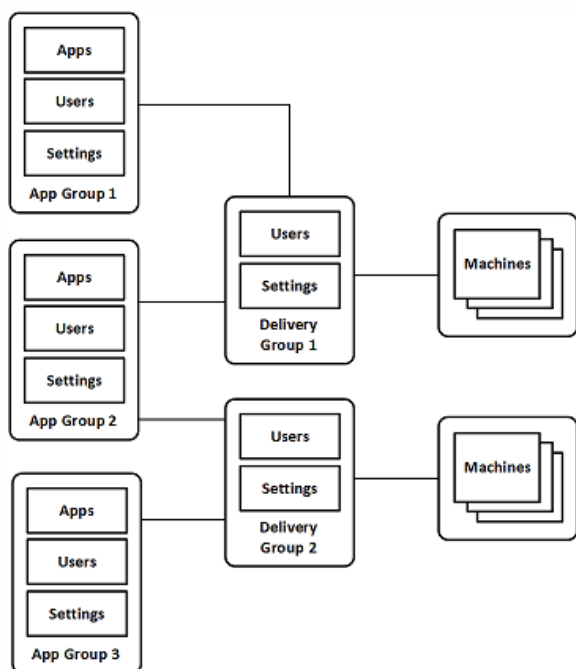
アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代替手段となります。デリバリーグループは複数のアプリケーショングループに関連付けることができ、アプリケーショングループは複数のデリバリーグループに関連付けることができます。

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。

構成例

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。



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に関連付けられています。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、関連付け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られているためです。

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に関連付けられています。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。

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間のセッション共有

アプリケーショングループを使用するときに、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許可または禁止できます。（これにより、以下の最初の例で説明するデリバリーグループのみを使用するときの標準のセッション共有動作が拡張されます。）アプリケーションセッションを共有すると、追加のアプリケーションセッション起動に関連するコストを節約できます。また、コピーアンドペースト操作のようなクリップボードを使用するアプリケーション機能も使用できるようになります。

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のユーザーがWordを起動することでアプリケーションセッションを開始し、次にWordがまだ実行されている間にExcelを起動しました。Controllerが同じサーバーにExcelを見つけると、セッションが共有されます。（これは、アプリケーショングループを使用していない場合に、デリバリーグループで使用される基本的なセッション共有機能です。）Excelが同じサーバーでは見つからないが、アプリケーショングループ1でセッション共有が有効にされている場合で、アプリケーショングループ1に関連付けられているデリバリーグループ、またはアプリケーショングループ2や3に含まれている別のサーバーで見つかった場合、Controllerはセッションを共有しようとします。

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。

マシンがフル稼働されている場合は、共有は許可されません。

セッションの事前起動や残留セッション機能を使用する場合は、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を有効にする必要があります。ただし、この機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にし構成する必要があります。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。

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。

デリバリーグループ

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**一覧には、選択できるデリバリーグループが含まれます。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**一覧には、選択することが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、そのグループが以前のXenDesktop 7.xバージョンで作成され、（2）デリバリーグループの編集権限がある場合は、デスクトップのみを配信する共有マシンを含む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。

Users

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。

- 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。

アプリケーション

ヒント：

- 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と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け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、[次へ] 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）。

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。互換性のないソースは、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。

スコープ

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。

概要

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。

アプリケーショングループの管理

Jul 07, 2016

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
- アプリケーションの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されます。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. 行った変更を適用してウィンドウを開いたままにするには[適用] をクリックし、変更を適用してウィンドウを閉じるには [OK] をクリックします。

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. 行った変更を適用してウィンドウを開いたままにするには[適用]をクリックし、変更を適用してウィンドウを閉じるには[OK]をクリックします。

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て、[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. 行った変更を適用してウィンドウを開いたままにするには[適用]をクリックし、変更を適用してウィンドウを閉じるには[OK]をクリックします。

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. 行った変更を適用してウィンドウを開いたままにするには[適用]をクリックし、変更を適用してウィンドウを閉じるには[OK]をクリックします。

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. 行った変更を適用してウィンドウを開いたままにするには[適用]をクリックし、変更を適用してウィンドウを閉じるには[OK]をクリックします。

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。

リモートPCアクセス

Jul 07, 2016

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。

Important

XenAppおよびXenDesktop7.9では、リモートPCアクセス展開にのみコマンドラインを使用してください。詳しくは、[コマンドラインを使ったインストール](#) および「[既知の問題](#)」[#637741]を参照してください。

社内PC上にインストールするVirtual Delivery Agent (VDA) により、そのPCが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）を作成しておくことで、各ユーザーが管理者による介在なく自分の社内PCをサイトに追加できます。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アクセスのスリープモードおよび休止状態モードはサポートされていません。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。これらのアカウントは、リモートPCアクセス用のデリバリーグループでユーザーを指定するときに使用します。

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。

マシンカタログ用のマシンアカウントを選択するときは、ほかのマシン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のすべてのマシンを、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、そのカテゴリ内のマシンカタログと対応するデ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。

社内PCでWindows XPが動作している場合は、そのPC用に専用のマシンカタログおよびデリバリーグループを作成します。この場合、Studioでマシンカタログのマシンアカウントを選択するときに、一部のマシンでWindows XPが動作していることを示すチェックボックスをオンにします。

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。このオプションにより、ヘルプデスクのスタッフはDirectorを使用して、Windowsリモートアシスタンスを用いたユーザーのセッションの表示や制御を行うことができます。

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および8.1でサポートされています。他のオペレーティングシステムでワークステーションVDAを展開する場合は、セキュアブートを無効にしてください。

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動作を「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他のコンポーネント。
- 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）。

リモートPCアクセスはほとんどのSurface Proデバイスでも使用できます。XenDesktop 7.9では、Windows 8.1または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。
- 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。

ユーザーが強制的にコンソールアクセスを取得しようとする場合、ローカルユーザーはCtrl+Alt+Delキーを10秒間隔で2回押し、リモートセッションのローカル制御を取得して、切断イベントを強制することができます。

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+Del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、「[インストールの準備](#)」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。

Wake on LAN

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。

- Intel社のActive Management Technology (AMT) をサポートするPC。
- BIOSでWake on LANオプションが有効になっているPC。

管理者は、Microsoft System Center Configuration Manager (ConfigMgr) 2012のWake on LAN機能を構成する必要があります。ConfigMgrでは、PCに対してAMTパワーコマンドを実行できます。また、ウェイクアッププロキシやマジックパケットがサポートされます。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。

さらに、以下を確認します。

- セキュリティおよび信頼性の高いAMTパワーコマンドの使用が推奨されますが、AMTを使用せずに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方法もあります。
- AMTに対応したマシンでは、StudioやDirectorからそのマシンを強制シャットダウンまたは強制再起動することもできます。また、StoreFrontおよびReceiverでは再起動操作も使用できます。

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。

ユーザーまたはサードパーティ製Wake on LANソリューションがSystem Center 2012 R2を必要とすることなくコネクタを作成できるようにする概念実証 (POC) Wake on LAN SDKについて詳しくは、[CTX202272](#)を参照してください。このリリースのWake on LAN SDKは評価のみを目的としており、実稼働環境での使用についてはサポートしていません。

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] ）、マシン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。

Install the VDA on the office PCs used for local and remote access. 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。

VDAをコマンドラインでインストールする時に、**/remotepc**オプションを含めます。デスクトップ（ワークステーション）OSで次のコンポーネントのインストールを無効にします。

- App V Component - Citrix Personalization for App-V - VDA
- UpmComponent - Citrix User Profile Manager
- UpmVdaPlugin Component - Citrix User Profile Manager WMI Plugin
- Mps Component - Machine Identity Service
- VDisk Component - Personal vDisk

アップグレード中、これらのコンポーネントがインストールされるとインストーラーが検出してアップグレードします。

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>またはモバイルデバイスでサポートされるアプリケーション配布システムで入手できます。

接続の詳細設定の構成

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。
- 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。

トラブルシューティング

Delivery Controllerは、リモートPCアクセスに関する以下の診断情報をWindowsのアプリケーションイベントログに書き込み

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

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。

App-V

Jul 07, 2016

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～現在の
5.0 SP3および5.1	XenDesktop 7.6以降 XenApp 7.6以降	7.6.300～現在の

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。

- **Management server (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。
- **Publishing server (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。
- **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。

管理方式

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ー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。

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
○	○	デリバリーグループへのApp-Vアプリケーションの追加

Microsoft App-Vの展開

App-Vの展開手順については、<http://technet.microsoft.com/en-us/virtualization/hh710199>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めすべての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。

パッケージングと配置

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、App-V Management serverでパッケージを公開します。

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。

StudioでのApp-Vサーバーアドレスの構成

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。

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マシンへのソフトウェアのインストール

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。

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に設定されていない場合は、**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。このとき、App-V公開コンポーネントにアクセスできるローカル管理者権限を持つアカウントも作成されます。

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。グラフィックインターフェイスで、**[機能]** ページの **[App-V公開コンポーネントのインストール]** 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で、**/no_appv** オプションを含めます。

VDAのインストール中にCitrix App-Vコンポーネントの機能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。

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

この手順は、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。

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。

デリバリーグループへのApp-Vアプリケーションの追加

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]** 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。**[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隣の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: ウィザードを終了します。

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。

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

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すると、Studioの[App-V公開]ノードからもその表示が消えます。ただし、アプリケーションはデリバリーグループからは削除されないため、そのアプリケーションは引き続き起動できます。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。

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。
- 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。
- 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。

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に設定されているかどうかを確認します。Falseに設定されていない場合、最初のApp-Vアプリケーションの起動に失敗します。
- (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Falseに設定します。
- VDAをインストール済みのマシンに、サポートされるバージョンの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「+;」形式 (「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ているマシンで、CtxAppVCOMAdminに管理者権限が設定されていることを確認します。通常、このユーザーはVDAのインストール時に作成され、そのVDAマシンのローカル管理者グループに追加されます。ただし、Active Directoryポリシーの設定によっては、このアカウントの管理者権限が無効になることがあります。compmgmt.mscを実行し、[ローカルユーザーとグループ]、[ユーザー]の順に選択します。CtxAppVCOMAdminが管理者ではない場合は、グループポリシーを編集して、このユーザーアカウントに管理者権限を付与します。
- 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クライアントは署名されていないため、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。

ログ

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:\ProgramFiles\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:\ProgramFiles\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。

AppDisk

Aug 26, 2016

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ーとは異なります。

- 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：

- 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。

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。

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で、デリバリーグループを作成するか編集し、含めるAppDiskを選択します。この手順を*AppDiskの割り当て*と言います (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、Machine Creation Services (MCS) またはProvisioning Services (PVS)、およびDelivery Controllerと連携して、選択されたAppDiskを配信します。

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 (最低限) で提供されるMCS、または使用中の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XenServerのリリース (「システム要件」を参照)、またはVMware (最低限のバージョンは5.1) (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。

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。

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、ラフォルトで有効になっています。

AppDiskで使用す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 3.5がインストールされている必要があります。

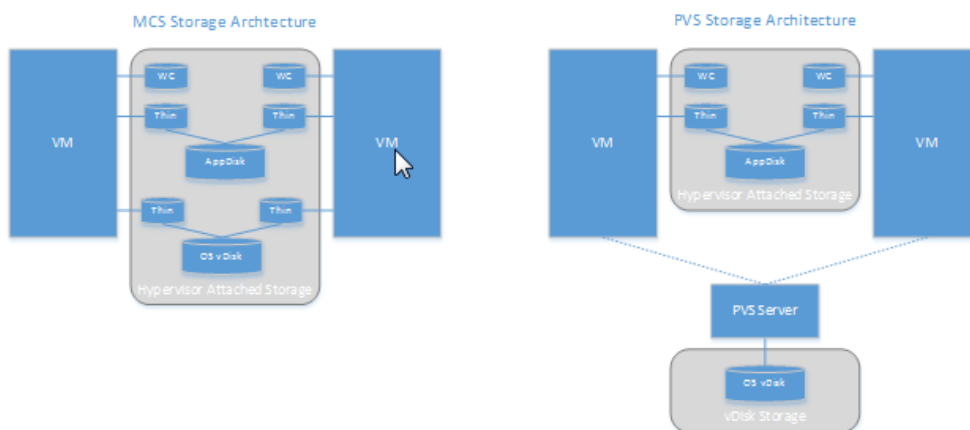
AppDiskはストレージに影響を及ぼす可能性があります。詳しくは、「[ストレージおよびパフォーマンスの考慮事項](#)」を参照してください。

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。

ストレージおよびパフォーマンスの考慮事項

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、ストレージが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。

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、自動的に分析が行われます。この間、StudioでのAppDiskのステータスは「分析中」となります。

PVSに関する注意事項

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。

主にStudioでAppDiskを作成する

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。**[完了]** をクリックします。

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（注意：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。

AppDiskをハイパーバイザーで作成してStudioにインポートする

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。

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。[次へ] 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。[完了] をクリックします。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。

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、選択することができません。
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おけるAppDiskの優先順位

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。

重要： 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。

ローカルアプリケーションアクセスとURLリダイレクト

Jul 07, 2016

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利用できるリダイレクト機能は、サーバーFTA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、https、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）

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、ファイルタイプの割り当て（FTA：File Type Association）による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、そのファイルにアクセスする必要があります。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に表示しない場合、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利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。
 - 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。
- 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ブラウザのアドレスバーに表示されるURLや、ブラウザ内ナビゲーションによるURLだけ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、そ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。

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するWebブラウザ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】、【User Experience】の順に開きます。
5. 【Local App Access settings】を選択します。
6. 【有効】を選択し、【Allow URL Redirection】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には

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する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くなくなります。

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する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を登録解除する場合：<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上でアドオンを登録解除する場合：<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
```

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に移動します。64ビットシステムの場合、HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session Stateに移動します。
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（ローカル環境で使用可能な場合）。
 - 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。

XenApp Secure Browser

Jul 07, 2016

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を使用する必要があります。アプリケーションを社内ですべてホストしていると、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に表示されます。たとえば、ユーザーがブラウザに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ブラウザのタブに表示されます。

XenApp Secure Browser Editionの展開

Citrixは、XenApp Secure Browser用のLifecycle Management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 Version 7.9の発売の一環として、すべての既存のXenAppおよびXenDesktopのお客様は、有効なソフトウェアメンテナンス（SWM）またはSubscription Advantage（SA）を所有している場合、Citrix Lifecycle ManagementのDeployエディションを利用できます。

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 Lifecycle Managementブループリントの使用

Citrix Lifecycle Managementブループリントを使用するには

1. [Workspace Cloud](#)のホームページから「サービス」に移動します。「Lifecycle Managementの試用を申請」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. 試用を申請した際に受信したメールで「管理」をクリックし、「Lifecycle Managementの概要」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 7.9 ISOをダウンロードします。

Secure Browser Edition 7.9 ISOのダウンロード後、以下を検討します。

- 『[Citrix Lifecycle ManagementブループリントによるXenApp Secureのインストール](#)』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の手動インストール

XenApp Secure Browser Version 7.9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 7.9 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。

サーバーVDI

Aug 26, 2016

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Windows 7の外観を持つデスクトップを提供できます。

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

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。

1. Windowsサーバーでインストールの準備を行います。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、およびユーザーのセッションが1つに制限されていることを確認します。
 - 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。
 - [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 2012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。
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。
3. 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。デフォルトでは、サーバーオペレーティングシステム上へのVDA for Windows Desktop OSのインストールはブロックされますが、コマンドラインを使うことでこれを回避できます。

XenDesktopVdaSetup.exe /quiet /servervdi

/controllers オプションを使用すると、コマンドラインを使ってVDAをインストール中にDelivery ControllerまたはControllerを指定できます。

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。

HDX 3D ProモードでVDAを構成するには、**/enable_hdx_3d_pro**オプションを追加します。

/baseimageや/xa_server_locationなど、サーバーVDIでサポートされていない機能のオプションを指定しないでください。

4. サーバーVDIのマシンカタログを作成します。

1. [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。
2. [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-シン] タブに表示されます。

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。

Personal vDisk

Jul 07, 2016

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が許可しながら、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、仮想マシンで使用す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。

Personal vDisk 7.6.1の新機能

このリリースには、以下の改善が含まれています。

- Personal vDiskのパフォーマンスが向上し、Personal vDiskカタログにイメージ更新を適用するときの時間が短くなりました。

このリリースでは、以下の問題が解決されています。

- 基本仮想マシン上のMicrosoft Office 2010をMicrosoft Office 2013にインプレースアップグレードすると、再構成のウィンドウが開いた後で「エラー25004。入力したプロダクトキーは、このコンピューターでは使用できません」というエラーメッセージが表示されることがありました。これまでのリリースでは、基本仮想マシンからOffice 2010をアンインストールしてからOffice 2013をインストールすることでこのエラーを避けることができました。このリリースでは、Office 2010をアンインストールせずにインプレースアップグレードできます (#391225)。
- ユーザーのPersonal vDisk上に新しいバージョンのMicrosoft .Netが存在する場合、イメージの更新時に基本仮想マシン上の以前のバージョンで上書きされるという問題がありました。この問題により、新しいバージョンの.Netを使用するPersonal vDisk上のアプリケーション (Visual Studioなど) が正しく動作しなくなることがありました (#439009)。
- Personal vDiskが有効なProvisioning ServicesイメージディスクでPersonal vDiskを使用しないマシンカタログを作成できないという制限事項がありました。このリリースでは、この制限事項はありません (#485189)。

Personal vDisk 7.6について

Version 7.6には、以下の新機能が追加されています。

- 拡張されたPersonal vDiskのエラー処理およびレポート。Personal vDiskが有効なマシンをStudioのマシンカタログで表示すると、[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。また、より詳細な状態情報が表示されるようになりました。
- 以前のバージョンで提供されていたPersonal vDiskイメージ更新の監視ツール (Image Update Monitoring Tool) が、ISOイメージのISO\Support\Tools\Scripts\PvdToolフォルダーに収録されています。以前のバージョンでも監視機能が提供されていましたが、このリリースではより高度なレポート機能が提供されます。
- Provisioning Servicesのテストモジュールを使用すると、テストカタログ内の更新済みイメージでマシンを起動できます。起動したマシンの安定性を確認した後で、テスト用のPersonal vDiskを実稼働用に昇格させることができます。
- インベントリ実行時に、(Personal vDiskデスクトップ単位ではなく) 2つのインベントリの相違を計算できるようになりました。新しく追加されたコマンドを使用して、MCSカタログの既存のインベントリをエクスポートしてインポートできます。(Provisioning ServicesのマスターvDiskの場合は、以前のインベントリが既に含まれています。)

Version 7.1.3で確認されVersion 7.6で解決された問題は以下のとおりです。

- Personal vDiskのアップグレードを中断すると、既存のPersonal vDiskが破損することがありました。[#424878]
- Personal vDiskを長時間実行して非ページメモリリークが発生すると、仮想デスクトップが応答不能になることがありました。[#473170]

Version 7.6で新たに確認された問題は以下のとおりです。

- 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プロセス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。[#326735]
- マスターイメージから継承されたファイル間のハードリンクは、Personal vDiskカタログで保持されません。[#368678]
- Personal vDiskマスターイメージ上のOffice 2010をOffice 2013にアップグレードすると、仮想マシン上でのOfficeの起動に失敗することがあります。これは、アップグレード時にOffice KMSライセンスプロダクトキーが削除されるために発生します。この問題を回避するには、マスターイメージ上でOffice 2010をアンインストールしてからOffice 2013を再インストールしてください。[#391225]
- Personal vDiskカタログはVMware Paravirtual SCSI (PVSCSI) コントローラーをサポートしません。デフォルトのコントローラーを使用してください。[#394039]
- Personal vDisk Version 5.6.0を使用する仮想デスクトップでユーザーが作成したファイルが、Personal vDisk Version 7への

アップグレード後に消失することがあります。この問題は、プールされた仮想マシンにログオンしたときに新しいユーザープロファイルが作成されるために発生します。現在、この問題を回避する方法はありません。[#392459]

- Windows 7を実行するPersonal vDiskでWindowsシステム保護機能が有効な場合、バックアップと復元機能を使用できません。システム保護を無効にするとユーザープロファイルがバックアップされますが、userdata.v2.vhdファイルは除外されます。システム保護を無効にしてバックアップと復元機能を使ってユーザープロファイルのバックアップを作成することをお勧めします。[#360582]
- ディスクの管理ツールを使用して基本仮想マシン上でVHDファイルを作成する場合、VHDをマウントできないことがあります。この問題を解決するには、Personal vDiskボリュームにVHDをコピーしてください。[#355576]
- Office 2010ソフトウェアを削除しても、そのショートカットが仮想デスクトップから削除されません。ショートカットに手作業で削除してください。[#402889]
- Microsoft Hyper-V環境でPersonal vDiskを使用するマシンカタログを作成するときに、ローカルに格納されたマシンとクラスターの共有ボリューム (CSV) に格納されたvDiskを指定すると、エラーが発生して処理に失敗します。この問題を回避するには、vDiskにほかのストレージを使用してください。[#423969]
- Provisioning Servicesを使用するマシンカタログの仮想デスクトップに初めてログオンする場合、(ctxpvd.exe -s resetコマンドで) Personal vDiskがリセットされていると、デスクトップの再起動を求めるメッセージが表示されます。この場合、デスクトップを再起動する必要があります。この問題は初回ログオン時にのみ発生し、それ以降のログオン時に再起動は不要です。[#340186]
- .NET 4.5をPersonal vDiskにインストールした後で、イメージの更新により.NET 4.0をインストールまたは修正すると、.NET 4.5に依存するアプリケーションを実行できなくなります。この問題を回避するには、基本イメージに.NET 4.5をインストールしてイメージを更新してください。
- XenApp/XenDesktop 7.6の「
— 既知の問題
」のトピックも参照してください。

Personal vDisk 7.1.3について

Version 7.1.1で確認されVersion 7.1.3で解決された問題は以下のとおりです。

- Personal vDisk 5.6.0からPersonal vDisk 7.xへの直接アップグレードにより、Personal vDiskに問題が発生することがありました。[#432992]
- Personal vDiskを使用する仮想デスクトップにユーザーが断続的に接続できなくなる場合があります。[#437203]
- Personal vDisk 5.6.5以降からPersonal vDisk 7.0以降へのアップグレード時にPersonal vDiskのイメージ更新処理が中断されると、それ以降の更新処理に失敗することがありました。[#436145]

Personal vDisk 7.1.1について

Version 7.1で確認されVersion 7.1.1で解決された問題は以下のとおりです。

- イメージ更新を介してSymantec Endpoint Protection 12.1.3を更新すると、symhelp.exeによりアンチウイルス定義の破損が報告されます。[#423429]
- サービスコントロールマネージャー (services.exe) がクラッシュすると、プールされたデスクトップがPersonal vDiskにより再起動されることがありました。[#0365351]

Version 7.1.1で新たに確認された問題はありません。

Personal vDisk 7.1について

Version 7.1には、以下の新機能が追加されています。

- Windows 8.1を実行するデスクトップを備えたPersonal vDiskを使用できるようになりました。また、イベントログ機能も向上しています。
- コピーオンライト (CoW) はサポートされなくなりました。Personal vDiskをバージョン7.0から7.1にアップグレードすると、CoWによって管理されたデータに対するすべての変更が失われます。これはXenDesktop 7の評価用機能であり、デ

フォルトでは無効になっていました。そのため、この機能を有効にしなかった場合には、特に影響を受けません。

Version 7.0.1で確認されVersion 7.1で解決された問題は以下のとおりです。

- Personal vDiskレジストリキーのEnableProfileRedirectionの値を1またはONに設定し、また後からイメージの更新中に値をまたOFFに変更すると、Personal vDiskスペース全体がユーザーによってインストールされたアプリケーションに割り当てられ、ユーザープロファイル用の領域がなくなってvDisk上に残ることがありました。このプロファイルのリダイレクトがカタログに対して無効で、イメージの更新中にそれを有効にする場合、ユーザーは仮想デスクトップにログオンすることができないことがあります。[#381921]
- Personal vDiskのインベントリ更新に失敗すると、デスクトップサービスによって正確なエラーがイベントビューアーに記録されませんでした。[#383331]
- Personal vDisk 7.xにアップグレードするときに、変更済の規則が保持されないという問題がありました。この問題は、Version 7.0からVersion 7.1へのアップグレードでは発生しません。ただし、Version 5.6.5をVersion 7.1にアップグレードする場合は、最初に規則ファイルを保存し、次にアップグレードの後で規則を再度適用する必要があります。[#388664]
- Windows 8が動作するPersonal vDiskで、Windowsストアからアプリケーションをインストールできないという問題がありました。この場合、「購入処理は完了できませんでした」という内容のエラーメッセージが表示されます。Windows Updateサービスを有効にしてもこの問題は解決しませんでした。現在はこの問題が解決されています。ただし、ユーザーがインストールしたアプリケーションは、システムの再起動後に再インストールする必要があります。[#361513]
- Personal vDiskを使用するWindows 7のプールされたデスクトップで、一部のシンボリックリンクが欠落するという問題がありました。この問題により、C:\Users\All Usersにアイコンを格納するアプリケーションでは、[スタート]メニューにアイコンが表示されませんでした。[#418710]
- インベントリの更新後にシステムに多くの変更を追加すると、更新シーケンス番号 (USN) ジャーナルオーバーフローが発生し、Personal vDiskが起動しないという問題がありました。[#369846]
- 状態コード0x20およびエラーコード0x20000028により、Personal vDiskが起動しませんでした。[#393627]
- Symantec Endpoint Protection 12.1.3により「Proactive Threat Protectionは誤動作しています」というメッセージが表示され、このコンポーネントのLive Update Statusを使用できませんでした。[#390204]

Version 7.1で新たに確認された問題については、XenDesktop 7.1の「

— 既知の問題

」のトピックを参照してください。

Personal vDisk 7.0.1について

Version 7.0.1の新機能：環境の変更に対してPersonal vDiskがより強固になりました。イメージ更新に失敗した場合でもPersonal vDiskを伴う仮想デスクトップをDelivery Controllerに登録できるようになっており、また安全でないシステムシャットダウンによりvDiskが使用不可となってしまうことがなくなりました。さらに、規則ファイルを使用することで、展開時にvDiskからファイルやフォルダーを除外できるようになりました。

Version 5.6.13で確認されVersion 7.0.1で解決された問題は以下のとおりです。

- プールされた仮想デスクトップ上でのユーザーによるグループのメンバーシップの変更内容が、イメージの更新後に失われることがありました。[#286227]
- Personal vDiskに十分な領域がある場合でも、イメージ更新がディスク容量不足によるエラーで失敗することがありました。[#325125]
- 一部のアプリケーションで仮想デスクトップのPersonal vDiskへのインストールに失敗し、再起動を求めるメッセージが表示されることがありました。これは、保留中の名前変更操作によるものです。[#351520]
- マスターイメージ内で作成されたシンボリックリンクが、Personal vDiskを使用する仮想デスクトップで正しく機能しないという問題がありました。[#352585]
- Citrix Profile managementとPersonal vDiskを使用する環境では、プロファイルのリダイレクトが有効な場合にシステムボリューム上でユーザープロファイルを調査するアプリケーションは正常に機能しないことがありました。[#353661]
- インベントリのサイズが2GBを超える場合に、マスターイメージ上でのインベントリの更新に失敗するという問題がありました。

した。[#359768]

- イメージの更新がエラーコード112により失敗し、Personal vDiskが破損することがありました。この問題は、更新に必要な空き領域がvDiskにある場合でも発生します。[#363003]
- カタログのデスクトップ数が250を超える場合に、サイズ変更スクリプトの処理が失敗するという問題がありました。[#363365]
- ユーザーによる環境変数に対する変更が、イメージの更新時に失われることがありました。[#372295]
- Personal vDiskを使用する仮想デスクトップ上で作成されたローカルユーザーが、イメージ更新時に失われるという問題がありました。[#377964]
- インベントリの更新後にシステムに多くの変更を追加すると、更新シーケンス番号 (USN) ジャーナルオーバーフローが発生し、Personal vDiskの起動に失敗するという問題がありました。この問題を避けるには、USNジャーナルのサイズをマスターイメージ内で32 MB以上に増やして、イメージ更新を実行します。[#369846]
- Personal vDiskでAppSense Environment Managerを置き換えモードで使用する場合、レジストリハイブが正しく処理されないという問題が確認されています。これは、Personal vDiskがインストールされときのRegRestoreKey APIの動作に関連しています。CitrixとAppSenseは共同でこの問題の解決にあたっています。[#0353936]

バージョンに依存しない既知の問題

- 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に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十分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をリセットしてください。[#474071]

インストールとアップグレード

Jul 07, 2016

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、Provisioning Servicesのドキュメントを参照してください。

Personal vDiskのインストールと有効化

マシン上の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も自動的にインストールされます。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 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。

VDAをインストールするときに、Personal vDiskを有効にするためのオプション（インストールウィザードの [Personal vDisk] チェックボックスまたはコマンドラインインターフェイスの/baseimageオプション）を選択できます。これらのオプションを選択せずに（つまりデフォルトのまま）VDAをインストールした場合でも、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ることができます。

Personal vDiskの追加

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。

PvDのアップグレード

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のみをアップグレードするには、[ここで提供されている](#)Personal vDiskのMSIファイルを使用します。

Personal vDiskのアンインストール

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。

構成と管理

Jul 07, 2016

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。

考慮事項：Personal vDiskのサイズ

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。

$$\text{追加されるスペース} = (5.0 - 4.7) \div 2 + 3.0 \div 2 = 1.65\text{GB}$$

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。

プロファイルの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、1

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、イメージのファイル数が250,000の場合、テンプレートVHDのサイズは約1,024,000,000バイト（1GB弱）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atalog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）追加領域を計算することを検討してください。

方法：Personal vDiskのサイズおよび割り当ての構成

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場合には、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ことがありますが、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、アプリケーション

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。

その他の設定：

- **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ことで、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。

考慮事項：マスターイメージ上のアプリケーション

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：

- 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

- 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（ dongle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。

考慮事項：Provisioning Services

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小さ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、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。

考慮事項：Machine Creation Services

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。

方法：vDiskからファイルやフォルダーを除外する

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。

方法：マスターイメージ更新時のインベントリの実行

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なくなります。これによりPersonal vDiskが機能なくなります。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。

方法：ホスト接続での同時操作を制限する

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操作** - 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 ($14000 \div 350 = 40$) 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操作] 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。

方法 : System Center Configuration Manager 2007とPersonal vDisk

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\smsecfg.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\Log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。

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。

ツール

Jul 07, 2016

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。

カスタムの規則ファイル

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。

- PersonalVDisk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 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。

サイズ変更とプール統計のスクリプト

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。

アプリケーション領域のリセット

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 \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。

Personal vDiskインベントリのエクスポートとインポート

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ネットワーク共有をマブします。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にアクセスできるアカウントが必要です。

- 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>.Citr\vdSvc.exe exportinventory \\share location\ExportedInventory Current inventory source location C:\Citrix\PvD\Settings\Inventory\VER-LAS ... Exporting
```

- 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。

Ctxpvdsv.exe importinventory "<path-to-exported-inventory>"

<path to exported inventory>には、エクスポート済みのインベントファイルのフルパス（通常<network location>\ExportedPvdInventory）を指定します。

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
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
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT

- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

バックアップと復元

重要：これらのスクリプトを実行しても、Personal vDiskのストレージの場所を変更することはできません。これを行うには、ほかの方法を使用してください。

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る2つのPowerShellスクリプトを使用して、Personal vDisksをバックアップして復元することができます。バックアップと元用のスクリプトを使用して、既存のPersonal vDiskとユーザーの関連付けを別のカタログに移行できます。この方法は、Personal vDiskストレージを変更するときにも使用できます。バックアップスクリプトを実行すると、既存のカタログのメタデータを含むXMLファイルが作成されます。このメタデータには、Personal vDiskの現在のストレージの場所と関連付けられているユーザーの情報が含まれます。このXMLファイルを復元スクリプトで使用すると、Personal vDiskが新しいカタログに関連付けられ、ユーザーが割り当てられます。

- migration-backup.ps1は、各ユーザーとマシンカタログ内のPersonal vDisk間のマッピング情報をXMLファイルとして保存します。
- migration-restore.ps1は、そのXMLファイルを使ってマシンカタログ内でユーザーのデスクトップを再作成します。

バックアップや復元を実行する前に、以下の点に注意してください。

- これらのスクリプトではハイパーバイザーAPIを使用するため、スクリプトを実行するControllerにハイパーバイザーのPowerShellスナップインをインストールしておく必要があります。
- 対象のマシンカタログのControllerにアクセスできる場所でスクリプトを実行する必要があります。
- これらのスクリプトがサポートするハイパーバイザープラットフォームは、Citrix XenServer、Microsoft Hyper-V、およびVMware ESXです。

マシンカタログのバックアップ

マシンカタログを変更するたびにバックアップを作成してください。カタログ内のマシンが使用中の場合でもバックアップを実行できます。

Personal vDiskを持つマシンカタログをバックアップするには、migration-backup.ps1を使用します。このスクリプトの実行時に、マシンカタログ名とハイパーバイザーの接続情報を入力する必要があります。すると、マシンカタログ内の各マシンについてPersonal vDiskストレージと割り当てられたユーザーの間のマッピング情報が保存されます。この情報はXMLファイルに格納されます。このXMLファイルの構造は以下のとおりです。

- PvdMigration.hypervisor.Typeは、ハイパーバイザーの種類（VMware ESX、Citrix XenServer、またはMicrosoft Hyper-V）です。
- PvdMigration.PVDは、Personal vDiskの格納場所と、そのPersonal vDiskに割り当てられているユーザーの情報です。
- PvdMigration.PVD.DiskIdは、バックアップしたハイパーバイザー上のvDiskの一意なIDです。
- PvdMigration.PVD.DiskNameは、VHDまたはVMDKファイルの名前です。
- PvdMigration.PVD.SRNameは、バックアップを実行したときのストレージプロバイダーの名前です。
- PvdMigration.PVD.SRIDは、バックアップしたハイパーバイザー上のストレージプロバイダーの一意なIDです。
- PvdMigration.PVD.UserNameは、このvDiskに割り当てられているユーザーの名前です。
- PvdMigration.PVD.UserSidは、このvDiskに割り当てられているユーザーのSIDです。
- PvdMigration.PVD.Stateは、このvDiskの状態を示し、「backed up」または「processed」のいずれかです。初回のバックアップの後は「backed up」になります。このXMLファイルを使ってバックアップを復元すると、状態が「processed」に変更されます。

マシンカタログの復元

復元を実行する前に、次の点に注意してください。

- バックアップしたマシンカタログと同じマスターイメージを共有するマシンカタログだけを復元できます。
- バックアップしたマシンカタログのマスターイメージのインベントリを更新して、新しいマスターイメージを作成する必要があります。

Personal vDiskを持つマシンカタログをバックアップから復元するには、migration-restore.ps1を使用します。このスクリプトの実行時に、以下の情報を入力する必要があります。

- バックアップ時に生成されたXMLファイル。
- 復元するマシンカタログの名前。
- 未アタッチのPersonal vDiskの格納場所の名前。この情報は、バックアップ時のXMLファイル内に記述されています。
- ハイパーバイザーの接続情報

migration-restore.ps1スクリプトはマシンカタログ内の未割り当てマシンを検索し、それにユーザーを割り当てます。また、ユーザーのPersonal vDiskをマシンにアタッチします。

シナリオ例1：新しいマシン名を使用したマシンカタログおよびそのPersonal vDiskの復元

このシナリオでは、マシンカタログ全体とそのマシンにアタッチされたPersonal vDiskが復元されます。各マシンには新しい名前が指定されます。以下の手順は、ハイパーバイザーやストレージホストで障害が生じた場合、または新しいインフラストラクチャにユーザーを移行する場合に使用します。

1. migration-backup.ps1を実行して、ユーザーとPersonal vDiskとのマッピングをXMLファイルにバックアップします。
2. 何らかのバックアップソリューションを使用して、元のマシンカタログから任意のディスク上にPersonal vDiskを移動またはキャプチャします。
 - VMware ESXまたはMicrosoft Hyper-Vの場合：Personal vDiskは、Controllerにより指定されたストレージ上の、vDiskのアタッチ先マシン名を示すフォルダー内にあります。
 - Citrix XenServerの場合：Personal vDiskは、Controllerにより指定されたストレージのルートにあります。各vDiskの名前はGUIDです。
3. 何らかのストレージバックアップソリューションを使用して、元のマシンカタログからPersonal vDiskを復元します。
 - ESXまたはHyper-Vの場合：新しいストレージリソースの新しいフォルダーにvDiskを配置します。または、新しいストレージリソース上で、バックアップ元と同じパスにvDiskを配置します。
 - XenServerの場合：新しいストレージリソース上のルートにvDiskを配置します。
4. 障害が発生したマシンカタログの作成元のマスターイメージから、Provisioning Services vDiskまたはMachine Creation Servicesスナップショットを作成します。
5. vDiskまたはスナップショット上の「スタート」メニューから「インベントリの更新」を実行します。
6. Studioでマシンカタログを再作成します。このとき、障害が発生した（オリジナルの）マシンカタログと異なる規則で名前を指定します。これにより、新しいPersonal vDiskを持つ新しいマシンカタログが作成され、サイトデータベースに認識されます。
7. 再作成されたマシンカタログが正しいデリバリーグループに割り当てられていることを確認します。
8. デリバリーグループがメンテナンスモードで、そのグループの各マシンがシャットダウン状態であることを確認します。
9. バックアップスクリプトにより生成されたXMLファイルを編集します。
 - ESXまたはHyper-Vの場合：手順3で新しいストレージリソース上の新しいフォルダーにvDiskを復元した場合、ファイル内のすべてのセクションについて、のフォルダー名を新しいフォルダー名に置き換えます。バックアップ元と同じパスにvDiskを復元した場合は、この手順をスキップします。
 - XenServerの場合：この手順をスキップします。
10. Controller上でmigration-restore.ps1を実行し、XMLファイルの名前およびバックアップされたvDiskの格納場所を指定します。

シナリオ例2：既存のマシン名を再使用したマシンカタログおよびそのPersonal vDiskの復元

このシナリオでは、マシンカタログ全体とそのマシンにアタッチされたPersonal vDiskが復元されます。各マシンには、元の名前が再使用されます。以下の手順は、ハイパーバイザーやストレージホストで障害が生じた場合に使用します。

1. migration-backup.ps1を実行して、ユーザーとPersonal vDiskとのマッピングをXMLファイルにバックアップします。
2. 何らかのバックアップソリューションを使用して、元のマシンカタログから任意のディスク上にPersonal vDiskを移動またはキャプチャします。
 - ESXまたはHyper-Vの場合：Personal vDiskは、Controllerにより指定されたストレージ上の、vDiskのアタッチ先マシン名を示すフォルダー内にあります。
 - XenServerの場合：Personal vDiskは、Controllerにより指定されたストレージのルートにあります。各vDiskの名前はGUIDです。
3. 何らかのストレージバックアップソリューションを使用して、元のマシンカタログからPersonal vDiskを復元します。
 - ESXまたはHyper-Vの場合：新しいストレージリソースの新しいフォルダーにvDiskを配置します。
 - XenServerの場合：新しいストレージリソース上のルートにvDiskを配置します。
4. 障害が発生したマシンカタログの作成元のマスタートレージから、Provisioning Services vDiskまたはMachine Creation Servicesスナップショットを作成します。
5. vDiskまたはスナップショット上の「スタート」メニューから「インベントリの更新」を実行します。
6. Studioでマシンカタログを再作成します。このとき、障害が発生した（オリジナルの）マシンカタログと同じ規則で名前を指定します。これにより、新しいPersonal vDiskを持つ新しいマシンのカタログが作成され、サイトデータベースに認識されます。
7. 再作成されたマシンカタログが正しいデリバリーグループに割り当てられていることを確認します。
8. デスクトップグループがメンテナンスモードで、そのグループの各マシンがシャットダウン状態であることを確認します。
9. バックアップスクリプトにより生成されたXMLファイルを編集します。
 - ESXまたはHyper-Vの場合：ファイル内のすべてのセクションについて、のフォルダー名をvDiskの復元先フォルダー名に置き換えます。
 - XenServerの場合：この手順をスキップします。
10. Controller上で、編集したXMLファイルを指定してmigration-restore.ps1スクリプトを実行します。スクリプトにより、vDiskが移動せずにアタッチされます。
11. ユーザーデータが正しく復元されていることを確認します。

シナリオ例3：マシンカタログの一部のPersonal vDiskの復元

このシナリオでは、マシンカタログ内の一部のPersonal vDiskで障害が発生したため、そのvDiskだけを復元します。カタログ内の仮想マシンでは障害が発生していません。

1. migration-backup.ps1を実行して、ユーザーとPersonal vDiskとのマッピングをXMLファイルにバックアップします。
2. XMLファイルには、マシンカタログの各ユーザーに対応するセクションがあります。Personal vDiskを復元する必要がないユーザーについて、ファイルからそれらのユーザーおよび関連セクションを削除します。
3. ほかのシナリオで説明しているように、何らかのバックアップソリューションを使って元のマシンカタログからPersonal vDiskを復元します。
 - 新しいマシン名を使用する場合は、シナリオ例1を参照してください。
 - マシン名を保持する場合は、シナリオ例2を参照してください。
4. カタログに十分な未割り当てマシンがあることを確認します。必要な場合は、マシンを追加します。vDiskを復元する各ユーザーについて、新しいマシンが1つ必要です。
5. デスクトップグループがメンテナンスモードで、そのグループの各マシンがシャットダウン状態であることを確認します。
6. Controller上で、編集したXMLファイルを入力として指定してmigration-restore.ps1スクリプトを実行します。
7. ユーザーデータが正しく復元されていることを確認します。

表示、メッセージ、およびトラブルシューティング

Jul 07, 2016

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\PvDAActivation.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。

エラーメッセージ: Version 7.6以降

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ゴールデン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。**
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。
- **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。

エラーメッセージ：Version 7.6より前のバージョン

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。
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イルスソフトウェア（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 (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により記録されるイベント

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。
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コンテナの作成に必要な領域がありません。

コンポーネントの削除

Jul 07, 2016

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とをお勧めします。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ト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ア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。

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には

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には

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。

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には

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。

アップグレードと移行

Jul 07, 2016

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。次のアップグレードが可能です。

- XenDesktop Version 5（以降）から最新リリースのXenDesktopへのアップグレード
- XenApp 7.5から最新リリースのXenAppへのアップグレード

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。

XenDesktop 5（以降）ファームまたはXenApp 7.5サイトをアップグレードするには、以下の操作を行います。

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を検出され、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。

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、Knowledge Centerの[CTX201988](#)を参照してください。

XenApp 6.5ワーカーを最新のVDAにアップグレードするには、以下の操作を行います。

1. XenApp 6.5ワーカー上でXenApp 7.6インストーラーを実行します。XenApp 6.5ファームからそのワーカーが削除され、XenApp 6.5ソフトウェアがアンインストールされた後、新しいXenApp VDA for Windows Server OSがインストールされます。
2. アップグレードが完了したら、そのサーバーをXenAppサイトのマシンカタログとデリバリーグループに追加します。

詳しくは、「[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。

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 6.5またはXenDesk 4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。

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。

XenDesktop 4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XenDesktopサイトを作成します。
2. XenDesktop 4ファームで、エクスポートコマンドツールを使用して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XenDesktopのサイトで、インポートコマンドツールを使用してXMLファイルからファーム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、「[XenDesktop 4からの移行](#)」を参照してください。

環境のアップグレード

Aug 26, 2016

ここでは次のことについて説明します。

- はじめに
- アップグレードできる製品コンポーネントのバージョン
- 要件、制限、および準備
- 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
- アップグレードの順序

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する前に、一部の環境をアップグレードすることができます。これをインプレースアップグレードと呼びます。 次のアップグレードが可能です。

- XenDesktop Version 5（以降）から最新リリース（現在）のXenDesktopへのアップグレード
- XenApp Version 7.5（以降）から最新リリース（現在）のXenAppへのアップグレード

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。XenApp 6.5の移行について詳しくは、「[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。 アップグレードが必要なコンポーネントが自動的に特定され、それらがアップグレードされます。 各コンポーネントをアップグレードしたら、アップグレードしたStudioを使ってサイトデータベースとサイトをアップグレードします。

ここで製品という語は、特に明記されていない限り、XenApp 7.xまたはXenDesktop 7.xを指します。

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とStudio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。

- Delivery Controller 5以降
- VDA 5.0 SP1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。 MSI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 5.0 SP1～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

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。
- Microsoft System Center Virtual Machine Manager（SCVMM）。現在の製品はSCVMM 2012およびSCVMM 2012 SP1をサポートします。XenDesktop 5.xはそれより前のバージョンをサポートします。ダウンタイムの発生を避けるには、次の順序でアップグレードします。
 1. XenDesktop 5.6 FP1より前のバージョンを実行しているControllerがある場合は、それらをXenDesktop 5.6 FP1にアップグレードします（そのバージョンのXenDesktopのドキュメントを参照してください）。
 2. SCVMMサーバーをSCVMM 2012にアップグレードします。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。
 3. XenDesktopコンポーネントを最新バージョンにアップグレードします。
 4. 必要に応じて、SCVMMサーバーをSCVMM 2012 SP1にアップグレードします。
- StoreFront。

要件、制限、および準備

- 製品の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ってコアコンポーネントとVDAをアップグレードする必要があります。以前の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はできません。
- 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、ControllerとStudioの新しいバージョンがリリースされた場合、Controllerだけをアップグレードすると古いバージョンのStudioでサイトを管理できなくなります。
- Citrixライセンスサーバーをアップグレードする前に、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2016.0518以降である必要があります。
- 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。
- アップグレードを開始する前に、CTX135207の説明に従ってデータベースをバックアップしてください。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。
- 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。
- 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。
- アップグレードを開始する前に、管理コンソールおよびPowerShellセッションを含む、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。）

- 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。
- 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。
- 一部のVDAを最新バージョンにアップグレードしない場合は、「VDAの混在環境のサポート」を確認してください。
- Web Interfaceを使用していた環境では、StoreFrontを使用することをお勧めします。
- 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。
- サイトの停止に備えるために、後述のアップグレードの順序を確認してください。

以下のアップグレードはサポートされていません。

- Early Release版またはTechnology Preview版からのアップグレード
- Version 7.5よりも前のバージョンのXenAppからのアップグレード（サーバー上のXenApp 6.5ソフトウェアを新しいVDA for Windows Server OSに置き換える場合を除く。「XenApp 6.xからの移行」参照）
- Version 5.6よりも前のバージョンのXenDesktopからのアップグレード（「XenDesktop 4からの移行」参照）
- XenAppからXenDesktopへ、またはXenDesktopからXenAppへのアップグレード

推奨事項：アップグレード前およびアップグレード中に、サイトの正常性を確認してください。以下の各チェックポイントで【サイトのテスト】を実行します。

- バックアップの作成前。
- 各コントローラーがアップグレードされた後。
- VDAおよびほかのコンポーネントがアップグレードされた後。
- Studioからサイトがアップグレードされた後。

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 7.1サイトとXenDesktop 7.5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。

Citrixは、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推奨します。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。後述の「VDAの混在環境のサポート」を参照してください。

- 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。

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Receiver 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Windows 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。

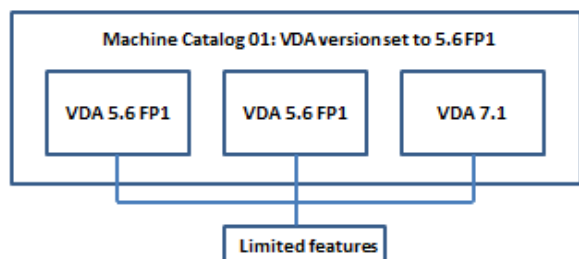
VDAの混在環境のサポート

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。たとえば、Version 7.6の製品でサポートされるセッションの事前起動、セッション残留、および認証が不要なユーザーの機能を使用するには、Version 7.6以降のVDAがインストールされている必要があります。

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、マシンカタログに複数のバージョンのVDAが混在していると、意図しない問題が生じることがあります。

上述のとおり、環境にWindows XPおよびWindows Vistaのシステムが含まれている場合は、以前のバージョンのVDAを使用する必要があります。それらのマシンを含むマシンカタログでは、VDAのバージョンとして[5.6 FP1]を指定する必要があります。これにより、VDAがControllerに登録されますが、それらのマシンでVersion 7.xの新機能（StoreFrontなど）を使用する

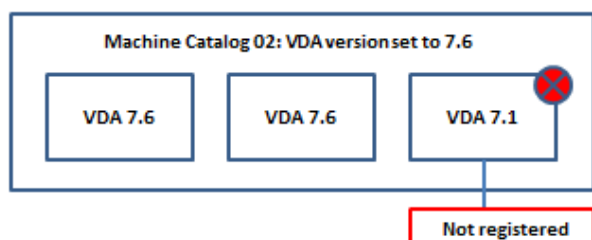
ことはできません。これは、そのカタログにVDA 7.xがインストールされたマシンを追加した場合にも当てはまります。次の図はこのことを示しています。



上の例で、以前のバージョンのVDAを引き続き使用する必要がある場合は、それらのマシンで専用のマシンカタログを作成します。

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。

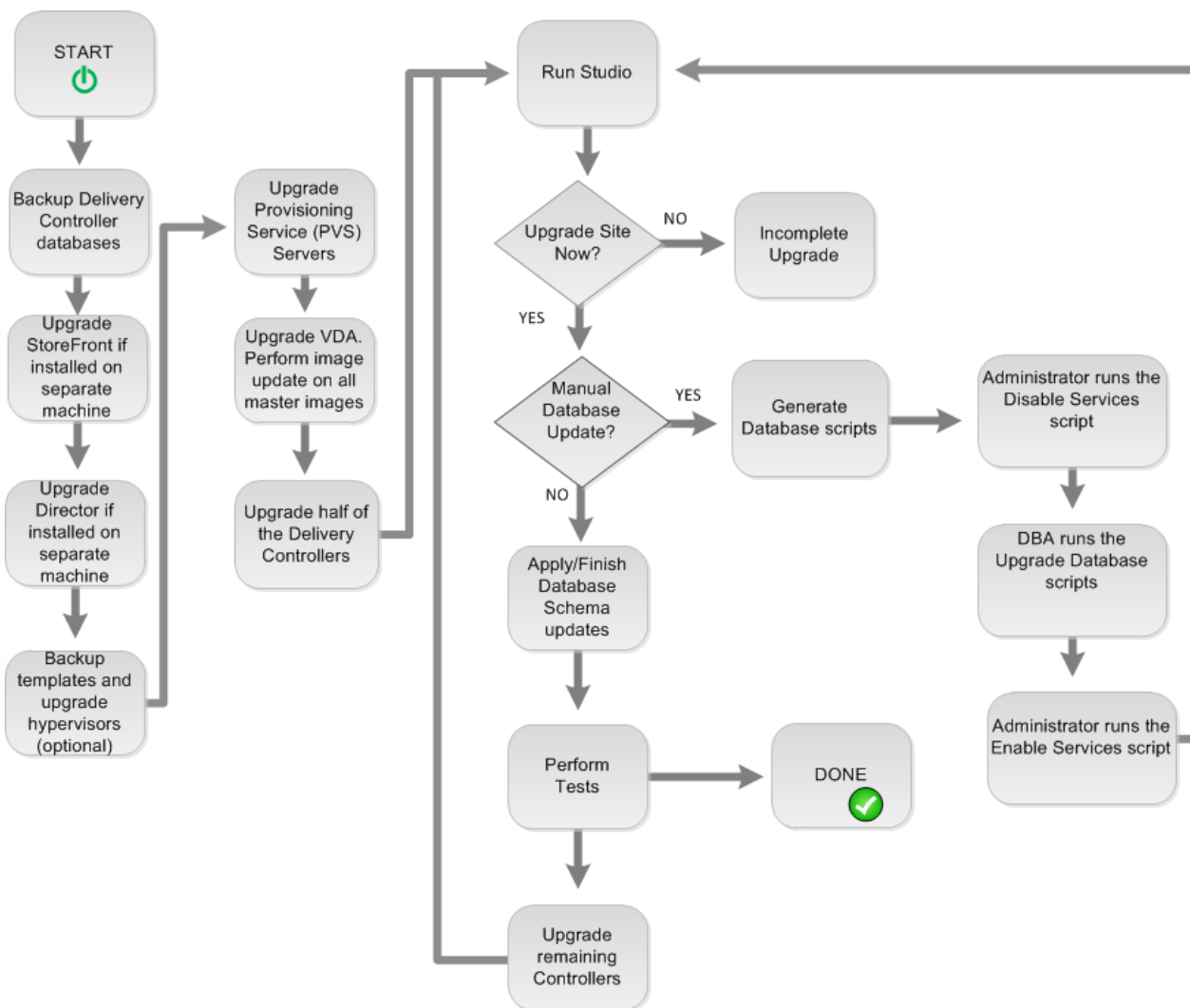
たとえば、VDAの最新バージョンが7.6である場合に、VDAのバージョンとしてデフォルトの [7.6 (推奨。最新機能を使用できます)] を指定してマシンカタログを作成し、VDA 7.6の2つのマシンとVDA 7.1の1つのマシンを追加したとします。



この場合、VDA 7.1のマシンはControllerに登録されません。そのVDAをアップグレードできない場合は、VDAのバージョンとして [7.0 (またはそれ以降)] を指定した別のマシンカタログを作成してそのマシンを追加します。これにより、Version 7.6の新機能は使用できませんが、そのマシンをControllerに登録できるようになります。

アップグレードの順序

次の図にアップグレードの順序を、その後に説明を示します。コンポーネントが複数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。



コンポーネントのアップグレード

製品インストーラーのグラフィック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。

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。 Controller以外のコアコンポーネントがほかのマシン上にインストールされている場合は、各マシンでインストーラーを実行します。この場合、ライセンスサーバー、StoreFront、Directorの順にアップグレードすることをお勧めします。
2. Provisioning Servicesのドキュメントの指示に従って、Provisioning Servicesのサーバーとクライアントをアップグレードします。
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。 VDAのアップグレードはControllerの前でも後でも可能ですが、Controllerの前にアップグレードすることをお勧めします。これにより、アップグレード後に新しい機能をすぐに有効にできます。

物理マシン（リモートPCアクセス用のマシンも含まれます）上にインストールされているVDA 7.xからアップグレードする場合、コマンドラインインターフェイスでパラメーター「/EXCLUDE "Personal vDisk","Machine Identity Service"」を使用します。次に例を示します。

C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"

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。
5. 前の手順で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。
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。
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。
8. 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。
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。
10. アップグレードの完了時に **完了** を選択すると、Citrixのカスタマーエクスペリエンス向上プログラム (CEIP) に登録するかどうかを選択できるページが表示されます。CEIPでは、使用環境に関する情報が匿名で収集されます。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。
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、Studioで以下のタスクを実行します。
 - アップグレードし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。
 - アップグレードしたVDAを使用するマスターイメージをすべて更新します。
 - マシンカタログとデリバリーグループをアップグレードします。

サイトデータベースとサイトのアップグレード

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。

- 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。SQLスクリプトを手動で実行する場合は、SQLCMDユーティリティあるいはSQLCMDモードのSQL Management Studioのいずれかを使って実行する必要があります。これ以外の場合に不正確なエラーが生じることとなります。

重要：データベースをアップグレードする前にバックアップすることを強くお勧めします。手順については、[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- この方法ではスクリプトを生成して実行します。

1. 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。
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
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SQL Server Management Studioなどのツールを使って実行するSQLスクリプト。
UpgradeMonitorDatabase.sql	監視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SQL Server Management Studioなどのツールを使って実行する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SQL Server Management Studioなどのツールを使って実行する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。

3. 表示された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し、[よく使うタスク]に戻る]を選択します。

XenApp 6.5ワーカーから新しいVDAへのアップグレード

Jul 07, 2016

XenApp 6.5ワーカーサーバー上で現在の製品インストーラーを実行すると、以下の処理が行われます。

- XenApp 6.5ファームからそのワーカーが削除される（このタスクでは自動的にXenApp 6.5インストーラーのコマンドラインインターフェイスが使用されます）。
- XenApp 6.5ソフトウェアがアンインストールされる。
- 新しいVDA for Windows Server OS（XenApp 7.6またはそれ以降のバージョン）がインストールされる。

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、新しいXenAppサイトにVDA for Windows Server OSをインストールするときと同じウィザードを使用します。同様に、コマンドラインインターフェイスでのインストールでも、ほかのVDAのインストールと同じコマンドおよびパラメーターを使用します。

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のコアコンポーネントおよびほかのVDAをインストールしたことがある場合は、そのときと同じ方法でインストーラーを操作します。XenApp 6.5ワーカーサーバーでインストーラーを起動するか（「[グラフィカルインターフェイスを使ったインストール](#)」参照）、コマンドを実行します（「[コマンドラインを使ったインストール](#)」参照）。

ヒント：

- このアップグレードは、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XenApp 6.5サーバーで有効です。
- XenApp 6.5のアンインストール時に、サーバーの再起動が何回か必要です。コマンドラインでのインストールでは、/NOREBOOTオプションを指定することで自動再起動を無効にできます。ただし、アンインストール処理を完了して次のインストール処理を行うためには、サーバーを再起動する必要があります。
- XenAppの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ログを参照してください。アンインストールログは、%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\フォルダーに生成されます。
- アップグレード後、IMA固有のシステム設定とレジストリのエントリに加えて、HDX関連のシステム設定とレジストリを見直します。すでに利用できなくなっている設定や、以前と同じには動作しなくなっている設定が存在する可能性があります。
- XenApp 6.5ワーカーをアップグレードしたら、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。
- XenApp 6.5のコントローラーサーバーからポリシーやアプリケーション設定を移行した場合（[XenApp 6.xからの移行](#)参照）は、移行した公開アプリケーションのデリバリーグループを、XenApp 6.5でこれらのアプリケーションをホストしていたマシンカタログに割り当てます。

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. コントロールパネルで以下のソフトウェアをアンインストールします。
 1. Citrix XenApp 6.5
 2. Microsoft Visual C++ 2005 Redistributable (x64), version 8.0.56336
 4. サーバーを再起動します。
 5. XenAppのインストーラーを実行してVDA for Windows Server OSをインストールします。

XenApp 6.xからの移行

Jul 07, 2016

重要：移行を開始する前に、このアーティクル全体をよくお読みください。
XenApp 6.xの移行ツール（以下移行ツール）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ができます。

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。

このリリースでの新機能

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-xenapp-7x/>) 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、ReadIMAZipとImportFMAzipという2つのパッケージが含まれています。XenApp 6.xサーバーからのエクスポートでは、ReadIMAZipのみが必要です。XenApp 7.6サーバーへのインポートでは、ImportFMAzip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。
- 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

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。

- ReadIMAZip - 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。

制限事項

- 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は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。

セキュリティに関する注意事項

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、各ポリシーのプロ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に別のユーザー、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。

ログとエラー処理

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/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。

要件、準備、およびベストプラクティス

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、移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。次に例を示します。

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。
- 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

- 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には付い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 IM 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、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、アプリケーションのファイ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。

手順：データのエクスポート

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。

- 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。ReadIMAZipおよびImportFMAZipの2つのZIPファイルが展開されます。
- 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インします。
- 共有フォルダーのReadIMAZip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ReadIMAZip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。
- 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。次に例を示します。
cd C:\XAMigration
- 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。
- 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。次に例を示します。
Set-ExecutionPolicy RemoteSigned
- 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ための場合は、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ための場合は、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。
- 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

パラメーター 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：「 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のため、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：「 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。

パラメーター -SuppressLogo	説明 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のため、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、MyFarmlogという以前のログファイルに記録されます。MyFarmXML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。

手順：データのインポート

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。次に例を示します。

```
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：「 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のため、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

パラメーター	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：「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のため、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。
-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："<xenapp-farm-name> - Delivery Group"
-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。

パラメーター -NotMatchFolder " <string>"	説明 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。

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、MyFarmlog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。

移行後のタスク

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、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。
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。
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、「[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提供します。

高度な使用方法

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、ワーカークラウド）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、ワーカークラウド、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](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、ワーカークラウド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、ワーカークラウド「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.*"
 - 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せんが、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。

トラブルシューティング

- 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

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パラメータを削除したことを確認してください。

インポートされないポリシー設定

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ーやコンポーネントに置き換えられ、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 (%)
- 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
- Prompt for password
- 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

インポートされないアプリケーションの種類

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）

アプリケーションプロパティの対応

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
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。

FMAのプロパティ	値
UUID	読み取り専用でControllerにより割り当てられます。
Visible	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。
Accounts	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。

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。

IMAのプロパティ	コメント
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。
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。

XenDesktop 4からの移行

Jul 07, 2016

移行ツールを使用して、XenDesktop 4ファームのデータや設定をXenDesktop 7.xサイトに転送できます。移行ツールは、XenDesktopインストールメディアの [Support] > [Tools] > [MigrationTool] フォルダーにあります。このツールには、以下のコンポーネントが含まれます。

- エクスポートツールXdExport。このツールにより、XenDesktop 4ファームのデータがXMLファイル（デフォルト名：XdSettings.xml）にエクスポートされます。XMLファイルスキーマはファイルXdFarm.xsd内にあります。
- インポートツールXdImport。このツールにより、データをインポートするPowerShellスクリプトImport-XdSettings.ps1が実行されます。

移行ツールを正しく使用するには、XenDesktop 4ファームとXenDesktop 7.xサイトでハイパーバイザーのバージョン（XenServer 6.2など）とActive Directory環境が同じである必要があります。

このツールでXenAppファームを移行することはできません。また、XenDesktop 4ファームをXenAppに移行することはできません。

ヒント：XenDesktop 5（またはそれ以降のバージョンのXenDesktop）は、新しいXenDesktopバージョンにアップグレードできます。詳しくは、「[展開のアップグレード](#)」を参照してください。

制限事項

すべてのデータや設定がエクスポートされるわけではありません。以下の構成項目はエクスポートされますがインポートできません。このため、これらの設定は移行できません。

- 管理者
- 委任管理設定
- デスクトップグループフォルダー
- ライセンス構成
- レジストリキー

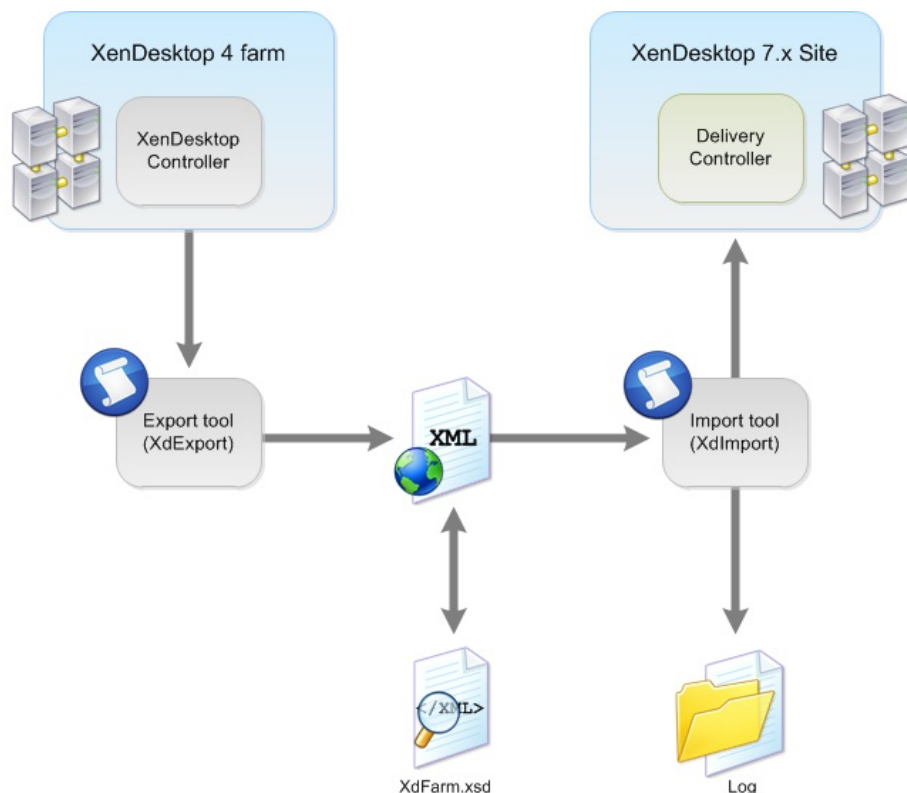
移行時に以下を行うことはできません。

- ポリシー、デスクトップグループ、およびホスト設定のマージ（統合）。
- プライベートデスクトップのランダムデリバリーグループへのマージ。
- 移行ツールによる既存のコンポーネント設定の変更。

詳しくは、「[移行される項目と移行されない項目](#)」を参照してください。

移行手順

次の図は、移行プロセスの概要です。



以下の順序で移行します。

1. XenDesktop 4 Controller上のStudioコンソールで、エクスポートするすべてのマシンをメンテナンスモードにします。
2. XdExportを使って、データおよび設定をXenDesktop 4ファームからXMLファイルへエクスポートします。 [XenDesktop 4ファームからのエクスポート](#) を参照してください。
3. エクスポートされたXMLファイルを編集して、新しいXenDesktopサイトにインポートしないデータや設定を削除して、必要な変更を行います。「[移行ツールXMLファイルの編集](#)」を参照してください。
4. XdImportを使って、XMLファイルから新しいXenDesktopサイトにデータおよび設定をインポートします。 [XenDesktop 4データのインポート](#) を参照してください。
5. 変更を追加するには、手順3.と手順4.を繰り返します。変更を追加した後で、既存のデリバリーグループに追加のデスクトップをインポートすることができます。これを行うには、インポートするときにMergedesktopsパラメーターを使用します。
6. 移行後のタスクについては、「[移行後のタスク](#)」を参照してください。

準備

移行を開始する前に以下のタスクを完了しておく必要があります。

- エクスポートおよびインポートできるデータの種類を確認し、どのように展開に適用できるのかについて把握する必要があります。「[移行される項目と移行されない項目](#)」を参照してください。
- サイトのデータベースを手動でバックアップしておくことを強く推奨します。これにより、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。
- XenDesktop 7.xコンポーネントをインストールして、データベースおよびサイトを作成します。
- XenDesktop 4から移行するには、すべてのVDAをXenDesktop 5.xバージョンにしておく必要があります。これにより、XenDesktop 4とXenDesktop 7.xの両方のControllerとの互換性が保持されます。XenDesktop 7.xへの移行が完全に完了したら、Windows 7上のVDAをXenDesktop 7.xバージョンにアップグレードできます。詳しくは、「[移行例](#)」を参照してください。

XenDesktop 4ファームからのエクスポート

Jul 07, 2016

エクスポートツールのXdExportは、単一のXenDesktop 4ファームからデータを抽出し、そのデータ値を使ってXMLファイルを作成します。

XMLファイルのスキーマは、移行ツール（XdExport.zipおよびXdImport.zip）と一緒にダウンロードされるXdFarmxsdファイルに定義されています。

移行元のXenDesktop 4ファームで動作するController上でXdExportを実行します。このマシンには、XenDesktop 4 PowerShell SDKがインストールされている必要があります。データをエクスポートするには、以下の権限が必要です。

- ファームの読み取り専用Citrix管理者以上の権限。
- レジストリの読み取り権限。

必要な場合は、ユーザーがVDAにログオンしている場合など、稼働しているXenDesktop Controller上でツールを実行することもできます（ただしお勧めしません）。

以下のことを強くお勧めします。

- ツールを実行するXenDesktop 4 Controllerに最新のパブリックHotfixを適用しておいてください。
- エクスポートの実行中は、デスクトップグループの削除など、サイトの構成を変更しないでください。

- XdExport.zipをダウンロードして、内容をXenDesktop 4のController上に抽出します。
- コマンドプロンプトでXdExport.exeを実行します。以下のパラメーターを指定できます。

パラメーター	説明
-Verbose	詳細な進捗情報を提供するメッセージを生成します。
-FilePath <path>	XMLファイルのエクスポート先のパスを指定します。デフォルト値は、.\XdSettings.xmlです。
-Overwrite	-FilePathで指定した場所にあるファイルを上書きします。このパラメーターを指定しない場合、エクスポート先に同名のファイルがあると「Error: File already exists. Specify -Overwrite to allow the file to be overwritten.」
-? または -help	各パラメーターについての説明を表示します。データはエクスポートされません。

- ツールの実行に成功すると、「Done」というメッセージが表示されます。-FilePathパラメーターで指定した場所にXdSettings.xmlファイルが出力されます。ツールの実行に失敗した場合は、エラーメッセージが表示されます。

移行ツールXMLファイルの編集

Jul 07, 2016

XenDesktop 7.xサイトへの移行を複数回に分けて実行し、一部のユーザー、デリバリーグループ、およびポリシーを他のデータよりも前にインポートする場合は、エクスポートツール (XdExport) により生成されたXMLファイルの内容を確認し、必要に応じて編集してから、データをインポートする必要があります。

ファイルの内容を表示または変更するには、任意のテキストエディターを使用します。Microsoft XML Notepadなど専用のXMLエディターを使用することもできます。

インポートツール (XdImport) でXMLファイルを正しくインポートするためには、そのファイルに特定のXML要素が存在している必要があります。

必要なXMLスキーマは、移行ツールと一緒にダウンロードされるXdFarmxsdファイルに定義されています。このファイルを編集する場合は、次の点に注意してください。

- minOccurs属性の値が1以上である場合、その要素が1つ以上記述されていなければなりません。
- インポートツールで指定するXMLファイルが無効な場合は、ツールが停止してXMLファイルの問題箇所を示すエラーメッセージが表示されます。

デスクトップまたはデリバリーグループのサブセットのインポート

特定のデリバリーグループやデスクトップのみをインポートする場合は、要素の内容を編集します。要素は複数の要素を保持でき、各要素には複数の要素を保持できる要素が1つあります。

すべての要素を削除する場合でも、要素は削除しないでください。同様に、すべての要素を削除する場合でも、各要素内の要素を削除しないでください。

特定のマシンやデリバリーグループを移行しない場合は、その要素または要素全体を削除します。たとえば、次のような内容のXMLファイルがあるとして。

```
... ..
```

このファイルを以下のように編集すると、デリバリーグループGroup1がインポートされなくなり、Group2のMACHINE3のみがインポートされます。

```
... ..
```

同じ名前のデリバリーグループの管理

XenDesktop 4のデスクトップグループでは、同じ名前のデスクトップグループを異なるフォルダーで管理できました。また、ユーザーにはこのデスクトップグループ名が表示されました。このリリースのXenDesktopでは、デリバリーグループをフォルダーで管理できないため、一意のデリバリーグループ名が必要です。また、ユーザーには、このデリバリーグループID (内部デリバリーグループ名) とは別のものが表示されます。この仕様の違いに対処するため、移行時にデスクトップグループ名の変更が必要になる場合があります。

たとえば、XenDesktop 4ファームでは、2人の異なるユーザーに対して同じ「My Desktop」という名前の2つの異なるデスクトップグループを作成して、これらを個別のフォルダーで管理できました。これらのデリバリーグループをXenDesktop 7.xサイトに移行する場合、XMLファイルでデスクトップグループ名を変更して一意の名前を付ける必要があります。

また、移行先のXenDesktop 7.xサイトに、移行するデスクトップグループと同じ名前のデリバリーグループがある場合も、XenDesktop 4のデスクトップグループ名をXMLファイルで変更しておく必要があります。ただし、移行するデスクトップグループがXenDesktop 7.xのデリバリーグループと同一で、XMLファイルに出力されたすべてのマシンを既存のデリバリーグループに統合する場合は、デスクトップグループ名を変更する必要はありません。その代わりに、インポートツールにMergeDesktopsパラメーターを指定します。たとえば、次のような内容のXMLファイルがあるとして。

... \Sales ... \Finance

次のように、重複した名前を変更します。

... \Sales ... \Finance

ポリシーのインポートの管理

XMLファイルから特定のポリシーを削除したり、ポリシー名の重複を避けるために一意の名前を指定したりできます。ポリシーをマージすることはできません。

- XMLファイルのポリシーデータはすべてインポートされます。ただし、何らかの問題がある場合にはいずれのポリシーもインポートされません。
- 多くの設定を含んでいる多数のポリシーのインポートには数時間かかることがあります。
- 複数のポリシーを複数回に分けてインポートすると、元の優先度設定が変更されることがあります。インポートするポリシーの相対的な優先度は維持されますが、インポート先サイトの既存のポリシーよりも高い優先度が設定されます。たとえば、優先度1、2、3、および4の4つのポリシーを2回に分けてインポートする場合、優先度3および4のポリシーを先にインポートする必要があります。これは、後からインポートするポリシーの優先度が自動的に高くなるためです。

XenDesktop 7.xサイト内にポリシーのサブセットのみをインポートするには、要素の内容を編集します。要素には、多くの要素が含まれている場合があります。すべての要素を削除する場合でも、要素は削除しないでください。XenDesktop 4ファームの特定のポリシーを移行しない場合は、その要素全体を削除します。たとえば、次のような内容のXMLファイルがあるとします。

... ..

XenDesktop 7.xサイトの既存のポリシーとの競合を避けるために、XenDesktop 4のすべてのポリシーを移行対象から除外する場合は、次のようにすべての要素を削除します。

または、ファイルを編集して次のようにポリシーが別の名前でもインポートされるようにします。

... ..

XenDesktop 4データのインポート

Jul 07, 2016
インポートツール (Xdlimport) は、エクスポートツールのXdExportによって生成されたXMLファイルに含まれているXenDesktop 4の設定を読み取って、既存のXenDesktop 7.xサイトにそれらの設定を適用します。このインポートツールでは、PowerShellスクリプトImport-XdSettings.ps1を使用します。

エクスポートされたデータの一部のみを適用するには、インポートツールを実行する前にXMLファイルを編集します。たとえば、XenDesktop 7.xサイトに移行する必要がないデスクトップグループやポリシーをXMLファイルから削除しておきます。エレメント全体を空のままにしてインポートツールを実行すると、そのエレメントのすべての項目（デスクトップグループなど）を削除できます。XMLファイルをインポートするときに、そのファイルの内容がツールにより検証されます。

すべてのXenDesktop 7.x SDKがインストールされている任意のマシン上でXdlimportを実行します。このツールを実行するには、XenDesktopに対して完全な権限を持つ管理者アカウントが必要です。

インポートする前に、データベースを含め、XenDesktop 7.xサイトを正しくセットアップしておく必要があります。ユーザーのテストや全般的なサイト構成を行う前に、XenDesktop 7.xへのインポートを完了しておくことを推奨します。既存の構成にインポート内容を統合する場合は、サイトの非使用時にインポートを実行してください。

- 1. XenDesktop 7.xサイトを作成します。
- 2. Xdlimport.zipをダウンロードして、このツールを実行するマシン上にファイルを抽出します。
- 3. PowerShellセッションでImport-XdSettings.ps1を実行します。以下のパラメーターを指定します。

パラメーター	説明
- HypervisorConnectionCredentials	(必須) ハイパーバイザーコネクションの作成に必要なハイパーバイザーアドレスをPSCredentialインスタンスにマップするPowerShellハッシュテーブルで、さらに、XenDesktop 4ファームの接続先ハイパーバイザーの資格情報を入力します。 単一のハイパーバイザーの場合は、次のような引数を作成します。 \$credential = Get-Credential \$mappings = @"["http://" = \$credential] .\Import-XdSettings.ps1 -FilePath .\XdSettings.xml -HypervisorConnectionCredentials \$mapping ハッシュテーブルで指定されるアドレスは、XMLファイルに出力されたアドレスと正確に一致する必要があります。 たとえば、XenServerおよびVMwareハイパーバイザーでは、次の引数を作成します。 \$Xencredential = Get-Credential \$VMWcredential = Get-Credential \$mappings = @"["http://" = \$Xencredential;"http://SDK" = \$VMWcredential] .\Import-XdSetting
-FilePath <path>	(の値は必須) ファームデータをインポートするXMLファイルの場所です。
-AdminAddress	XenDesktop 7.xサイトのControllerの名前です。デフォルト値: localhost
-MergeDesktops	XMLファイルに出力されたデスクトップグループを、XenDesktop 7.xサイトの同名のデリバリーグループに統合 (つまりデスクトップを追加) します。割り当てられたこのパラメーターを指定しない場合、XenDesktop 7.xサイトの既存のデリバリーグループにはデスクトップが追加されません。
-SkipMachinePolicy	サイトレベルの設定を保持するマシンポリシーの作成を省略します。このパラメーターを指定せず、サイトのマシンポリシーが存在する場合、スクリプトが
-WhatIf	インポート処理によりXenDesktop 7.xサイトに加えられる変更や追加を事前に確認することができます。このパラメーターを指定すると、ログファイルに3
-LogFilePath <path>	ログファイルのフルパスを指定します。ログファイルには、インポート処理によりXenDesktop 7.xサイトに加えられたすべての変更内容が出力されます。
-? または-help	各パラメーターについての説明を表示します。データはインポートされません。

XMLファイルのポリシーデータはすべてインポートされます。ただし、何らかの問題がある場合にはいずれのポリシーもインポートされません。多くの設定を含んでいる多数のポリシーのインポートには数時間かかることがあります。

スクリプトの実行が完了すると、「Done」というメッセージが表示されます。XMLファイルからのデータのインポートに成功したら、追加のエクスポートやインポートを行ったり、すべてのデータをインポートした後の「移行後のタスク」を実行したりできます。

移行後のタスク

Jul 07, 2016

XenDesktop 4ファームからXenDesktop 7.xサイトへのデータのインポートが完了したら、新しいXenDesktop 7.xサイトを実稼働環境で使用する前に以下のタスクを実行する必要があります。

- Virtual Delivery Agent (VDA) をアップグレードします。Controller、Studio、またはDirectorをアップグレードする前にVDAをアップグレードしておくことをお勧めします。
 - Windows VistaおよびWindows XPの場合、XenDesktop 5.6 Feature Pack 1のVirtual Desktop Agentにアップグレードします。
 - Windows 7の場合、XenDesktop 7.xのVirtual Delivery Agentにアップグレードします。
- 必要に応じて、XenDesktop 7.xサイトに必要な管理者を作成します。
- ユーザーデバイスをアップデートします。ユーザーデバイス上のCitrix Receiverを最新のバージョンにアップデートすることをお勧めします。これにより、Hotfixによる修正が適用され、新しい機能がサポートされます。
- インポートしたデスクトップでレジストリベースのController検出が使用されるように変更して、次のいずれかの方法でXenDesktop 7.xのControllerを指定します。
 - レジストリを手動で編集して不要な組織単位 (OU) のGUIDレジストリエントリを削除し、ListOfDDCsレジストリエントリを追加します。
 - Active Directoryポリシー (GPMC.msc) で、Controllerの一覧をデスクトップに配信するためのマシンポリシーを設定します。Studioでこの設定を構成することはできません。

XenDesktop 7.xのデフォルトではレジストリベースのController検出が使用されますが、Active Directoryベースの検出も使用できます。

- オプションとして、XenDesktopのレジストリベースの登録に関するベストプラクティス ([CTX133384](#)) を参照して、以下のレジストリキーを設定します。
 - HeartbeatPeriodMS
 - PrepareSessionConnectionTimeoutSec
 - MaxWorkers
 - DisableActiveSessionReconnect
 - ControllersGroupGuid

XenDesktop 7.xへの移行後にこれらのレジストリキーを設定しない場合、XenDesktop 7.xのデフォルトの設定が適用されます。

- XenDesktop 4でのXMLファイルの生成時にメンテナンスモードのマシンがあった場合は、メンテナンスモードを解除します。
- XenDesktop 7.xの設定をチェックします。特に、XenDesktop 4でPortICAConfig XMLファイルを変更していた場合は、移行後の設定内容について確認します。
- 移行したすべてのコンポーネントについて、移行が正しく行われたことを確認します。

移行例

Jul 07, 2016

例1：単一の大規模XenDesktop 4ファームをXenDesktop 7サイトに移行する

ここでは、使用中の単一XenDesktop 4ファームで説明します。このXenDesktop 4ファームには50のデスクトップグループが構成されており、各グループに平均100のデスクトップが追加されています。XenDesktop 4デスクトップはProvisioning Services (PVS) でプロビジョニングされ、仮想マシンはVMware ESXハイパーバイザー上で動作しています。すべての仮想マシンにXenDesktop 4のVDAがインストールされています。

移行手順

1. すべてのXenDesktop 4 VDAをXenDesktop 5.6 Feature Pack 1バージョンのVDAにアップグレードします。これにより、VDAをXenDesktop 4のControllerとXenDesktop 7のDelivery Controllerの両方に登録できます。
2. XenDesktop 4ファームにログオンしているユーザーがいいることを確認します。
3. すべてのマシンがメンテナンスモードであることを確認します。
4. XenDesktop 4ファームでエクスポートツール (XdExport) を実行します。
5. XenDesktop 7の各コンポーネントをインストールします。
 1. Studioを使用して完全な実稼働環境サイトを作成します。
 2. Provisioning Servicesを使用している場合は、Provisioning Servicesサーバーおよびエージェントをアップグレードします。
 3. ライセンスサーバーおよび関連ライセンスをアップグレードします。
6. インポートツール (XdImport) の圧縮を解除して、XenDesktop 7 Controllerのローカルディレクトリ上に抽出します。
7. 手順4.で生成したエクスポートツールのXMLファイル (XdSettings.xml) を上記のローカルディレクトリにコピーします。
8. StudioでXenDesktop 7サイトのルートノードのPowerShellコンソールを開き、PowerShellセッションを起動します。
9. ハイパーバイザーの資格情報およびコピーしたXMLファイルのパスを指定してインポートツール (XdImport) を実行します。
10. Studioの「管理者」ノードで管理者設定を再作成します。詳しくは、「[委任管理](#)」を参照してください。
11. インポートされたデスクトップでレジストリベースのController検出が使用されるようにして、新しいXenDesktop 7のControllerを指定します。
12. Windows 7上のVDAについては、それらのVDAをXenDesktop 7 VDA for Windows Desktop OSにアップグレードすることをお勧めします。これにより、XenDesktop 7のすべての機能を使用できるようになります。
カタログまたはデリバリーグループのマシンのVDAソフトウェアをXenDesktop 7にアップグレードしたら、カタログとデリバリーグループをアップグレードします。
13. デリバリーグループのメンテナンスモードを解除します。
14. Web Interfaceで提供していたデスクトップがStoreFrontで提供されるように構成します。詳しくは、StoreFrontのドキュメントを参照してください。

例2：XenDesktop 4ファームの一部をXenDesktop 7.1サイトに移行する

この例では、デスクトップをいくつかのグループに分けて段階的に移行します。ここでは、使用中の単一XenDesktop 4ファームと、作成済みで使用中の単一XenDesktop 7.1サイトで説明します。このXenDesktop 4ファームには50のデスクトップグループが構成されており、各グループに平均100のデスクトップが追加されています。XenDesktop 4デスクトップはProvisioning Servicesでプロビジョニングされ、仮想マシンはCitrix XenServerハイパーバイザー上で動作しています。すべての仮想マシンにXenDesktop 4のVDAがインストールされています。

移行手順

1. XenDesktop 4ファームでエクスポートツールを実行します。
 1. XenDesktop 4ファームの任意のController上でエクスポートツール (XdExport) の圧縮を解除します。
 2. Citrix管理者アカウントで、パラメーターを指定せずにエクスポートツールを実行します。
2. 生成されたXMLファイルを開き、移行対象のグループおよびデスクトップ以外のエントリを削除します。
3. XenDesktop 4ファームで、移行対象のデスクトップにログオンしているユーザーがいないことと、それらのデスクトップがメンテナンスモードであることを確認します。
4. インポートツール (XdImport) の圧縮を解除して、XenDesktop 7.1 Delivery Controllerのローカルディレクトリ上に抽出します。
5. 編集したXMLを上記のローカルディレクトリにコピーします。
6. StudioでXenDesktop 7.1サイトのルートノードのPowerShellコンソールを開き、PowerShellセッションを起動します。
7. ハイパーバイザーの資格情報およびコピーしたXMLファイルのパスを指定してインポートツール (XdImport) を実行します。
8. Studioの「管理者」ノードで管理者設定を手動で再作成します。詳しくは、「委任管理」を参照してください。
9. インポートされたデスクトップでレジストリベースのController検出が使用されるようにして、新しいXenDesktop 7.1のControllerを指定します。
10. すべてのVDAを適切なバージョンにアップグレードします。
11. カタログまたはデリバリーグループのマシンのVDAソフトウェアをXenDesktop 7にアップグレードしたら、カタログとデリバリーグループをアップグレードします。
12. デリバリーグループのメンテナンスモードを解除します。
13. Web Interfaceで提供していたデスクトップがStoreFrontで提供されるように構成します。詳しくは、StoreFrontのドキュメントを参照してください。

移行される項目と移行されない項目

Jul 07, 2016

移行される項目

次の表は、このリリースへの移行時に各種データがどのように移行されるかについて説明しています。特に明記されていない限り、以下の種類のデータがインポートされます。

データの種類	注
デスクトップグループ	「デスクトップグループ」は、このリリースでは「デリバリーグループ」と呼ばれます。デスクトップグループのアイコンはエクスポートされません。 XenDesktop 4のDefaultEncryptionLevelがBasicでない場合、SecureIcaRequiredはTrueに設定されます。 XenDesktop 4ファームのデスクトップグループと同じ名前のデリバリーグループが移行先のXenDesktop 7.xサイトにある場合、XenDesktop 4ファームのデスクトップグループのデスクトップをXenDesktop 7.xサイトのデリバリーグループに追加できます。 これを行うには、インポートツールの実行時にMergeDesktopsパラメーターを指定します。XenDesktop 7.xのデリバリーグループの設定が、XenDesktop 4のデスクトップグループの設定で上書きされることはありません。このパラメーターを指定せず、XMLファイルで定義されているものと同じ名前のグループがある場合は、エラーメッセージが表示され、データはインポートされません。
デスクトップ	プライベートデスクトップをランダムデリバリーグループに追加することはできません。ランダムデスクトップを静的デリバリーグループに追加することはできません。
マシン	マシンは4つのマシンカタログにインポートされます。インポートツールにより、XenDesktop 7.xサイトに以下のマシンカタログが作成されます。 ● インポートされた既存のランダム（プールされた仮想マシン用） ● インポートされた既存の静的（割り当てられた仮想マシン用） ● インポートされた物理的ランダム（プールされたPCまたはブレード用） ● インポートされた物理的静的（プライベートPCまたはブレード用） これ以降に実行されるいずれのマシンのインポートにも、同じ4つのマシンカタログが使用されます。
プール管理 プール	複数プールのプール、およびスケジュールを含むアイドルプール設定が含まれます。 ● PeakBufferSizePercentは、デフォルトで10%に設定されます。 ● OffPeakBufferSizePercentは、デフォルトで10%に設定されます。 ● XenDesktop 4のBusiness days設定で未選択の日は、週末電源時間スキームの一部としてインポートされます。 ● HostingXD4操作時間は、直近の分に切り上げられます。 ● Start時間は、直近の時間に切り下げられます。 ● End時間は、直近の時間に切り上げられます。
ファーム	以下のファーム設定は、マシンポリシーとしてインポートされます。

設定の種類	● IcaKeepAlive ● AutoClientReconnect ● SessionReliability
	Flash Playerを有効にする設定はインポートされません。
Policies	一部のポリシーデータがインポートされます。フィルター、設定、およびプリンターは、ユーザーポリシーとしてインポートされます。ユーザーポリシーのエクスポートおよびインポートについては、このドキュメントのほかの表を参照してください。 ● XenDesktop 4のデスクトップグループの設定から、新しいアクセスポリシー規則が作成されます。 ● インポートされるポリシーの相対的な優先度は保持されます。ただし、XenDesktop 7.xサイトの既存のポリシーよりも高い優先度が設定されます。 ● 移行元のポリシーを移行先のポリシーに統合することはできません。 ポリシーをActive Directoryにインポートすることはできません。ポリシーは常にサイトに格納されます。
ユーザー割り当て	
ハイパーバイザー設定	XdlImportツールの必須パラメーターです。 ハイパーバイザーアドレスはエクスポートされますが、ハイパーバイザーにアクセスするための資格情報はエクスポートされません。XenDesktop 7.xサイトにハイパーバイザー接続を作成するには、XMLファイルからアドレスを抽出し、対応する資格情報インスタンスにマップするPowerShellハッシュテーブルを作成します。次に、インポートツールのHypervisorConnectionCredentialsパラメーターでこのハッシュテーブルを指定します。詳しくは、「XenDesktop 4データのインポート」を参照してください。 既存のデスクトップグループやハイパーバイザー接続のハイパーバイザー設定をマージしたり更新したりすることはできません。
管理者	(インポートされません)。委任管理者に関するものも含め、管理者データはインポートされません。XenDesktop 7.xサイトで新しい管理者を作成してください。
ライセンス構成	(インポートされません)。ライセンスサーバー名やエディションなどの情報も含め、ライセンス構成はインポートされません。ライセンスファイルはエクスポートされません。
デスクトップグループフォルダー	(インポートされません)。このリリースは、デスクトップグループフォルダーをサポートしません。デスクトップグループ名が重複する場合 (XenDesktop 4ファームの異なるフォルダーに同名のグループがある場合など)、XMLファイルを編集してからインポートしないと処理が停止します。
レジス	(インポートされません)。レジストリキーの実装については、 移行後のタスク を参照してください。

ポリシー の種類	注

ユーザーポリシーデータ

次の表は、ユーザーポリシーデータがどのようにエクスポートおよびインポートされるかについて説明しています。

XenDesktop 4でのカテゴリと設定	XMLファイル	XenDesktop 7.xでのカテゴリと設定
帯域幅\視覚効果\セッションの制限 OEM仮想チャネル	ClientOEMVCBandwidth	インポートされません
クライアント\デバイスマッピング\その他 OEM仮想チャネルを無効にする	DisableOEMVirtualChannels	インポートされません
ユーザーのワークスペース\タイムゾーン サーバーのタイムゾーンを使用する	DoNotUseClientLocalTime	インポートされません
セキュリティ\暗号化レベル SecureICA暗号化	ClientSecurityRequirement	インポートされません
帯域幅\SpeedScreen イメージアクセラレーション	LossyCompressionの設定による	ICA\視覚表示\静止画 非可逆圧縮のレベル 非可逆圧縮のしきい値 ヘビーウェイト圧縮 ICA\視覚表示\動画 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
帯域幅\視覚効果 デスクトップの壁紙を無効にする	TurnOffWallpaper	ICA\デスクトップUI デスクトップの壁紙
帯域幅\視覚効果	TurnOffMenuWindowAnimation	ICA\デスクトップUI

XenDesktop 4でのカテゴリと設定 帯域幅\視覚効果 ドラッグ中にウィンドウの内容を表示する機能を無効にする	XMLファイル DoNotShowWindowContentsWhileDragging	XenDesktop 7.xでのカテゴリと設定 ICA\デスクトップUI ドラッグ中にウィンドウの内容を表示する
帯域幅\視覚効果\セッションの制限 オーディオ	ClientAudioBandwidth__AllowedBandWidth	ICA\帯域幅 オーディオリダイレクトの最大帯域幅 (Kbps)
帯域幅\視覚効果\セッションの制限 Clipboard	ClientClipboardBandwidth__AllowedBandWidth	ICA\帯域幅 クリップボードリダイレクトの最大帯域幅 (Kbps)
帯域幅\視覚効果\セッションの制限 COMポート	ClientComBandwidth__AllowedBandWidth	ICA\帯域幅 COMポートリダイレクトの最大帯域幅 (Kbps) XenDesktop 7.0～7.8 へのインポートなし
帯域幅\視覚効果\セッションの制限 ドライブ	ClientDriveBandwidth__AllowedBandWidth	ICA\帯域幅 ファイルリダイレクトの最大帯域幅 (Kbps)
帯域幅\視覚効果\セッションの制限 LPTポート	ClientLptBandwidth__AllowedBandWidth	ICA\帯域幅 LPTポートリダイレクトの最大帯域幅 (Kbps) XenDesktop 7.0～7.8 へのインポートなし
帯域幅\視覚効果\セッションの制限 セッション全体	OverallBandwidth__AllowedBandWidth	ICA\帯域幅 セッション全体の最大帯域幅

帯域幅、視覚効果、セッションの制限 XenDesktop 4でのカテゴリと設定 プリンター	LimitPrinterBandWidth__AllowedBandWidth XMLファイル	ICA\帯域幅 XenDesktop 7.xでの カテゴリと設定 ファイルリダイレク トの最大帯域幅 (Kbps)
クライアント\デバイスマッピング\オー ディオ マイク	ClientAudioMicrophone__TurnOn	ICA\オーディオ クライアントマイク リダイレクト
クライアント\デバイスマッピング\オー ディオ 音質	ClientAudioQuality__Quality	ICA\オーディオ 音質
クライアント\デバイスマッピング\オー ディオ スピーカーを無効にする	DisableClientAudioMapping	ICA\オーディオ クライアントオーデ イオリダイレクト
クライアント\デバイスマッピング\ドライ ブ Connection	ConnectClientDriveAtLogon__TurnOn	ICA\ファイルリダイレ クト ドライブへの自動接続
クライアント\デバイスマッピング\ドライ ブ フロッピーディスクドライブ	DisableClientDriveMapping__DisableFloppyDrive	ICA\ファイルリダイレ クト クライアント側フロッ ピードライブ
クライアント\デバイスマッピング\ドライ ブ ハードディスクドライブ	DisableClientDriveMapping__DisableHardDrive	ICA\ファイルリダイレ クト クライアント側固定ド ライブ
クライアント\デバイスマッピング\ドライ ブ CD-ROMドライブ	DisableClientDriveMapping__DisableCdrom	ICA\ファイルリダイレ クト クライアント側光学式 ドライブ
クライアント\デバイスマッピング\ドライ ブ	DisableClientDriveMapping__DisableRemote	ICA\ファイルリダイレ クト

リモートドライブ XenDesktop 4でのカテゴリと設定	XMLファイル	クライアント側ネットワーク XenDesktop 7.xでの カテゴリと設定
クライアント\デバイスマッピング\ドライブ USBディスクドライブ	DisableClientDriveMapping__DisableUSB	ICA\ファイルリダイレクト クライアント側リムーバブルドライブ
クライアント\デバイスマッピング\ドライブ最適化 非同期書き込み	CDMAsyncWrites	ICA\ファイルリダイレクト 非同期書き込みを使用する
クライアント\デバイスマッピング\その他 クリップボードマッピングを無効にする	DisableClientClipboardMapping	ICA 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\デバイスマッピング\ポート COMポートを無効にする	DisableClientCOMPortMapping	ICA\Port Redirection クライアントCOMポートリダイレクト XenDesktop 7.0 ~ 7.8 へのインポートなし
クライアント\デバイスマッピング\ポート LPTポートを無効にする	DisableClientLPTPortMapping	ICA\Port Redirection クライアントLPTポートリダイレクト XenDesktop 7.0 ~ 7.8 へのインポートなし
クライアント\デバイスマッピング\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USBデバイス クライアントUSBデバイスリダイレクト
印刷\クライアントプリンター 自動作成	ConnectClientPrinterAtLogon__Flag	ICA\印刷\クライアントプリンター クライアントプリンターを自動作成する

印刷\クライアントプリンター XenDesktop 4でのカテゴリと設定 従来のクライアントプリンター	LegacyClientPrinters__TurnOn XMLファイル	ICA\印刷\クライアントプリンター XenDesktop 7.xでのカテゴリと設定
		クライアントプリンター名
印刷\クライアントプリンター プリンタープロパティの保存	ModifiedPrinterProperties__WriteMethod	ICA\印刷\クライアントプリンター プリンタープロパティの保存
印刷\クライアントプリンター 印刷ジョブの送信	ClientPrintingForNetworkPrinter__TurnOn	ICA\印刷\クライアントプリンター プリントサーバーへの直接接続
印刷\クライアントプリンター クライアントプリンターのマッピングを無効にする	DisableClientPrinterMapping	ICA\印刷 クライアントプリンターリダイレクト
印刷\ドライバー ネイティブプリンタードライバーの自動インストール	PrintDriverAutoInstall__TurnOn	ICA\印刷\ドライバー 付属のプリンタードライバーの自動インストール
印刷\ドライバー ユニバーサルドライバー	ClientPrintDriverToUse	ICA\印刷\ドライバー ユニバーサル印刷の使用
印刷\セッションプリンター セッションプリンター	NetworkPrinters	ICA\印刷 セッションプリンター
印刷\セッションプリンター クライアントのデフォルトプリンターの選択	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\印刷 デフォルトプリンター

移行されない項目

XenDesktop 4の一部のコンポーネントは、このリリースでサポートされません。以下の項目は、移行されません。

- **Virtual Delivery Agent** — XenDesktop 4の仮想デスクトップをXenDesktop 7.x Delivery Controllerで管理できるようにするには、VDAをXenDesktop 5.x以降のVDAにアップグレードする必要があります。
- **Controller** — 新しいControllerサーバーを展開する必要があります。XenDesktop 4のControllerをXenDesktop 7.xサイトにアップグレードすることはできません。XenDesktop 7.xサイトをXenDesktop 4ファームに追加したりXenDesktop 4 ControllerをXenDesktop 7.xサイトに追加したりすることはできません。また、バージョンによってサーバー要件が異なります。XenDesktop 4にはWindows Server 2003が必要であり、XenDesktop 7.xにはより新しいバージョンのWindows Serverが必要です。
- **Web Interface** — XenDesktop 7.xではStoreFrontを使用することをお勧めします。インストールとセットアップについて詳しくは、StoreFrontのドキュメントを参照してください。XenDesktopのインストール時にWeb Interfaceが検出されるとStoreFrontがインストールされますが、Web Interfaceは削除されません。
- **Active Directory組織単位 (OU) 構成** — 1つの組織単位 (OU) をファーム間またはサイト間、またはファームとサイト間で共有することはサポートされていません。新しいサイトを作成して、デフォルトのレジストリベースのController検出の代わりにActive DirectoryベースのController検出を使用する場合は、そのための新しいOUを作成する必要があります。
- **PortICAConfig XMLファイル** — このファイルに対するデフォルトの設定を変更している場合は、新しいサイトでグループポリシーオブジェクトを使用してこれらの設定を構成する必要がある場合があります。
- **XenDesktop 4 Service Pack 1**で提供される構成ログ設定。
- **Provisioning Services**関連のデータ。
- アプリケーション。
- **Controller**の一覧。
- **NetScaler Gateway**。
- イベントログの調整設定。

セキュア

Jul 07, 2016

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用い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、社外作業員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。

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。

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

Aug 26, 2016

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マシン向けの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プ境界を含む）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を含むエンクレープ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ミ

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。

ユーザーアカウントの管理

Virtual Delivery Agent (VDA) インストール時に、App-V公開コンポーネントをインストールするオプションが選択された場合、あるいはこの機能を後で追加する場合は、ローカル管理アカウントCtxAppVCOMAdminがVDAに追加されます。App-V公開機能を使用する場合は、このアカウントに変更を加えないようにします。App-V公開機能を使用する必要がない場合は、インストール時にこのアカウントを選択しないでください。後でApp-V公開機能が不要になった場合には、機能を無効にしたり削除したり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、「デリバリーグループの管理」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ができません。
- 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。

ログオン権限の管理

ユーザーには、必要なログオン権限だけを付与します。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。ネットワーク上でログオン。バッチジョブとしてログオン。サービスとしてログオン。

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他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を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)。

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。現在、これらのサービスは使用されないため、無効にされています。これらのサービスは有効にしないでください。

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)

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ファイルシステム上で8.3ファイル名およびフォルダーの作成を可能にする必要はなくなりました。8.3のファイル名およびフォルダーの作成を不可能にするには、レジストリキー**NtfsDisable8dot3NameCreation**を構成します。**fsutil.exe behavior set disable8dot3**コマンドを使用して構成することもできます。

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追加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に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他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避けられないものです。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小化させます。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

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入力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。

管理権限の委任

Jul 07, 2016

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。

- **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
domain/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）
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者 ヘルプデスク管理者	すべて 営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫

管理者	役割	スコープ
domain/peter	デリバリーグループ管理者	Win7
	マシンカタログ管理者	

- 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」にしようとしたましたが、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。

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

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、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 (') は使用できません。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

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。これらのオブジェクトに対する管理者は、マシンカタログまたはデリバリーグループで割り当てることができず。

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、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 (') は使用できません。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る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（営業部で使用す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
-Path <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。

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"
```

スマートカード

Aug 26, 2016

スマートカードおよび同等の技術は、ここで説明しているガイドラインの範囲内でサポートされます。XenAppまたはXenDesktopでスマートカードを使用するには：

- 組織の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把握します。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。
- スマートカードとともに、どのようなユーザーデバイス、オペレーティングシステム、公開アプリケーションが使用されるかを決定します。
- スマートカードテクノロジー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。
- 分散環境でデジタル証明書を展開する方法を理解します。

スマートカードのタイプ

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ログイ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でなく、共有シークレットが含まれます。これらのスマートカードは支払い（たとえばChip-and-Signature式またはChip-and-PIN式のクレジットカード）をサポートできます。Windowsログインや通常のWindowsアプリケーションはサポートしません。これらのスマートカードを使用するには、専用のWindowsアプリケーションや適切なソフトウェアインフラストラクチャ（たとえば、支払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でのこれらの専用アプリケーションのサポートについては、Citrixの担当者に連絡してください。

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 Trusted Platform Module (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ートされており、Microsoft WHQL (Windows Hardware Quality Lab) により承認されている必要があります。ハード

ウェアPC/SCコンプライアンスについて詳しくは、Microsoft社のドキュメントを参照してください。他のタイプのユーザーデバイスがPS/SC標準に準拠することもあります。詳しくは、<http://www.citrix.com/ready/>のCitrix Readyプログラムを参照してください。

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は、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。デバイスドライバーは、多くの場合スマートカードミドルウェアパッケージに含まれており、Citrixパートナーから入手できます。スマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、暗号化サービスプロバイダー (CSP)、Key Storage Provider (KSP)、またはミニドライバーと呼ばれる場合もあります。

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)

他のタイプ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。

他のタイプ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
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型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。ZKA (Zentraler Kredit Ausschussor または Central Credit Committee) 標準は、接触型カードリーダーの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。

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。

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。

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ず。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 for 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
 - 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： VDAs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。

スマートカード展開

Jul 07, 2016

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。その他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モード認証を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。

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。

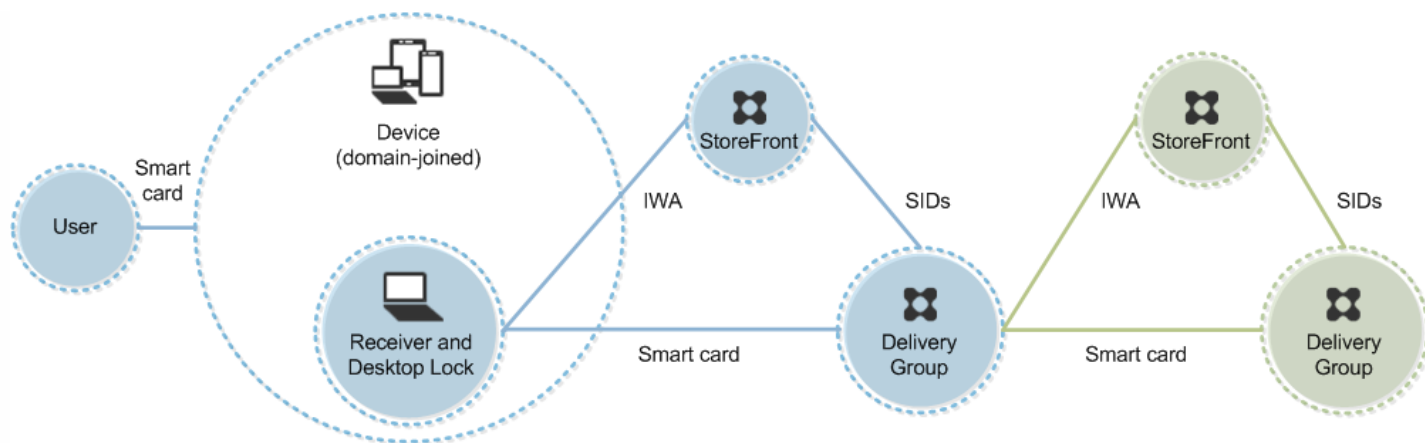
ポリシー設定	デスクトップの動作
何もしない	何もしません。
ワークステーションをロック	デスクトップセッションは切断され、仮想デスクトップはロックされます。
ログオフを強制する	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効な場合、セッションはログオフされてユーザーのデータは消失します。
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

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。

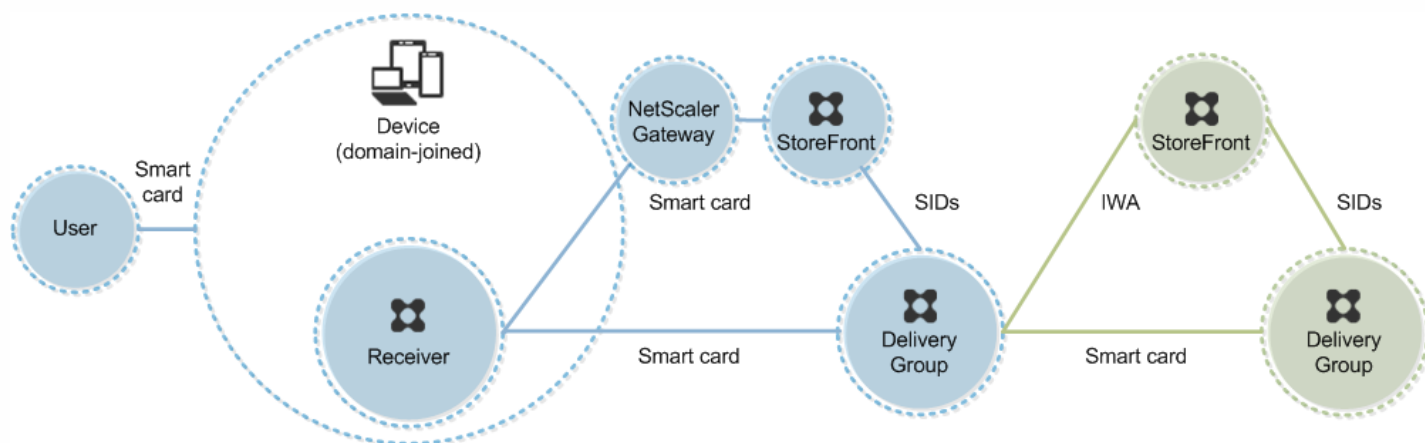


ユーザーは、スマートカードとPINを使ってデバイスにログオンします。Receiverは、StoreFrontサーバーにアクセスするユーザーを統合Windows認証（IWA）で認証します。StoreFrontにより、ユーザーのセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。Receiverでシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要はありません。

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。

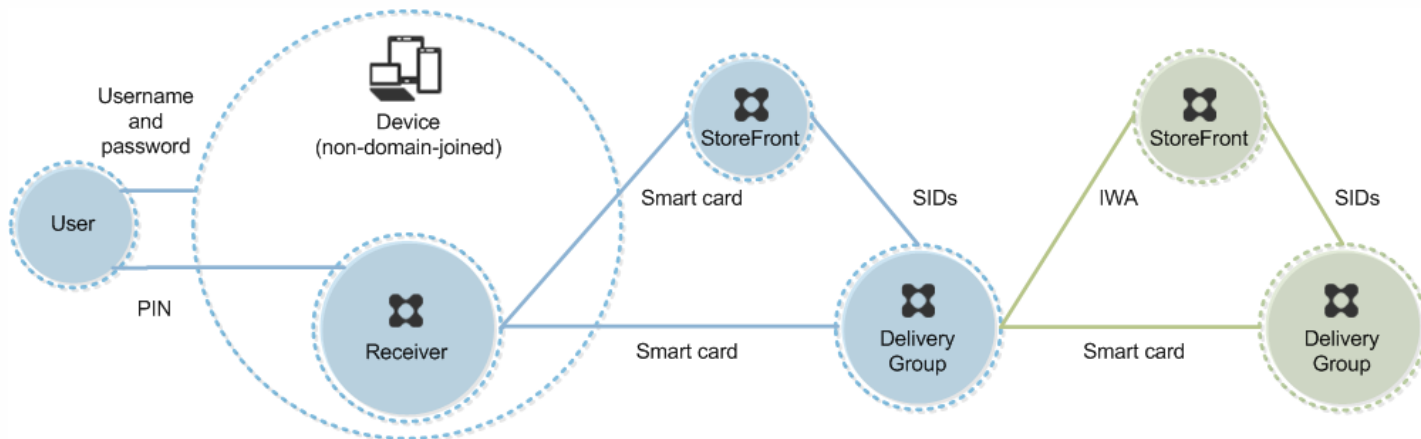
ユーザーは自動的にStoreFrontにログオンし、ユーザーセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。Receiverでシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要はありません。

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

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。最初の接続で使った認証方法を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

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。



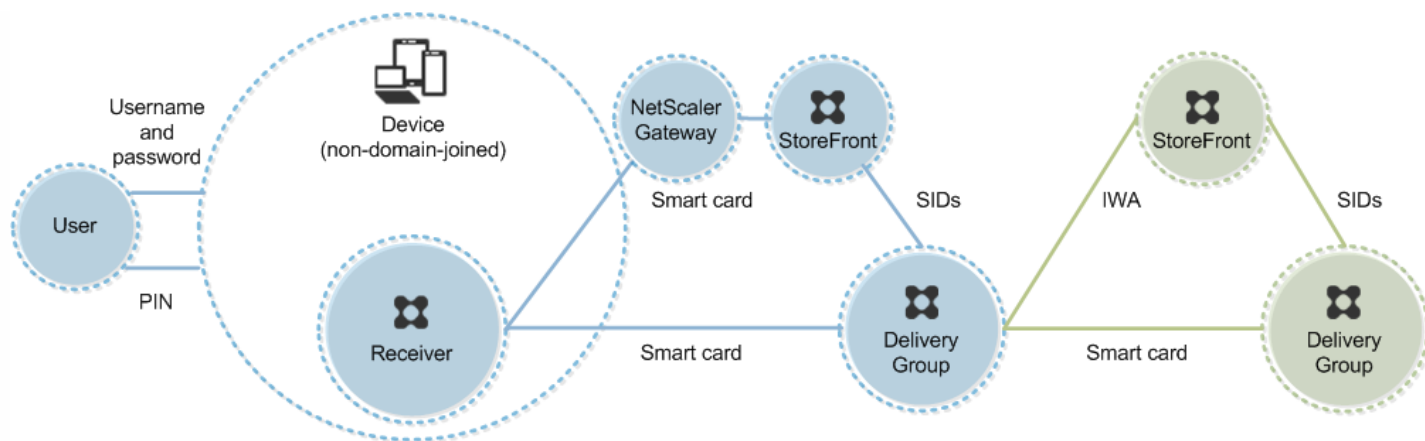
ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力必須ではありません。この展開では2モード認証を使用できるため、ReceiverではスマートカードとPIN、またはユーザー名とパスワードのいずれかの入力が必要です。その後、ReceiverがStorefrontへの認証を実行します。

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。最初の接続で使った認証方法を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。



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必要です。その後、ReceiverがStorefrontへの認証を実行します。

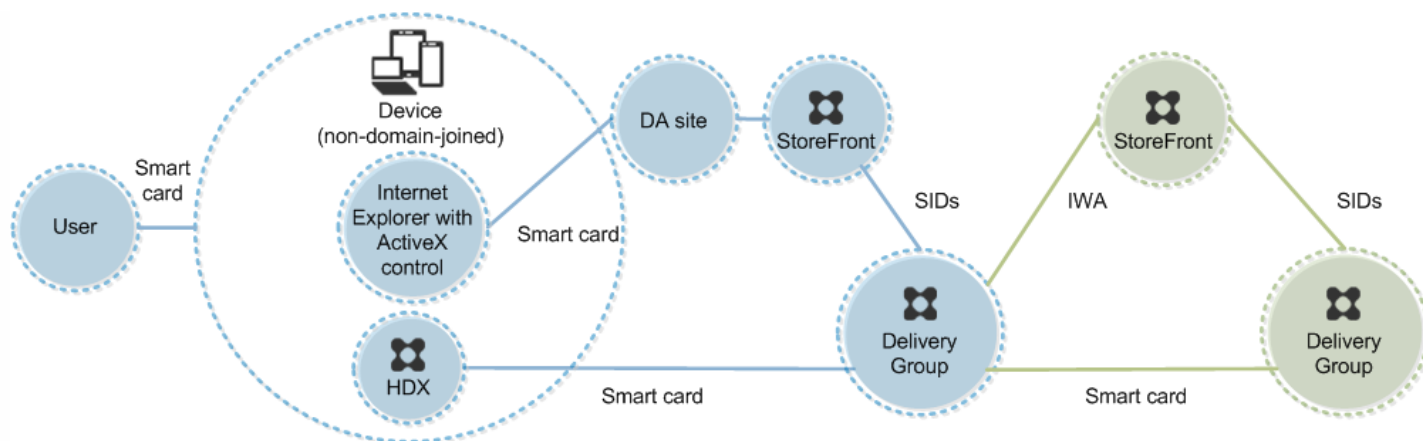
StoreFrontにより、ユーザーのセキュリティ識別子 (SID) がXenAppまたはXenDesktopに渡されます。この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときにPINを再入力する必要があります。

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。最初の接続で使った認証方法を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：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。



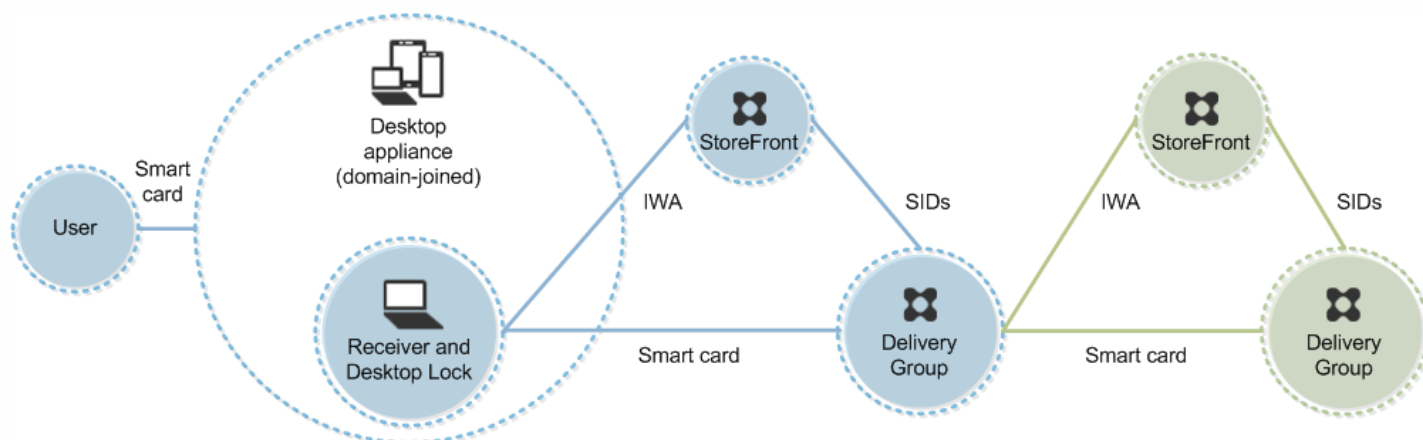
ユーザーは、スマートカードを使ってデバイスにログオンします。Desktop Lockを実行するデバイスは、キオスクモードで動作するInternet Explorerを介してデスクトップアプライアンスサイトを起動するように構成されます。サイトのActiveXコントロールによりPINの入力が求められ、それがStoreFrontに送信されます。StoreFrontにより、ユーザーのセキュリティ識別子（SID）がXenAppまたはXenDesktopに渡されます。割り当てられたデスクトップグループ一覧で使用可能な（アルファベット順で）最初のデスクトップが起動します。

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、

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。最初の接続で使った認証方法を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。

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

Jul 07, 2016

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。

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によるパススルー認証は、Windows Server 2008およびWindows Server 2012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、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ドキュメントの「[認証サービスの構成](#)」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：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。この画面ではログオンできないため、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。

Transport Layer Security (TLS)

Aug 26, 2016

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。

- サーバー証明書を手入手して、すべてのDelivery Controller上にインストールして登録します。さらに、SSL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SSL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。

Windowsレジストリの編集が必要なタスク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ます。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。

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、[CTX139664](#)を参照してください。

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。サーバー証明書を手入手してController上にインストール、および登録し、SSL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/205/09/08/how-to-create-a-web-server-ssl-certificate-manually.aspx>を参照し、SSL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\(W5.10\).aspx](http://technet.microsoft.com/ja-jp/library/cc736326(W5.10).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SSL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。

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BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>を実行します。

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: 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
```

HTTPSトラフィックのみを適用する

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値を設定してからBroker Serviceを再起動します。

HTTPトラフィックを無視するには、XmlServicesEnableNonSslを0にします。

HTTPSトラフィックを無視するレジストリ値はXmlServicesEnableSslです。この値が0に設定されていないことを確認します。

VDA上のTLS設定について

VDA上のTLSを構成すると、インストールされているSSL証明書のアクセス権が変更され、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。

- 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、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。

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暗号が許可されるのか。**
暗号スイート（Cipher Suite）とは、一般的なTLS暗号の一覧を指します。クライアントが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内にクライアントのいずれかのSSL暗号と一致するものがあるかどうかチェックされ、あった場合にのみ接続が確立されます。一致するSSL暗号がない場合、その接続はVDAにより拒否されます。

サポートされている暗号スイートはGOV（emment）、COM（mercial）、およびALLの3つです。これらの暗号スイートに含まれる暗号は、WindowsのFIPSモードによって異なります。Window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、各暗号スイートに含まれる暗号を示しています。

TLS暗号スイート	GOV	COM	すべて	GOV	COM	すべて
FIPSモード	Off	Off	Off	On	On	On
RSA_KEYX	○	○	○	○	○	○
RSA_SIGN	○	○	○	○	○	○
3DES	○		○	○		○
RC4		○	○			
MD5	○	○	○			
SHA	○	○	○	○	○	○
SHA_256	○	○	○	○	○	○
SHA_384	○	○	○	○	○	○
SHA_512	○	○	○	○	○	○
AES	○	○	○	○	○	○

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上のTLS構成：PowerShellスクリプトの使用

VDA上でEnable-VdaSSLps1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）

この結果、ユーザーはTLSでのみ接続できるようになり、Raw ICA、CGP、またはWebSocketで接続することはできなくなります。

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。

-Enableまたは-Disableパラメーターの指定は必須です。そのほかのパラメーターはオプションです。

構文

Enable-VdaSSL {-Enable | -Disable} [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite "<suite>"] [-CertificateThumbPrint "<thumbprint>"]

パラメーター	説明
-Enable	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。
-Disable	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。
-SSLPort <port>	TLSポート指定します。デフォルト：443
-SSLMinVersion "<min-ssl-version>"	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："SSL_3.0"、"TLS_1.0"、"TLS_1.1"、および"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。

パラメーター -SSLCipherSuite "<suite>"	説明 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："GOV"、"COM"、および"ALL"。デフォルト："ALL"
- CertificateThumbPrint "<thumbprint>"	証明書ストア内のSSL証明書の拇印を二重引用符で囲んで指定します。通常、証明書ストア内に複数の証明書が配置されている場合にこのパラメーターを使用します。この拇印により、スクリプトで適切な証明書が選択されます。デフォルト：証明書ストアの [ローカルコンピューター] > [個人] > [証明書] で最初に検出された証明書

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。
Enable-VdaSSL -Enable

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にして、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。
Enable-VdaSSL -Enable -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

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。

- 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）。
- MMCに証明書スナップインを追加します。
 - [ファイル] > [スナップインの追加と削除] の順に選択します。
 - [証明書] を選択して [追加] をクリックします。
 - [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。
 - [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。
- 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。
- [<FriendlyName> private keysのアクセス許可] ダイアログボックス（<FriendlyName>はSSL証明書の名前）が開きます。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"
- SSL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。
- regeditを実行して、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawdを開きます。
 - SSLThumbprintキーを編集して、SSL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。
 - 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）。
 - 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）。
- 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には、 [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）。
- 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。
- 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。

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。

- StudioからPowerShellコンソールを開きます。
- 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。
- Get-BrokerAccessPolicyRule -DesktopGroupName '<delivery-group-name>' | Set-BrokerAccessPolicyRule -HdxSslEnabled \$trueを実行します。
ここで、<delivery-group-name>はSSLを構成するデリバリーグループの名前です。
- 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。

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（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）が表示される場合があります。

コントローラーとVDAの間の通信

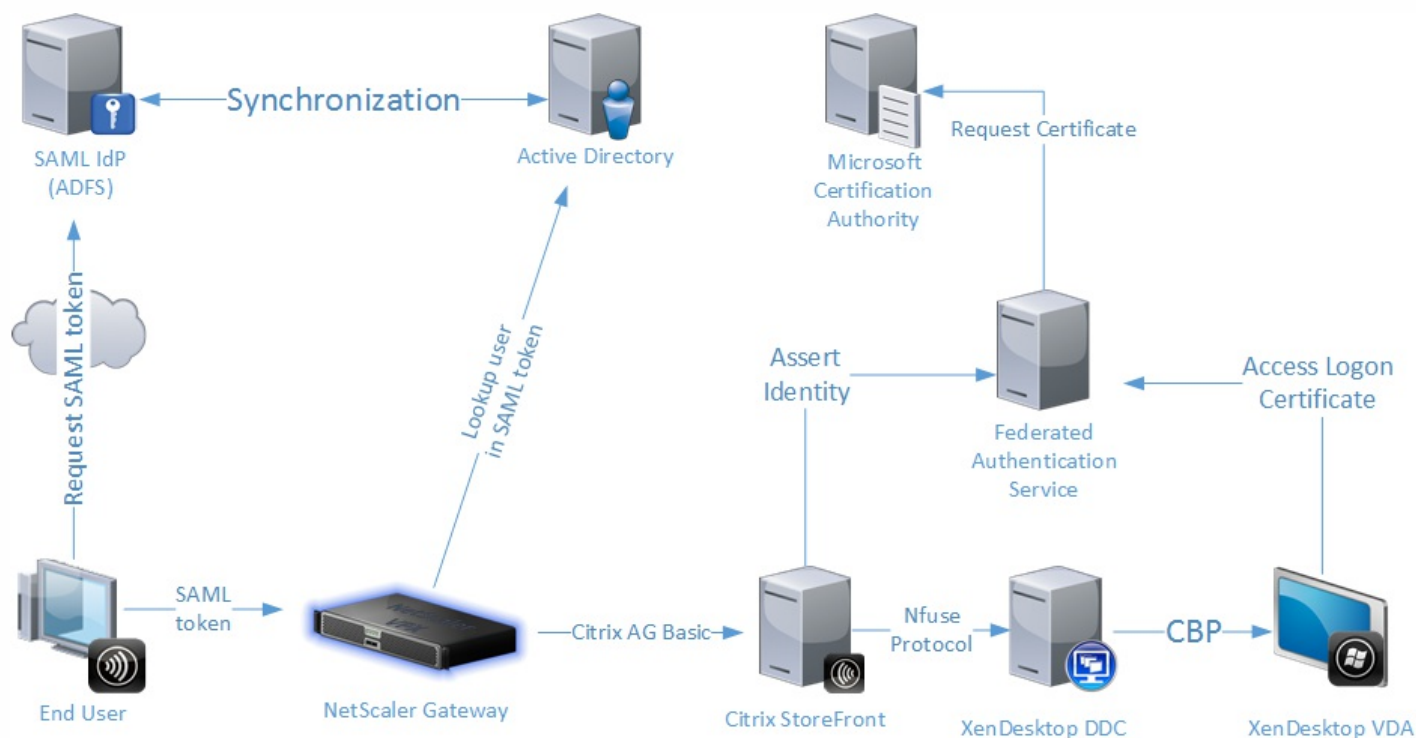
コントローラーとVDAの間の通信は、Windows Communication Framework（WCF）のメッセージレベル保護によって保護されます。TLSを使用する追加のトランスポートレベル保護は必要ありません。WCF構成は、コントローラーとVDAの間の相互認証にKerberosを使用します。暗号化ではAESをCBCモードで使用します。キーは256ビットです。メッセージの整合性にはSHA-1を使用します。

Federated Authentication Service

Jul 15, 2016

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が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

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. ユーザーロールの構成

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 Authentication Service
- 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

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。

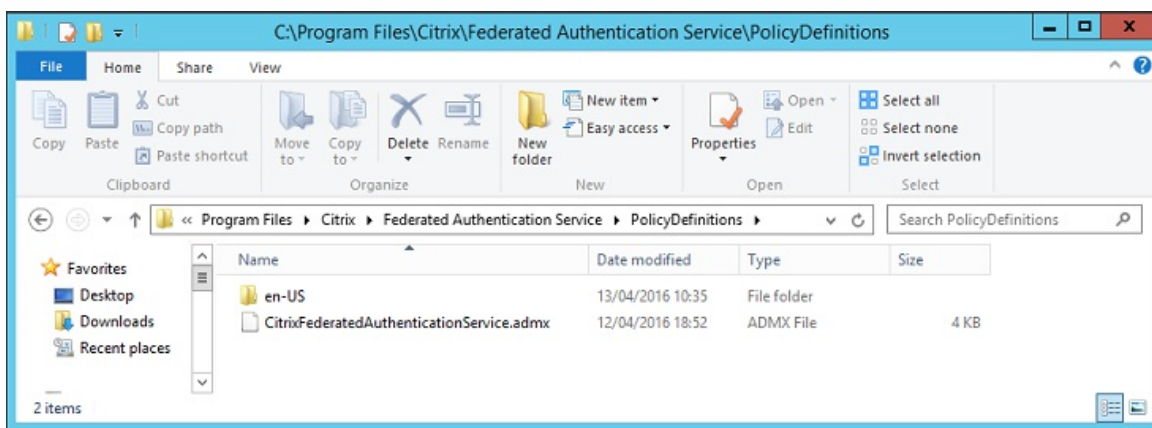
グループポリシーの構成

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。

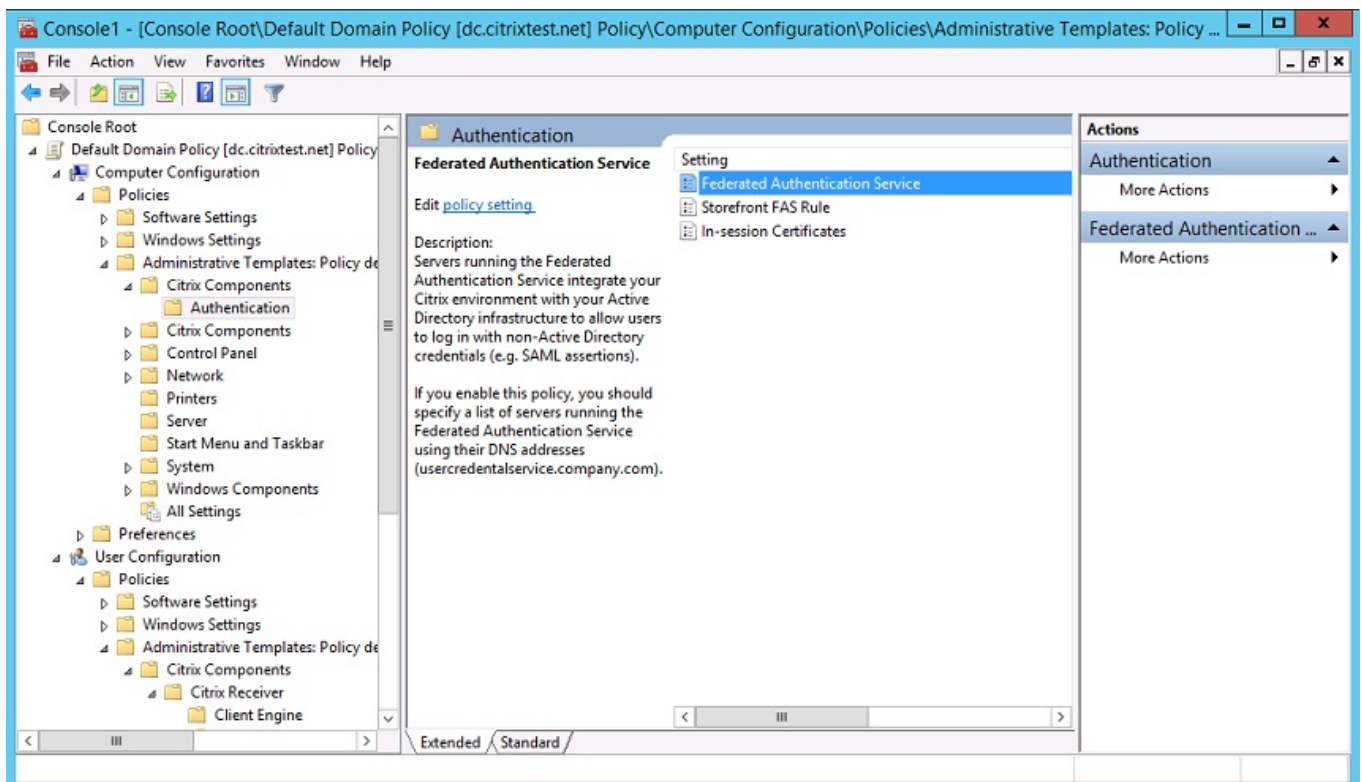
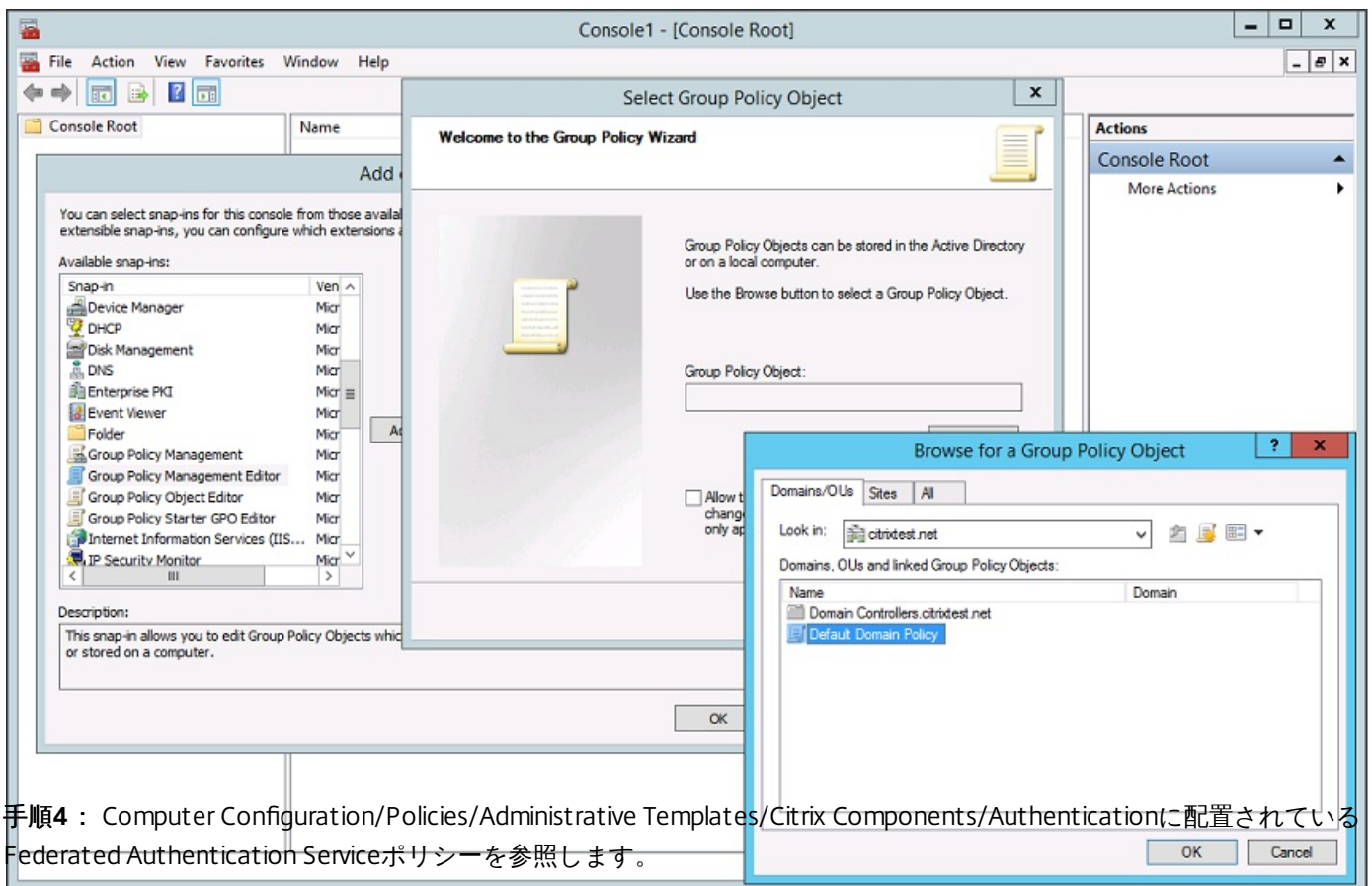
手順1：FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admxファイルおよびen-USフォルダーを見つけます。



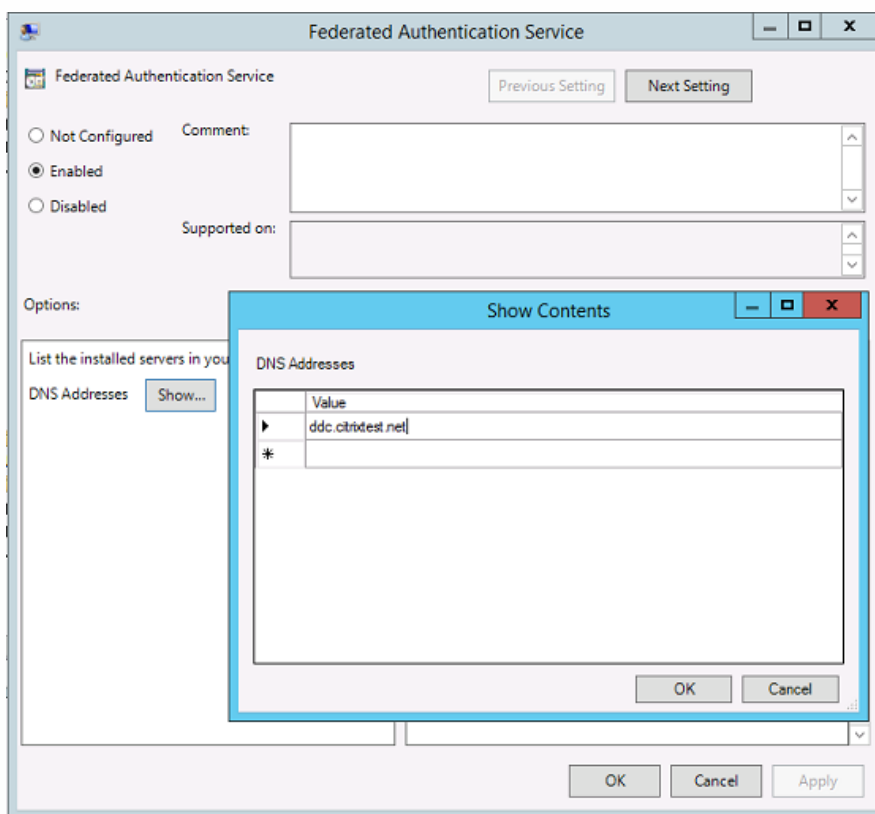
手順2：これらをドメインコントローラーにコピーして、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

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。



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。

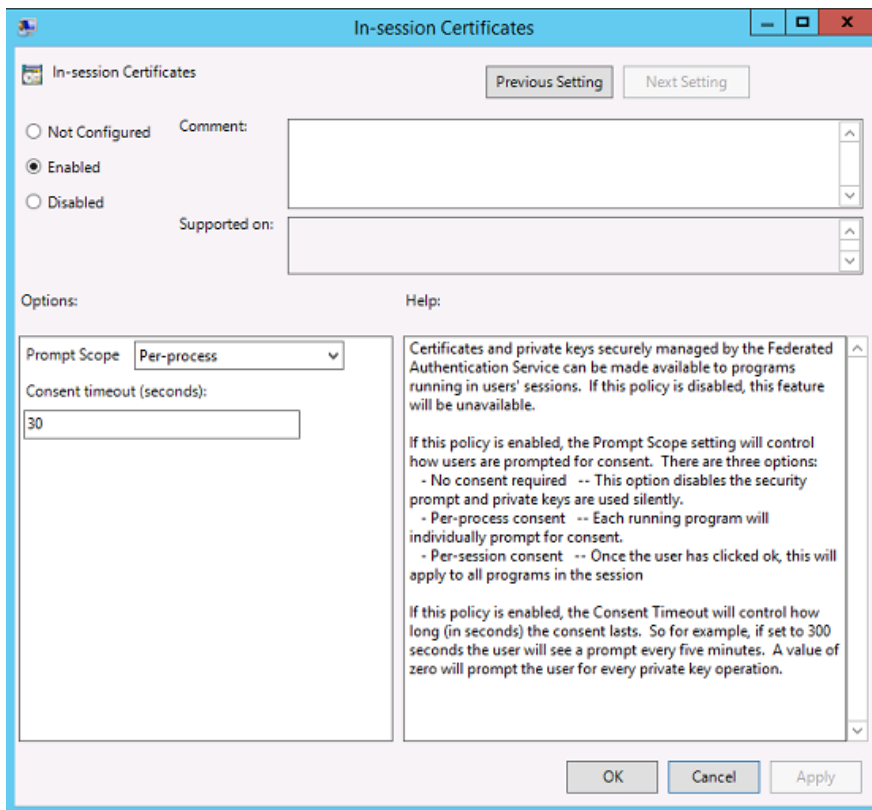
注意：複数のアドレスを入力する場合は、StoreFrontサーバーとVDA間で一覧の順番が統一されている必要があります。これには、空白や使用されないエントリも含まれます。

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

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

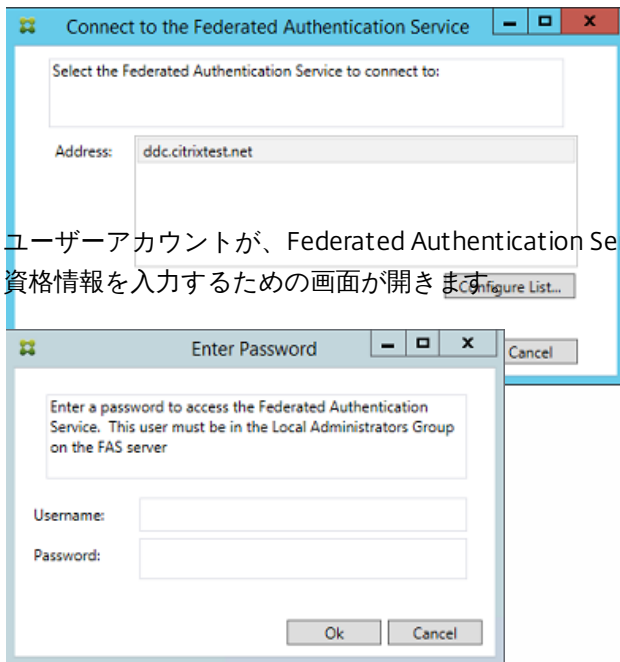
グループポリシーテンプレートには、セッション中の証明書についてのシステムの構成のサポートが含まれます。これにより、ログオン後に、アプリケーションが使用できるようにユーザーの個人証明書ストアに証明書が配置されます。たとえば、VDAセッション内でWebサーバーへのTLS認証が必要な場合、証明書はInternet Explorerによって使用されます。デフォルトで、VDAはログオン後の証明書へのアクセスを許可しません。



Federated Authentication Service管理コンソールの使用

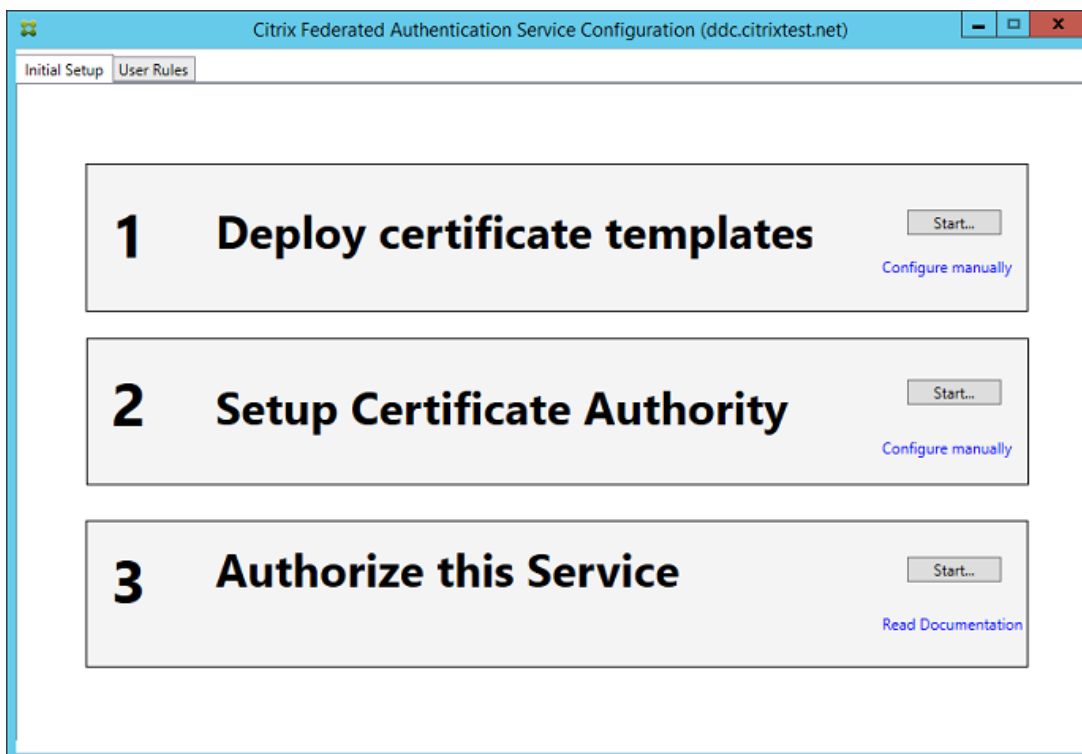
Federated Authentication Service管理コンソールは、Federated Authentication Serviceの一部としてインストールされます。[スタート]メニューにアイコン (Citrix Federated Authentication Service) が配置されます。

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。



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。

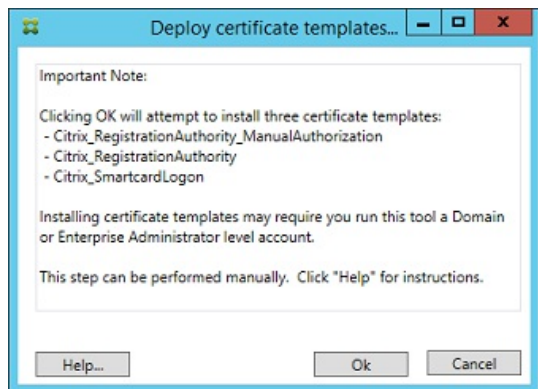


証明書テンプレートの展開

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。

-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)

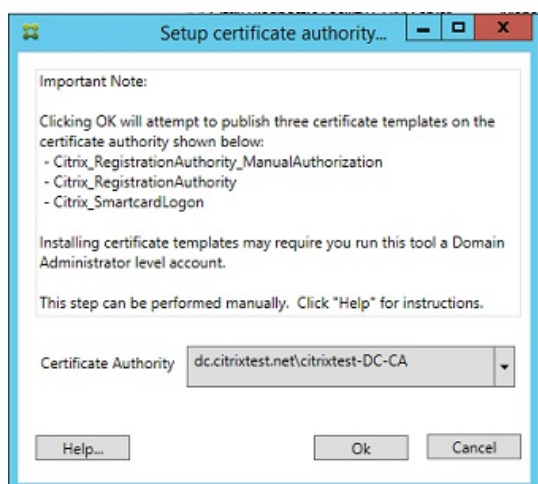
$writabletemplate.Commit(1, $NULL)
```

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。

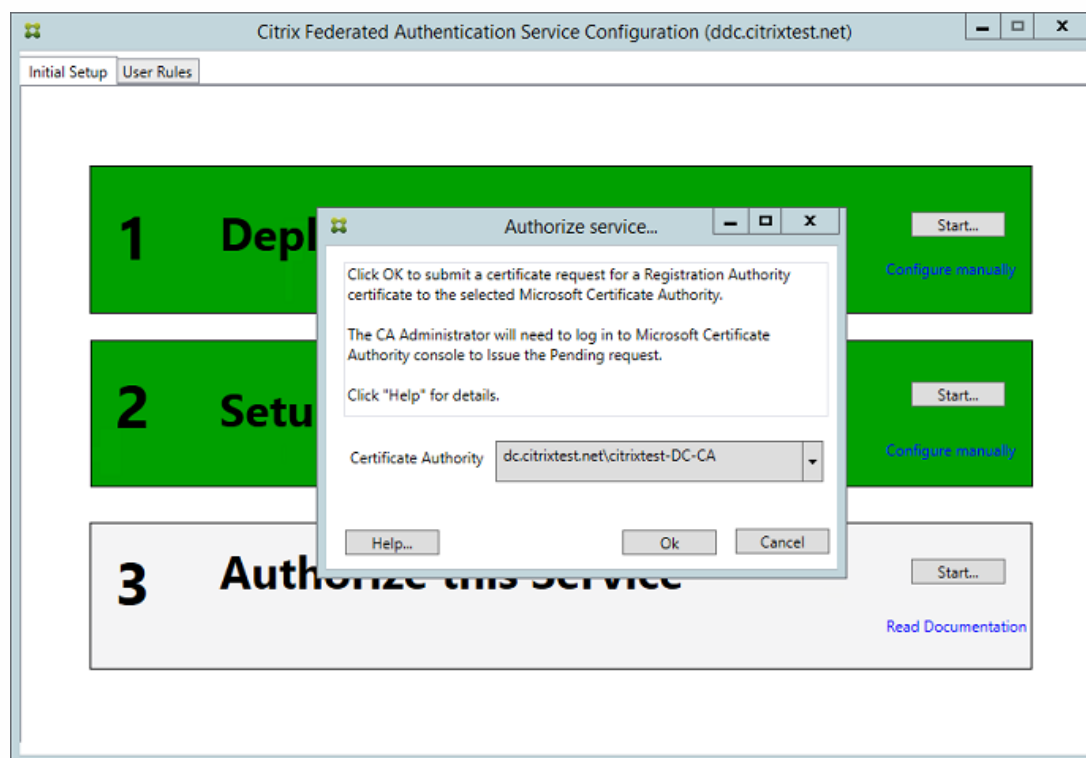
どのサーバーでもテンプレートが公開されていない場合は、**証明書機関のセットアップツール**によって公開できます。このツールは、証明機関の管理権限のあるユーザーとして実行する必要があります。

(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。)

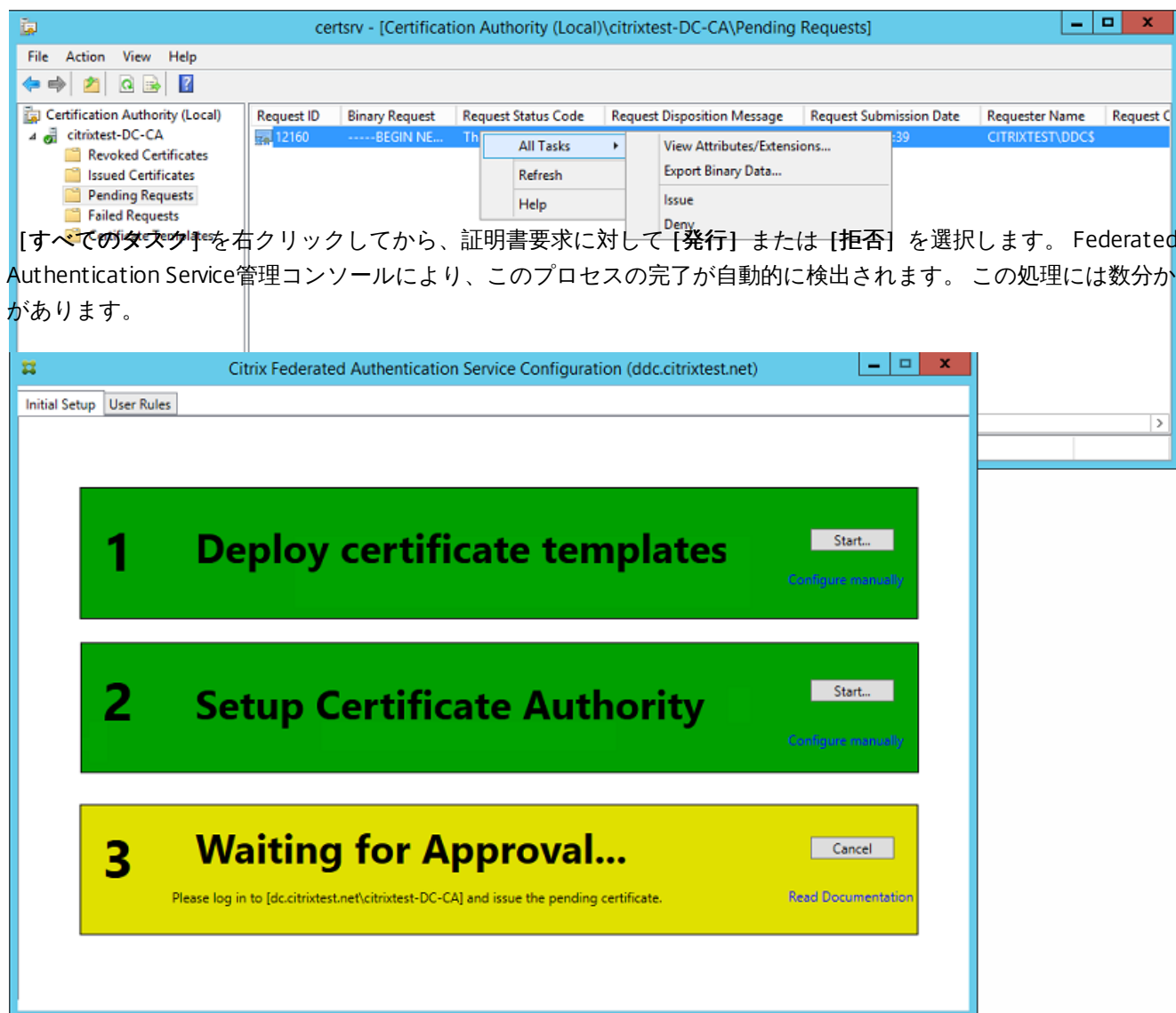


Federated Authentication Serviceへの権限付与

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。



ユーザーールの構成

ユーザーールにより、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与与されます。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。

Citrix Federated Authentication Service Configuration (ddc.citrixtest.net)

Initial Setup User Rules

Create "User Rules" that correspond to different types of smartcard-class certificates that will log your users into a Citrix environment.

Rule name: default

Add... Remove

Certificate Authority: dc.citrixtest.net/citrixtest-DC-CA

Certificate Template: Citrix_SmartcardLogon

☒ Available after logon

Security Access Control Lists

Edit List of Storefront servers that can use this rule

Edit List of VDA desktops and servers that can be logged into by this rule

Edit List of users that StoreFront can log in using this rule

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。

Permissions for Storefront Servers

Security

Group or user names:

DDC (CITRIXTEST\DDCs)

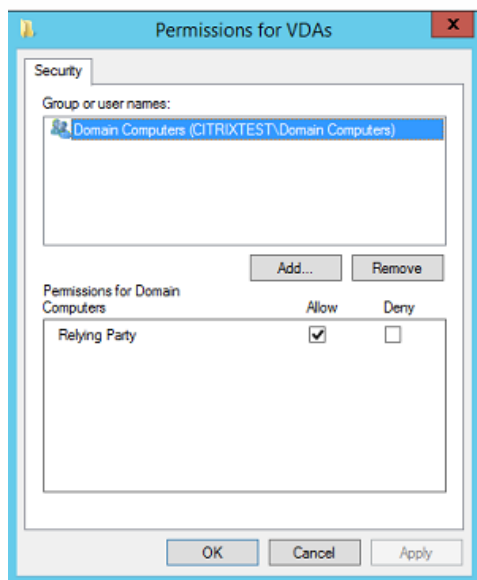
Add... Remove

Permissions for DDC

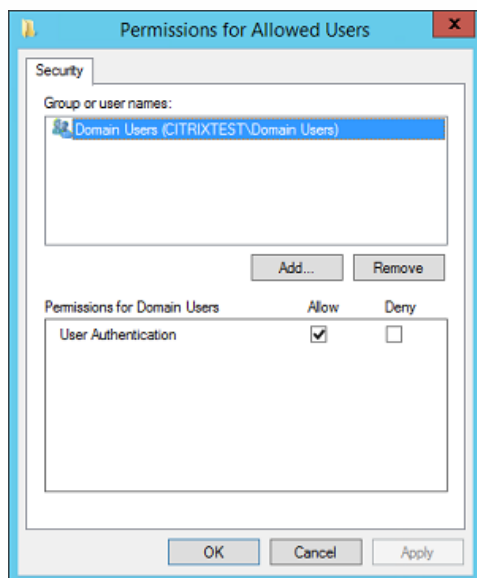
	Allow	Deny
Assert Identity	☒	☐

OK Cancel Apply

【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。



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。

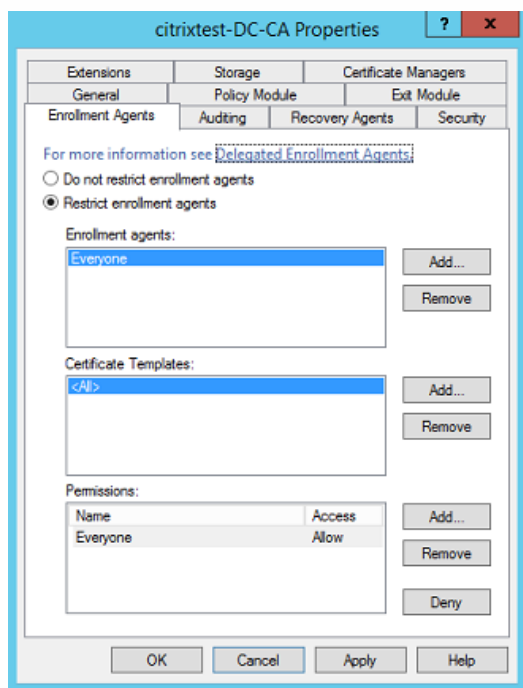
新しい証明書テンプレートを作成するには、Microsoft証明機関コンソールでCitrix_SmartcardLogonテンプレートを複製して名前を（Citrix_SmartcardLogon2などに）変更し、必要に応じて変更を加えます。[追加]をクリックして新しい証明書テンプレートを参照し、新しいユーザールールを作成します。

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。



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)。

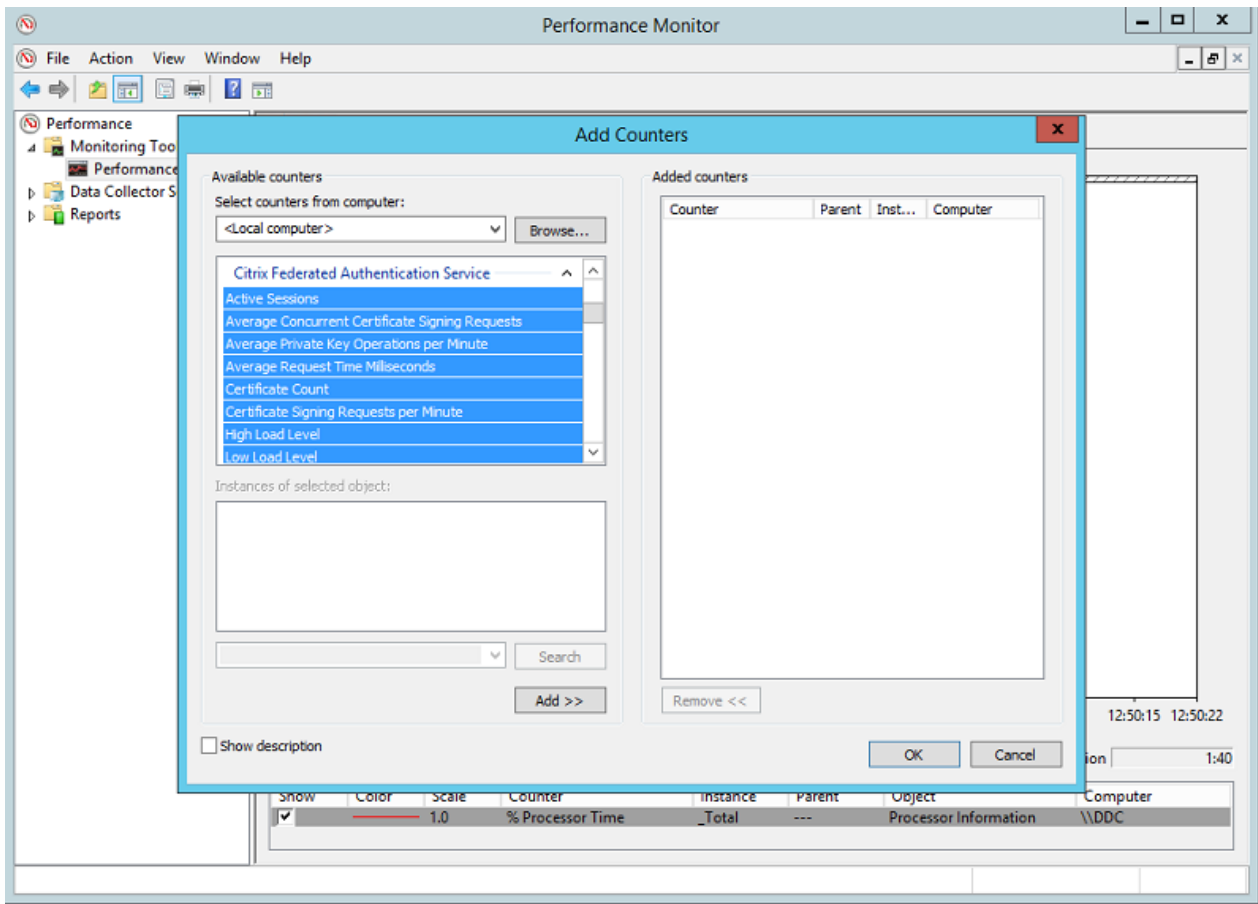
コマンド	概要
*-FasServer	現在の環境のFASサーバーを一覧表示および再構成します。
*-FasAuthorizationCertificate	登録機関証明書を管理します。
*-FasCertificateDefinition	FASが証明書の生成に使用するパラメータを制御します。
*-FasRule	Federated Authentication Serviceで構成済みのユーザールールを管理します。
*-FasUserCertificate	Federated Authentication Serviceによってキャッシュされた証明書を一覧表示および管理します。

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。



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、

名前	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。

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}]

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

れます。

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]

[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、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。

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
[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 - 承認待ち機継続中
[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
[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。

Federated Authentication Serviceのアーキテクチャの概要

Jul 15, 2016

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テクノロジー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ーを、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。

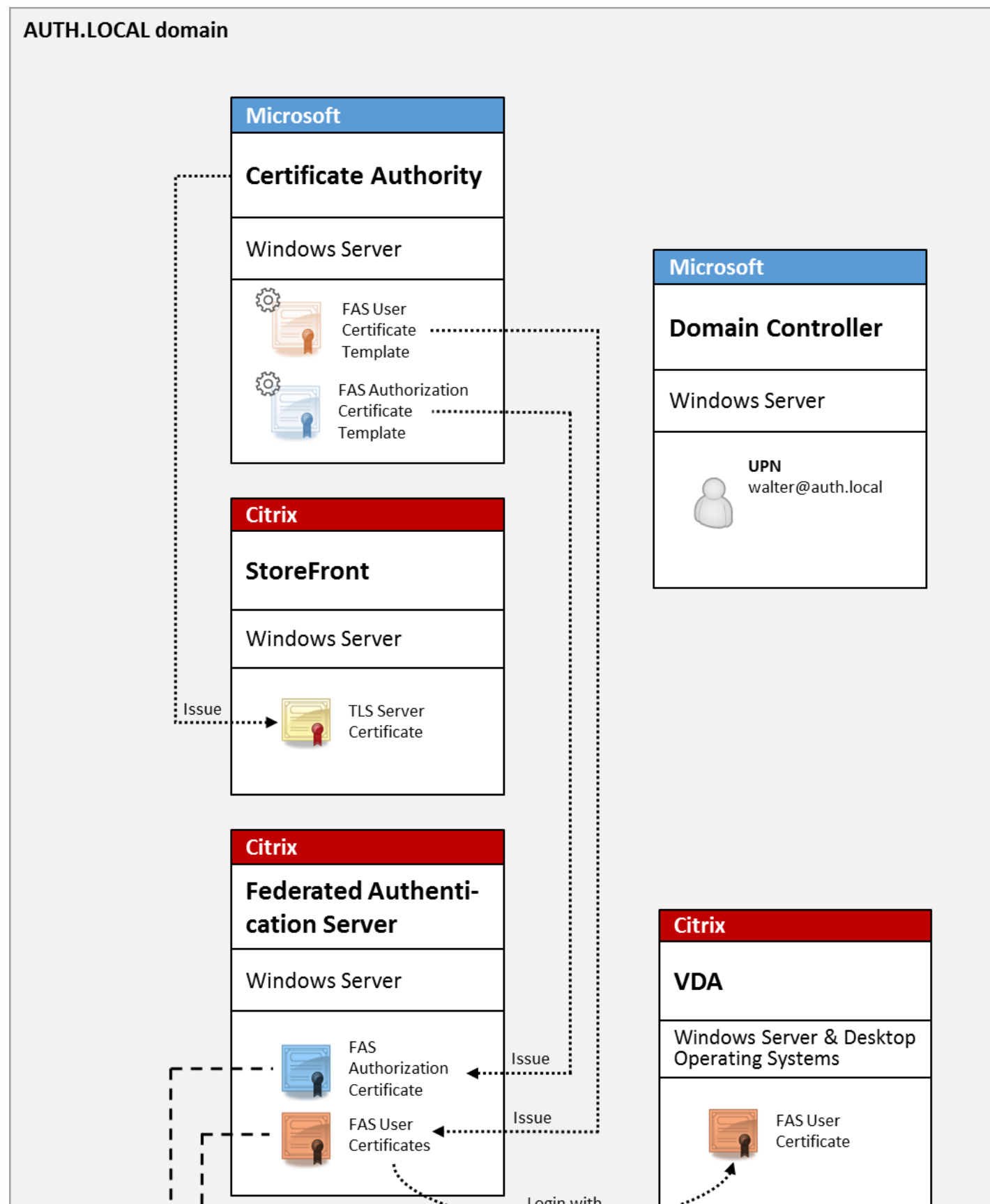
内部展開

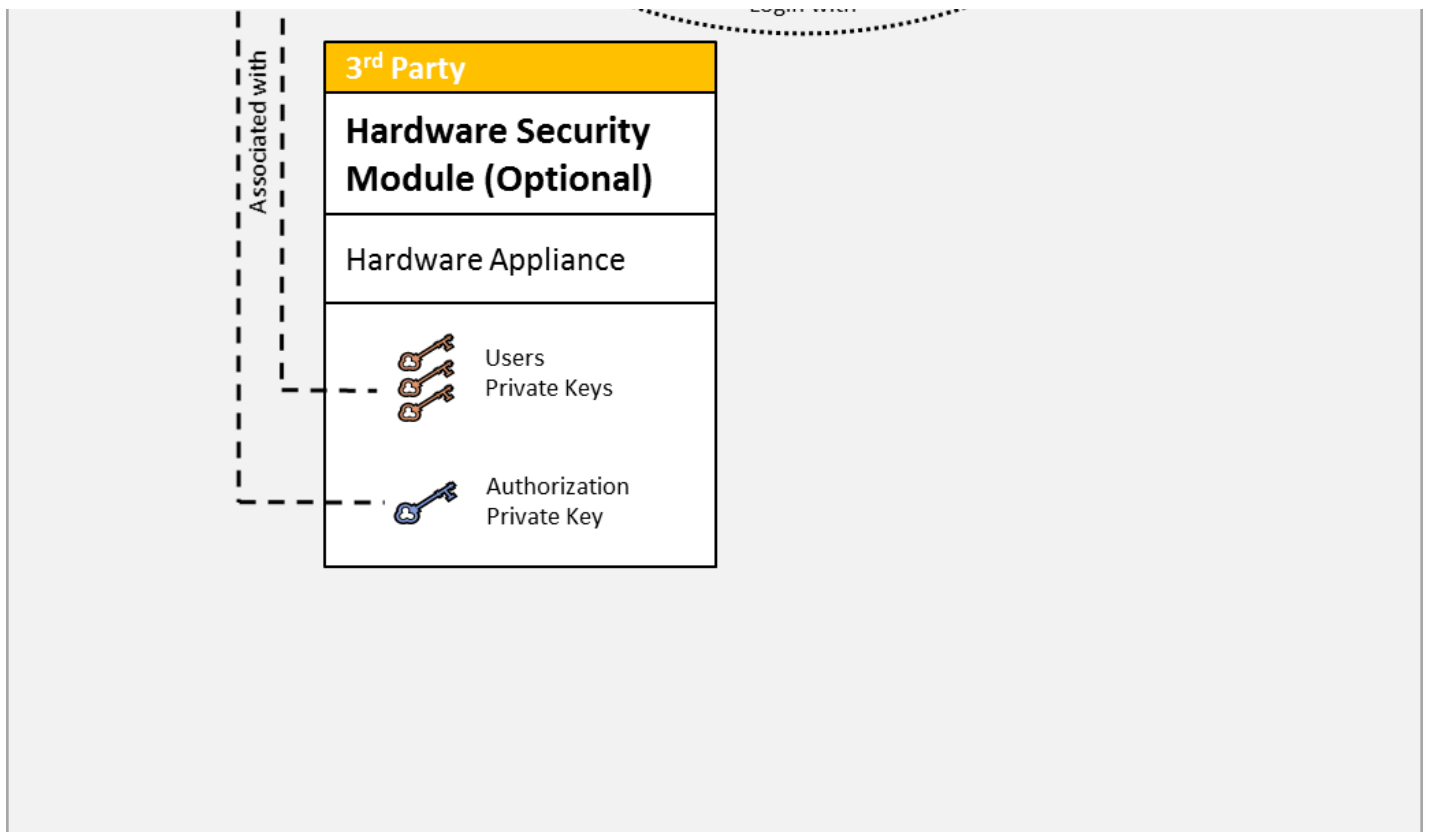
FASでは、さまざまな認証オプション (Kerberos シングルサインオンを含む) を使用したStoreFrontへの安全なユーザー認証、および十分に認証されたCitrix HDXセッションへの接続が可能です。

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。

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。





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

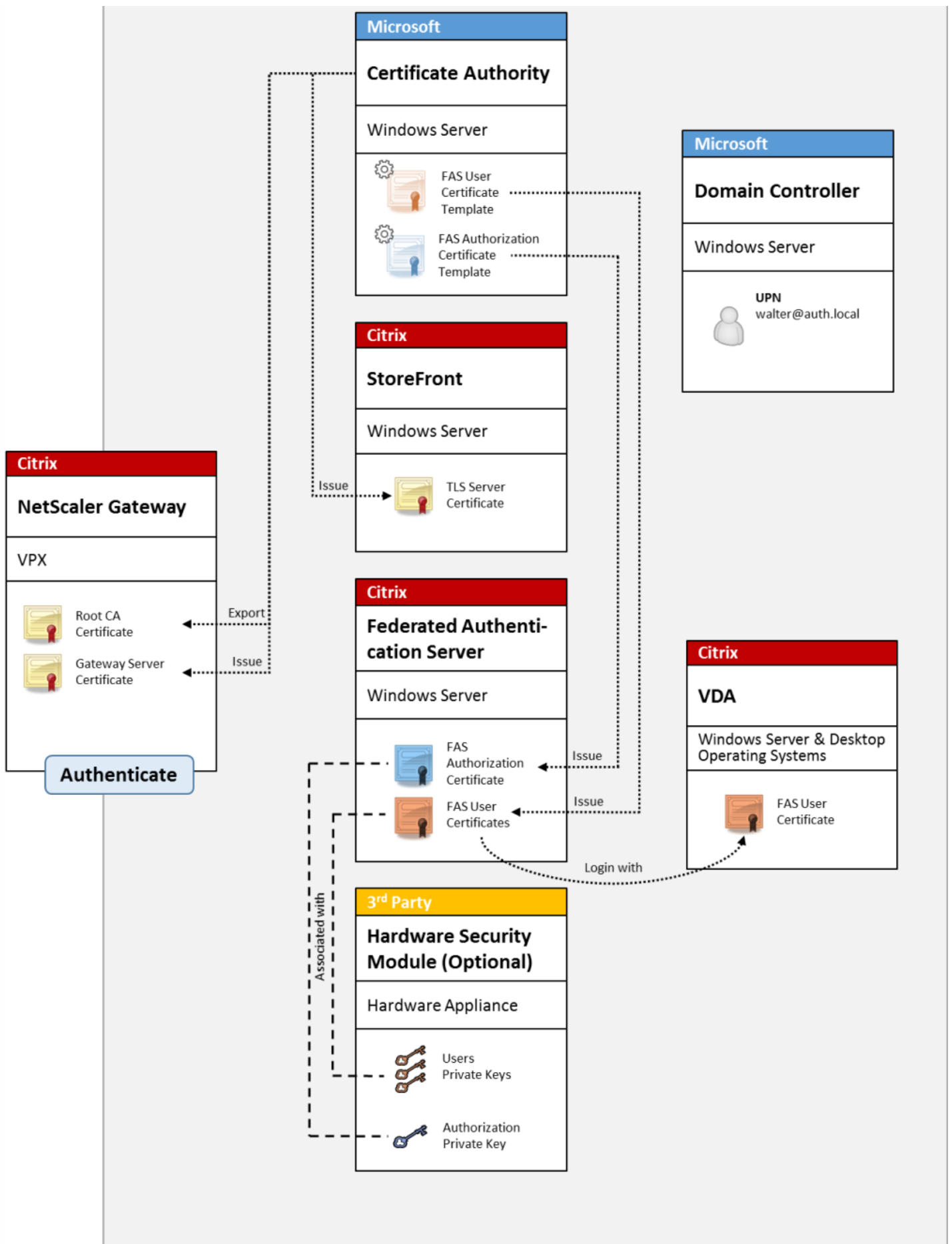
- キーは、ハードウェアセキュリティモジュール（HSM）やビルトインのトラステッドプラットフォームモジュール（TPM）に保存できます。詳しくは、「[Federated Authentication Serviceの秘密キー保護](#)」を参照してください。
- 「[Federated Authentication Service](#)」では、FASのインストールと構成の方法について説明します。

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認証テクノロジーを利用することができます。

AUTH.LOCAL domain



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。

Add NetScaler Gateway Appliance

StoreFront

- General Settings
- Secure Ticket Authority
- Authentication Settings**
- Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address (optional): v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

Callback URL (optional): https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx

⚠ When no Callback URL is specified, Smart Access is not available.

Back Create Cancel

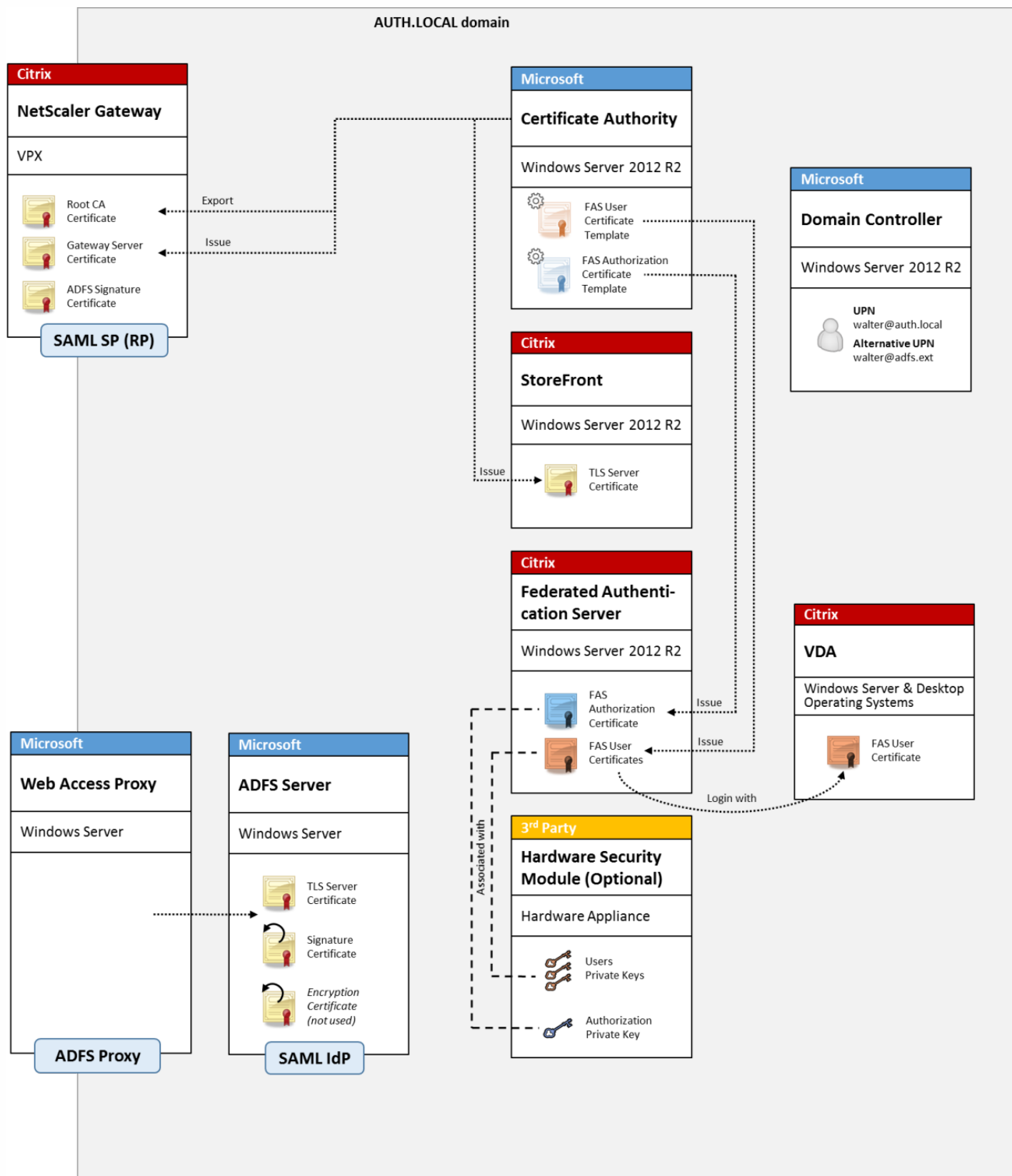
関連情報

- 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ーにより、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

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。



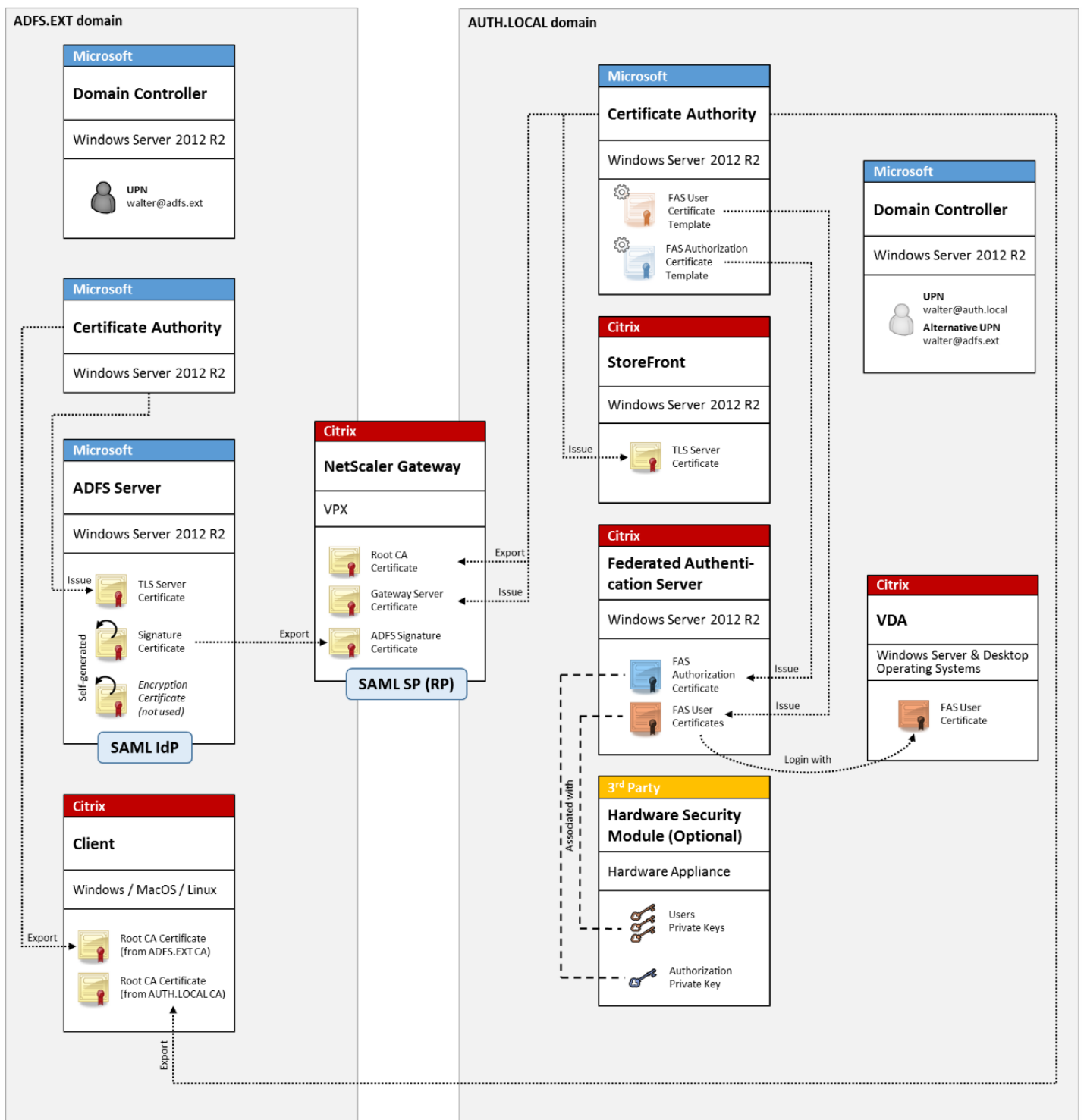
ADFSは、一般的にインターネットを利用して企業リソースにリモートでユーザーを安全に認証するために使用され、たとえば、Office 365の統合に多く利用されます。

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。



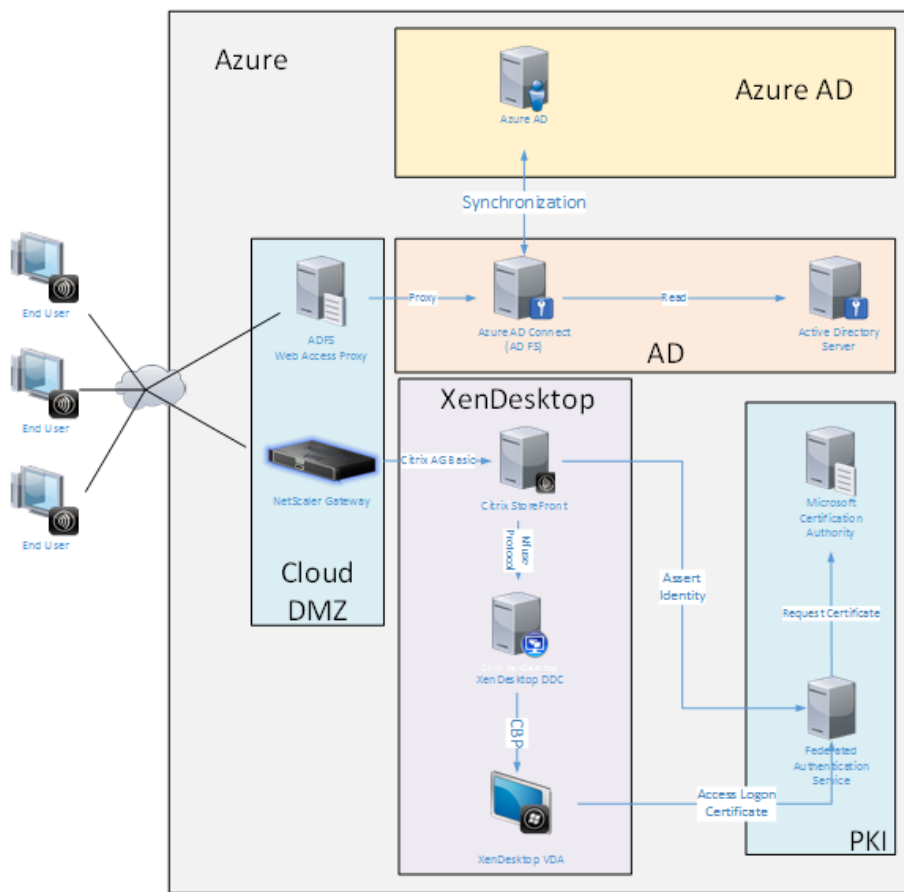
関連情報

- 「[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

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、「社内のエンドユーザー」という概念が事実上まったくない例です。ラップトップの登録と認証は、Azure ADの最新機能によってすべてインターネット上で行われます。

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、あるいはその他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。

Federated Authentication ServiceのADFSの展開

Jul 15, 2016

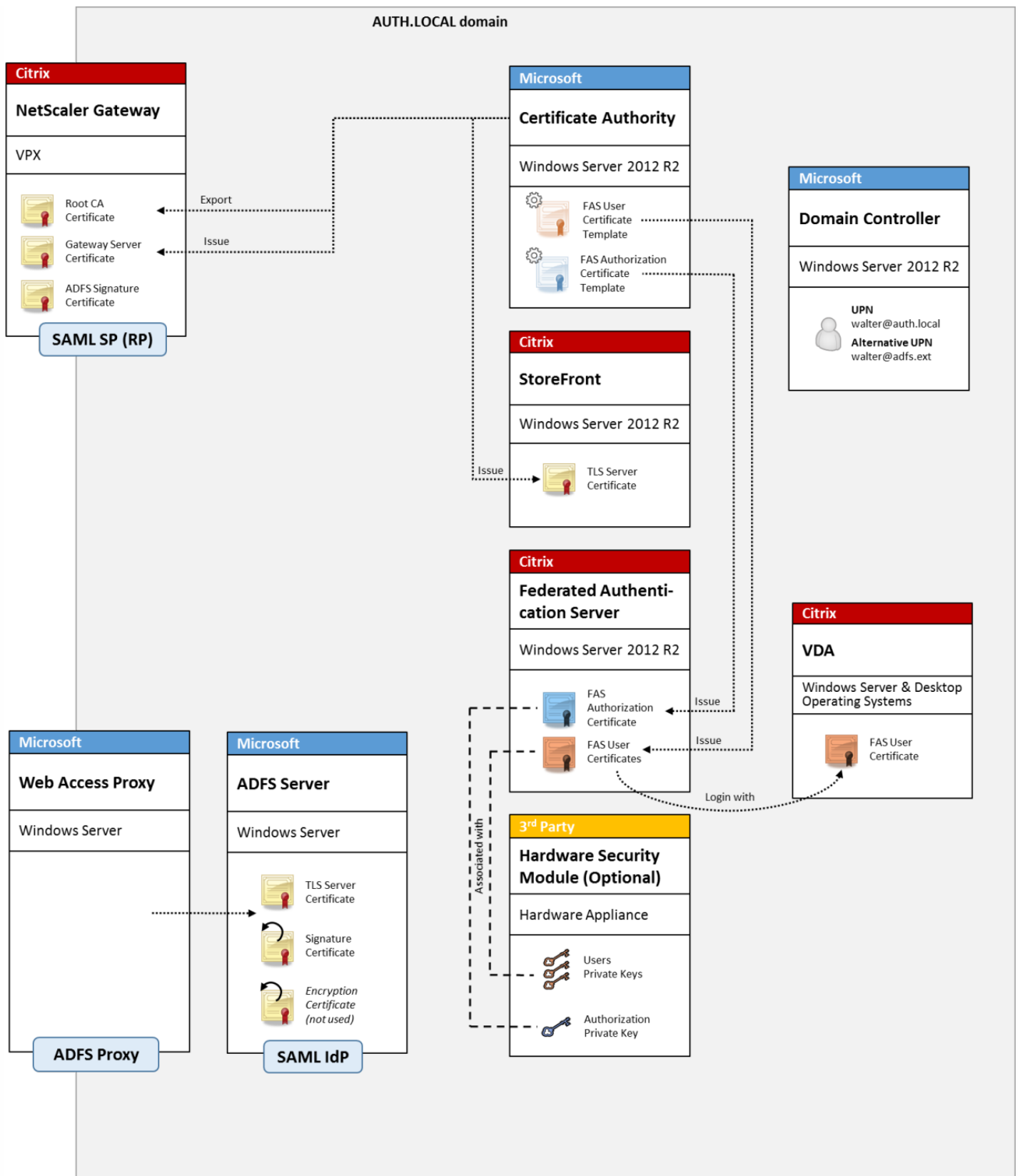
はじめに

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。



SAMLの概要

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/loginpage

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。

NetScaler > NetScaler Gateway > Policies > Authentication > SAML > Policies

PoliciesServers

AddEditDeleteShow BindingsPrimary VPN Global Bindings

Search

Name	Expression	Request Server
StoreFrontSAML	NS_TRUE	AzureAd

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にリダイレクトし、ADFSの署名したSAML認証XMLブロックを代わりに受け取ります。

Create Authentication SAML Server

Create Authentication SAML Server

Name*

Authentication Type

SAML

IDP Certificate Name*

Redirect URL*

Single Logout URL

User Field

Signing Certificate Name

Issuer Name

Reject Unsigned Assertion*

SAML Binding*

Default Authentication Group

Skew Time(mins)

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

Attribute Consuming Service Index

Requested Authentication Context*

Authentication Class Types

Signature Algorithm*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*

☐ SHA1 ☒ SHA256

☐ Send Thumbprint

☒ Enforce Username

Attribute 1

Attribute 3

Attribute 5

Attribute 7

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。

Federated Authentication ServiceのAzure ADの統合

Aug 26, 2016

ここでは次のことについて説明します。

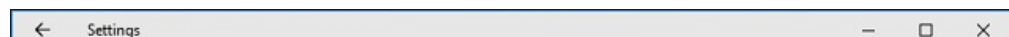
- はじめに
- アーキテクチャ
- DNSゾーンの作成
- クラウドサービスの作成
- Windows仮想マシンの作成
- 内部DNSの構成
- 外部DNSアドレスの構成
- セキュリティグループの構成
- ADFS証明書の作成
- Azure ADのセットアップ
- Azure ADへの参加の有効化
- XenAppまたはXenDesktopのインストール
- 新しいAzure ADアプリケーションをStoreFrontへのシングルサインオンに構成
- NetScaler Gatewayのインストールと構成
- StoreFrontアドレスの構成
- NetScaler SAML認証サポートの有効化
- エンドツーエンドシステムの検証
- 付録

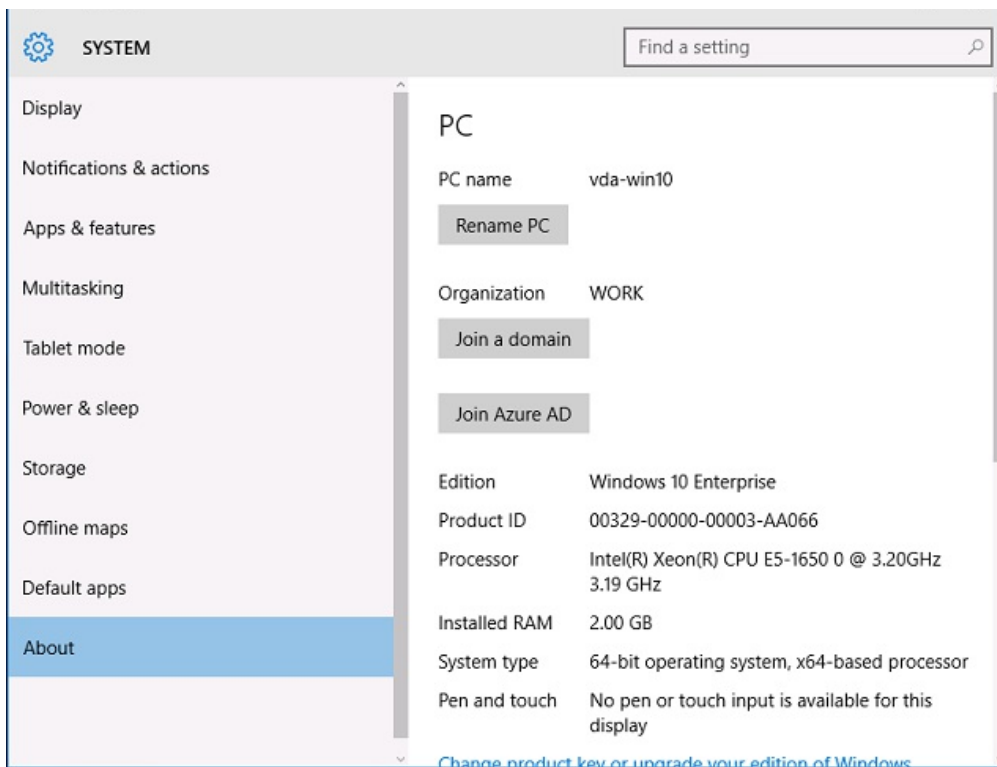
はじめに

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。

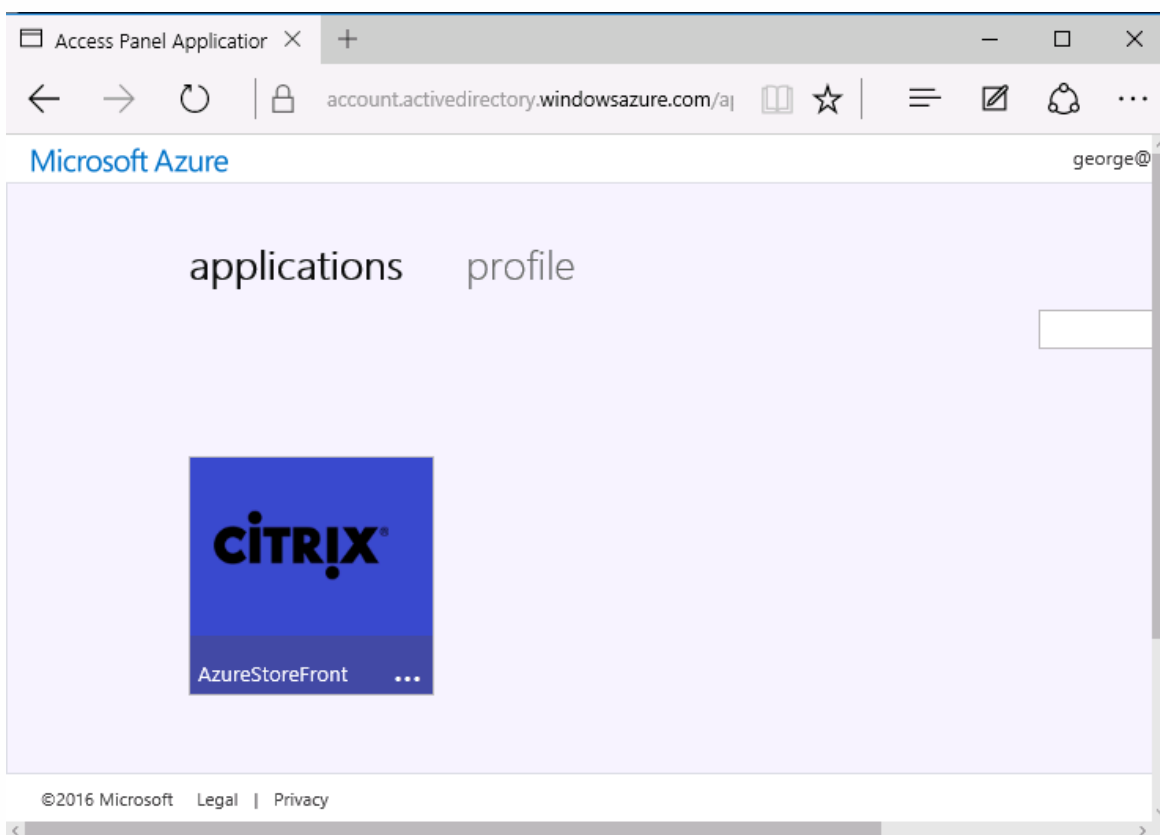
Windows 10が導入したAzure ADは、ドメイン参加の新しいモデルです。これを利用すれば、管理とシングルサインオンの目的で、ローミングラップトップを、インターネット上で企業ドメインに参加させることができます。

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。





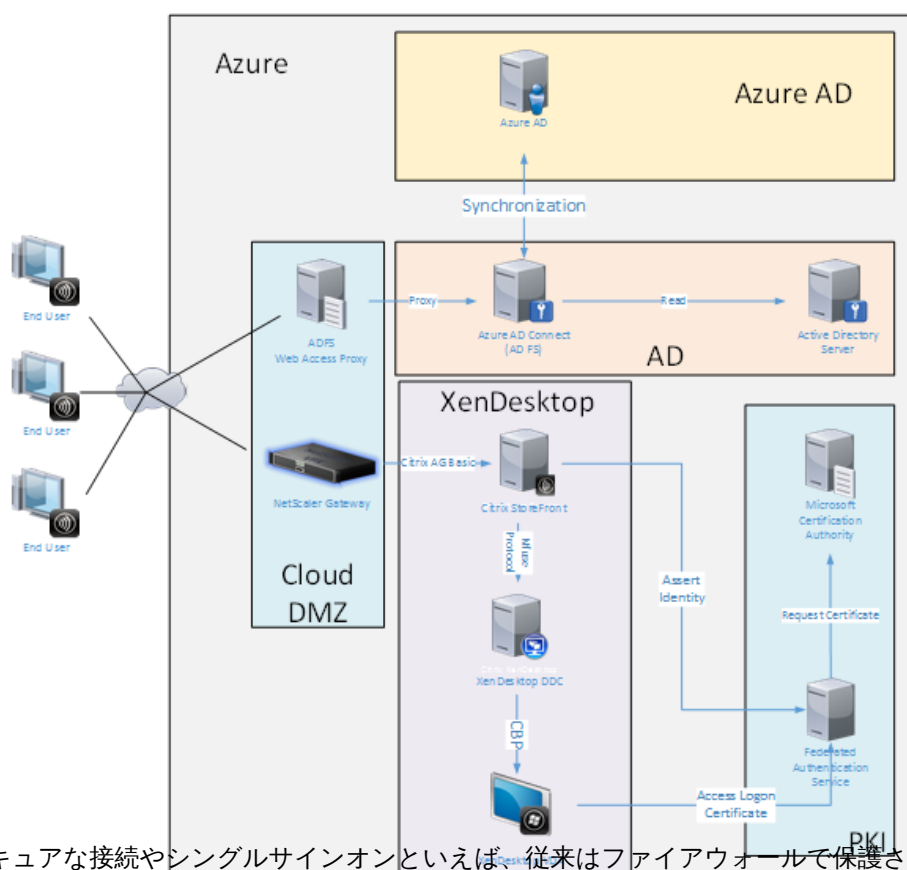
ラップトップが登録されると、Microsoft EdgeのWebブラウザーは、Azure SaaSアプリケーションのWebページから、会社のWebサイトやCitrixの公開アプリケーション、およびOffice 365などのAzureアプリケーションに自動的にサインオンします。



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ーとの統合により、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ド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。



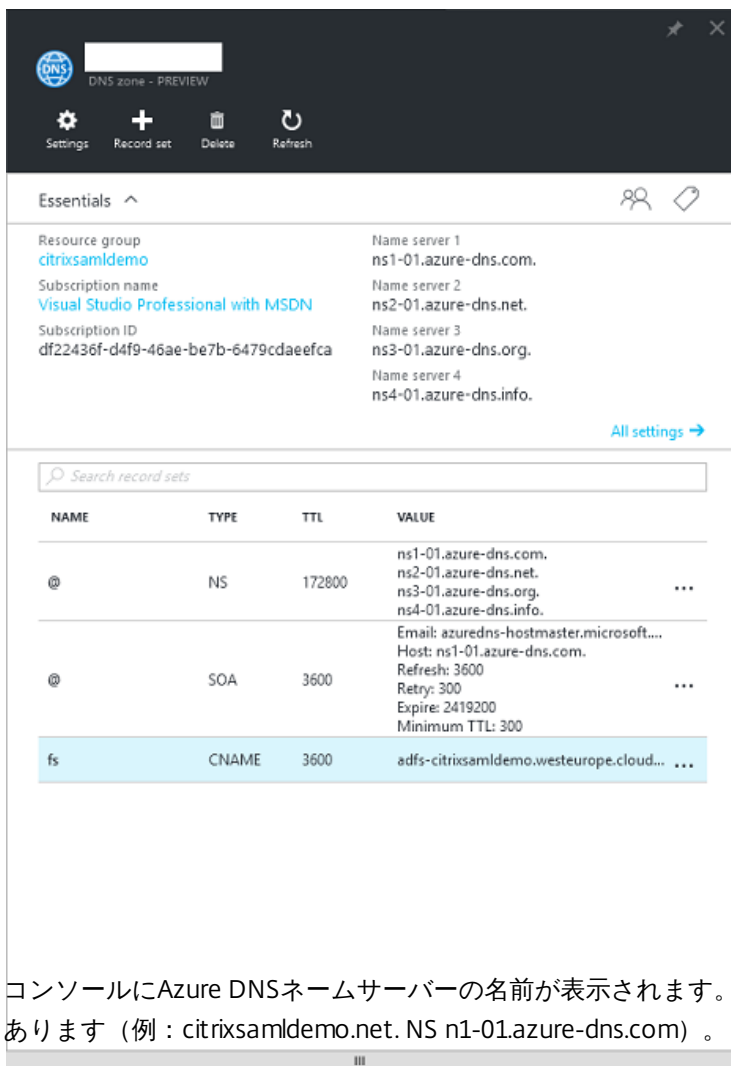
セキュアな接続やシングルサインオンといえば、従来はファイアウォールで保護されたLANや、Kerberos認証およびNTLM認証でしたが、このアーキテクチャでは、AzureへのTLS接続およびSAMLがこれらに取って代わります。AzureアプリケーションのAzure ADへの参加により、新しいサービスが生み出されています。Active Directoryを必要とする既存のアプリケーション（SQL Serverデータベースなど）は、AzureクラウドサービスのIaaS部分にある、標準的なActive Directoryサーバーの仮想マシンを使用して実行できます。

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。



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）。

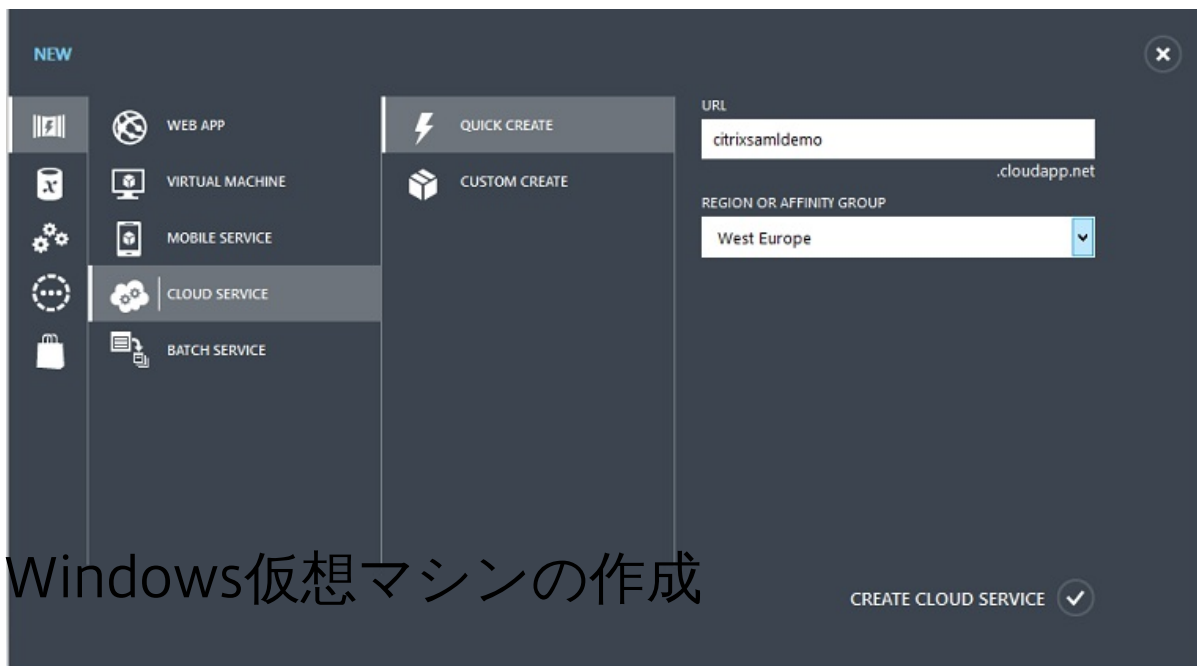
Azureで実行される仮想マシンへの参照を追加する場合は、CNAMEポインターを、Azureが管理する仮想マシンのDNSレコードに使用するのが最も簡単です。仮想マシンのIPアドレスが変更されている場合は、DNSゾーンファイルを手動で更新する必要はありません。

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（上のwap-citrixsamldemo...を指す）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

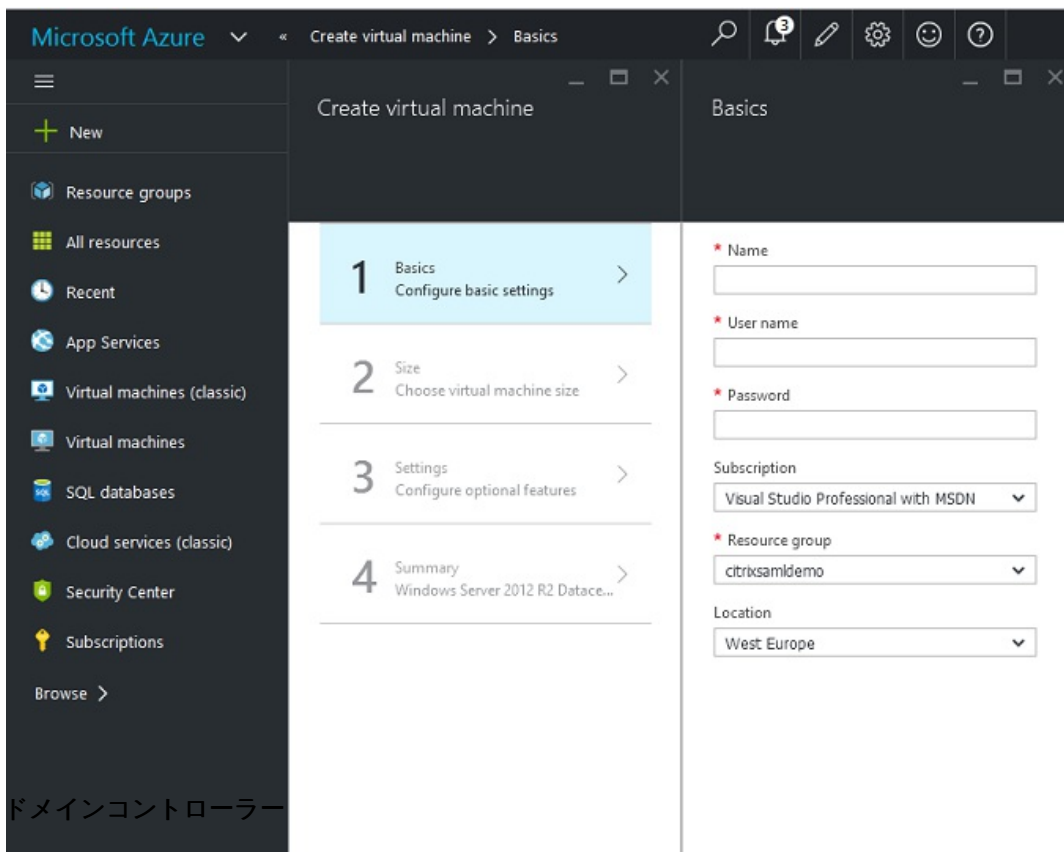
この例では、Azureで実行されるADFSサーバーが設置されたAD環境を含む、Citrix環境を構成します。クラウドサービスを作成し、「citrixsamldemo」と名づけます。



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)



- 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、citrixsamdemo.net）。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@citrixsamdemo.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

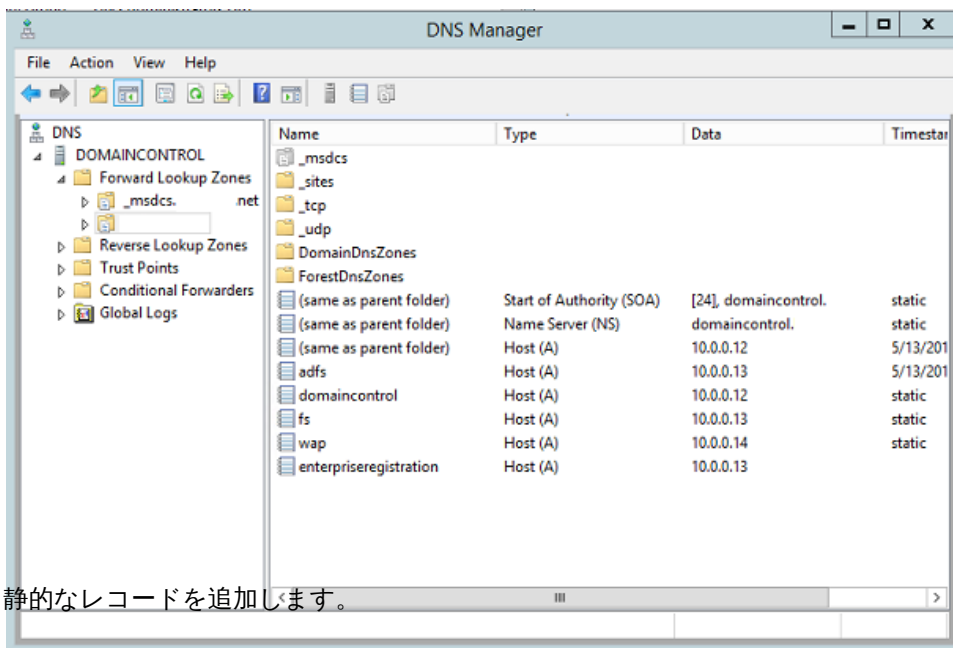
- ADFSサーバーをcitrixsamdemoドメインに参加させます。Webアプリケーションプロキシサーバーは、分離されたワークグループにとどまる必要があるため、AD DNSでDNSアドレスを手動で登録します。
- これらのサーバーでEnable-PSRemoting -Forceコマンドレットを実行して、Azure AD Connectツールからファイアウォール経由のPSリモートティングを有効にします。

XenDesktop Delivery ControllerとVDA

- XenAppまたはXenDesktop Delivery Controller、およびVDAを、citrixsamdemo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

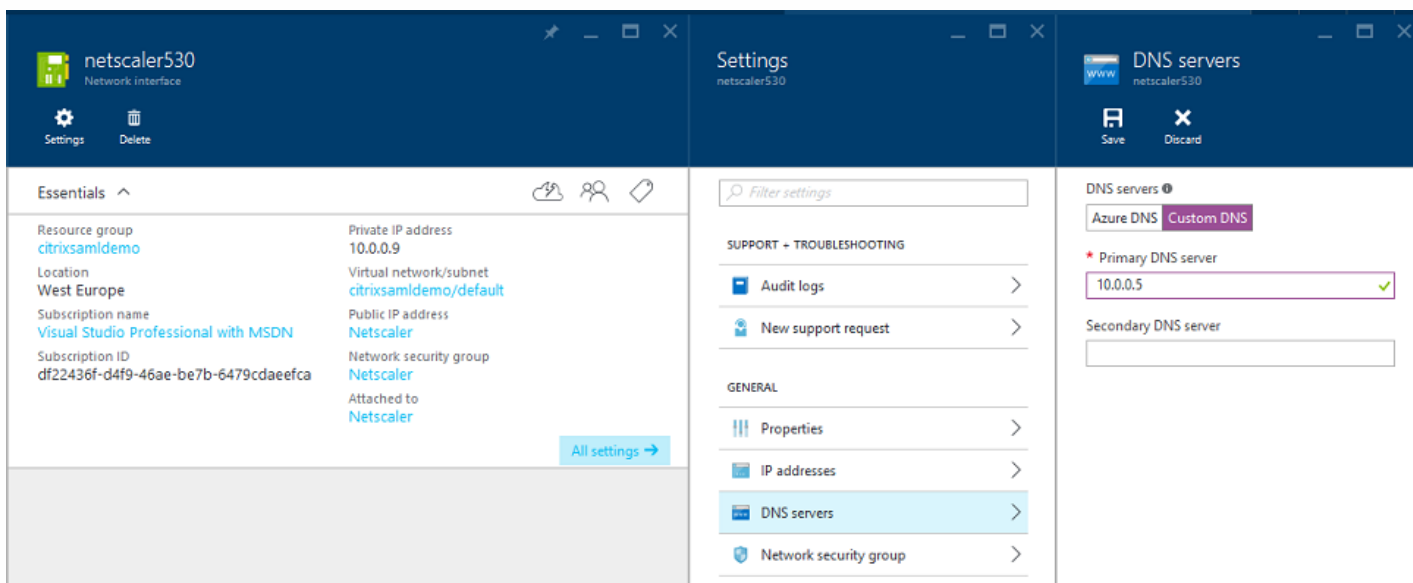
ドメインコントローラーのインストール後にDNSサーバーを構成し、citrixsamdemo.netの内部ビューを処理し、外部DNSサーバーに対してフォワーダーとして機能するように設定します（例：8.8.8.8）。



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。

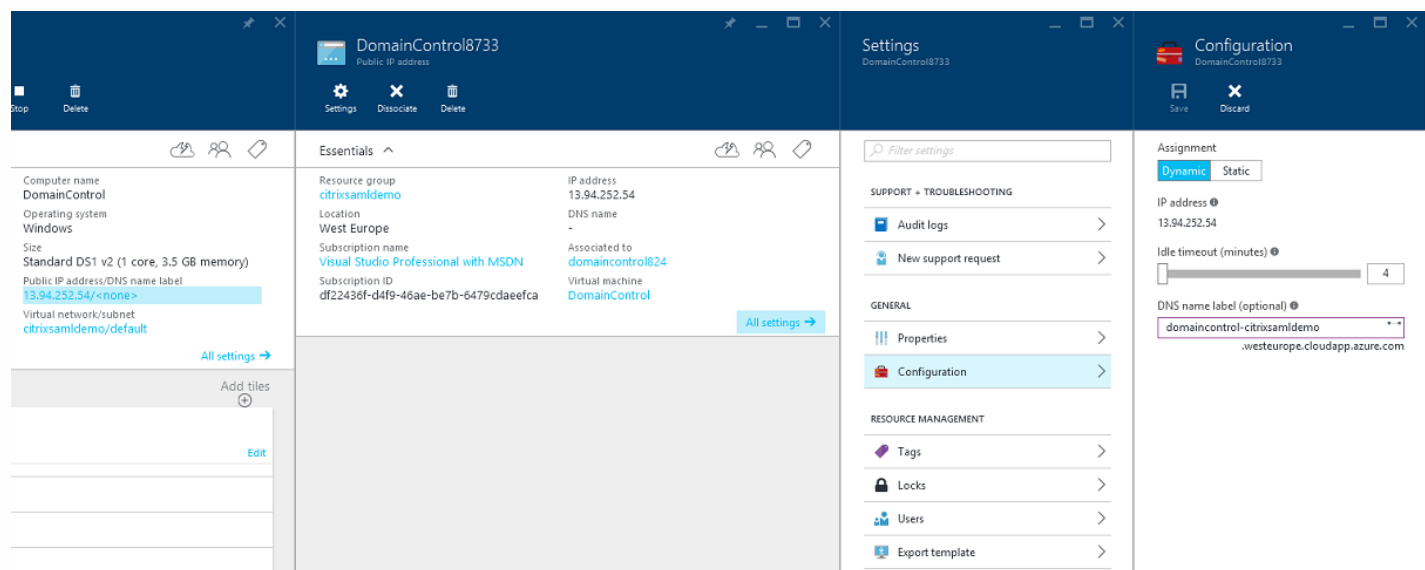


デフォルトでは、内部IP (10.0.0.9) アドレスは動的に割り当てられます。 IPアドレスの設定を使用して、IPアドレスを永続的に割り当てることができます。これは、Webアプリケーションプロキシサーバーとドメインコントローラーで実行する必要があります。

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

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。

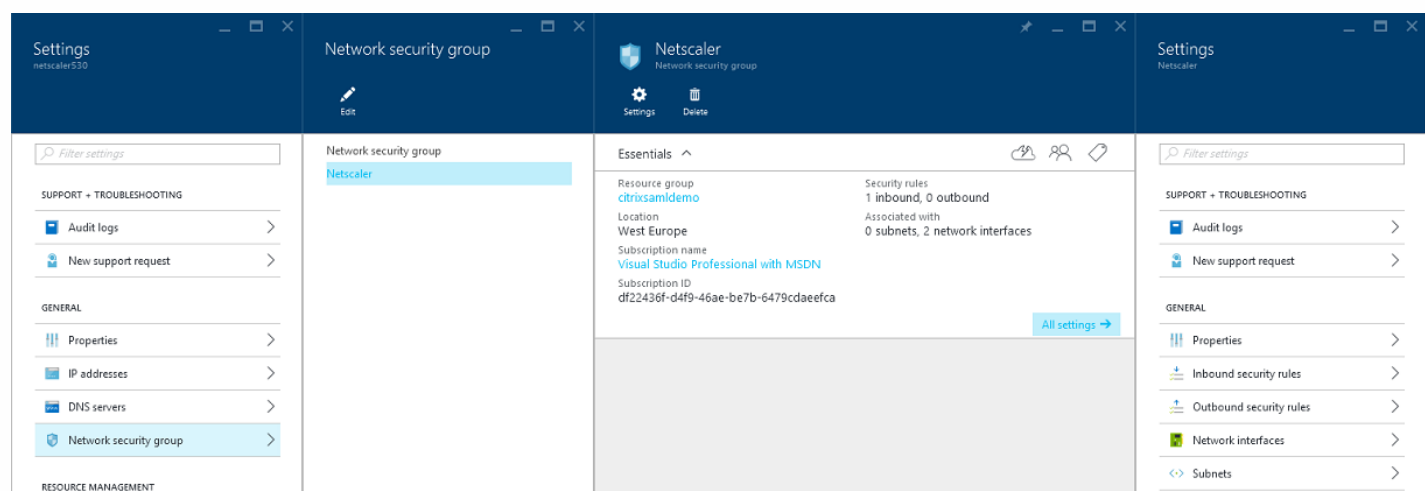


この例では、DNSアドレスdomaincontrol-citrixsaml-demo.westeurope.cloudapp.azure.comを、ドメインコントローラーに割り当てています。

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。

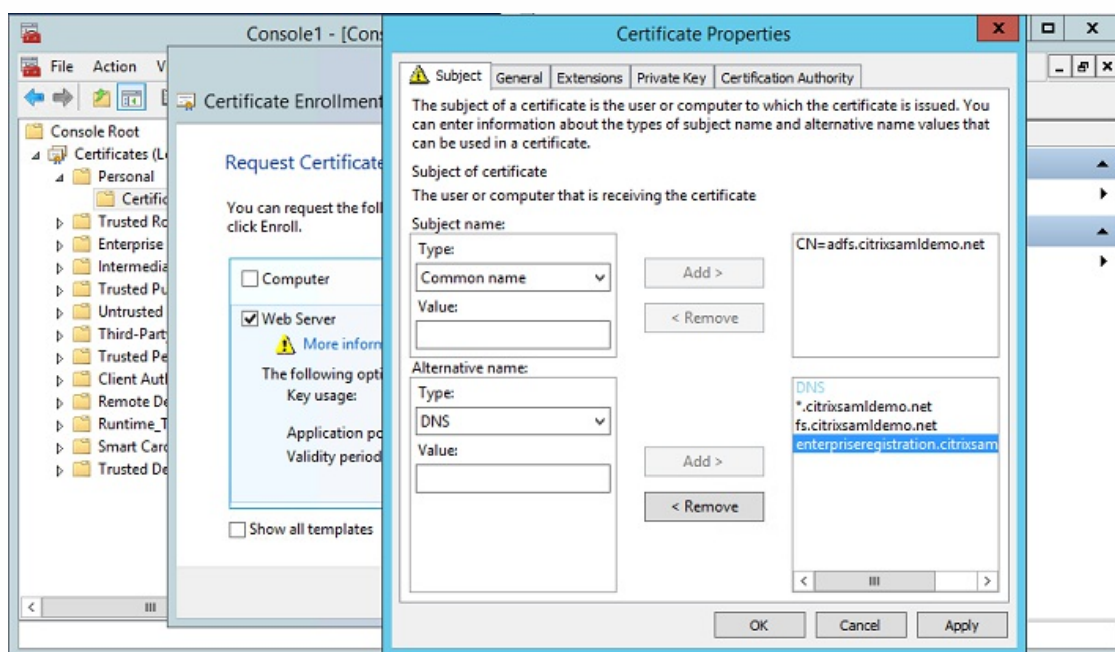


ADFS証明書の作成

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.citrixsaml demo.net [コンピューター名]
- SubjectAltname:
 - *.Citrixsaml demo.net [ゾーン名]
 - fs.citrixsaml demo.net [DNSのエントリ]
 - enterpriseregistration.citrixsaml demo.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インして、新しいディレクトリを作成します。

ADD DIRECTORY

DIRECTORY ?

Create new directory

NAME ?

CitrixSAMLdemo

DOMAIN NAME ?

citrixsaml demo .onmicrosoft.com

COUNTRY OR REGION ?

United Kingdom

PREVIEW

完了すると、概要ページが表示されます。

citrixsaml demo

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS LICENSES

Your directory is ready to use.
Here are a few options to get started.

☐ Skip Quick Start the next time I visit

I WANT TO Set Up Directory Manage Access Develop Applications

GET STARTED

- 1 Improve user sign-in experience**

Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.

Add domain
- 2 Integrate with your local directory**

Use the same user accounts and groups in the cloud that you already use on premises.

Download Azure AD Connect
- 3 Get Azure AD Premium**

Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.

Try it now

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インしてパスワードをセットアップします。

ADD USER

user profile

FIRST NAME
Azure

LAST NAME
Admin

DISPLAY NAME
Azure Admin

ROLE ?
Global Admin

ALTERNATE EMAIL ADDRESS

MULTI-FACTOR AUTHENTICATION ?
☐ Enable Multi-Factor Authentication

1 3

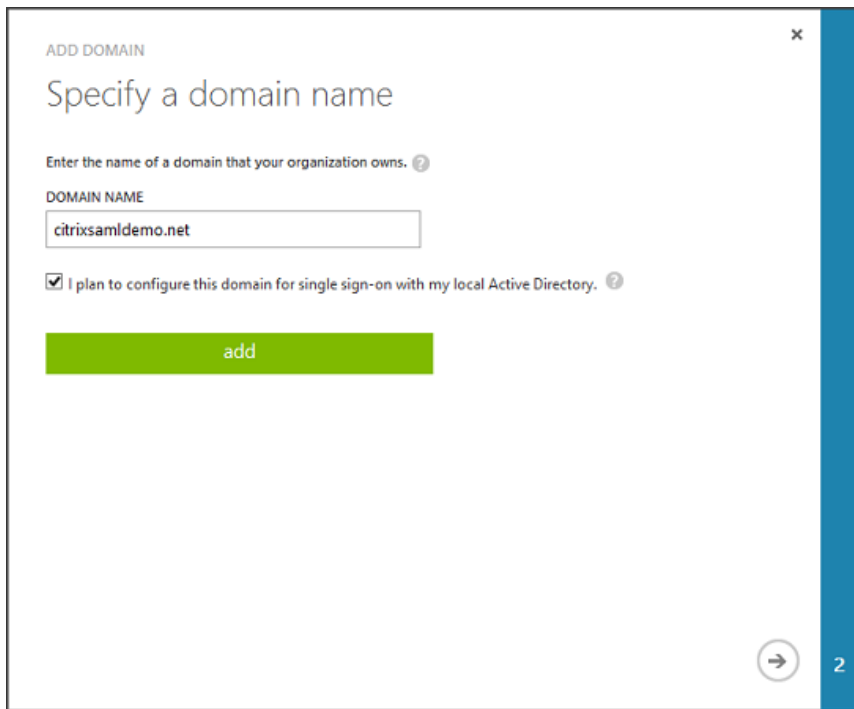
Azure ADを使用したドメインの登録

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citrixsaml demo.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。



ADD DOMAIN

Specify a domain name

Enter the name of a domain that your organization owns. ?

DOMAIN NAME

citrixsaml demo.net

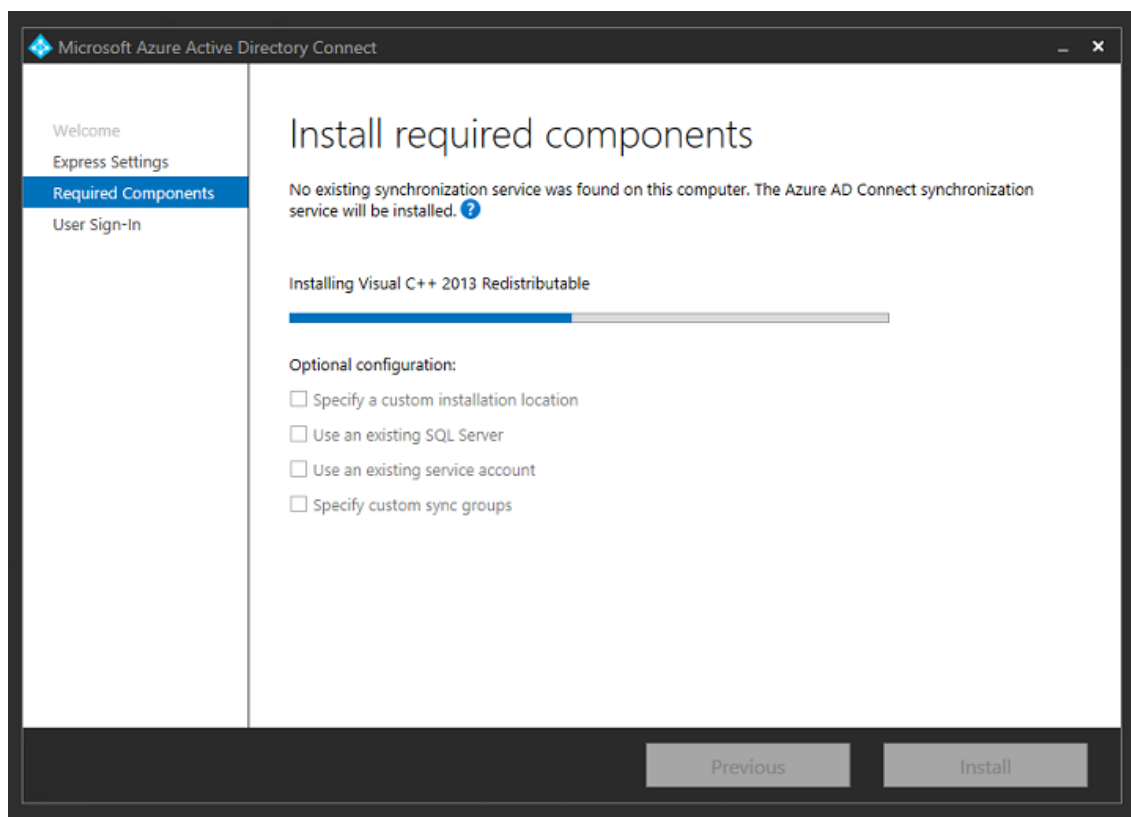
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

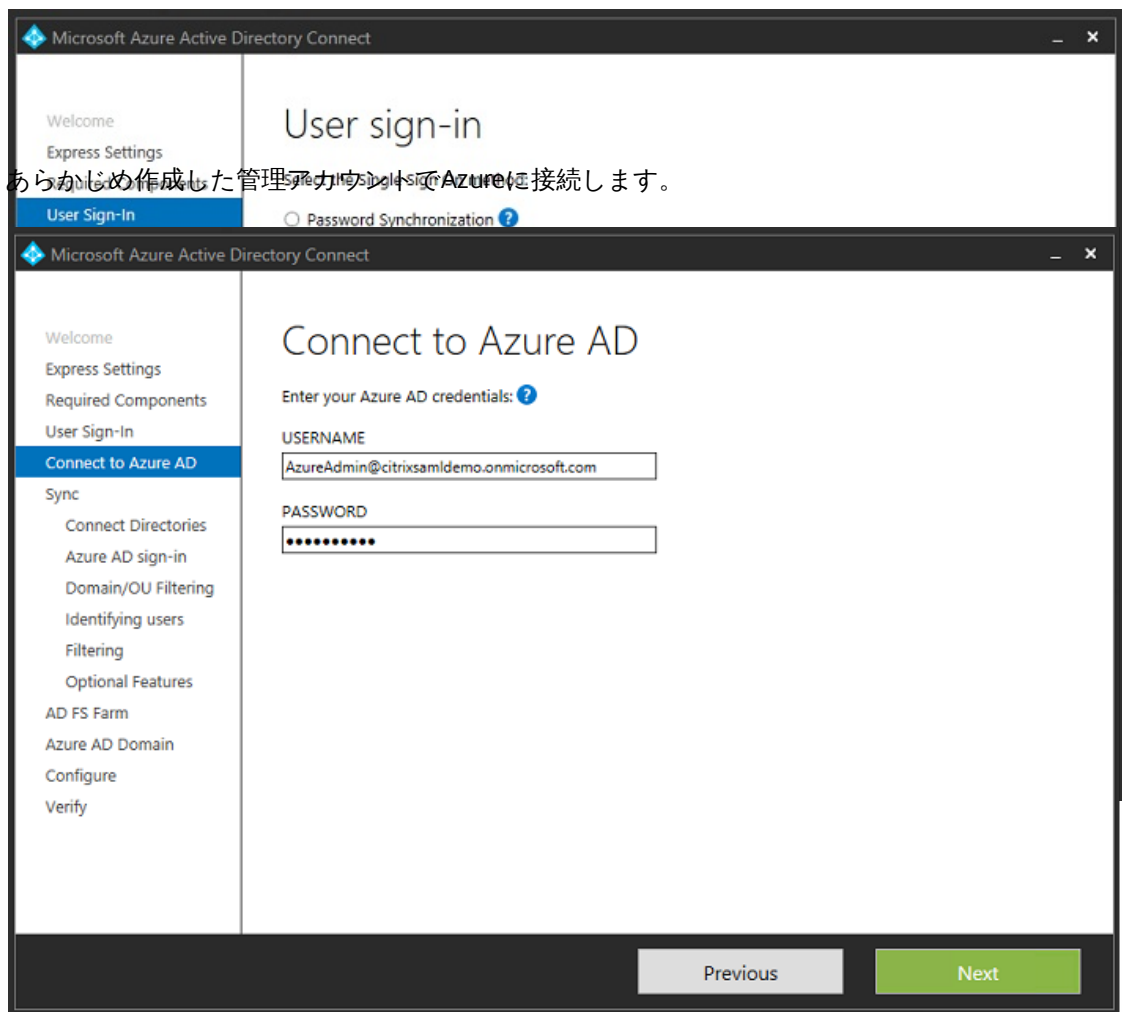
2

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。

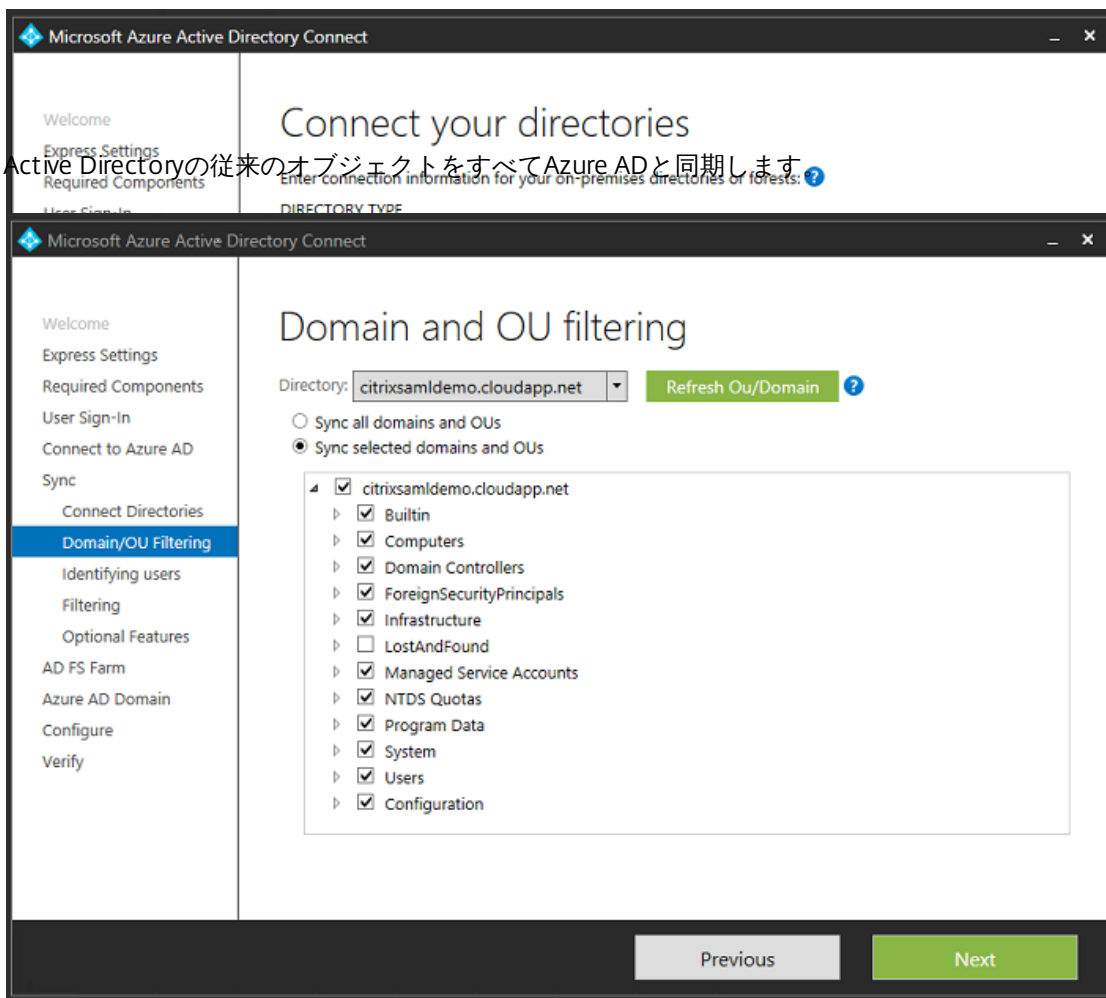


[AD FSとのフェデレーション] シングルサインオンオプションを選択します。



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。



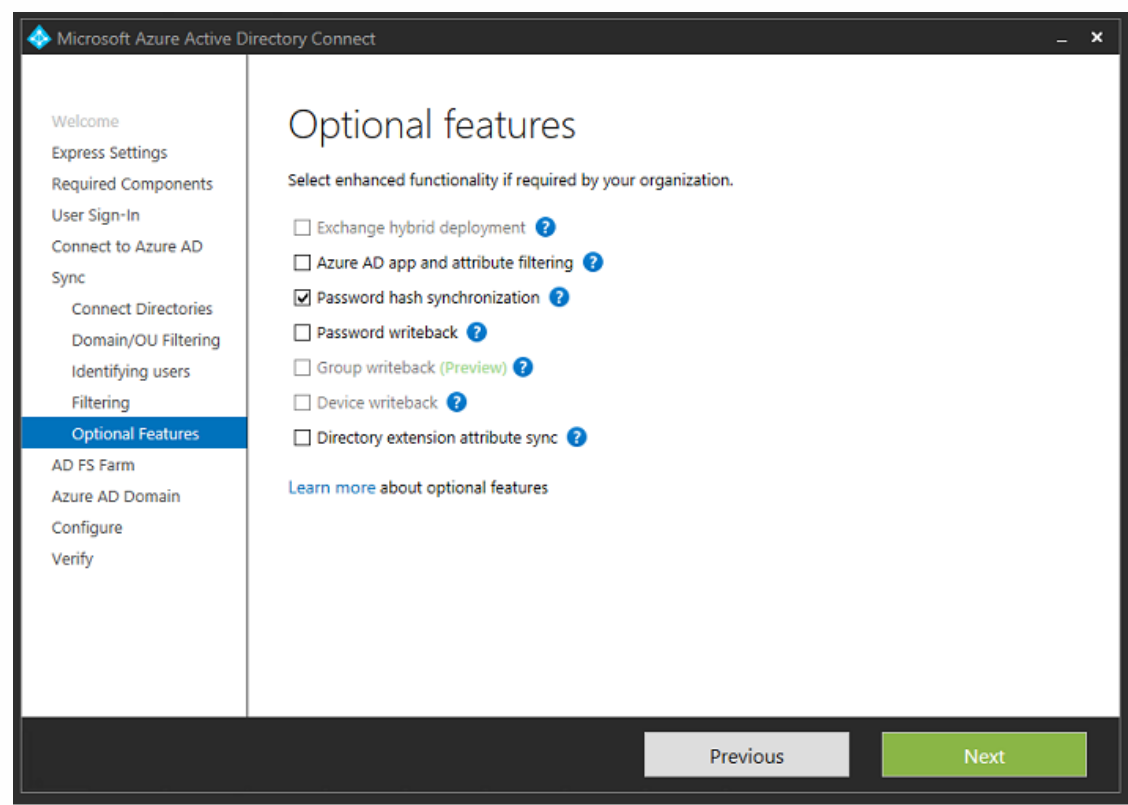
ディレクトリ構造がシンプルな場合は、ユーザー名の一意性に依存して、ログオンするユーザーを識別することができます。

The screenshot shows the 'Uniquely identifying your users' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with options: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, Identifying users (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area has the title 'Uniquely identifying your users' and a subtitle 'Select how users should be identified in your on-premises directories. ?'. There are two radio button options: 'Users are represented only once across all directories.' (selected) and 'User identities exist across multiple directories. Match using:'. Under the second option, there are three radio buttons: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', and 'SAMAccountName and MailNickName attributes'. Below these is a 'CUSTOM ATTRIBUTE' section with a text input field and a dropdown arrow. Further down, it says 'Select how users should be identified with Azure AD.' followed by 'SOURCE ANCHOR ?' with a dropdown menu showing 'objectGUID'. Below that is 'USER PRINCIPAL NAME ?' with a dropdown menu showing 'userPrincipalName'. At the bottom, there are 'Previous' and 'Next' buttons.

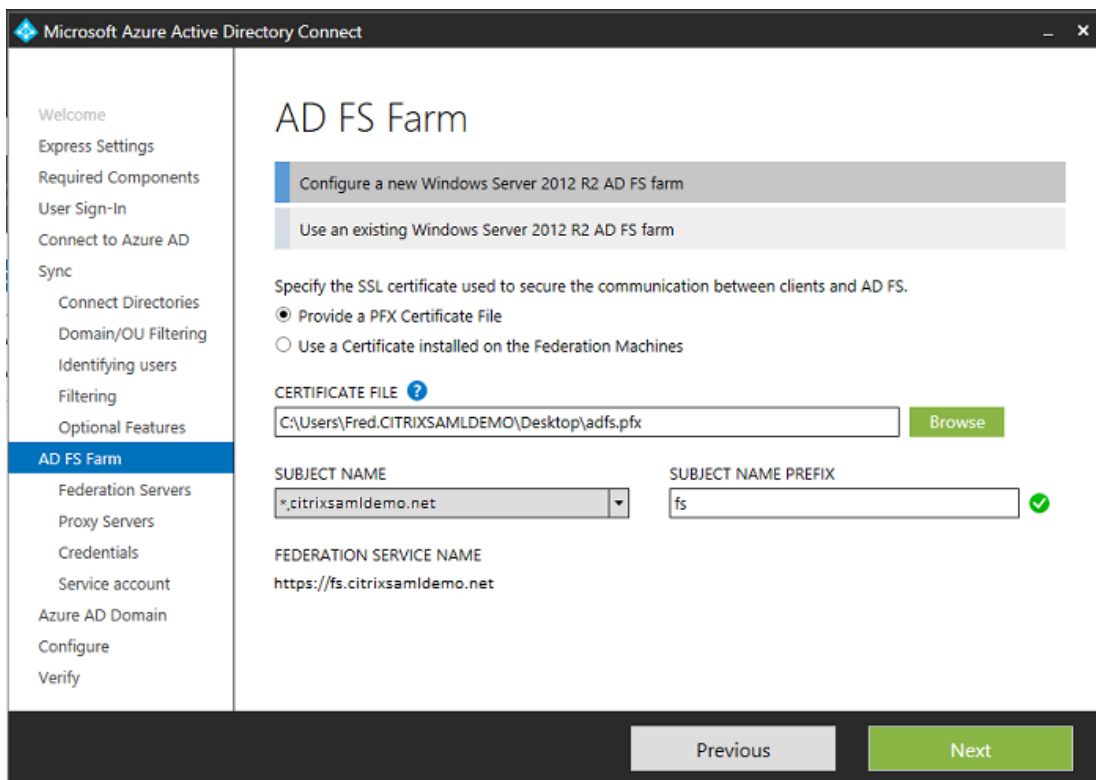
デフォルトのフィルタリングオプションを使用するか、あるいはユーザーとデバイスを特定のグループセットに制限します。

The screenshot shows the 'Filter users and devices' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar is the same as the previous screen, with 'Filtering' highlighted. The main content area has the title 'Filter users and devices' and a subtitle 'For a pilot deployment, specify a group containing your users and devices that will be synchronized.' There are two radio button options: 'Synchronize all users and devices' (selected) and 'Synchronize selected ?'. Below these is a 'FOREST' field with the value 'citrixsaml demo.cloudapp.net' and a 'GROUP' field with a placeholder 'Enter a name or DN of a group'. A 'Resolve' button is next to the GROUP field. At the bottom, there are 'Previous' and 'Next' buttons.

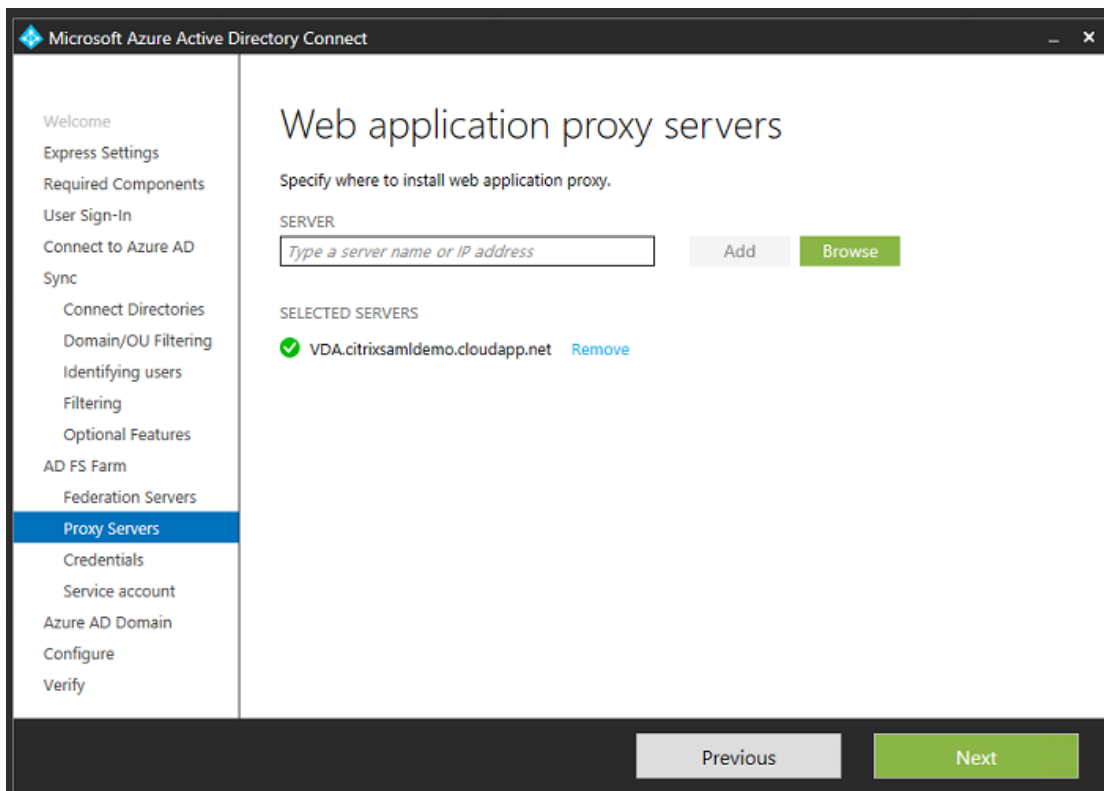
必要に応じて、Azure ADパスワードをActive Directoryと同期することができます。これは、通常、ADFSベースの認証では必要ありません。



証明書のPFXファイルをAD FSで使用するようを選択します。DNS名としてfs.citrixsamldemo.netを指定します。

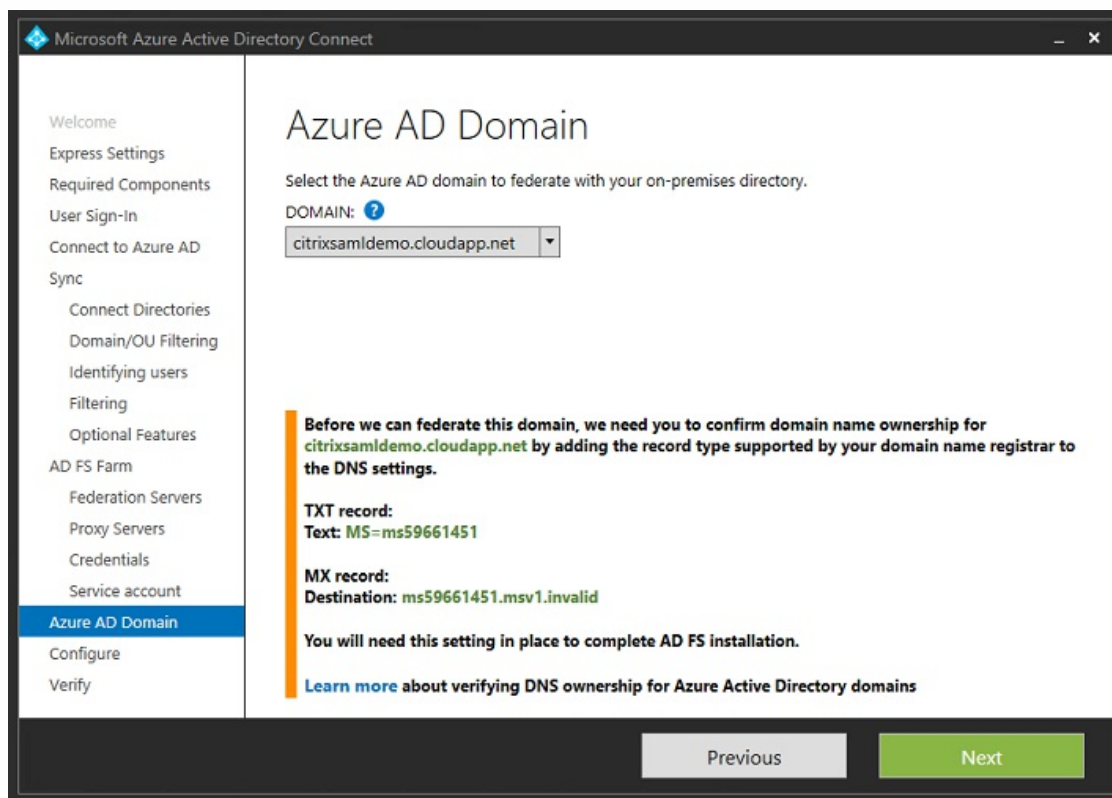


プロキシサーバーの選択を求める画面が表示されたら、wap.citrixsaml demo.netサーバーのアドレスを入力します。 Azure AD Connectが構成できるよう、Webアプリケーションプロキシサーバーの管理者として**Enable-PSRemoting -Force**コマンドレットを実行する必要がある場合があります。



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。

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。

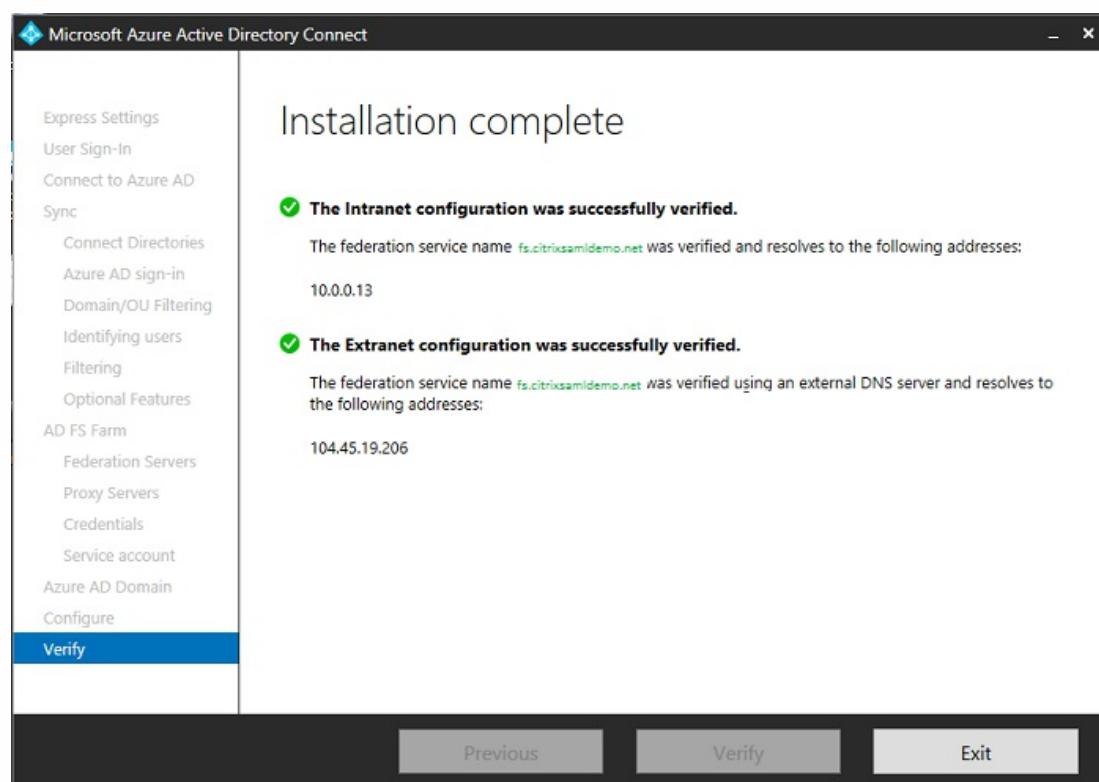
Search record sets			
NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info. ...
@	SOA	3600	Email: azuredns-hostmaster.microsoft... Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 ... Expire: 2419200 Minimum TTL: 300
Azure管理コンソールで[検証]をクリックします。 ...			

CitrixSamlDemo

DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN
citrixsaml demo.onmicrosoft.com	Basic	Active	Not Available	Yes
citrixsaml demo.net	Custom	Unverified	Not Configured	No

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.citrixsaml demo.netがポート443で接続されます。

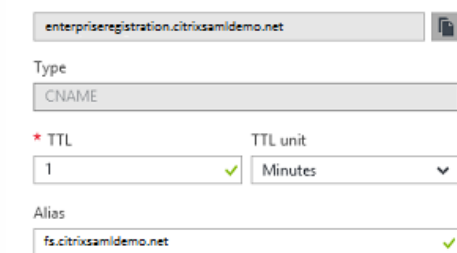


Azure ADへの参加の有効化

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

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.citrixsaml demo.netです。



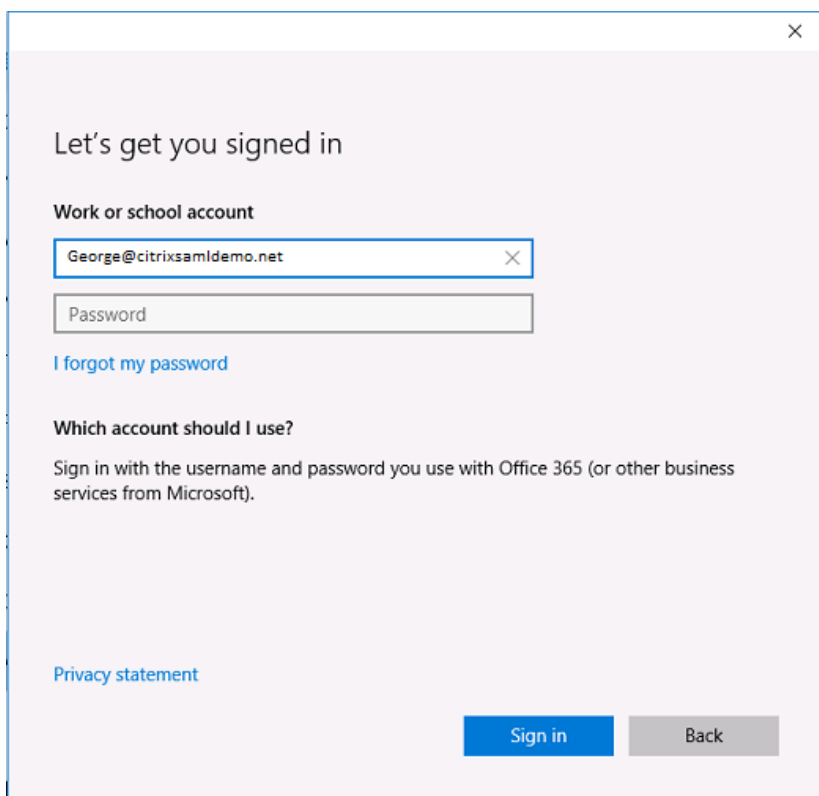
enterpriseregistration.citrixsaml demo.net

Type
CNAME

* TTL TTL unit
1 Minutes

Alias
fs.citrixsaml demo.net

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。



Let's get you signed in

Work or school account

George@citrixsaml demo.net

Password

[I forgot my password](#)

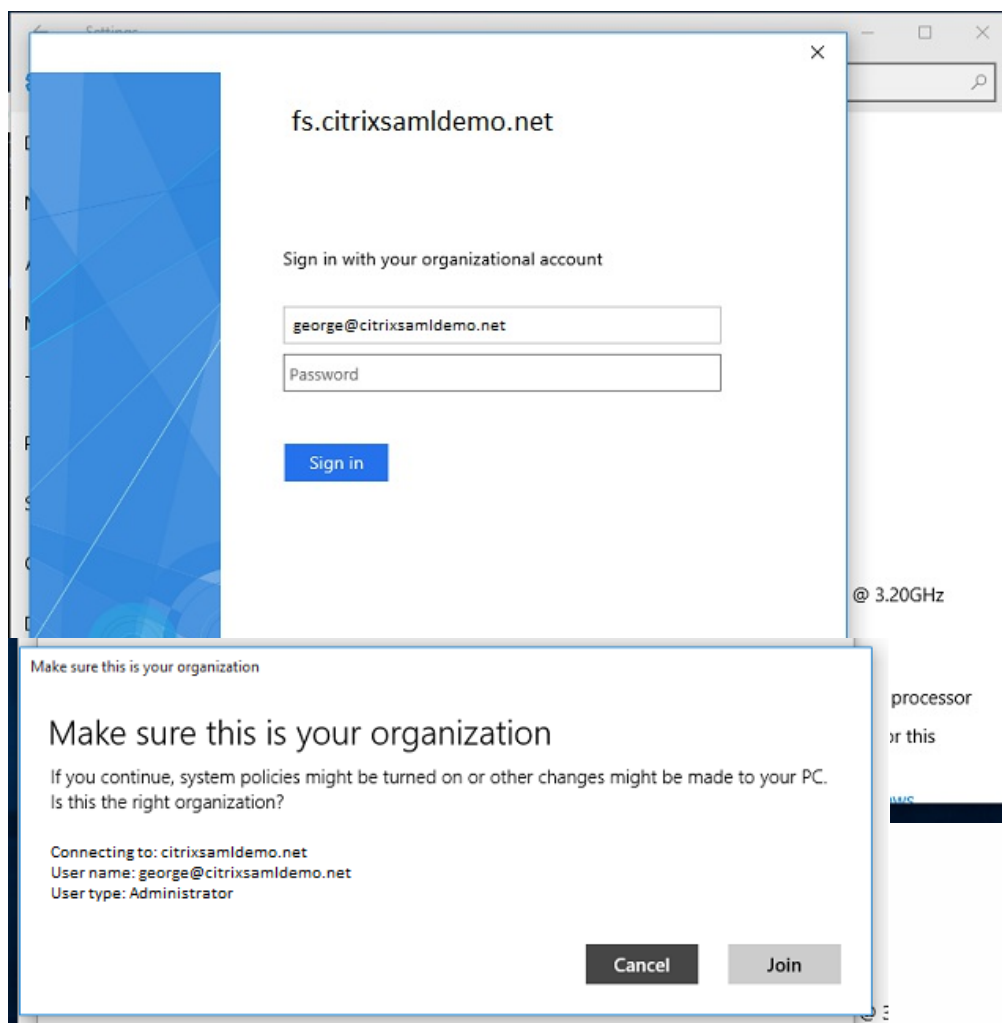
Which account should I use?

Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in Back

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。

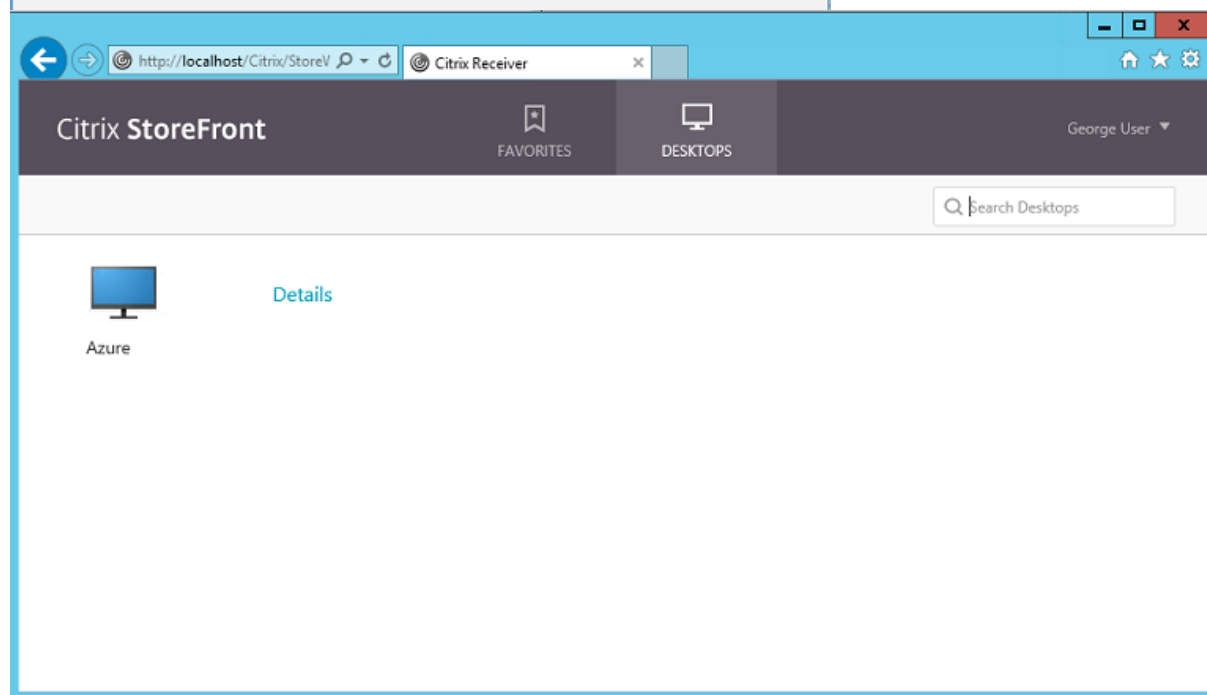


Microsoft Edgeを使用してマシンの再起動とログオンを行い、Azure ADへの参加が正常に行われたことを検証します。ログオンするとMicrosoft Edgeが起動して<http://myapps.microsoft.com>に接続します。このWebサイトでは、シングルサインオンが自動的に使用されます。
Your device has now been joined to your organisation in Azure AD.

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。

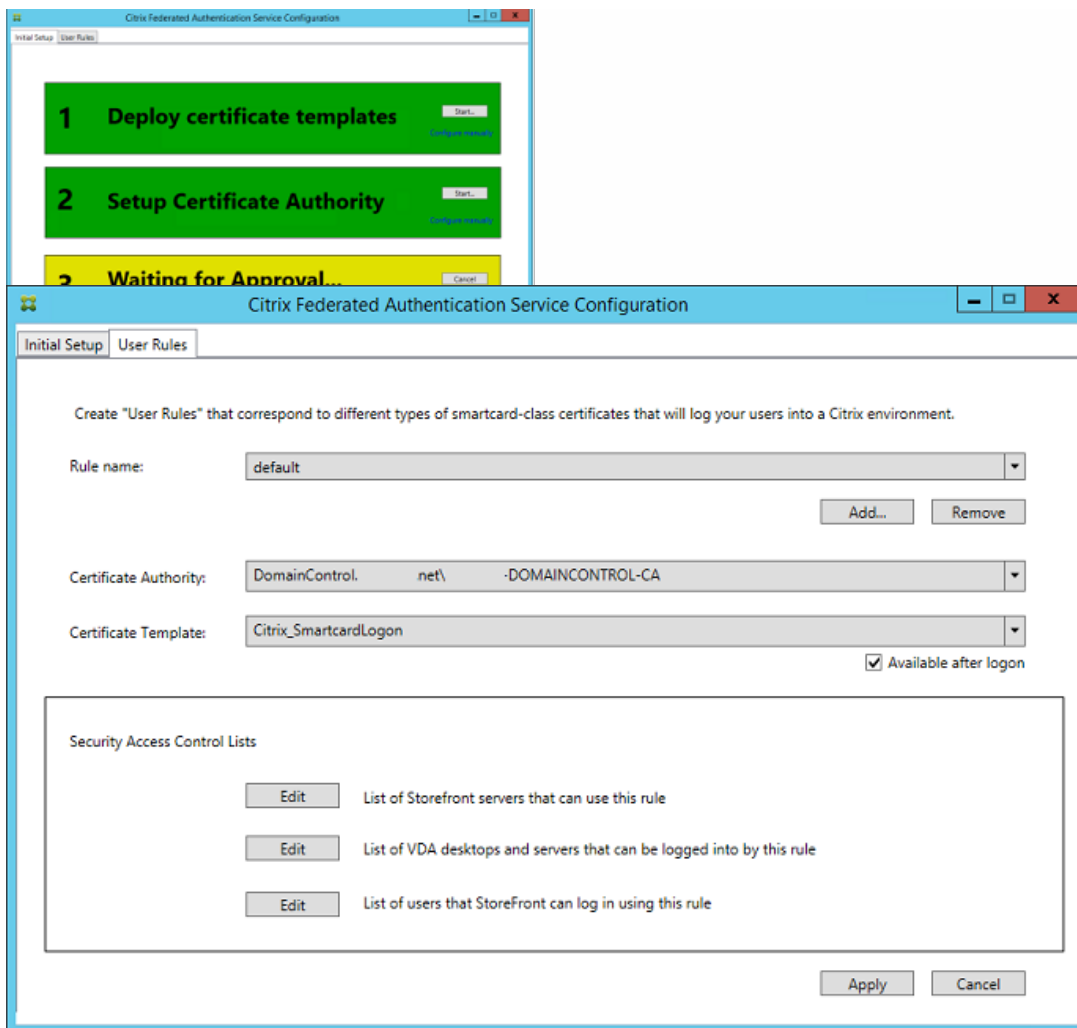
この例では、StoreFrontはDelivery Controllerと同じサーバーにインストールされています。VDAはスタンドアロンのWindows 2012 R2用RDSワーカーとしてインストールされ、Machine Creation Servicesとは統合していません（ただしオプションで構成することができます）。作業を続行する前に、ユーザーGeorge@citrixsamldemo.netがパスワードで認証できることを確認します。



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。

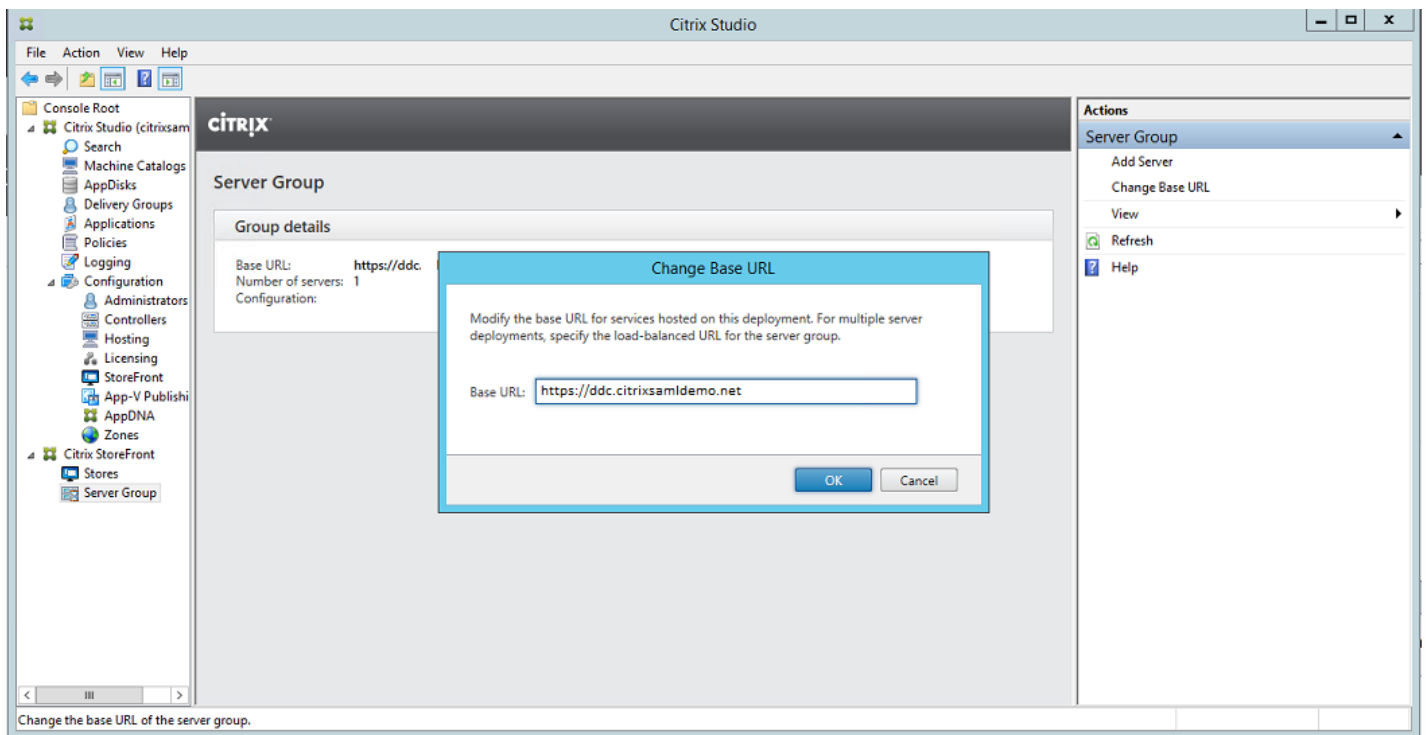
Federated Authentication Serviceのインストール

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。

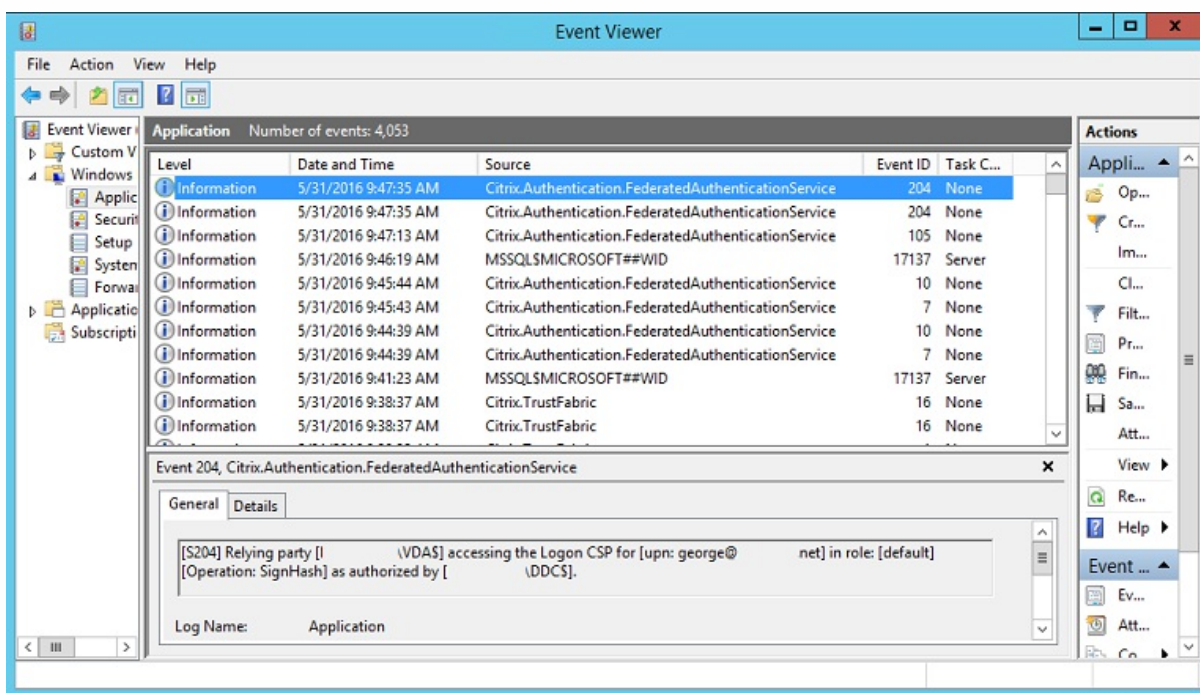


StoreFrontの構成

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。

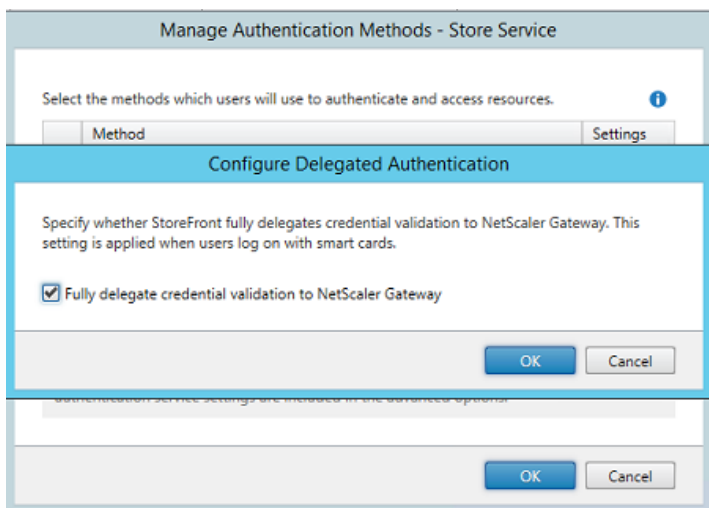


StoreFrontでFASサーバーが使用されるように構成し（「[Federated Authentication Service](#)」のPowerShellスクリプトを使用します）、Azure内で内部テストを行います。FASサーバーのイベントビューアーをチェックして、ログオンにFASが使用されることを確認します。

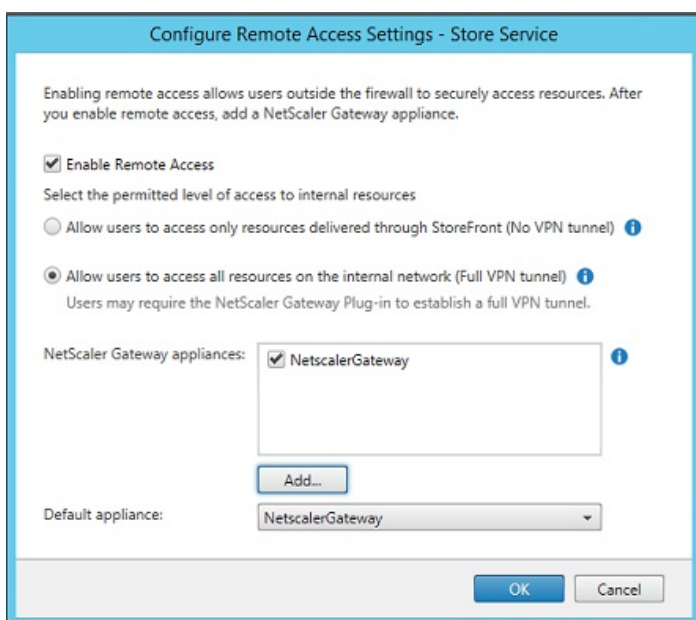


StoreFrontがNetScalerを使用するように構成

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。

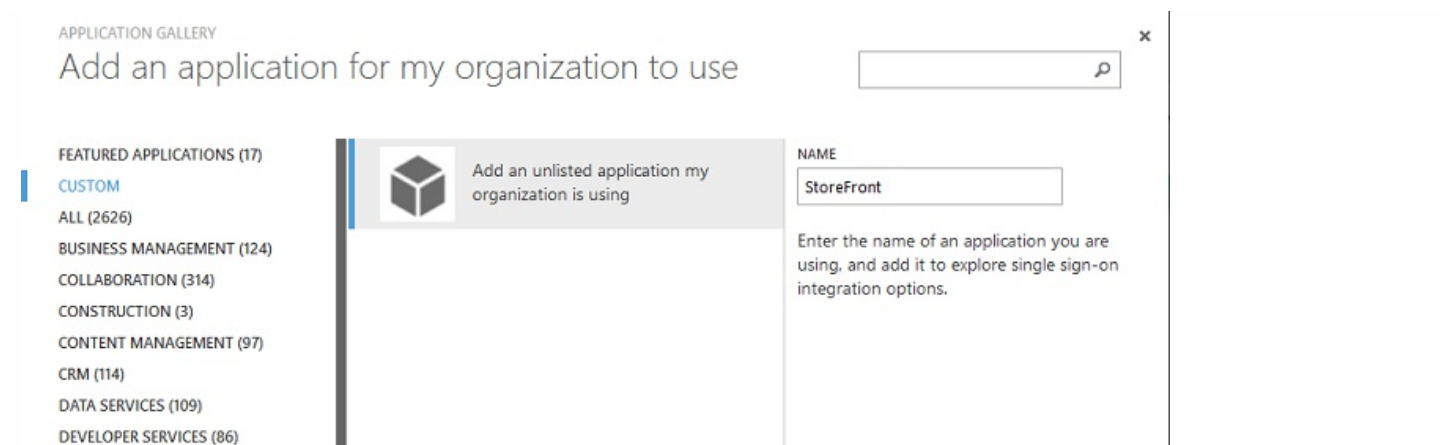


NetScaler認証オプションを統合するには、Secure Ticket Authority (STA) の構成およびNetScaler Gatewayアドレスの構成を行います。



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。



【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。

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。

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to StoreFront?

- ☒ **Microsoft Azure AD Single Sign-On**
Establish federation between Microsoft Azure AD and StoreFront
[Learn more](#)
- ☐ **Password Single Sign-On**
Microsoft Azure AD stores account credentials for users to sign on to StoreFront
[Learn more](#)
- ☐ **Existing Single Sign-On**
Configures Microsoft Azure AD to support single sign-on to StoreFront using Active Directory Federation Services or another third-party single sign-on provider.
[Learn more](#)

[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。

CONFIGURE SINGLE SIGN-ON

Configure App Settings

Enter the settings of AzureStoreFront application below. [Learn more](#)

IDENTIFIER

REPLY URL

☐ Show advanced settings (optional).☐ Configure the certificate used for federated single sign-on (optional).

CONFIGURE SINGLE SIGN-ON

Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

1. The following certificate will be used for federated single sign-on:
Thumbprint: 8D1E02EBF7C111EDD8BD325F526053BA9626A73B
Expiry: 05/31/2018 11:06:20 UTC

Download Certificate (Base 64 - most common)

Download Certificate (Raw)

Download Metadata (XML)

2. Configure the certificate and values in AzureStoreFront

ISSUER URL
`https://sts.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e/`

SINGLE SIGN-ON SERVICE URL
`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

SAML SERVICE URL
`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working

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。

storefront

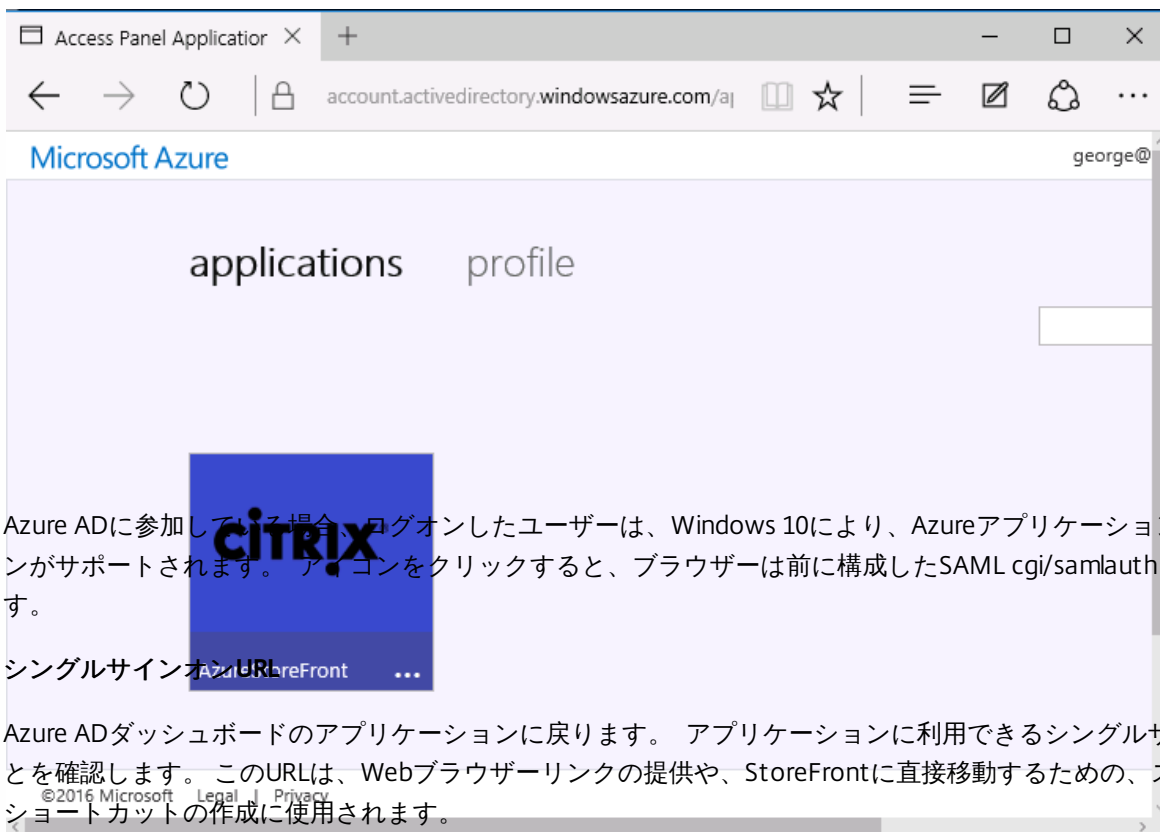
[DASHBOARD](#) [USERS AND GROUPS](#) [ATTRIBUTES](#) [CONFIGURE](#)

SHOW All Users

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Azure Admin	AzureAdmin@citrixsamld..			No	Unassigned	
George User	george@citrixsamldemo.net			No	Unassigned	
On-Premises Directory Sy...	Sync_ADFS_21a7e8060dcf...			No	Unassigned	

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。



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。

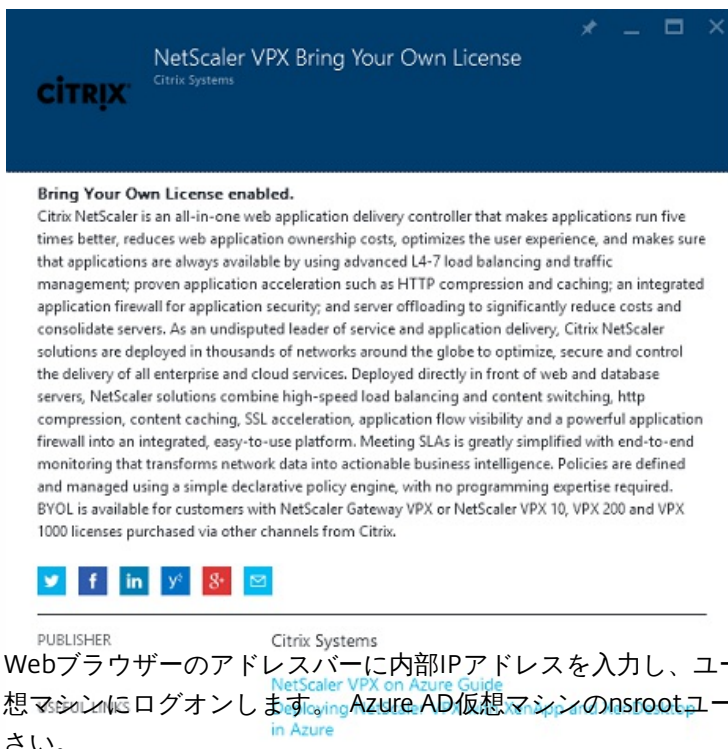
シングルサインオンURL

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。（その他のユーザーには、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。



Webブラウザ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。

XenApp/XenDesktop Setup Wizard

What is your deployment



What is your Citrix Integration Point?

StoreFront

Continue

Cancel

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。

NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

Virtual Server Name*

ns.citrixsamldemo.net

☐ Redirect requests from port 80 to secure port

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。

Server Certificate

Certificate Format*

pem

Certificate File*

ns.citrixsamldemo.net

☒ Private key is password protected

Private key password

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。

Primary authentication method*

Active Directory/LDAP

IP Address*

Load Balancing

Port*

389

StoreFront

StoreFront FQDN*

ddc.citrixsamldemo.net

Site Path*

/Citrix/StoreWeb

Single Sign-on Domain*

citrixsamldemo

Store Name*

/Citrix/StoreWeb

Secure Ticket Authority Server*

http://ddc.citrixsamldemo.net/sta

StoreFront Server*

10 . 0 . 0 . 15

Protocol*

SSL

Port*

443

Load Balancing

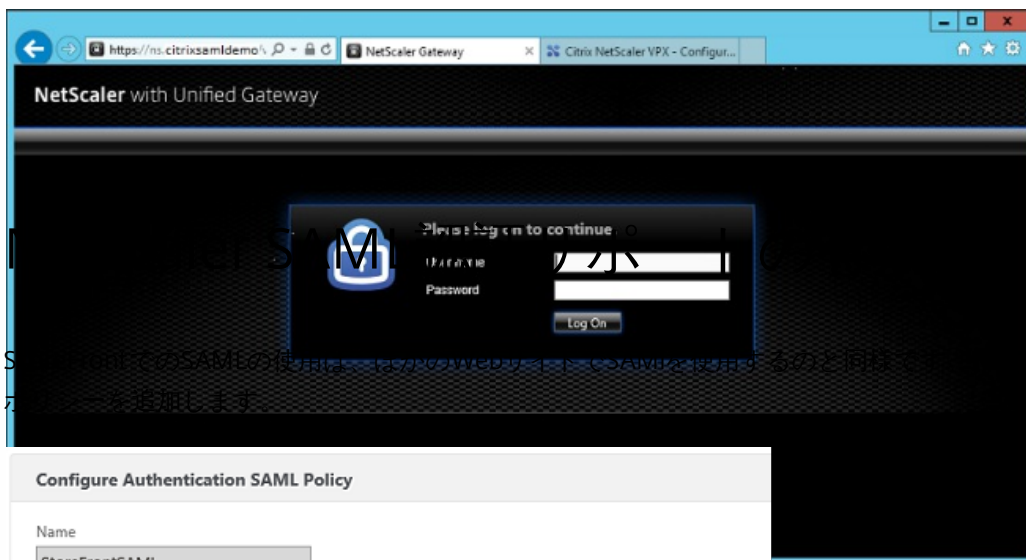
Continue Cancel

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。



Configure Authentication SAML Policy

Name
StoreFrontSAML

Authentication Type
SAML

Server*
AzureAd

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
NS_TRUE

OK Close

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。

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

Redirect URL
29f14c20-9826-14d5e484c62e/saml2

Single Logout URL
29f14c20-9826-14d5e484c62e/saml2

User Field
userprincipalname

Session Certificate Name
[]

5

Two Factor
☐ ON ☒ OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*

Authentication Class Types
InternetProtocol
InternetProtocolPassword

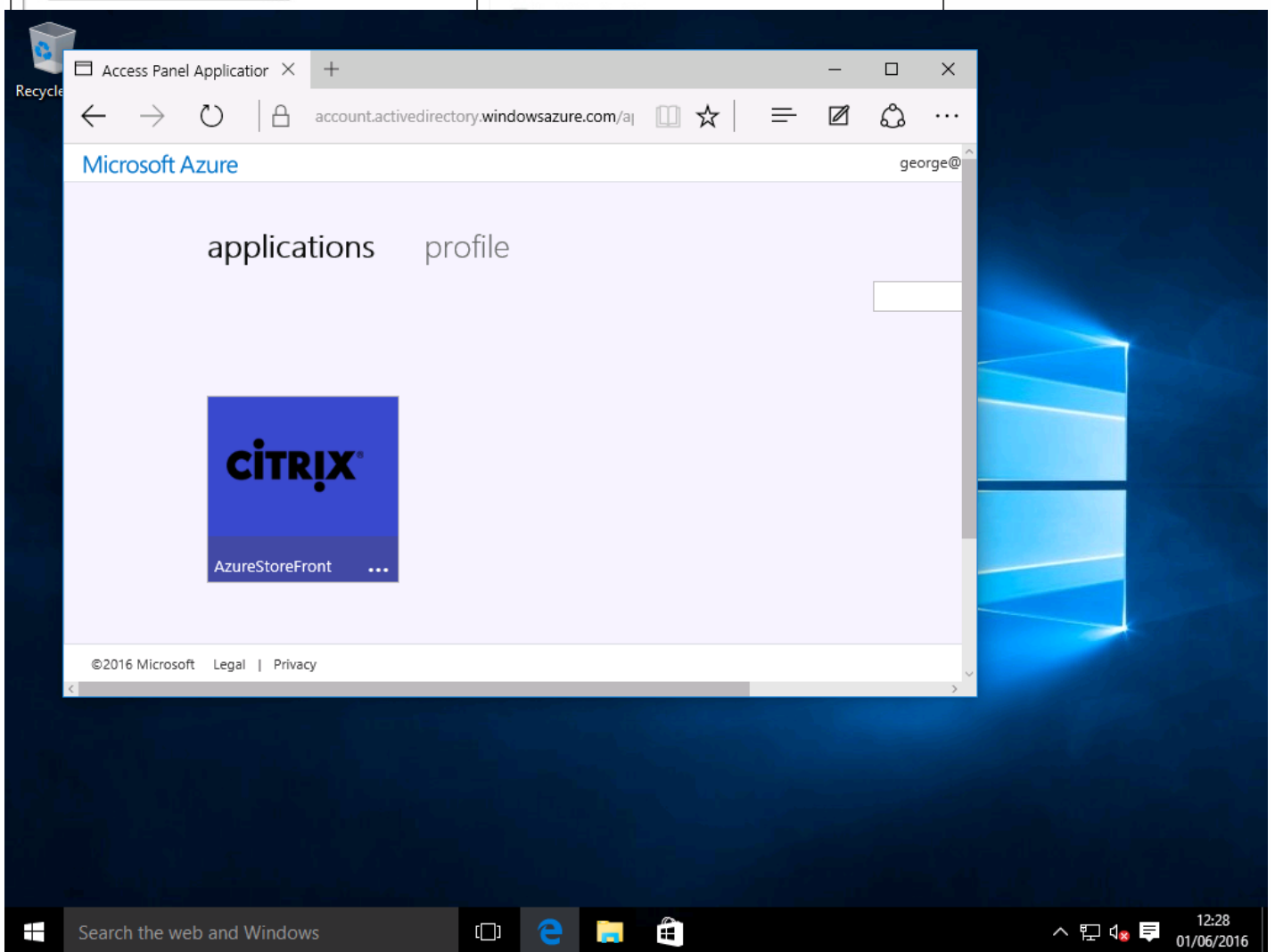
Signature Algorithm
[]

Digest Method*
☐ SHA1 ☒ SHA256

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。

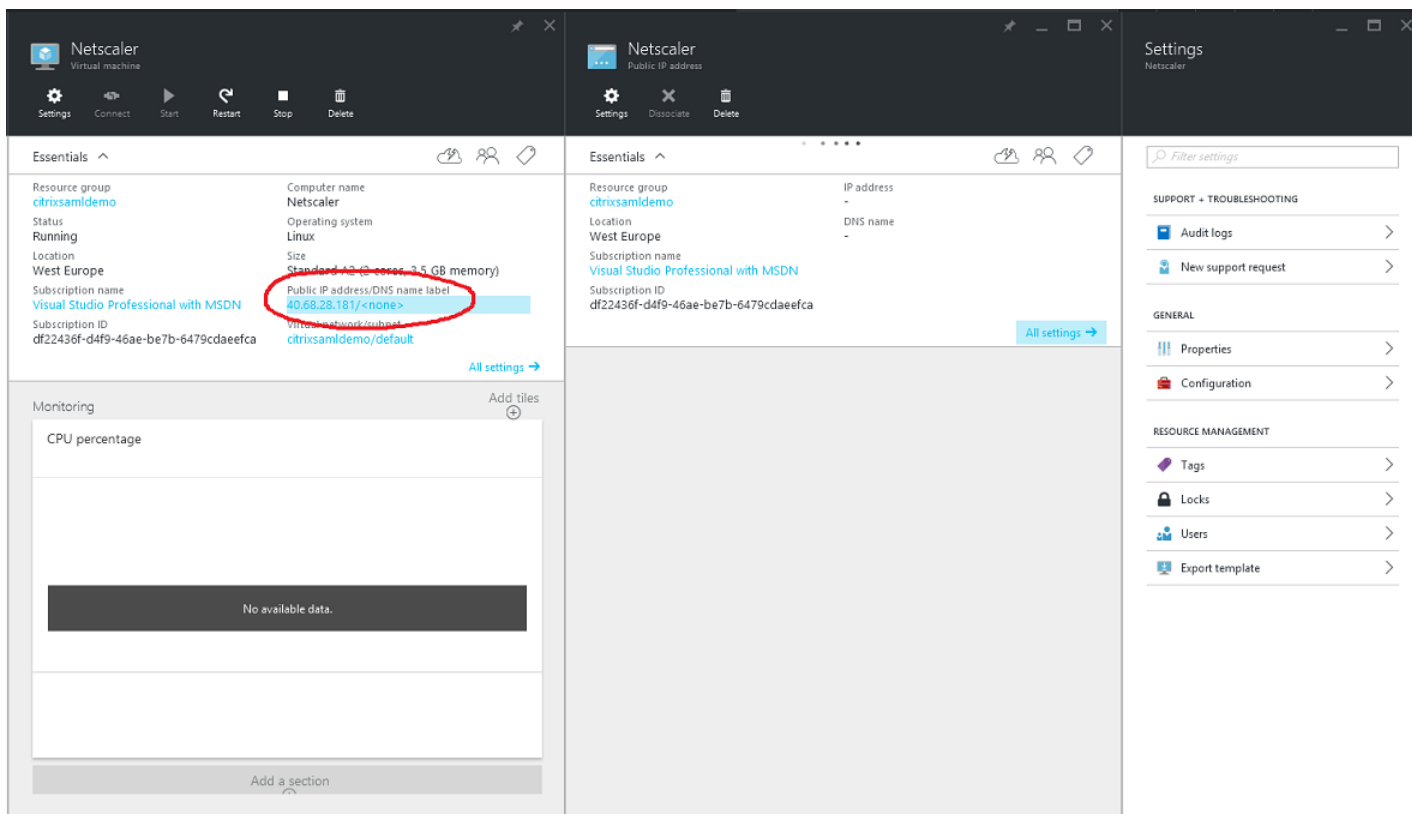
最後に、Azure ADに参加していないマシンも同じURLで動作することを確認します（ただし、最初の接続時に、Azure ADへの明示的なサインオンが1回行われます）。

付録

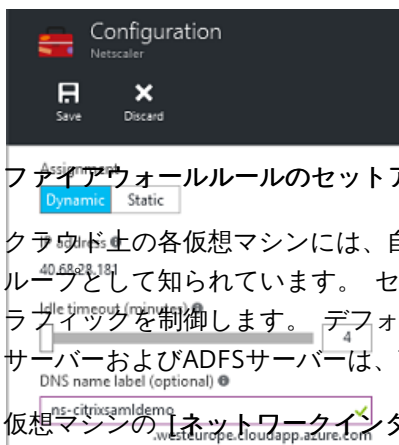
Azureで仮想マシンをセットアップする場合は、構成に必要な標準オプションがいくつかあります。

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。



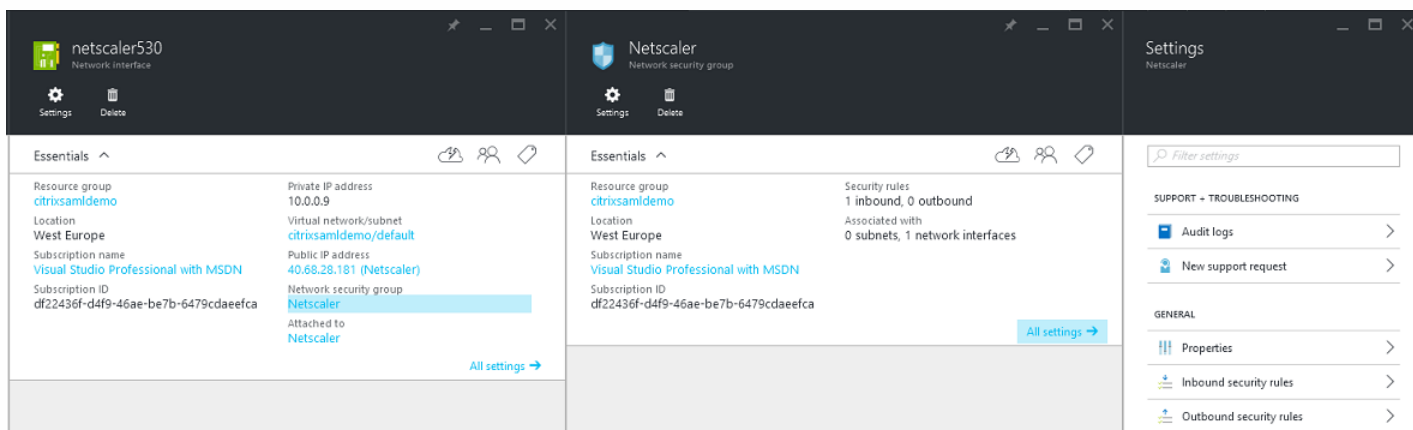
[パブリックIPアドレス/DNS名] ラベルの [構成] を選択します。 仮想マシンのパブリックDNSアドレスを選択します。 これは、ほかのDNSゾーンファイルでのCNAME参照に使用でき、IPアドレスが再割り当てされた場合も、すべてのDNSレコードが正しく仮想マシンをポイントするようにします。



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。

Federated Authentication Systemの方法：構成と管理

Aug 26, 2016

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他の記事へのリンクを掲載しています。

Federated Authentication Serviceの証明機関の設定

Jul 15, 2016

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。

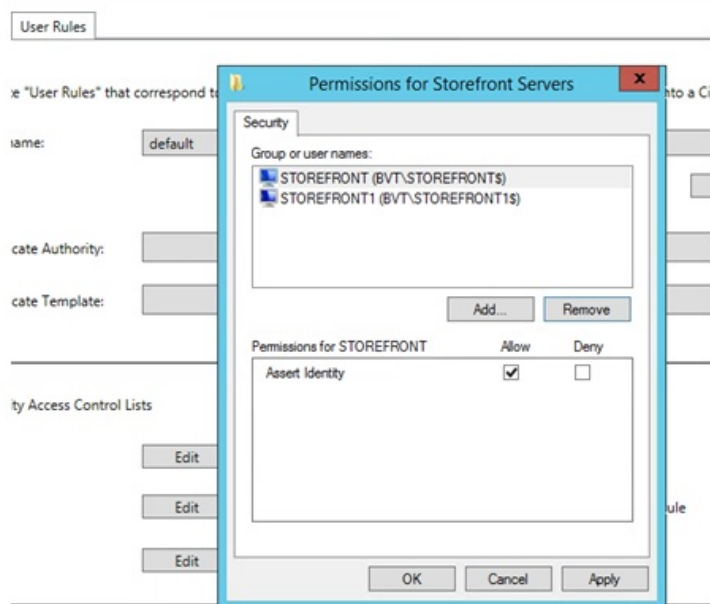
手順1：FASが検出できるCAサーバーの数の確認

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SDI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。



証明機関フィールドに複数のCAを追加（これはこのリリースで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

Certificate Authority:	DC1.bvt.local\bvt-DC1-CA	▼
Certificate Template:	Citrix_SmartcardLogon	▼
☒ Available after logon		

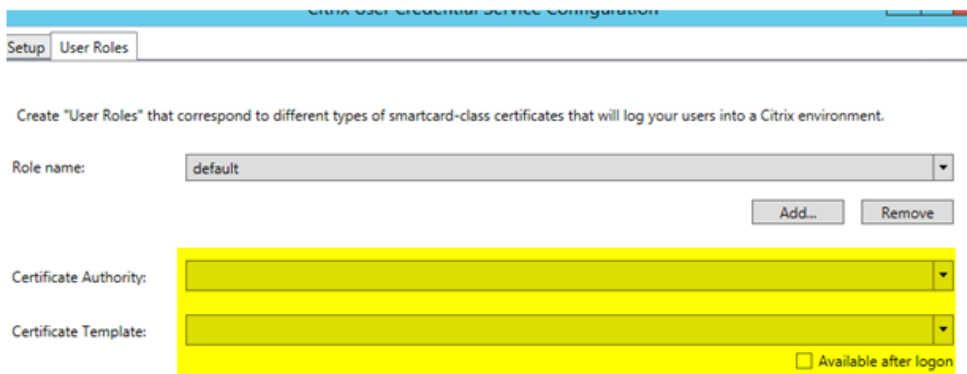
証明書定義の名前が特定できたら、証明書定義を変更してCertificateAuthoritiesが1つではなく一覧で含まれるようにします。

```
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。

```
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。



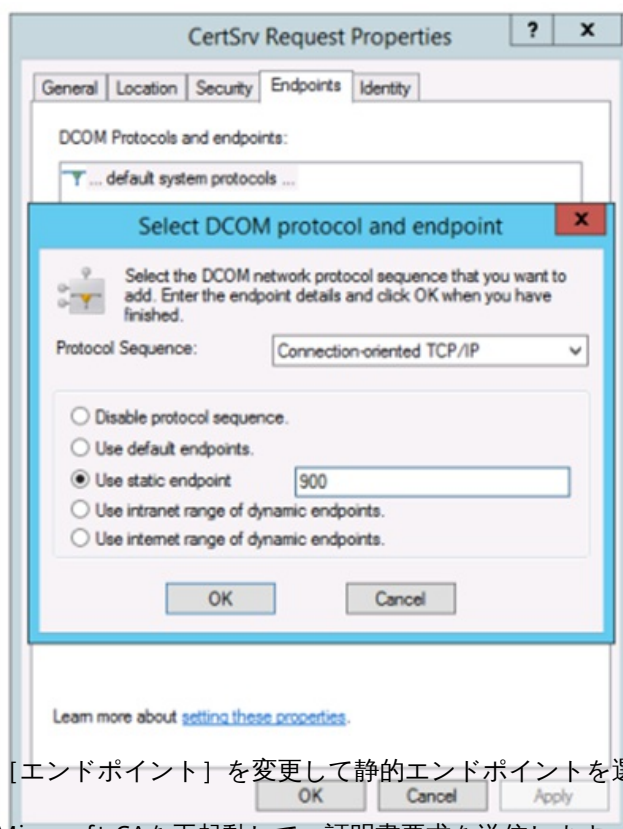
機能としては、FASに問題はありません。管理コンソールを使用してアクセス規則を変更する場合は、手順2を繰り返してすべての証明機関を表示します。

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。



「[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、certsrvがポート900をリスニング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。

Import-Module ActiveDirectory

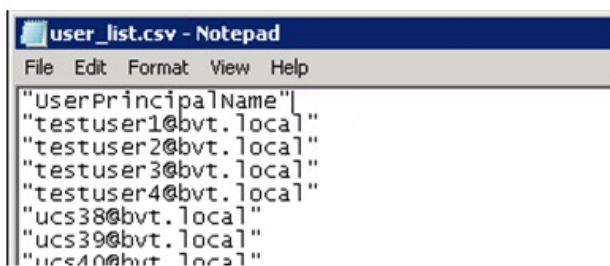
```
$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase -ne "") {
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
    UserPrincipalName | Select UserPrincipalName | Export-Csv -NoTypeInfoInformation -Encoding utf8 -delimiter ","
    $filename
} else {
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -Properties UserPrincipalName
    | Select UserPrincipalName | Export-Csv -NoTypeInfoInformation -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「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。

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 -UserPrincipalName $user.UserPrincipalName
```

```
    if ( $server.Server -ne $NULL ) {
```

```
        New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -  
CertificateDefinition $rule"_Definition" -Rule $rule
```

```
    }
```

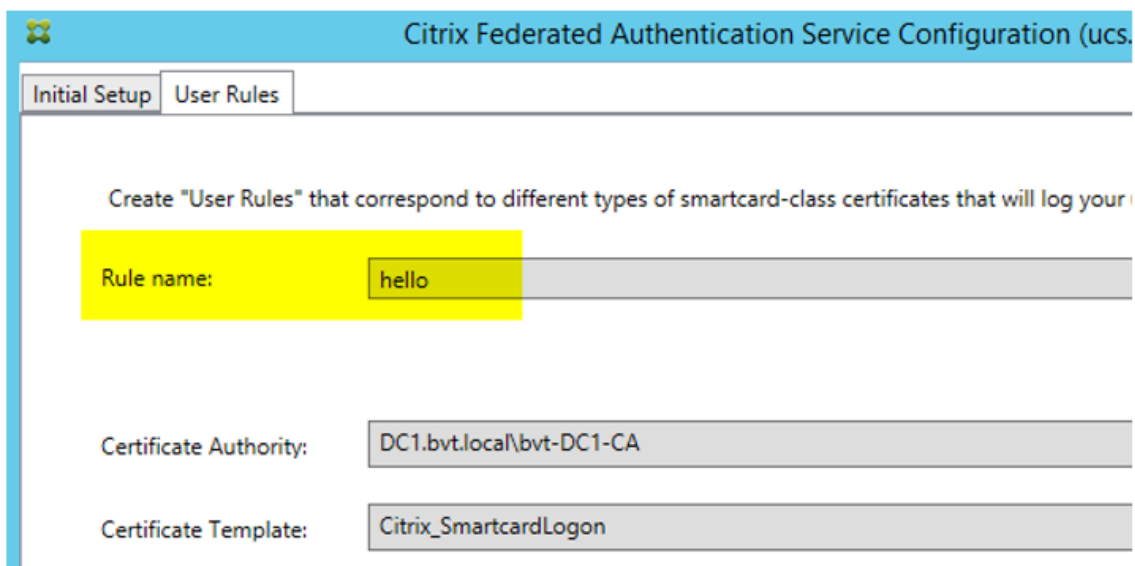
```
    if ( $server.Failover -ne $NULL ) {
```

```
        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。



Citrix Federated Authentication Service Configuration (ucs)

Initial Setup User Rules

Create "User Rules" that correspond to different types of smartcard-class certificates that will log your

Rule name: hello

Certificate Authority: DC1.bvt.local\bvt-DC1-CA

Certificate Template: Citrix_SmartcardLogon

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。

```
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」記事を紹介しています。

Federated Authentication Serviceの秘密キー保護

Jul 15, 2016

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ありませんが、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。

```
<?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"/></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間の切り替え）

値	Comment
true	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	Comment
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

	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	Comment
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。

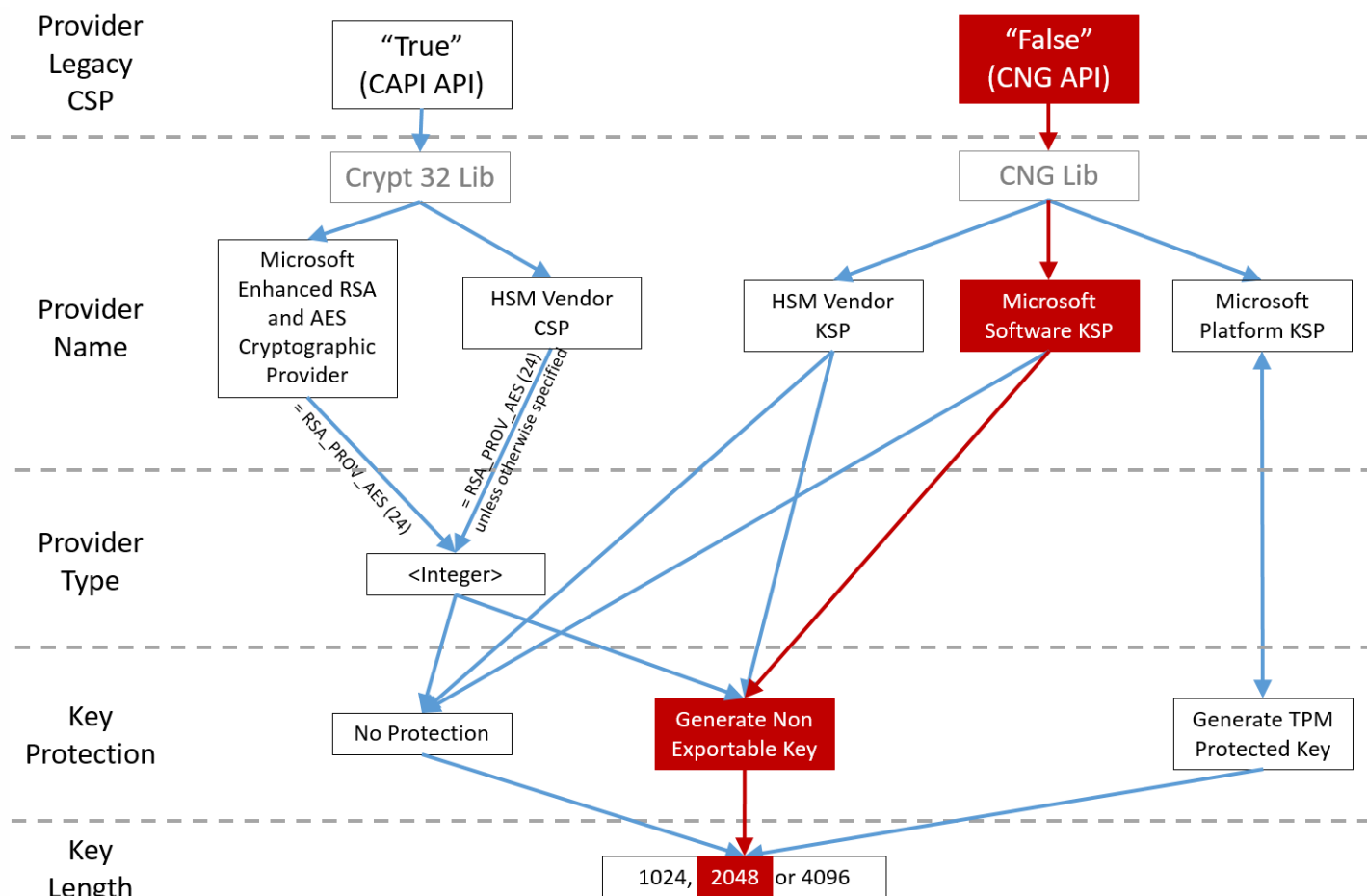
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (FASが秘密キー操作を実行する必要がある場合は、ここで使用されている値を使用します) 秘密キーの [エクスポート可能] フラグを制御します。 ハードウェアでサポートされている場合は、TPMキーストレージの使用が許可されます。

値	Comment
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	Comment
2048	Default。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)。



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。

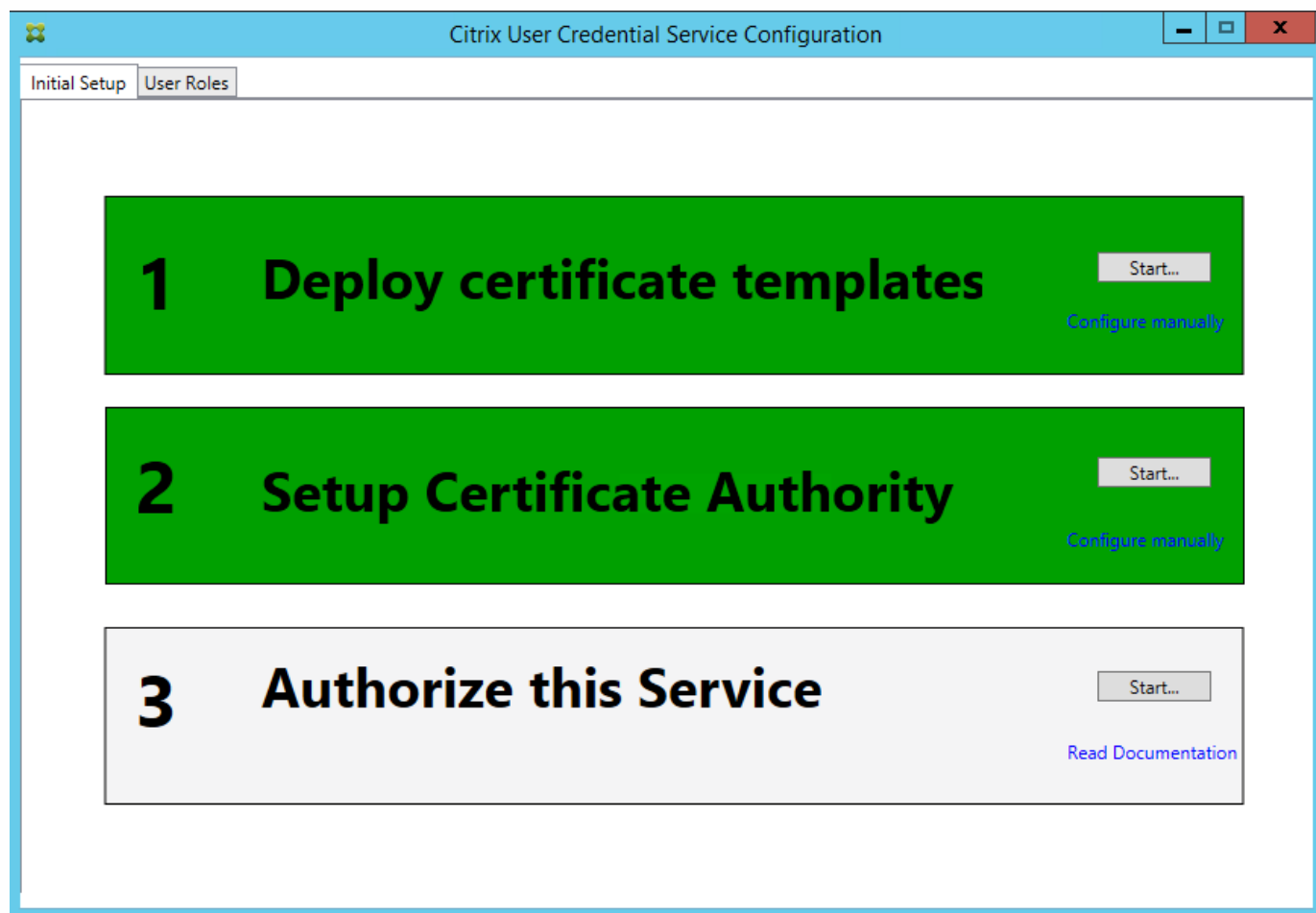
このシナリオでは、TPMの製造元のドキュメントに基づいて、FASサーバーのマザーボード上のTPMはBIOSで有効化され、その後Windowsで初期化されているものとみなしています。詳しくは、[https://technet.microsoft.com/ja-jp/library/cc749022\(v=ws.10\).aspx](https://technet.microsoft.com/ja-jp/library/cc749022(v=ws.10).aspx)を参照してください。

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

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。

手順3：CAサーバーで、CA MMCスナップインを追加します。3. [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.FederatedAuthenticationServices.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。

```

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-----
MIICADCCAUACAQIwIzEhMB8GCGmSjomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
hkig9w0BAQEFAA0CAQ8AMIIICgKCAQEAAwAtwoCL%JuJ3yIscT8Y5v/7zuYqBhbHkhZU3wTMfR0XW
lhCMwi7X4YpTE7CbJtgjFY/9SEBa9StGeTUpEJi66gKoZCdxyc2BwX6JNZrLi9hAf1bInFPgrz+
vbG3YjKuKtK35JpGqWUjUEDzKiQFaob3Dkh/pwP3U7DcEVthxB8CfbaN9MH0EFbepoSY0CAfunXW
snwIbX091c/fGyH/3f94P4fBMrjEIOHc+4Dy/WsPgPRgcq9XBwRjzpGj0gOWRoJS9g220Y5PwD77
7f7vZvQkRy5NXXATJ+xxYEPp9JuJaE1WkrTJG+XP3Sn6/oCCPit7iUIIc9FjGa3qTUQIDAQAB
oAAwDQYJKoZIhvcNAQENBQ0ggEBAlJU8jR9XWH1vztpjxPeJzAV0srLp0sCfNdYvYn9u+I7J8Gsr
4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUzoAf6eLg1Vht2RUfb6d7Ns6+Mc+F5bFegLHs8c
Y1ITN0tmcHFKt4L0z505E+tkw39MProEj3p7GwF7Hr6Y+QSBFD38rbl19Z5cfNYYqMbsgyMgdR8F
3SmagQjN3C81yqT8z1iF4132xlm0rP/4XQvr1F+T015PM5Fxi6PEKwopWTY2XGzSc1ufxevc01K
+tTH9tQYJM6xw3+6TlcfuW0jrd8KJjTdG5SMu7LJu1ajTNZ5Z+1eM61TAT03XG/AB7o=
-----END CERTIFICATE REQUEST-----
Status      : WaitingForApproval

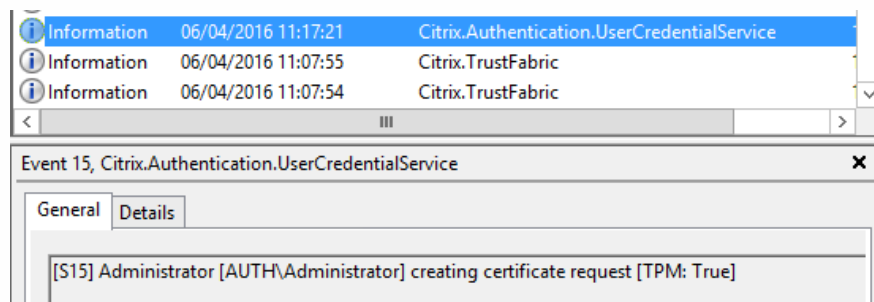
PS C:\Users\Administrator.AUTH>

```

注：

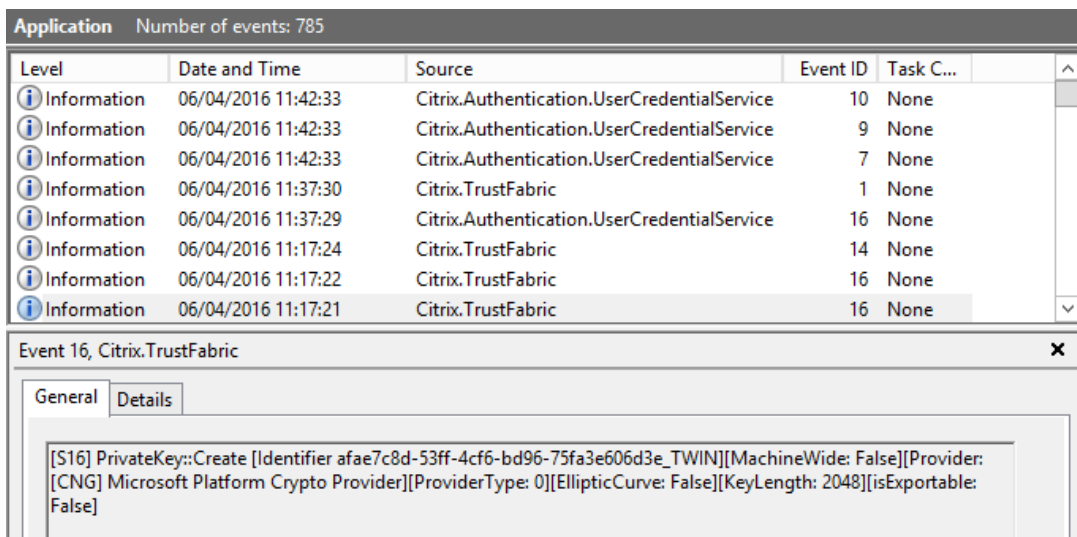
- Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は後続の手順で必要です。
- このPowerShellコマンドレットは、RA証明書の秘密キーの生成に使用される一時的な「上書き」と認識してください。
- このコマンドレットを実行する場合、FASサービスが開始されるときに構成ファイルから読み込まれる値がチェックされ、使用するキーの長さが決定されます（デフォルトは2048です）。
- この手動のPowerShellによって開始されるRA証明書秘密キー操作で-UseTPMが\$trueに設定されているため、ファイルからの値でTPMの使用に必要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。



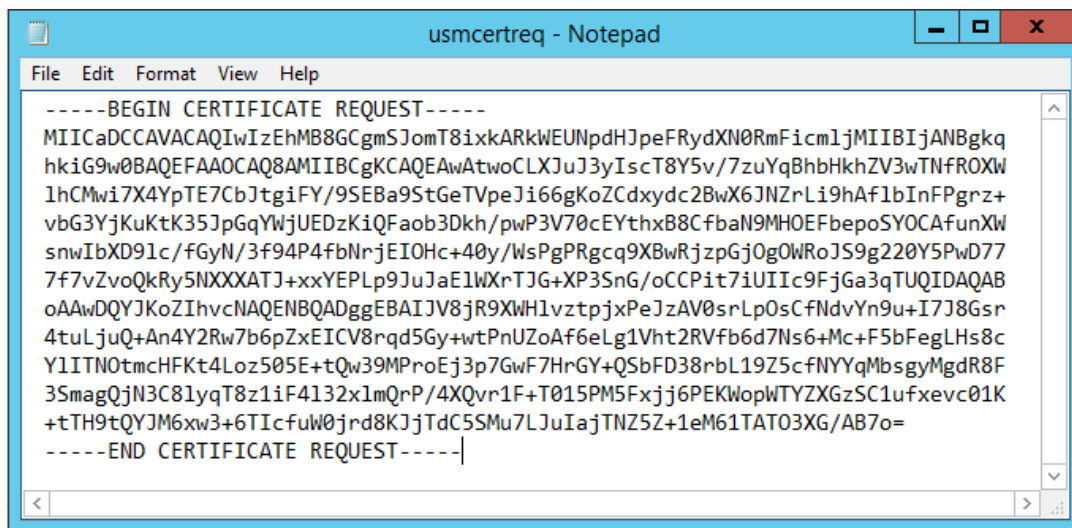
「[TPM:True]」を確認します。

ログは以下のように続きます。



「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
```

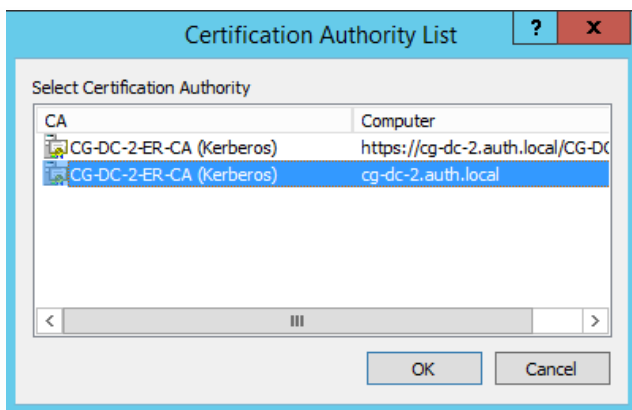
以下が表示されます。

```

PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0B0C-4021-A4FD-2E29502177C2}
ldap:

```

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。

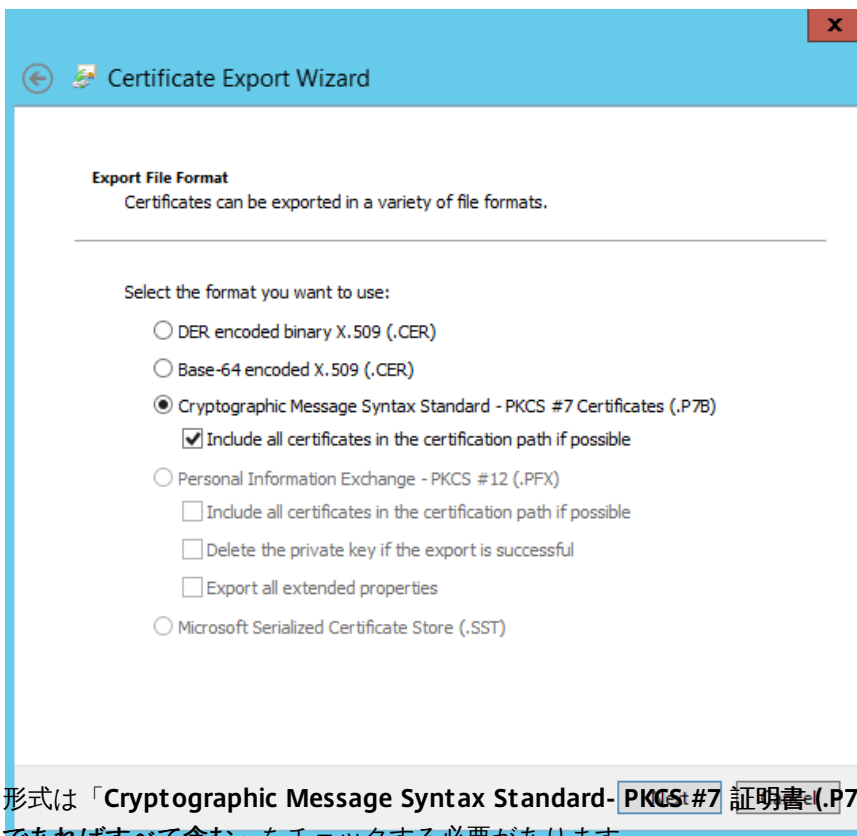


CAが指定されると、PowerShellによってRequestIDが表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0B0C-4D21-A4FD-2E295D2177C2}
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。**【Next】**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。



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：エクスポートされた証明書を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。

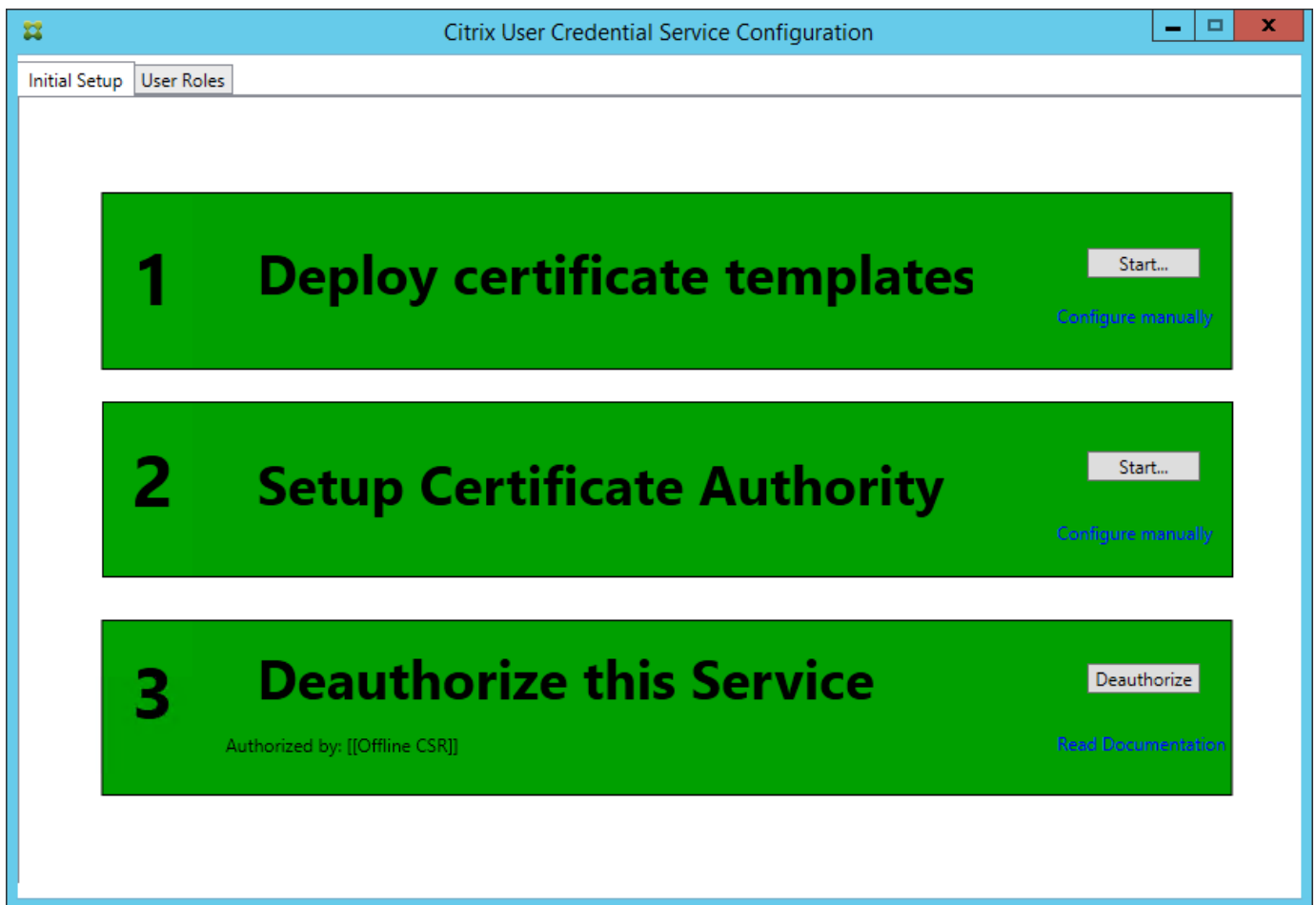
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

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       : 0k
```

手順12：FAS管理コンソールを終了して再起動します。



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。下部のエントリは「Authorized by: Offline CSR」を示しています。

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。

```
<?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.Suppress" 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"/></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。

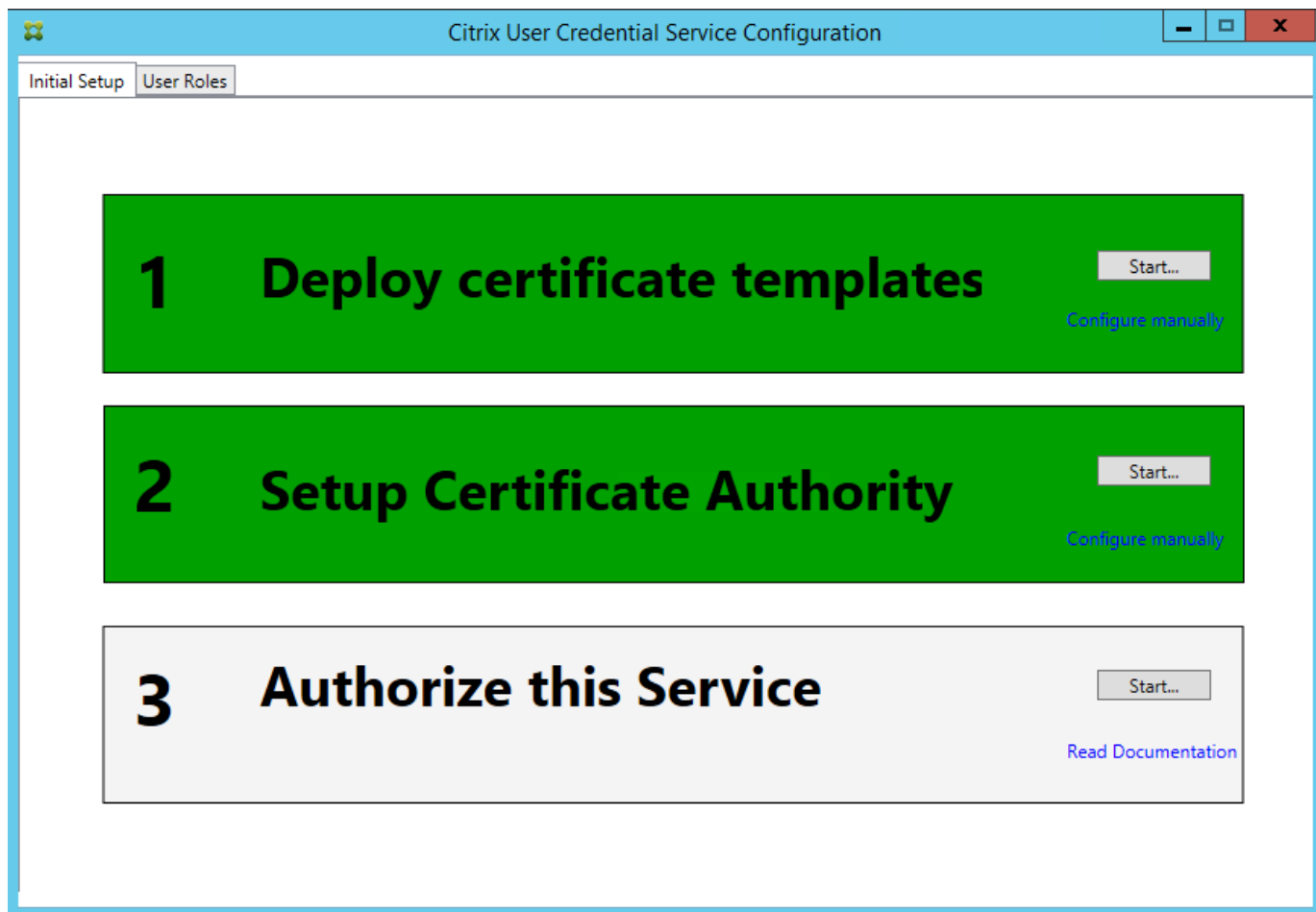
例3

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

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の値を確認してください。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。

```
<?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.Suppress" 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]
```

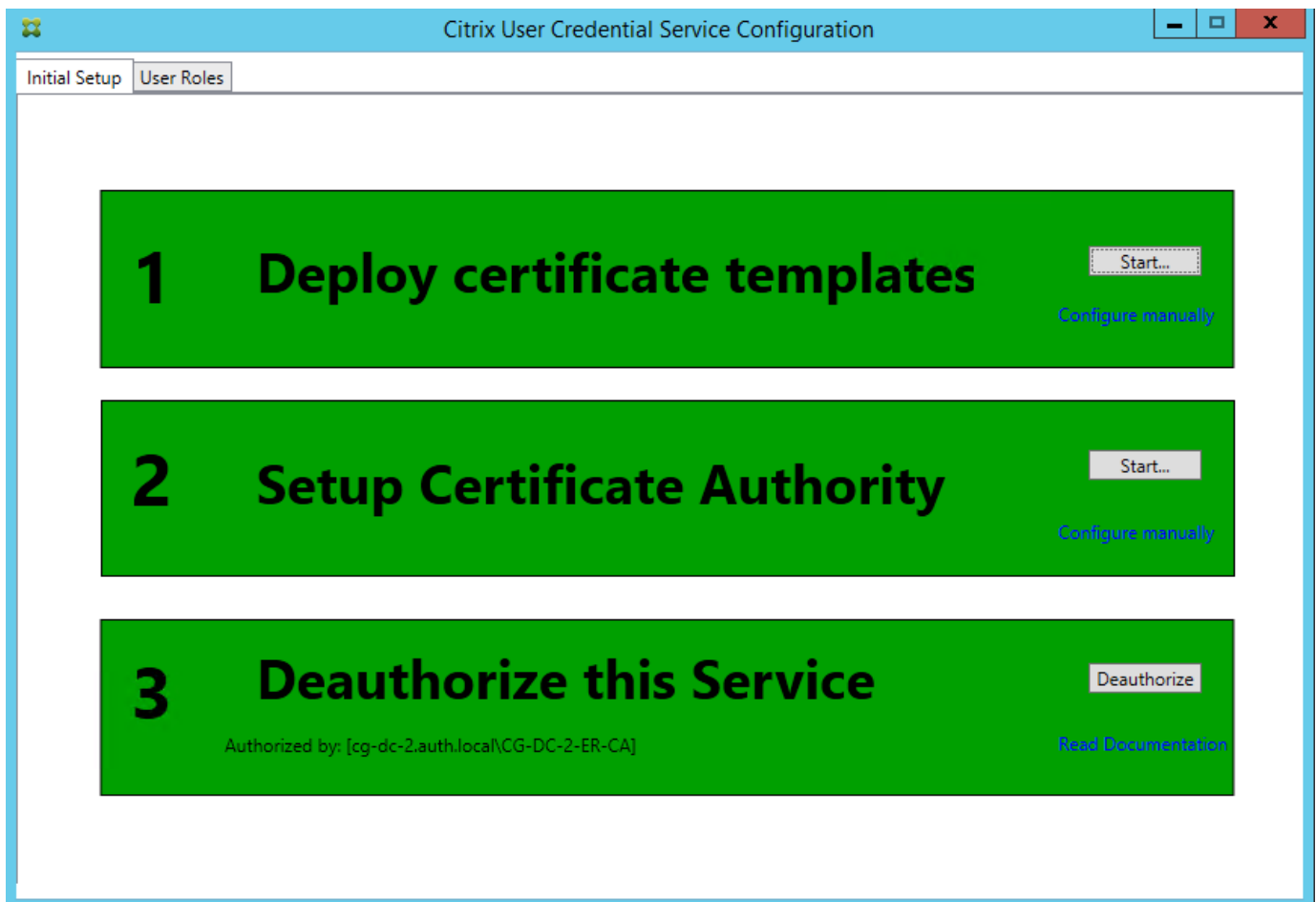
[Provider: [CNG] HSM_Vendor's Key Storage Provider]を確認します。

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\UCSHSMS	

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。下部のエントリは「Authorized by: []」を示しています。



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
```

```
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
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAxyNzaiwX8DhUnOZMS2YVSDhr36AV5BGeIY0GVCFKvZPe
Rmm/x0VM6cNKsLbew3dYlbo+vdgiWg86DFRVxTORho1lV86iazDZy0iYGgxe9/s8YZzCspVwN1nB1
zX0UJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
ECz/CbXR00uiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfD/1Bb3e1ZKA400oi90u64Q916
3ba9BniHqxIgvwWIL0myUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhQ7Ppn1wIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKggcJNJO/MU7/7X
bZB46drLPFzpzF88DkmFoCEg0x1bzFX9waaifS9CHC/AcEzb1N925y1gq1jsfC315TCKBAeLFoM1
PSEkfYMQU0SBYCuL1kFn1LXLSeQ3qJtz5vptYR0awFmUMLffwLSR1v0uS8DJSrpASrwdXJk3T0a
G10/xJo/NRM0wMH+AvGb8sgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIy0MLGZ00aiER+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」記事を紹介しています。

Federated Authentication Serviceのセキュリティとネットワークの構成

Jul 15, 2016

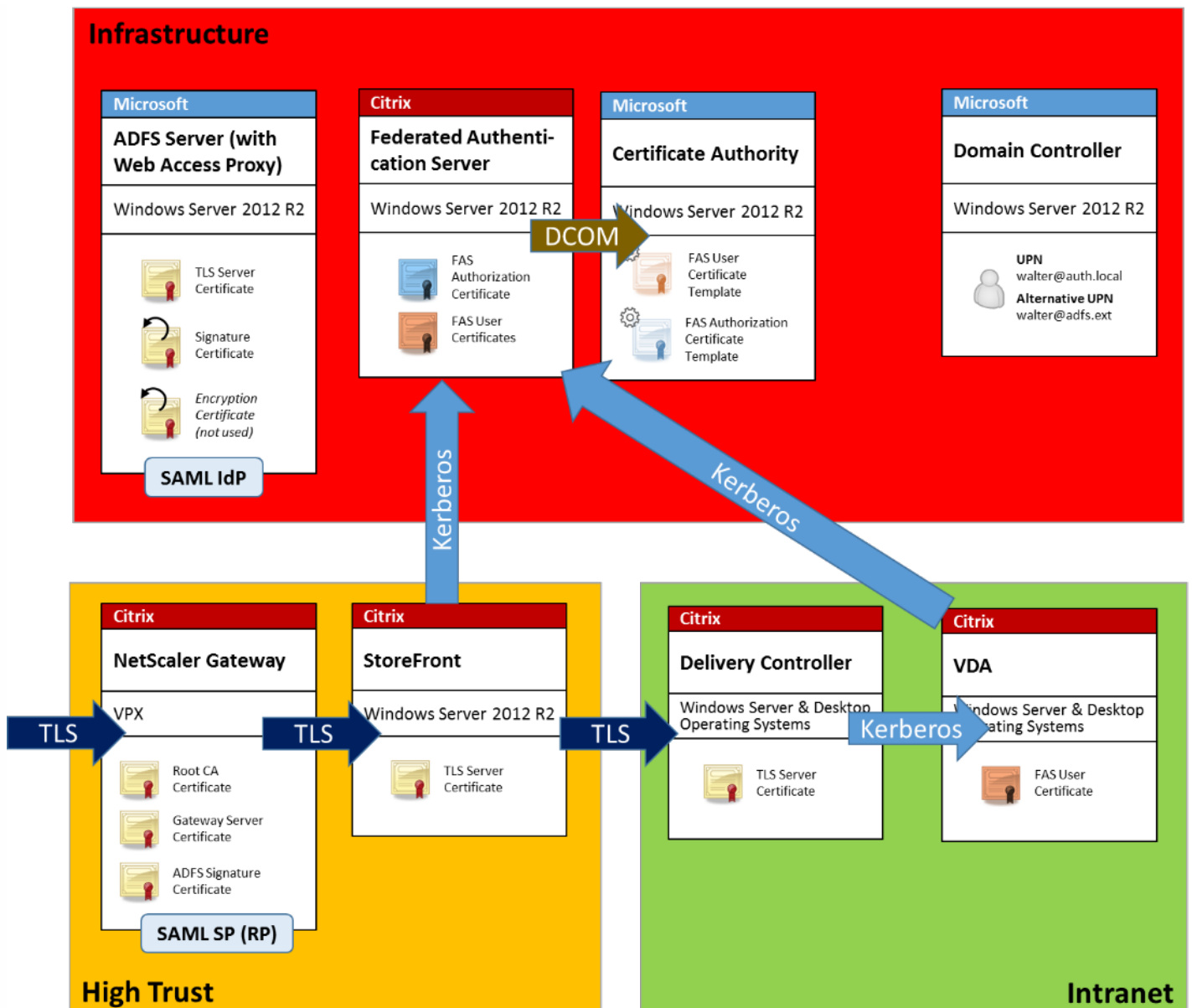
CitrixのFederated Authentication Service (FAS) は、Microsoft Active DirectoryおよびMicrosoft証明機関 (CA) と密接に統合しています。ドメインコントローラーやその他の重要なインフラストラクチャと同様に、セキュリティポリシーを展開することによって、システムの適切な管理と保護を行うことが重要です。

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。その他の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。



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。

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 Authentication Service	[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。

名前	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

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

エンタープライズ管理者によって、「フォレスト中に」証明書テンプレートがインストールされます。セキュリティに関する主要な考慮事項として、次の4点が挙げられます。

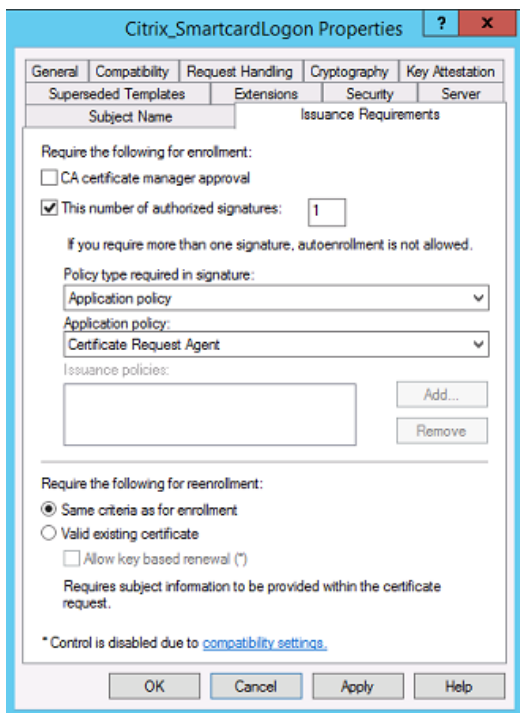
登録機関テンプレートのインストール

FASインストーラーは、登録機関（RA）テンプレートおよびスマートカードログオンテンプレートの、2種類の証明書テンプレートを提供します。

ランタイムに必要なのはスマートカードログオンテンプレートだけです。RAテンプレートはインストールしない（つまりRA証明書は別のオフラインのCAを使用して、手動で発行する必要があります）、またはFASサーバーの承認後にRAテンプレートを無効にすることができます。

アプリケーションポリシーOID

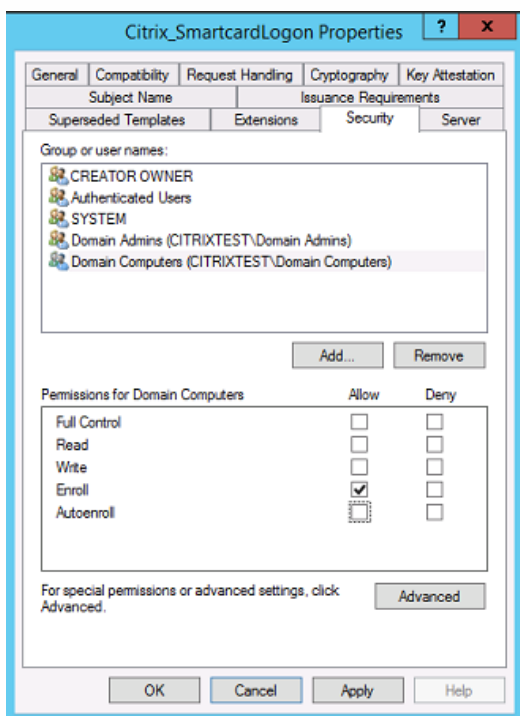
RA証明書は、オブジェクトID（OID）「証明書要求エージェント」を、拡張キー使用法の拡張機能に含めることによって識別されます。このOIDが別のシステムで使用されている可能性がある場合は、カスタムOIDに変更できます。



アクセス制御リスト (ACL)

各テンプレートには、証明書を発行できるユーザーおよびコンピューターを管理する、アクセス制御リストがあります。

FASサーバーのマシアカウントのみに証明書の要求を許可するよう、ACLを明示的に再構成することをお勧めします。 ネットワークのファイアウォールポリシーを使用して、さらに制限できます。



サブジェクト名、拡張機能、およびパス名の制約事項

標準的なサブジェクト名および拡張機能は、RFC 5280の標準機能を使用して、発行された証明書の使用目的を管理するよう構成できます。 これにより、公開キー基盤 (PKI) を通じて発行された証明書の使用目的についての、基本レベルの管理が実

現します。

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。

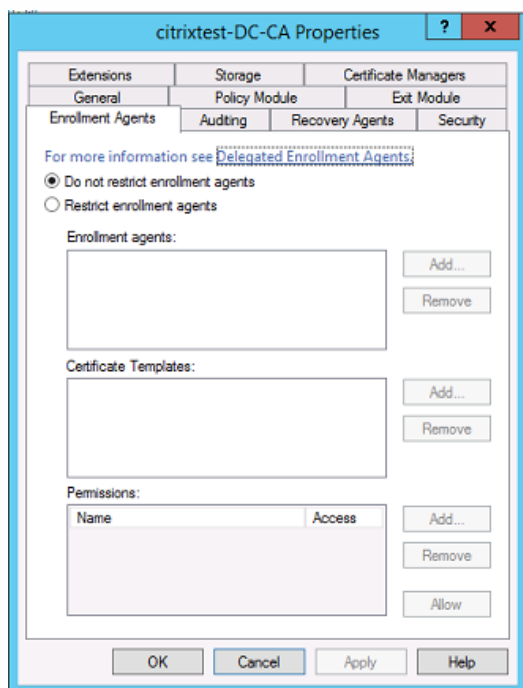
シンプルなセキュリティ対策としては、FASサーバーのインストール時にのみRA証明書テンプレートを公開するか、またはオフラインの証明書発行手続きを選択することです。いずれの場合も、CA管理者はRA証明書の要求の承認において全面的なコントロールを維持し、FASサーバーの承認に関するポリシーを持つ必要があります。

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。



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。
Users	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、より権限の異なる「ログオン」証明書はログオン時にのみ使用するよう、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イルスソフトウェアを使用する必要があります。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」記事を紹介しています。

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

Aug 26, 2016
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への認証のため、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
- **ルート証明書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社のドキュメント<https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx>を参照してください。

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

	のオプションは、そのフィルターを上書きします。
EnumerateECCerts	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、この機能を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

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:mydomaini
```

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。

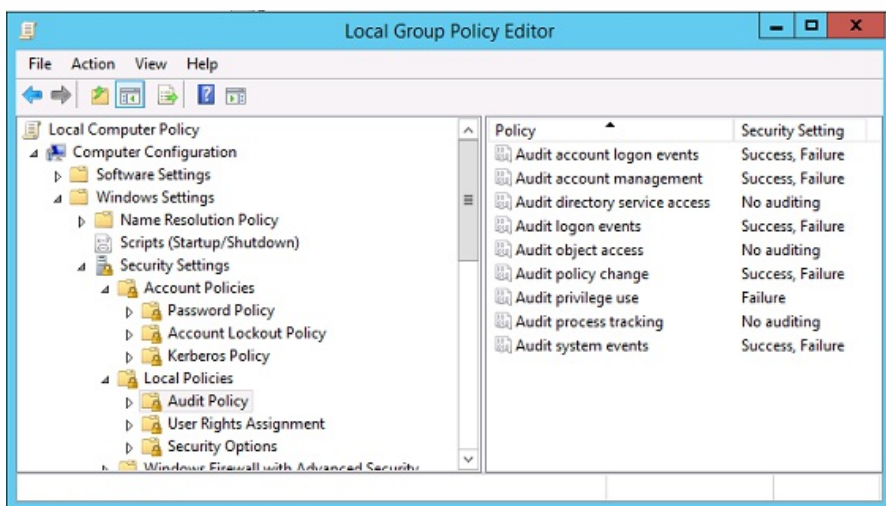
使用中のドメインコントローラーの識別

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。



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/CAPIC2/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0xffffffff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

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

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。

Operational Number of events: 6					
Level	Date and Time	Source	Event ID	Task Category	
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy	
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 Revocation	
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation	
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain	

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
```

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。

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	21/06/2016 15:14:56	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:56	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations
Audit Success	21/06/2016 15:14:54	Security-Auditing	4768	Kerberos Authentication Service
Audit Success	21/06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations
Audit Success	21/06/2016 15:14:54	Security-Auditing	4634	Logoff
Audit Success	21/06/2016 15:14:54	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:54	Security-Auditing	4624	Logon

Event 4768, Security-Auditing

General Details

☒ Friendly View ☐ XML View

+ System

- EventData

TargetUserName fred

TargetDomainName CITRIXTEST.NET

TargetSid S-1-5-21-390731715-1143989709-1377117006-1106

ServiceName krbtgt

ServiceSid S-1-5-21-390731715-1143989709-1377117006-502

TicketOptions 0x40810010

Status 0x0

TicketEncryptionType 0x12

PreAuthType 16

IpAddress ::ffff:192.168.0.10

IpPort 49348

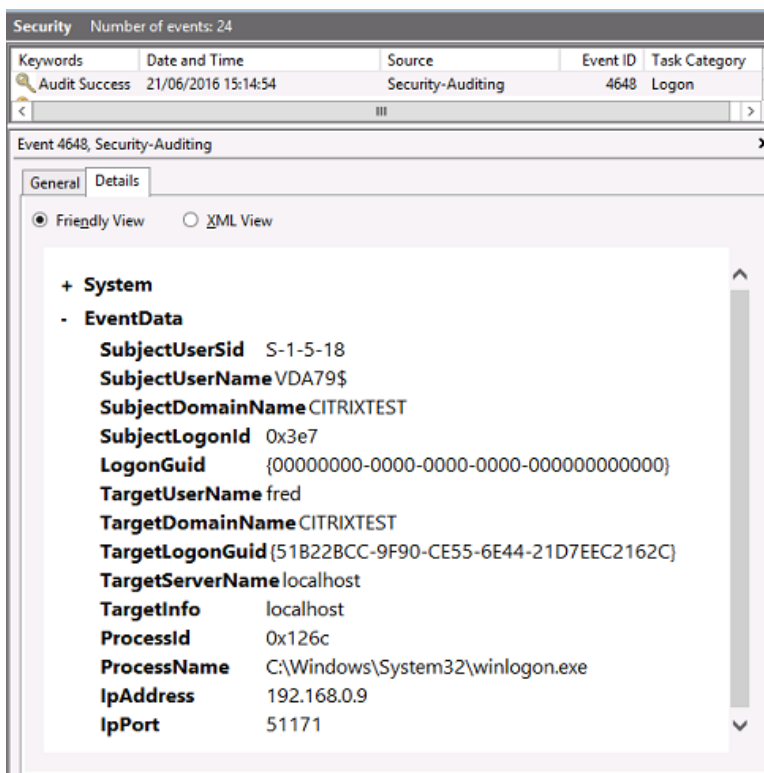
CertIssuerName citrixtest-DC-CA

CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC

CertThumbprint 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

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。



VDA CAPIログ

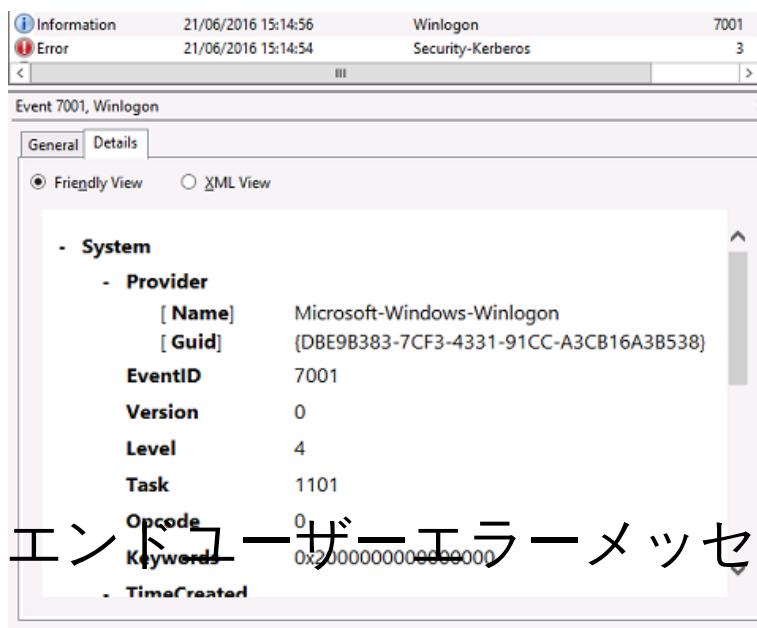
このサンプルのVDA CAPIログは、lsass.exeから単一のチェーンビルドおよび検証シーケンスを示しており、ドメインコントローラー証明書（dc.citrixtest.net）を検証しています。

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]   813C6D12E1E1800E61B8D8071E186EB912B7
      [ 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。



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。この項の「 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。この項の「 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。

	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。	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

- 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>

Federated Authentication ServiceのPowerShell SDK

Aug 26, 2016

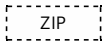
シンプルな展開ではFederated Authentication Service管理コンソールも使用できますが、PowerShellインターフェイスにはより詳細なオプションがあります。コンソールでは使用できないオプションを使用する場合は、PowerShellのみを使用して構成を行うことをお勧めします。

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。

 [Federated Authentication ServiceのPowerShellコマンドレットのヘルプファイル](#)

印刷

Jul 15, 2016

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言及が含まれます。
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。

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、セッションへのロ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

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。

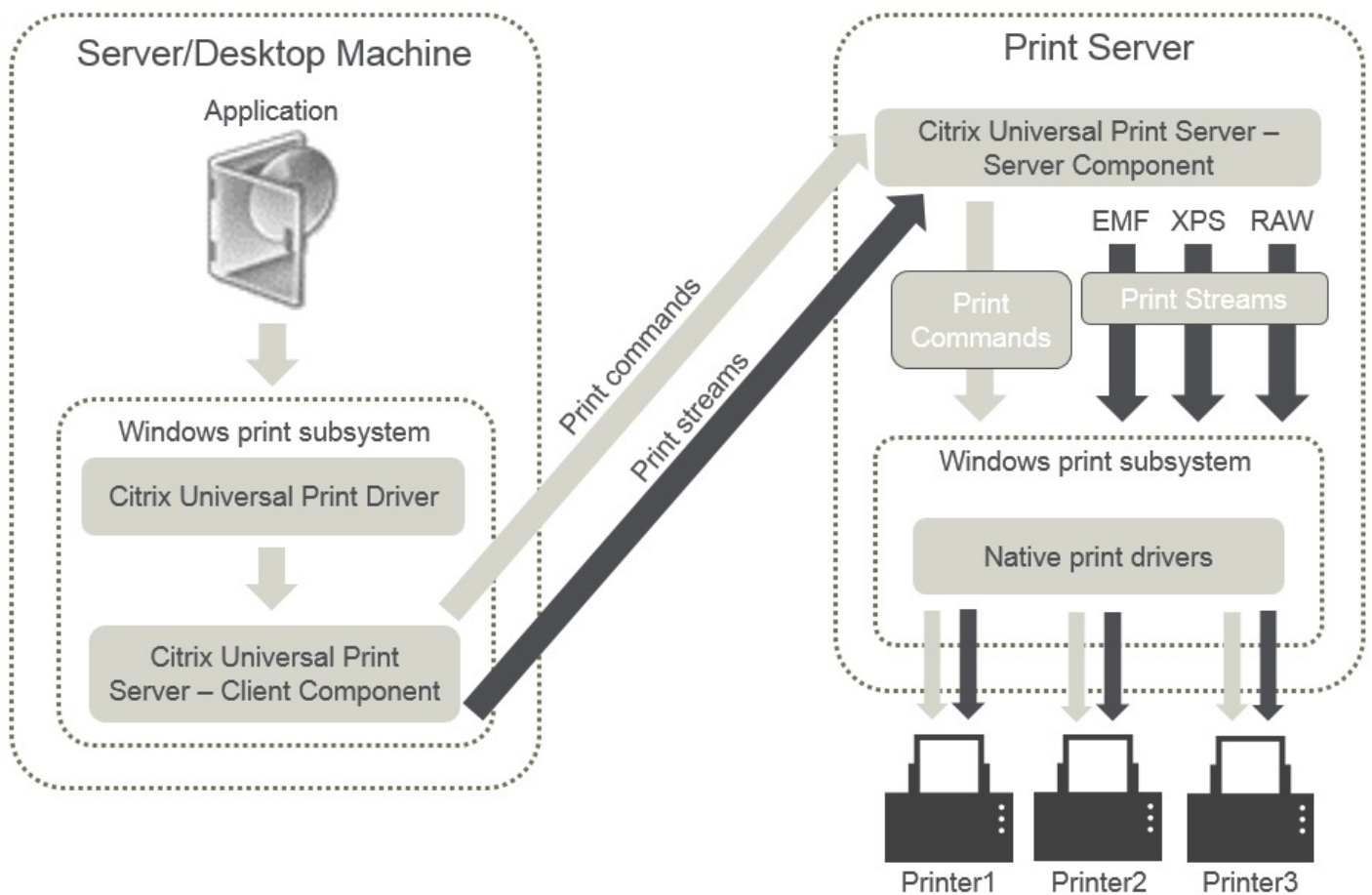
Universal Print Serverの機能は以下のコンポーネントで構成されます。

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。



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も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。

- セッションプリンターの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。

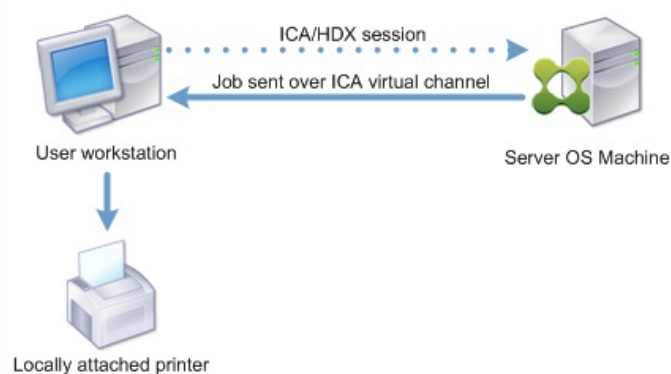
印刷ジョブの送信

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。



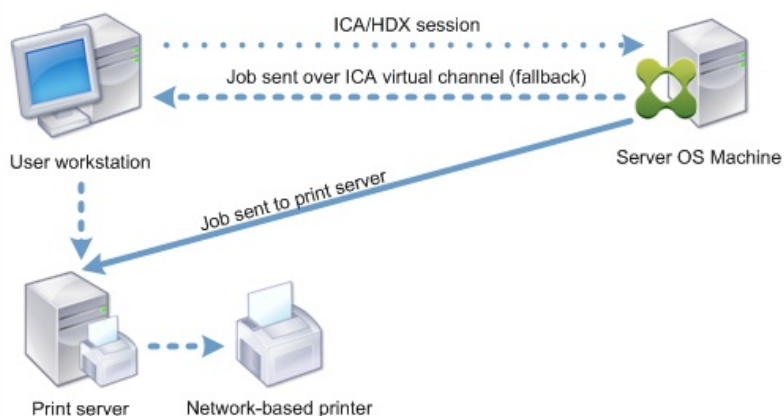
ネットワーク上のプリンター

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。

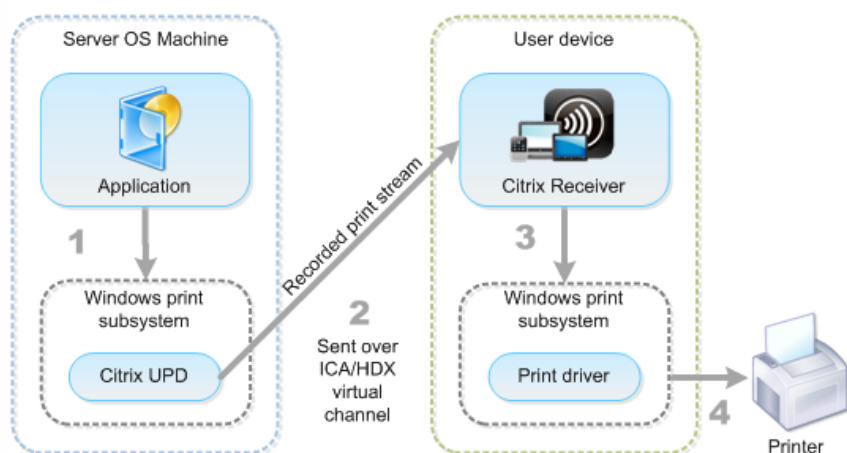


プリンタードライバーの管理

この環境での印刷を簡素化するため、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。ユニバーサルプリンタードライバーは、あらゆる印刷デバイスをサポートする、デバイスに依存しないドライバーで、必要なドライバーの数を減らして管理業務を簡素化します。

Citrix XPSユニバーサルプリンタードライバーは、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、Microsoft印刷機能テクノロジーを使用して、ネイティブドライバーで利用可能になっている場合に利用できます。ネイティブドライバーでは、印刷機能XMLの標準印刷スキーマキーワードを使用する必要があります。非標準キーワードを使用すると、Citrix XPSユニバーサルプリンタードライバーで詳細なプリンター機能を使用できません。

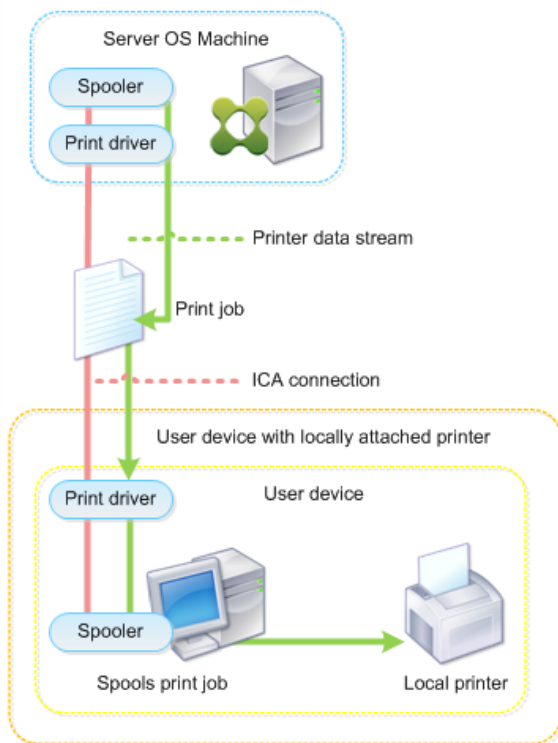
次の図は、ユニバーサルプリンタードライバーコンポーネントとデバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



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。



- 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](#)

印刷構成の例

Jul 07, 2016

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があります。

印刷環境を設定するときは、以下の事項を考慮します。

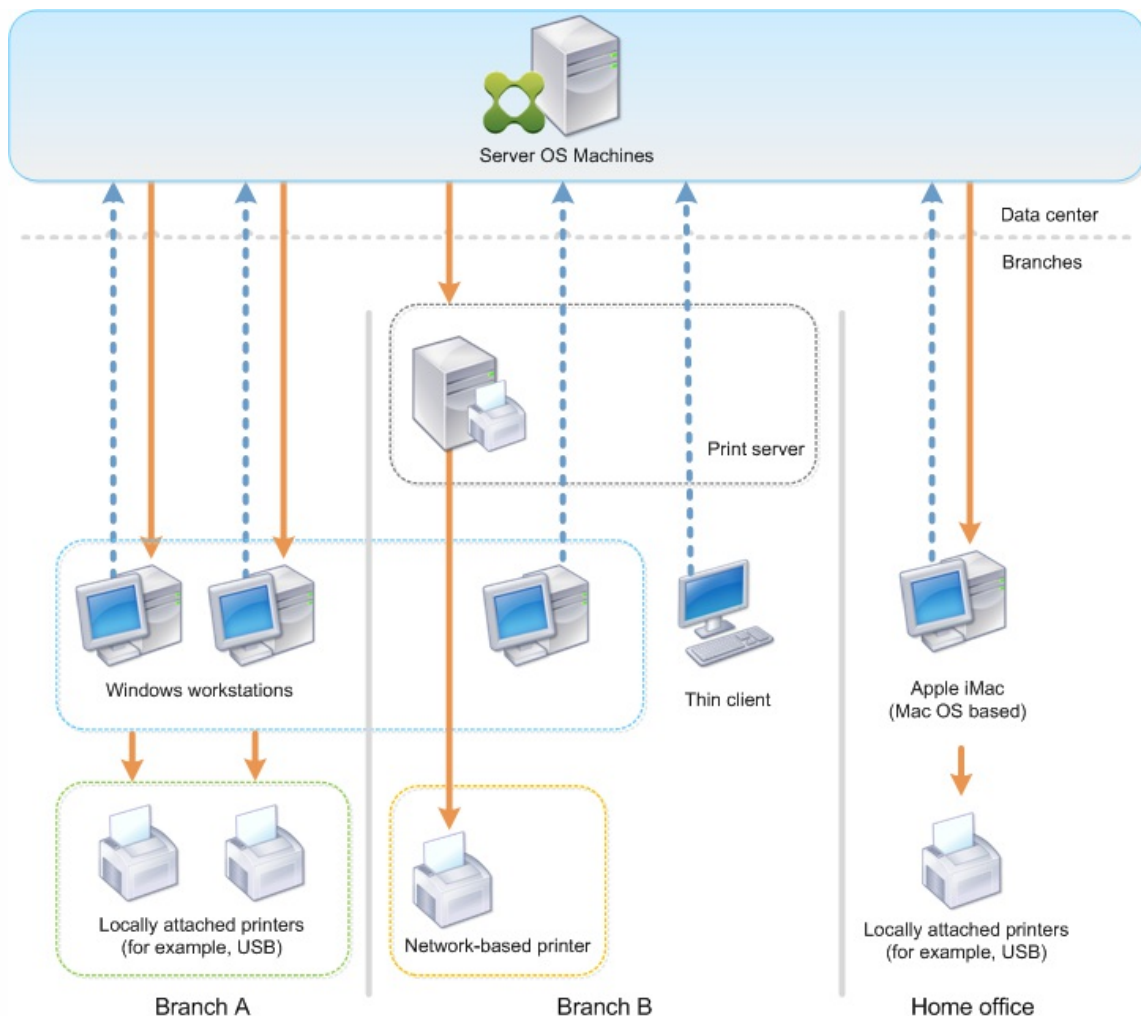
- 業務上のニーズと既存の印刷インフラストラクチャ。
組織のニーズに基づいて、印刷環境を設計します。既存の印刷環境（ユーザーが自分でプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるか、など）を確認し、それに沿って印刷環境を構成できます。
- 組織のセキュリティポリシー。人事部用のプリンターなど、特定のユーザー用に予約されたプリンターがあるかどうかを確認します。
- メインのワークステーションとは離れた場所で印刷するユーザーがいるかどうか。たとえば、複数のワークステーションを移動しながら作業したり、出張先で印刷したりするユーザーがいるかどうかを確認します。

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ときと同様なユーザーエクスペリエンスを提供することを目指します。

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。
- **支店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。



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。

- 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は不要です。ドライバ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。

- シンククライアントの場合 - シンク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内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管理者が適切なポリシーの[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

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へのフォールバックおよびプリンタードライバ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。

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

Jul 07, 2016

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。印刷ジョブ

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。

印刷に関するポリシーと設定

Jul 07, 2016

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築できます。

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。印刷設定は通常のCitrixポリシーにしたがいます。

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、その後でそのほ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。

プリンターのプロビジョニング

Jul 15, 2016

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が使用されます。このドライバはサーバーOSマシン上の単一のドライバで、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が使用されます。Windowsネイティブドライバのみ、またはユニバーサルプリンタードライバ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、「[グラフィカルインターフェイスを使ったインストール](#)」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. 「スタンドアロンVDAインストーラーの使用」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。

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されています。 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。 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。

- 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。詳しくは、「[Universal Print Serverのポリシー設定](#)」を参照してください。

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。

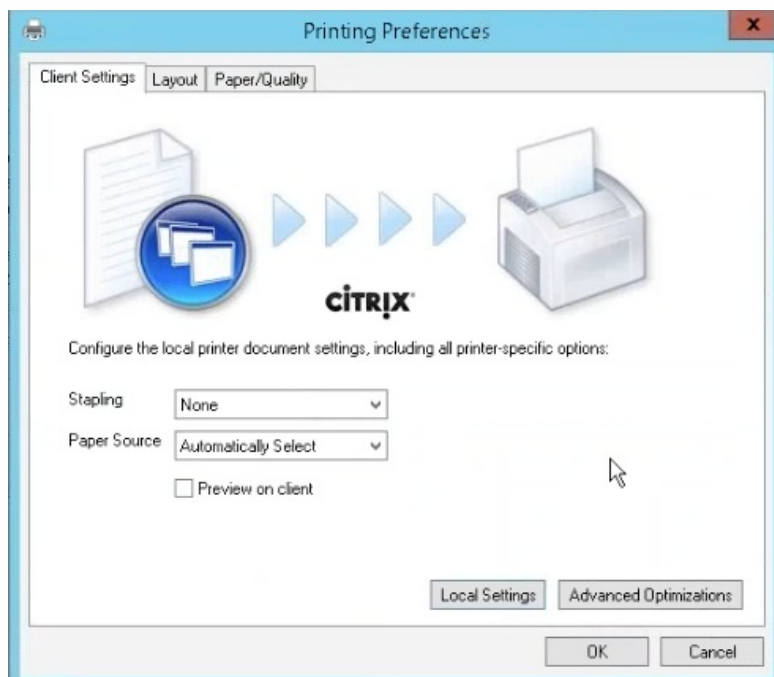
ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターを自動作成する	Universal Print Serverが有効な場合、ネイティブドライバーの代わりにユニバーサルプリンタードライバーを使ってクライアントネットワークプリンターが作成されます。ユーザー側には、同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリンタードライバー関連のポリシー設定によりセッションプリンターが構成されます。
プリントサーバーへの直接接続	Universal Print Server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 XPSのユニバーサルプリンタードライバは、ホチキス留めや給紙方法などの詳細なプリ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。

これらの機能は、ネイティブドライバがMicrosoftの印刷機能テクノロジー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 XPSのユニバーサルプリンタードライバ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。

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、リソース使用量が大幅に軽減され、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** -デバイスに依存しないプリンタードライバ。Citrixユニバーサルプリンタードライバを構成すると、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が使用されます。Citrixユニバーサルプリンタードライバ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の優先度**：ユニバーサルプリンタードライバ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から順に使用されます。この一覧では、ドライバを追加、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、[CTX114420](#)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。
- 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もっと少なくするために、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。
 - ネットワークプリンター名。 [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、ここで説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。

印刷環境の保守

Jul 07, 2016

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言

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にわたって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。

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	Location
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	On	Microsoft管理コンソールの [印刷の管理] スナップイン
		Off	Windows 8より古いバージョン： [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	On	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
		Off	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）	クライアント印刷経路	On	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
		Off	Windows 8より古いバージョン： [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	On	プリントサーバーの [コントロールパネル]
		Off	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。

HDX

Jul 07, 2016

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	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 MediaStream機能により、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	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。 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、環境のさまざまな条件に応じて最適な機能が適用され、パフォーマンスと消費帯域幅のバランスが最適化されます。
データセンターで	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。圧縮されたマルチメディア情報は、本来の形式のままユーザーデバイスに直接送信されます。 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。 Network InspectorとPerformance ManagementをDirectorに統合したものであるHDX Insightは、ICAトラフィックに関するデータを収集して、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往復時間値などの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。

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。

- HDXによりビデオコンテンツが仮想デスクトップ上でどのように再生されるかを体験するには、
<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>などのWebサイトにアクセスして、高品位ビデオを再生します。
- Flashリダイレクトにより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ツールバーの「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に機能するため、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る場合、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。
- 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、すべてのクライアントの仮想デスクトップユーザーにWindows Aeroエクスペリエンスを配信します。
- 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、Windows Mediaリダイレクトの設定に基づいてサーバー側からユーザーデバイスにリダイレクトされます。通常、Windows Mediaリダイレクトに関するポリシーを変更する必要はありません。

ヒント：

- HDX機能のサポートと要件については、「[システム要件](#)」を参照してください。特に注記のあるものを除き、サポートされる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ます。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。

Windowsデスクトップで消費される帯域幅の抑制

HDXのデフォルトでは、Windowsデバイスから仮想デスクトップにアクセスするユーザーに、良好なレスポンスのWindows AeroまたはWindows 8デスクトップエクスペリエンスが提供されます。これを可能にするため、ユーザーデバイス側のGPU (Graphics Processing Unit) またはIGP (Integrated Graphics Processor) を使用してローカルのDirectXグラフィック処理を行います。この機能は「デスクトップコンポジションリダイレクト」と呼ばれ、サーバー側の負荷軽減にも役立っています。詳しくは、<http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/>の「What to do with all these choices」を参照してください。

ユーザーセッションで消費される帯域幅を抑えるには、以下のポリシー設定の調整を検討してください。ただし、これらの変更によりユーザーエクスペリエンスが低下する場合があります。

- デスクトップコンポジションリダイレクト — WindowsユーザーデバイスからアクセスするWindowsデスクトップOSマシンにのみ適用され、Windowsデスクトップの表示にのみ効果があります。Citrixポリシー設定の「ローカルアプリケーションのアクセスを許可する」で「許可」を指定しても、アプリケーションウィンドウの表示はサーバー側で処理されます。
- デスクトップコンポジションの画質 — シームレスアプリケーションまたはローカルアプリケーションアクセスが無効な場合に、デスクトップコンポジションで高品質なグラフィックが使用されます。消費帯域幅を抑えるには、グラフィックの品質を下げます。
- 動的ウィンドウプレビュー — 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。消費帯域幅を抑えるには、このポリシー設定を無効にします。

ユーザーデバイスに送信されるイメージ品質の改善

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。
- 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。通常、大きい値を指定することでユーザーエクスペリエンスが向上します。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。
- 表示メモリの制限。セッションのビデオバッファ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。3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。

ビデオ会議パフォーマンスの改善

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。HDX Plug n-Play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。

Citrix Receiver for Windowsのデフォルトでは、HDX Webカメラビデオ圧縮が有効になっています。Receiver for Linuxでは、構成の変更が必要です。詳しくは、Citrix Receiverのドキュメントを参照してください。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メディアリダイレクト

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では追加の帯域幅が使用されるため、狭帯域幅接続には適していません。低帯域幅ネットワークで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。

ユーザーエクスペリエンスの向上よりもサーバースケーラビリティの改善を選択する

ユーザーエクスペリエンスの向上よりもサーバースケーラビリティの改善が重要な環境では、従来のグラフィックモードが使用されるように設定します。これを行うには、ポリシーの[従来のグラフィックモード]設定を追加して、個々のグラフィックポリシー設定を構成します。従来のグラフィックモードを使用すると、WANやモバイル接続時のユーザーエクスペリエンスが低下することがあります。

Thinwire互換モード

Jul 07, 2016

Thinwire互換モードは、エンドユーザーエクスペリエンスを犠牲にすることなく帯域幅の使用を抑えて高度なサーバースケーラビリティを実現する新しい画面分解およびキャッシュテクノロジーを使用します。

Thinwire互換モードには、次の機能があります。

- ビットマップ専用プロバイダー用のインテリジェントビットマップ一致。
 - ウィンドウ移動およびスクロールを効率的にするためのビットマップ変換解析です。
- 後方互換性。クライアントまたはCitrix Receiverのアップグレード、あるいはハードウェアアクセラレーションに対する要件はありません。
 - テストは、最新のものから5年を越えるものまでの古いシンクライアントで実行されています。
- サーバーCPUの使用をとて低くするために最適化、およびサーバースケーラビリティの改善。
- 通常のワークロードについて帯域幅をさらに15~20%に減少するエミュレートされた16ビットモード。
- サーバー側でレンダリングするビデオコンテンツの遷移の検出。
 - 改善されたマルチメディアエクスペリエンスのためのマルチ遷移の処理。たとえば、複数のビデオまたは紙テープを見る場合。
 - 遷移状態のままにする地域を選択的にシャープにします。
- CloudBridgeアクセラレーションの最適化。テストでは、Officeタイプのワークロードについて、帯域幅の減少の比率は最大で6:1となりました。
- ポリシー設定を介して有効にできるアダプティブ表示。詳しくは、**動画のポリシー設定**の「**動画の圧縮**」を参照してください。
- Windows 10を含むVDAとWindowsをサポート。
- 低帯域幅でのユーザーエクスペリエンスをより良いものにするため応答性、相互作用性、および割り込み可能なシャープイを向上させる新しい3D Proの「操作時は低品質」モード。
- 従来のグラフィックモードよりも高い、デフォルトの静的写真画像品質。

表示品質設定の「低」、「中」（デフォルト）および「高」については、アダプティブ表示ポリシーに従って、遷移検出機能が動的に画面の更新を評価し高度にアニメ化された領域を低品質にして送信する必要があるかどうかを判別され、クライアントのパフォーマンスを向上させ、帯域幅の使用を減少させます。

【操作時は低品質】の画質については、Thinwire互換モードでは大画面の更新に対して「ファジーファースト」アプローチが用いられます。この設定は、3Dモデルまたはそのほかのグラフィック指向アプリケーションを操作する3D Proユーザーを対象にしたものです。アクティビティが続行する場合には、引き続き遷移的モードとして処理され、遷移的アクティビティが停止すると影響を受ける領域がシャープになりキャッシュされます。たとえばワイヤーフレームを回転するなど初期の大きな変更については、変更を受ける領域である種の簡易イメージ解析が実行され、「ファジー遷移性」を前提とするか、それとも「シャープ遷移性」（無損失）を前提とするかが判断されます。FPS（1秒あたりのフレーム数）および帯域幅については、Citrix無損失コーデックを使って単純なイメージをエンコードすることがより効率的であり、画質も損なわれません。

操作時は低品質のシャープ化から無損失のステップもまた異なります。影響のある領域が一度にシャープになるのではなく、その部分は事前決定されているブロックでシャープ化されるため、相互作用性と快適なユーザーエクスペリエンスを維持するのに役立ちます。遷移中に大きな変更領域をシャープにすると、特に低帯域幅回線においてたとえば3Dモデルの移動を一時的に停止してから再度実行することにより以前は「詰まり」を引き起こしていました。シャープ化するブロックのサイズは、ターゲットの最小フレームレート（アダプティブ表示ポリシー設定）を維持しようとするためにどのくらい品質を低下させたかにより異なります。品質を著しく低下させた場合、シャープにするブロックサイズはより小さく、最小で128 x 128ピクセルとなります。たとえばクライアントに十分な処理能力と帯域幅があるなど品質をそれほど低下させない場合は、シャープにするブロックサイズは最大で384 x 384ピクセルにできます。

Framehawk仮想チャネル

Jul 07, 2016

はじめに

Framehawk仮想チャネルによって、パケットロスや輻輳が頻繁に発生する、ブロードバンドワイヤレスネットワーク接続および損失を伴う長距離のブロードバンドネットワーク接続上での仮想デスクトップとアプリケーションのユーザーへの配信が最適化されます。Citrixポリシーを使用し、ネットワーク特性に適した方法で、ユーザー用にFramehawkまたはThinwireを実装し、全体的なスケーラビリティやパフォーマンスの要望に応じることができます。

一般に、ユーザーエクスペリエンスは、有益なユーザーエクスペリエンスのための基礎として、フレームレートと画質に焦点を当てていました。Framehawkは、線形性の理由を説明するためにこの定義を強化します。ユーザーは経験に気を取られるのではなく、これを楽しむ必要があります。劣化したネットワーク環境下では、ユーザーはすべてのプロトコルをむしろ「ラバーバンド」効果に苦しんでいます。これには、画面が反応するかどうかをユーザーが判断できないため、必要以上にクリックすることになり、結果がますます望ましくないものになっていくという「タップ待機タップ」症候群が含まれます。Framehawkはこのような現象を、特にネットワークが激しく活動している状況で解消します。

家庭用高速インターネット接続がパフォーマンスの問題を示すことはよくありますが、その原因は近所のWi-Fi信号との干渉、コードレスデバイスからのスペクトル干渉などいろいろ考えられます。3Gまたは4G/LTEセルラーネットワーク経由、またはインフラインターネットサービスを利用して、ホストされたアプリやデータに接続するユーザーはますます増えています。また、コーヒー店での休憩中や、滞在先のホテルで公衆Wi-Fiホットスポットを利用する人もいますが、この場合は輻輳がよく問題になります。

Framehawkでは、ユーザーは高遅延の状況で、文字のエコーバックの線形性がより高いインタラクティブなエクスペリエンスに気付いています。

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。動画や動くグラフィックのように急速に変化する画面エリアに関していえば、再生中に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はありません。

しかし、タスクとレイアウトバーのアイコン、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エリアは、人間の目が細部にまでこだわるところで、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、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、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。

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、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」と呼びます）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、信頼できるデータ通信のためにTCPをベースにしているため、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。

FramehawkはUDPベースで、データ送信ではベストエフォート方式を採用しています。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が、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4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を加えることをおすすめします。

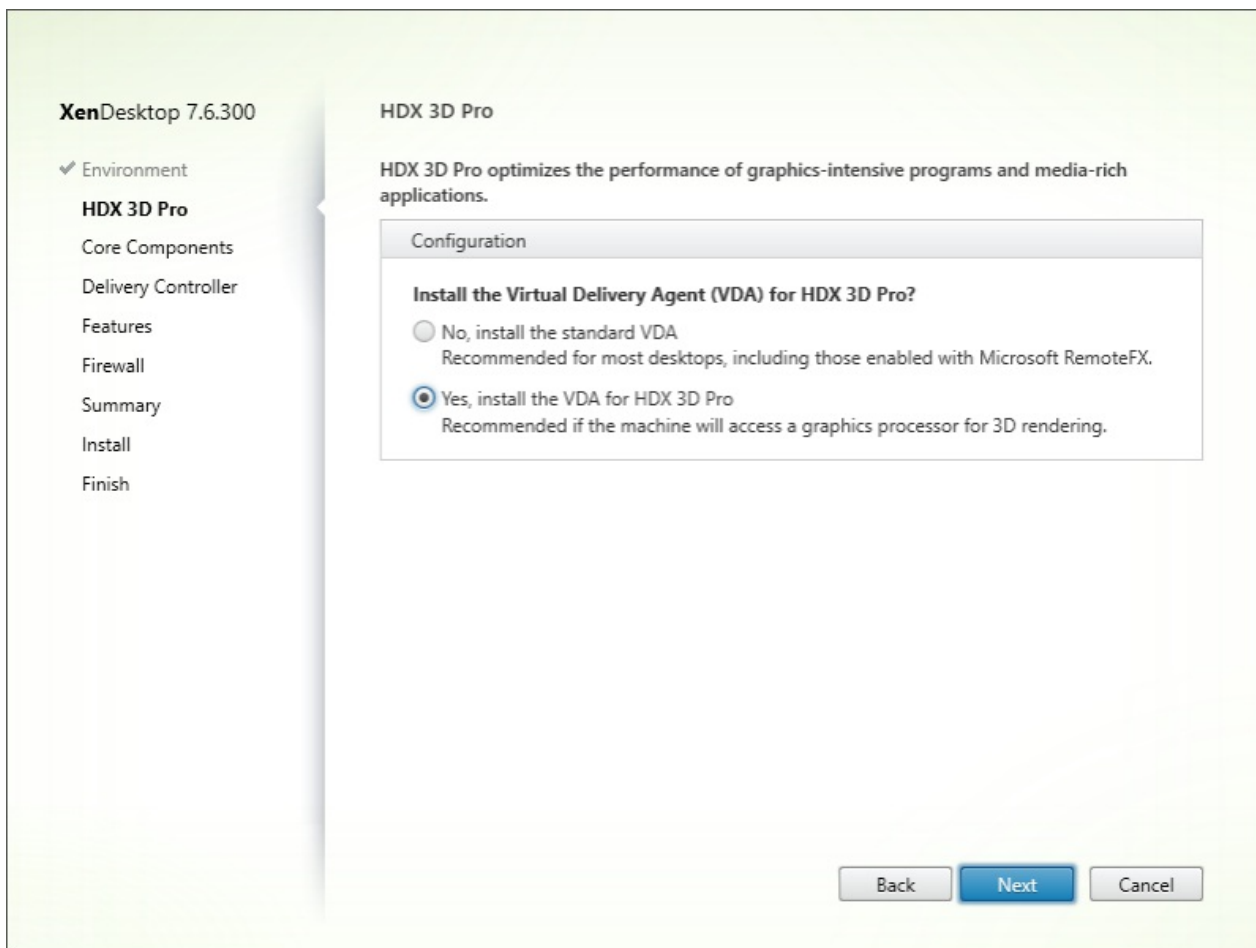
Citrixでは、Thinwireの帯域幅を基本の1.5 Mbpsに、ユーザー1人につき150 Kbps追加することを推奨していました（詳細は、XenAppおよびXenDesktop帯域幅ブログを参照）が、Thinwireでは3%のパケットが失われるため、有益なユーザーエクスペリエンスを保証するには、Framehawkよりもかなり大きな帯域幅が必要であることがわかります。

注：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るようになりました。早期のPreview版では、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、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した。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。

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。



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。

Framehawkでは、デフォルトで双方向の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のCitrix Receiverとの交換が行われます。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、必ず、十分な数のポートを定義します。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。

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。

Framehawk仮想チャネルを実装する前に、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。デフォルトのポート範囲を使用している環境では、外側のファイアウォールではUDPポート443、内側では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仮想チャネルはデフォルトでは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仮想チャネル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。

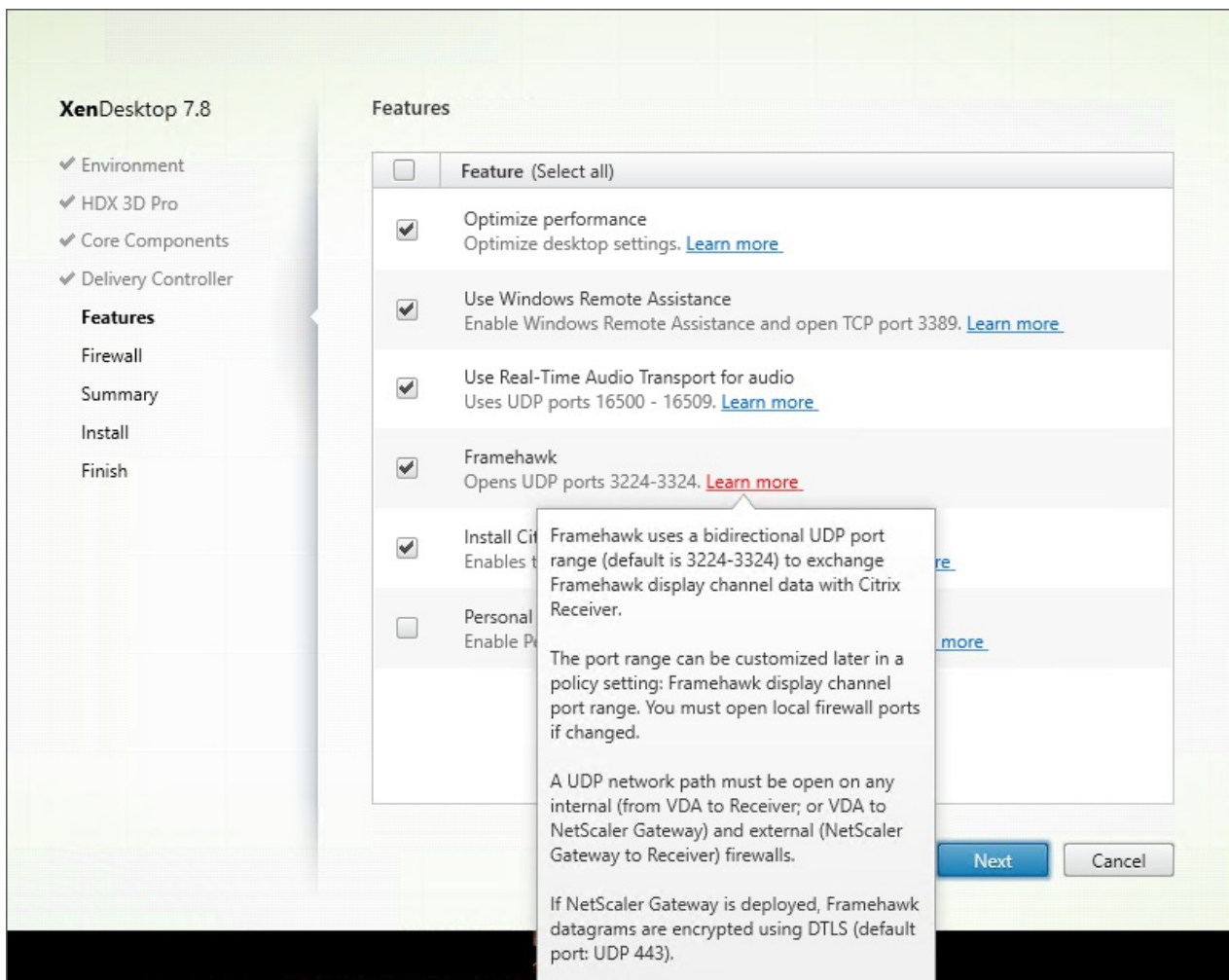
- **Framehawkディスプレイチャネル**：この機能を有効または無効にします。
- **Framehawkディスプレイチャネルのポート範囲**：VDAがユーザーデバイスとFramehawkディスプレイチャネルデータの交換に使用するUDPポート番号の範囲（最小ポート番号から最大ポート番号まで）を指定します。VDAは、各ポートの使用を試行します。まず、最小のポート番号から始めて、2回目以降の試行では1つずつ番号を増やしていきます。ポートは、受信トラフィックと送信トラフィックに使用されます。

Framehawkディスプレイチャネル用のポートの開放

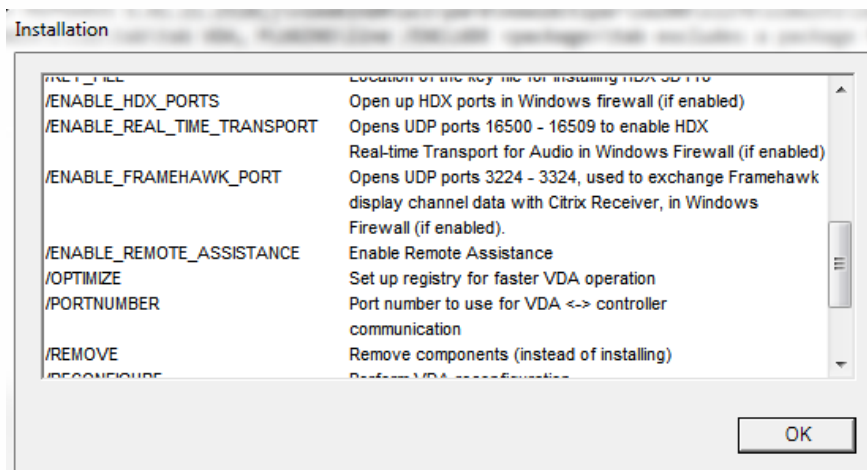
リリース7.8では、VDAインストーラーの**機能手順**でファイアウォールを再構成する新たなオプションが使用できるようになりました。このチェックボックスをオンにすると、WindowsのファイアウォールでUDPポート3224～3324が開放されます。以下の場合、手動でファイアウォールを構成する必要があることに留意してください。

- ネットワークファイアウォールの場合
- 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。

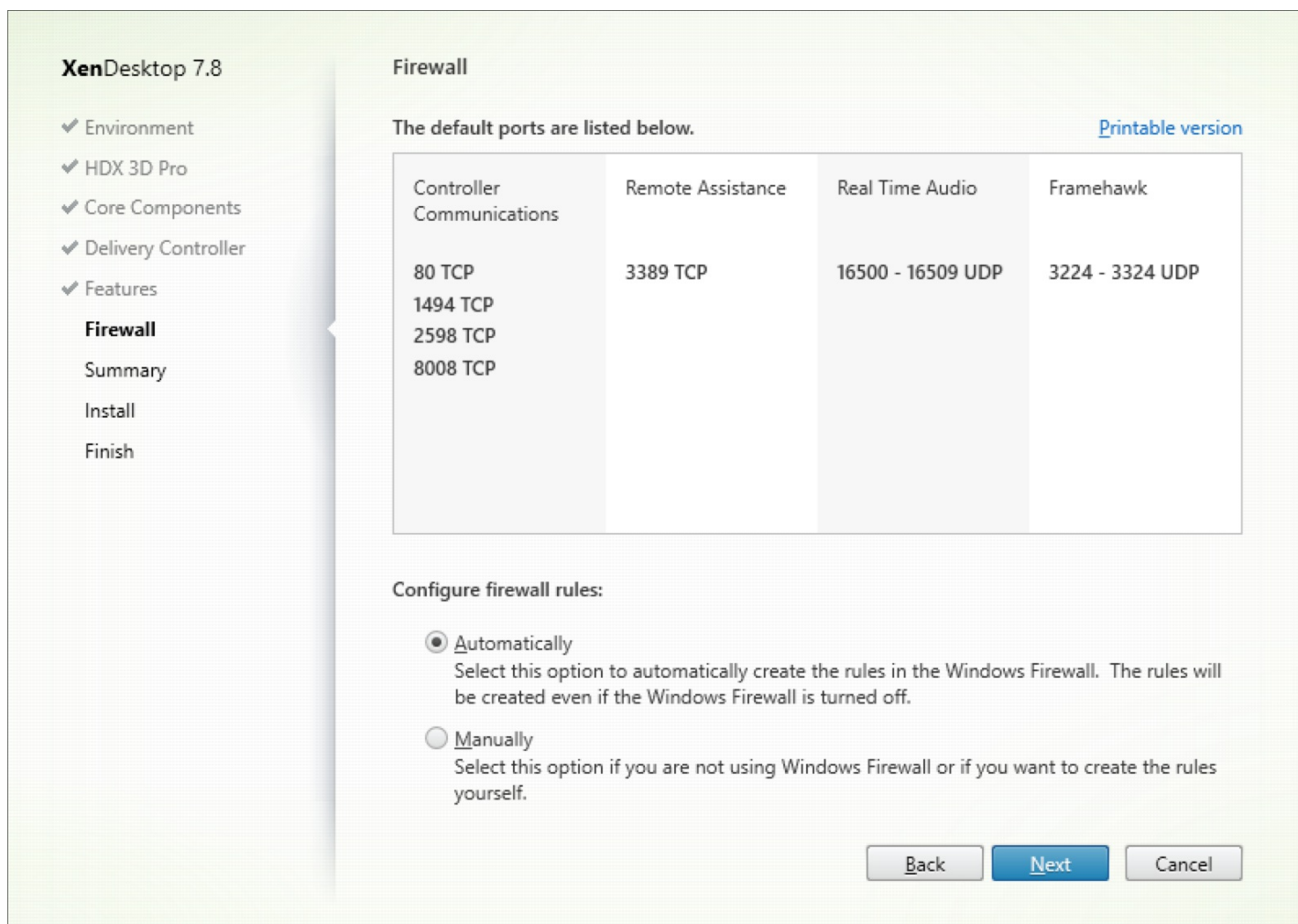


コマンドラインで `/ENABLE_FRAMEHAWK_PORT` を使用して、Framehawk 仮想チャネル用に UDP ポートを開放することもできます。

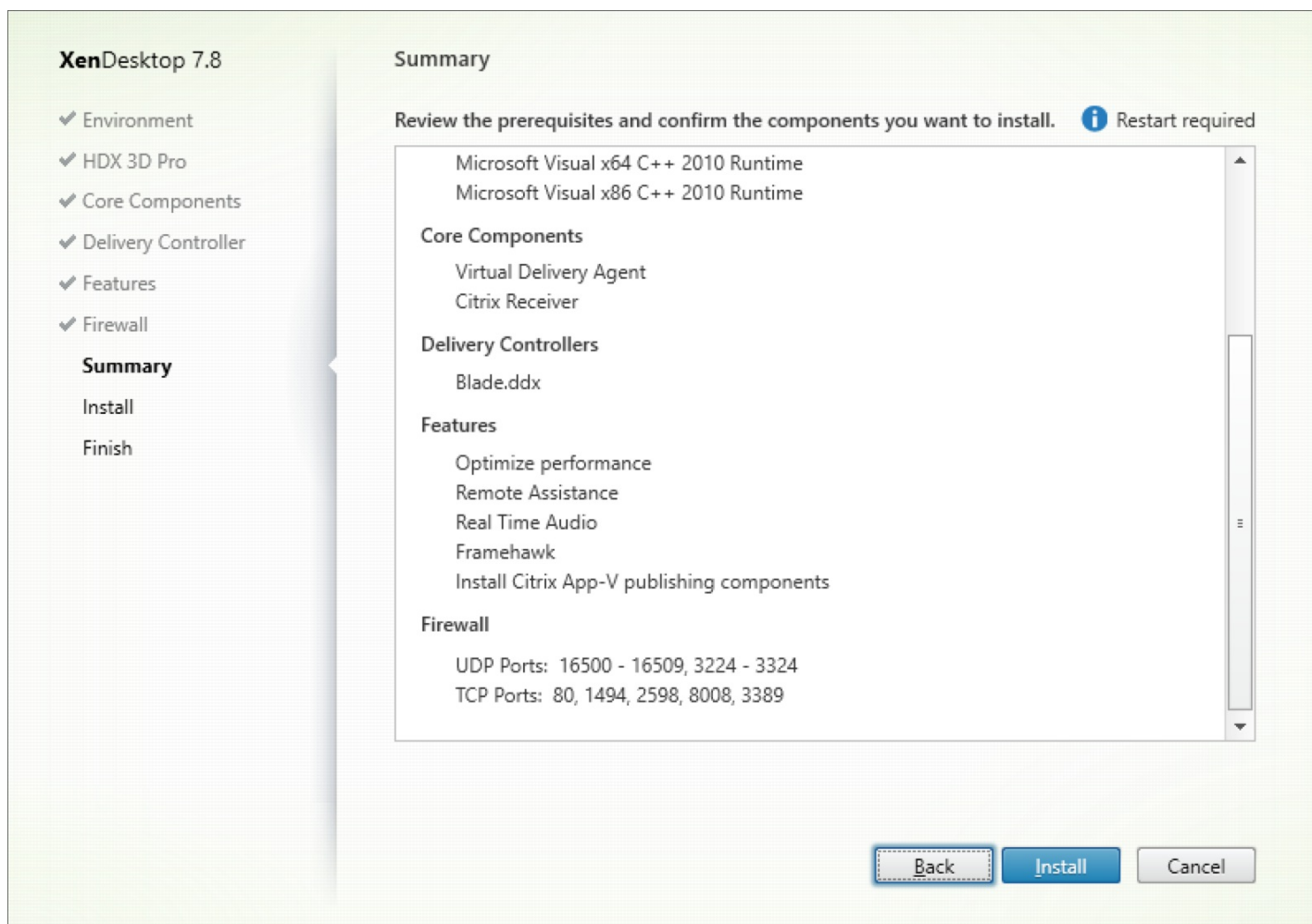


Framehawk の UDP ポートの割り当ての確認

インストール中に、Framehawk 仮想チャネルに割り当てられた 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。



[概要] 画面には、Framehawk仮想チャネル機能が有効になっているかどうかが表示されます。



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ーを参照します。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ディレクトリに接続します。
- 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を、Gateway VPN vServerはダミーのIP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Global Server Load Balancingの組合せです。

Framehawkでは、次のシナリオはサポートされません。

- HDX Insight
- IPv6モードのNetScaler Gateway
- NetScaler Gateway Double Hop
- NetScaler Gateway上の複数のSecure Ticket Authority (STA)
- 高可用性 (HA) 機能付きNetScaler Gateway
- 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	いいえ
IPv6モードのNetScaler Gateway	いいえ
NetScaler Gateway Double Hop	いいえ
NetScaler Gateway上の複数のSecure Ticket Authority (STA)	いいえ
高可用性 (HA) 機能付きNetScaler Gateway	いいえ
クラスターセットアップ付きNetScaler Gateway	いいえ

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。

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解除して再びバインドします。これは、NetScalerバージョン11.0.64.34以降をお使いの場合は行う必要がないことに注意してください。

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、証明書のキーペアをバインドするために、[+] をクリックします。
7. 前述の証明書のキーペアを選択し、[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における追加手順

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サーバーにバインドされているVPNvServer上で、DTLSパラメータを有効にします。

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

FramehawkをサポートするようにCitrix Receiver for iOSを構成するには、default.icaを手作業で編集する必要があります。

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。

これにより、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。Receive for Windowsを使用している場合、この手順は必要ありません。

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仮想チャネル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ングナリングチャネルで、これは最初のハンドシェイク中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。

HDX 3D Pro

Jul 07, 2016

HDX 3D Proを使用すると、OpenGLやDirectXテクノロジーを使用する専門的な3Dグラフィック処理アプリケーションなど、GPU（Graphics Processing Unit）でのハードウェアアクセラレーションに適したデスクトップおよびアプリケーションを配信できます。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、「[インストールの準備](#)」の「[VDAのインストール時に指定する事項](#)」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。

- ワイドエリアネットワーク（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。
- ローカルエリアネットワーク（LAN）接続の場合：帯域幅が100Mbpsの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。また、Citrix XenServerおよびNVIDIA社のGRID GPUを使用する環境では、WindowsデスクトップOSマシンで仮想GPU（vGPU）アクセラレーション機能を使用できます。サポートされるXenServerのバージョンについては、「[Citrix Virtual GPU Solution](#)」を参照してください。

Health Checkツールの後継であるHDX Monitorツールを使用すると、HDX仮想テクノロジー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。

Flashリダイレクト

Jul 07, 2016

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。

第2世代および従来のバージョンのFlashリダイレクトは個別のソリューションであり、異なる仮想チャネルで実行されます。

- 従来のバージョンのFlashリダイレクトは、クライアント側でのみサポートされます。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側でレンダリングされます。
- 第2世代の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。第2世代の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 7またはWindows 8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。

- [Flashアクセラレーションのデフォルトの動作] 設定を使用して、Flashアクセラレーションのデフォルトの動作を設定します。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（広告で使用するものなど）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。この機能を使用しても、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。
- [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：%Program Files%\Citrix\ICA Client\Configuration\ja
- 64ビットコンピューター：%Program Files (x86)%\Citrix\ICA Client\Configuration\ja

[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)。

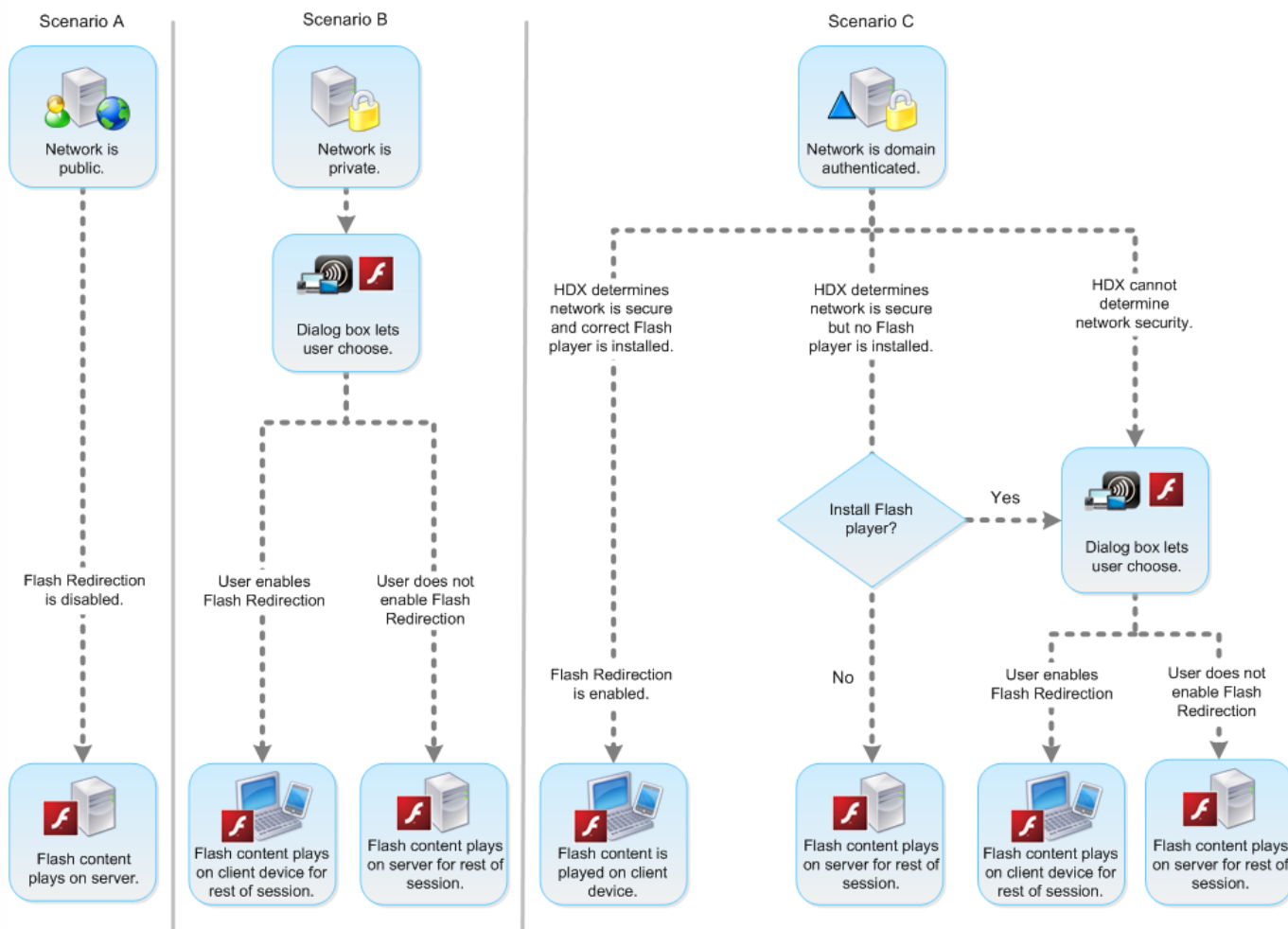
ポリシー設定が未構成である場合、Desktop Lock環境ではデフォルトでFlashリダイレクトが有効になります。

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。
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

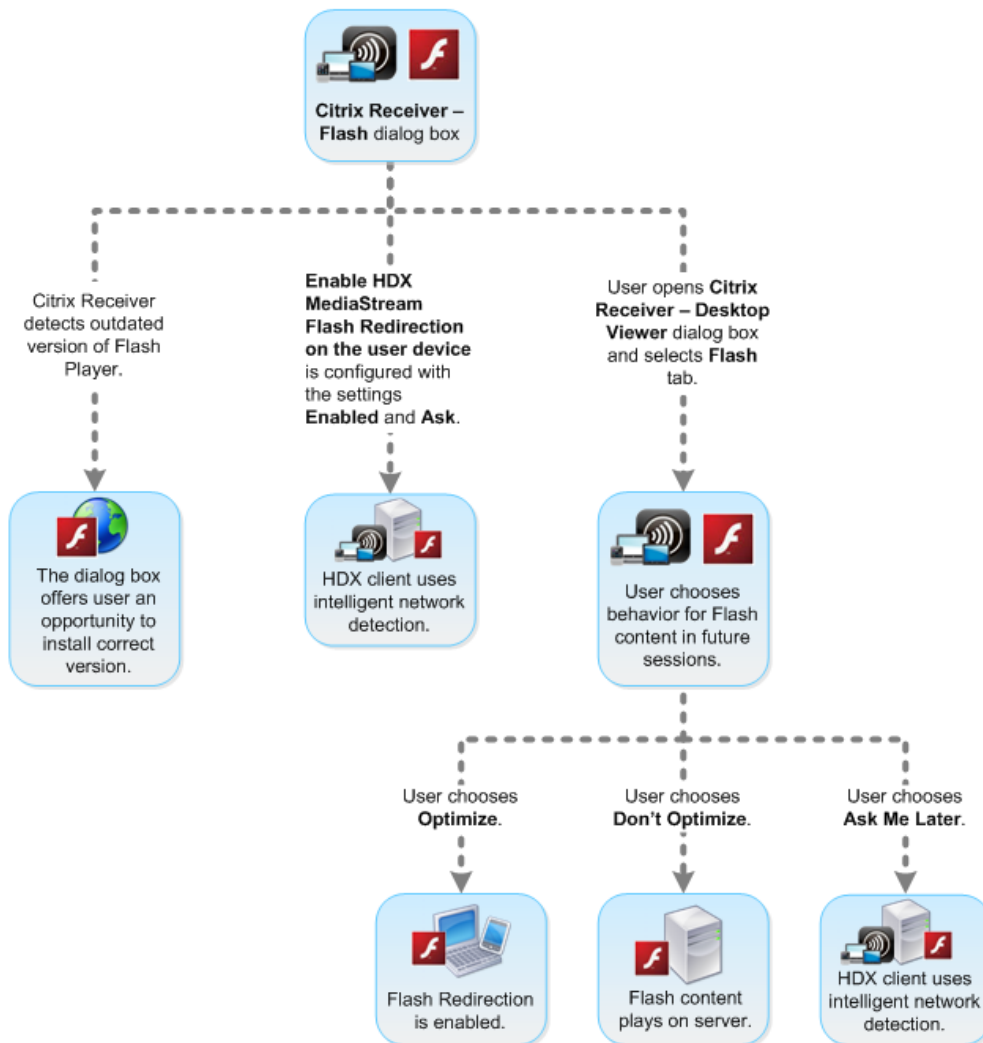
を使用するかどうかを確認するメッセージがユーザーに表示されます。ネットワークのセキュリティレベルを検出できない場合は、Flashリダイレクト機能を使用するかどうかを確認するメッセージがユーザーに表示されます。次の図は、さまざまなネットワークでFlashリダイレクトがどのように処理されるかを示しています。

Intelligent Network Detection for Flash Redirection



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。

User control of Flash redirection



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。

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。

第2世代の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つのオプションと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。

第2世代のFlashリダイレクトでは、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での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
Disabled	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[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アント側でのコンテンツ取得を使用する場合、Flashコンテ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Web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、Web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。デフォルトでは[未構成] が選択されています。[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。

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。

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。

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。現在、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に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Linux ICAクライアントを指定します。サブキーClientID0x1はWindows ICAクライアントを指定します。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。クライアントIDの完全な一覧は、Mobile SDK for Windows Appsドキュメント（<http://www.citrix.com/mobilitysdk/docs/clientdetection.html>）で確認できます。

32ビットVDAのレジストリ構成例

[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"

WindowsデスクトップOSのためのGPUアクセラレーション

Jul 15, 2016

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、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を含む物理ホストコンピューターと、GPUパススルー機能が有効なXenServer仮想マシン、および仮想GPUを持つXenServer仮想マシンをサポートします。

XenServerの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。

XenServerのvGPU機能を使用すると、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最適なWindows 7またはWindows 10デスクトップが提供されます。GPU共有では、NVIDIA GRIDカードがサポートされ（「[NVIDIA GRID](#)」参照）、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が使用されます。さらに、Intel Iris Graphicsを搭載した第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プロセッサのファミリーについて詳しくは、「[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](#)」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のデフォルトでは、CPUベースの深圧縮が使用されます。これにより、ネットワークの状態に応じて最適な圧縮が動的に適用されます。H.264ベースの深圧縮コーデックでは、NVIDIA GPU上のCUDAコアによるレンダリングが使用されません。深圧縮コーデックはCPU上で実行され、帯域幅消費が効率化されます。
- 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。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\Indicatorで新しいレジストリ設定を構成します。
 - 名前：HKLM_HotKey、種類：String
 - 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。

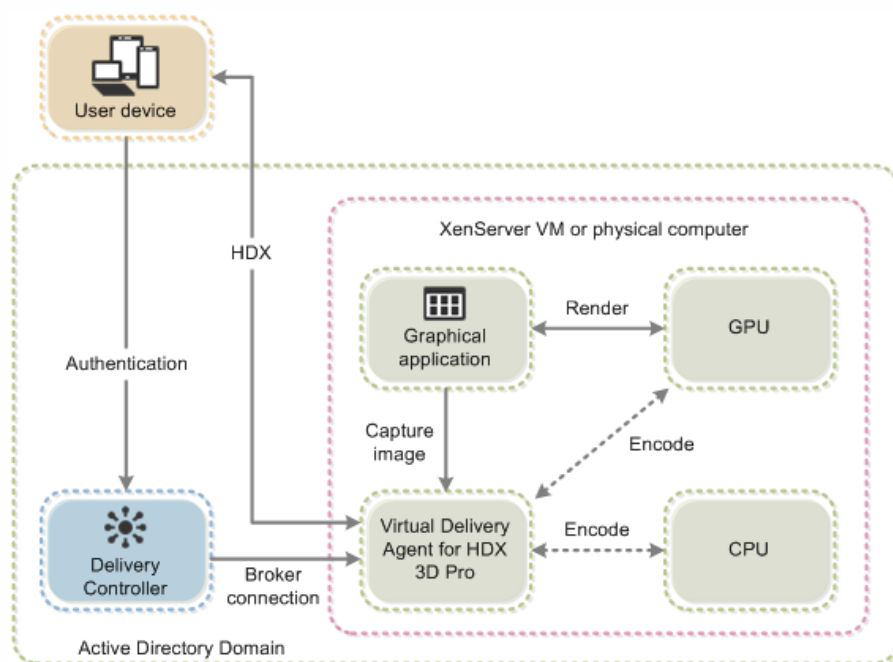
- 複数および高解像度モニターのサポート。Windows 10、Windows 8およびWindows 7のデスクトップでは、最大で4つのモニターが構成されたユーザーデバイスがサポートされます。ユーザーはそれらのモニターを自由に配置でき、解像度や向きが異なるモニターを組み合わせで使用できます。モニターの数は、ホストコンピュータのGPU、ユーザーデバイス、および使用できる帯域幅による制限を受けます。HDX 3D Proでは、ホストコンピュータ上のGPUでサポートされるすべてのモニター解像度がサポートされます。
また、Windows XPデスクトップでは、デュアルモニター構成が限定的にサポートされます。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 Kepler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](#)）。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。
- Intel Iris Pro Graphicsを搭載した第5世代および第6世代のIntel CPUがサポートされます。HDX 3D Proでは、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。サポートされるIntelプロセッサのファミリーについて詳しくは、「[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](#)」を参照してください。

以下の図を参照してください。

- ホストコンピュータは、Delivery Controllerと同じActive Directoryドメインに属している必要があります。
- 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 for HDX 3D Proをインストールしてください。 同様に、標準のVDA for Windows Desktop OSをVDA for HDX 3D Pro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 for HDX 3D Proをインストールしてください。

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。 Montereyenable.exe -enable -noreset コマンドを実行してからVDAを再起動します。

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Montereyenable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、Montereyenable.exe -disable -noreset コマンドを実行してからVDAを再起動します。

Intelドライバーのインストール

この手順は、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。

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を使用してコマンド **GfxDisplayTool.exe -vd enable** を実行し、次にVDAを再起動します。

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。

WindowsサーバーOSのためのGPUアクセラレーション

Jul 07, 2016

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。

HDX 3D Proにより、複数のユーザーがグラフィックカードを共有できるようになります。HDX 3D ProとXenServerのGPUパススルー機能を使用すると、単一のサーバーで複数のグラフィックカード（各仮想マシンに1つずつ）をホストできるようになります。

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ます。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。

- ペ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またはVMware vSphere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。
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

GPU共有でのスケラビリティは、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

たとえば、NVIDIA Q6000およびM2070Qカードを使用してESRI ArcGISなどのアプリケーションを実行する場合、8~10人のユーザーがサポートされました。これらのカードでは、6GBのビデオRAMが提供されます。より新しいNVIDIA GRIDのビデオ

オRAMは8GBで、処理能力も向上しています（より多くのCUDAコアで構成されている）。NVIDIA GRID K2カードの場合、GRID K2カードあたり最大20人のユーザーで良好なパフォーマンスが得られました。ほかのアプリケーションを使用する場合のスケラビリティはさらに高く、上位クラスのGPUで32人の同時ユーザーがサポートされます。

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 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 Server 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\ApplInit_Dlls\Multiple Monitor Hook]
"EnableWPFHook"=dword:00000001
 - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit_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、概念実証 (POC) としてのみサポートされます。この機能はデフォルトで無効になっていますが、テストまたは評価のために有効にすることができます。

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\ApplInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit_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\ApplInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit_Dlls\Graphics Helper]
"OpenCL"=dword:00000001

OpenGLソフトウェアアクセラレータ

Jul 07, 2016

OpenGLソフトウェアアクセラレータは、ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、CAD、およびCAM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。

重要：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、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。このソフトウェアは、一部のアプリケーションで動作しない場合があります。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で動作する場合は、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Support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。

- 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場合は、OpenGLアクセラレータを使用してテストを行います。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。

オーディオ機能

Jul 07, 2016

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。

重要：多くのオーディオ機能はICAストリームを使って転送され、ほかのICAトラフィックと同じ方法で保護されます。NetScaler Access Gatewayがパス上にない場合、ユーザーデータグラムプロトコル（UDP）オーディオでは、これとは別の保護されていない転送メカニズムが使用されます。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。

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、[音質] 設定で [高 - 高品位オーディオ] が指定されています。これにより、HiFiステレオオーディオが提供されますが、ほかの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。

たとえば、ダイヤルアップで接続するユーザーグループとLANまたはWANで接続するユーザーグループに、異なるポリシーを作成します。ダイヤルアップ接続では帯域幅が限られているため、低い音質レベルを指定したポリシーを適用して、音質よりもセッションパフォーマンスを向上させます。LANまたはWANで接続するユーザーグループに対しては、高い音質レベルを指定したポリシーを適用します。

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 [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、ポリシーに [クライアントオーディオリダイレクト] 設定を追加して [許可]（デフォルト）を指定します。

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

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、ポリシーに [クライアントマイクリダイレクト] 設定を追加して [許可]（デフォルト）を指定します。

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、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。

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。

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。
 - **設定しない**：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。
 - **Enabled**。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オーディオの場合のみ、[リアルタイムトランスポートを有効にする] 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。

-command

コピー

```
; 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
```

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。スピーカーとマイクは、近づけすぎず遠ざけすぎず、最適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。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。

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
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。

ネットワークトラフィックの優先度

Jul 07, 2016

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/IP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1つのUDP/RTPストリーム（ボイス）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 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、[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、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す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 CloudBridge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インする必要があります。

USBとクライアント側ドライブの考慮事項

Jul 07, 2016

HDX USBデバイスリダイレクト機能を使用すると、デスクトップでホストされるアプリケーションや仮想デスクトップを使用しているときに、ローカルコンピューターに装着したUSBフラッシュドライブにアクセスできるようになります。セッション内で、デジタルカメラなどの画像転送プロトコル (PTP) デバイス、デジタルオーディオプレーヤーやポータブルメディアプレーヤーなどの、メディア転送プロトコル (MTP) デバイス、およびPOS (Point-Of-Sale) デバイスを接続して使用できます。

デスクトップでホストされるアプリケーションのセッションでは、ダブルホップUSBはサポートされません。

USBリダイレクトは、Citrix Receiver for WindowsおよびCitrix Receiver for Linuxを使用しているユーザーに対してのみ有効です。

USBリダイレクトのデフォルトでは、特定のクラスのUSBデバイスでのみ許可され、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のドキュメントを参照してください。管理者は、リダイレクトするUSBデバイスの一覧を変更して、仮想デスクトップで使用可能になるUSBデバイスの種類を制限できます。

Important

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は、使用を禁止するUSBデバイスの種類についてユーザーに通知してください。

一般的なUSBデバイスをリダイレクトするための仮想チャネルが最適化されており、WAN接続でも良好なパフォーマンスが提供されます。サポートされる機能は、ユーザーデバイス上にインストールされたCitrix Receiverにより異なります。低速な狭帯域幅接続では、最適化された仮想チャネルを使用することで最高のパフォーマンスが得られます。

SMARTのUSBリダイレクトでSMARTボードを使用する場合、マウスとして処理されます。

ただし、最適化された仮想チャネルでUSB 3.0デバイスおよびUSB 3.0ポートを使用して、CDM仮想チャネルを使用してカメラ内のファイルを表示したり、ヘッドセットでオーディオを再生したりできます。USB 3.0デバイスをUSB 2.0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。

最適化された仮想チャネルを使用できない特殊なデバイスは、汎用USB仮想チャネルを使用してリダイレクトされます。XenDesktopでテストされているUSBデバイスについては[CTX123569](#)を参照してください。

Webカメラのヒューマンインターフェイスデバイス (HID) ボタンなど、一部のデバイス固有の機能は、最適化された仮想チャネルで正しく動作しない場合があります。問題が発生する場合は、汎用USB仮想チャネルを使用してください。

一部のデバイスはデフォルトではリダイレクトされず、ローカルセッションでのみ使用可能になります。たとえば、ユーザーデバイスの内部USBでシステムボードに装着されたネットワークインターフェイスカードは、リモートで動作する仮想デスクトップでの使用には適しません。

以下のCitrixポリシー設定を使ってUSBサポートを制御します。

- クライアントUSBデバイス最適化規則。たとえば署名デバイスや描画タブレットなど、class=03の入力デバイスで最適化モードはサポートされます。規則が指定されていない場合は、デバイス(インタラクティブモード (02) で制御されます。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。
- クライアントUSBデバイスリダイレクト。デフォルトでは「禁止」が設定されています。
- クライアントUSBデバイスリダイレクト規則。規則は汎用USBリダイレクトを使用するデバイスにのみ適用されます。このため、クライアント側ドライブマッピング (CDM) など、専用のリダイレクト機能や最適化されたリダイレクト機能を使用するデバイスには、規則が適用されません。
- 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。デフォルトで「許可」が設定されており、ユーザーセッションでのPTP、MTP、およびPOSデバイスのプラグアンドプレイ機能が有効になります。
- USBデバイスリダイレクトの最大帯域幅 (Kbps)。デフォルトでは0が設定されており、帯域幅に制限はありません。
- USBデバイスリダイレクトの最大帯域幅 (%)。デフォルトでは0が設定されており、帯域幅に制限はありません。

汎用USBリダイレクトについて

汎用USBリダイレクトは、最適化された仮想チャネルがないUSBデバイスに特化しています。この機能では、任意のUSBデバイスをクライアントマシンから仮想デスクトップにリダイレクトします。これにより、ユーザーはさまざまな種類の汎用USBデバイスを、デスクトップセッションに物理的に接続されているかのように使用できます。

以下の考慮事項があります。

- 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。

この機能は、Version 7.6以降のVDA for Desktop OSのデスクトップセッションでサポートされます。

この機能はまた、次の制限によりVersion 7.6以降のVDA for Server OSのデスクトップセッションでもサポートされます。

- VDAマシンはWindows Server 2012 R2で実行する必要があります。
- シングルホップのシナリオだけがサポートされます。
- USBクライアントドライバーはRDSH for Windows 2012 R2と互換性がある必要があります。
- USBストレージデバイス、オーディオデバイス、スマートカードリーダー、および完全には仮想化されていないデバイスではサポートされません。

汎用USBリダイレクトの構成について詳しくは、[CTX137939](#)を参照してください。

USBサポートの有効化

- ポリシーを作成し、[クライアントUSBデバイスリダイレクト]設定を追加して「許可」を選択します。
- 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。
- 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。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。

仮想デスクトップで利用できるUSBデバイスの一覧の変更 (Citrix Receiver for Windows 4.2)

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、デスクトップブ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。ただし、必ずしもすべてのUSBデバイスをリダイレクトするのが適切だとは限りません。詳しくは、[CTX123015](#)を参照してください。

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。USBデバイスを一覧に表示しないよう

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、クライアントおよびVDA上でデバイス規則を定義します。

- Citrix ReceiverおよびVDAのUSBデバイスリダイレクト規則でリダイレクトするUSBデバイスの種類を指定すると、デフォルトのUSBポリシー規則よりも優先されます。
- 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。
 - グループポリシー規則を介して、サーバーOSマシンの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

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ます、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
Class	デバイス記述子またはインターフェイス記述子のクラス。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

- 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。

Important

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。

マスのストレージデバイスなど、最適化されたデバイスを使用する場合は、一般的にポリシーの規則を使用せず、専用のCDMチャネルを使用してデバイスをリダイレクトします。ただし、これらにいては次のいずれか方法で無効にできます。

- 汎用USBリダイレクトを使って手動で最適化されたデバイスをリダイレクトするには、[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。
- 汎用USBリダイレクトを使って最適化されたデバイスを自動的にリダイレクトするには、ストレージデバイスの自動リダイレクトを設定し（たとえばAutoRedirectStorage = 1）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。

- 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 # Allow Logitech SpaceNavigator 3D Mouse      Deny: VID=046D # Deny all Logitech products
```
 - 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 # Deny MS Active Sync devices      Allow: Class=EF SubClass=01 # Allow Sync devices      Allow: Class=EF # Allow all USB-Miscellaneous devices
```

仮想デスクトップで利用できるUSBデバイスの一覧の変更

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、デスクトップブライアンモードを使用している場合や、デスクトップでホストされるアプリケーションを実行している場合も、USBデバイスが自動的にリダイレクトされます。ただし、必ずしもすべてのUSBデバイスをリダイレクトするのが適切だとは限りません。詳しくは、[CTX123015](#)を参照してください。

Desktop Viewerのユーザーは、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。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、ユーザーデバイスおよびVDA上でデバイス規則を定義します。

- Citrix ReceiverおよびVDAのUSBデバイスリダイレクト規則でリダイレクトするUSBデバイスの種類を指定すると、デフォルトのUSBポリシー規則よりも優先されます。デバイス規則は、Citrix ReceiverとVDAの両方に適用されます。デバイスが正しくリダイレクトされるように、両方の規則を変更する必要があります。
- ユーザーデバイスのレジストリ（またはCitrix Receiver for Linuxの場合は.iniファイル）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。
- サーバーOSマシン上のVDAレジストリにある、管理者による上書き規則を編集します。 インストールメディアに収録されているADMファイル (\\os\\lang\\Support\\Configuration\\vda_usb.adm) により、Active Directoryのグループポリシーを使用してVDA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
Class	デバイス記述子またはインターフェイス記述子のクラス。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

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。

Important

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。

マストレージデバイスなど、最適化されたデバイスを使用する場合は、一般的にポリシーの規則を使用せず、専用のCDMチャネルを使用してデバイスをリダイレクトします。ただし、これらについては次のいずれか方法で無効にできます。

- 汎用USBリダイレクトを使って手動で最適化されたデバイスをリダイレクトするには、[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。
- 汎用USBリダイレクトを使って最適化されたデバイスを自動的にリダイレクトするには、ストレージデバイスの自動リダイレクトを設定し（たとえばAutoRedirectStorage = 1）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。

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 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
- 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 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices

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マストレージデバイス

マストレージデバイスの場合はクライアント側ドライブのマッピング機能が適用され、ユーザーのログオン時にユーザーデバイス上のマストレージデバイスが自動的に仮想デスクトップ上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]カテゴリの [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。

クライアント側リムーバブルドライブマッピングとUSBサポートの2つの設定の主な違いは以下のとおりです。

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

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
読み取り専用アクセスの構成が可能	はい	いいえ
セッション中にデバイスを安全に取り外せる	いいえ	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。

マップされたクライアントドライブのファイルアクセス

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。

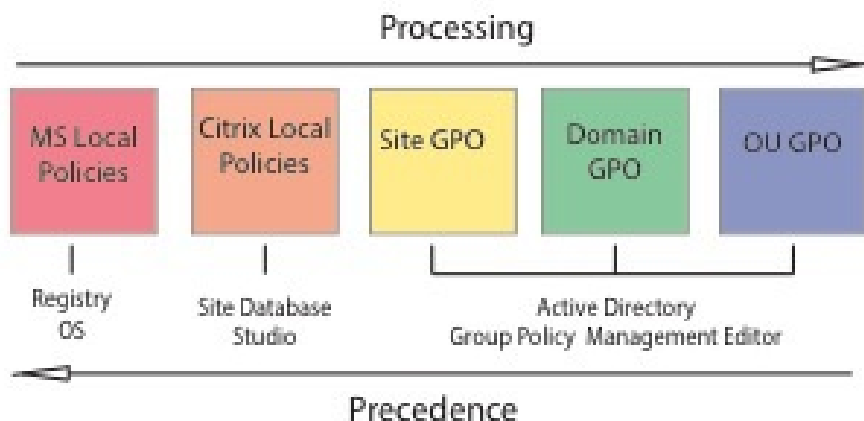
マップされたクライアント側ドライブ上のフォルダーやファイルの追加や変更を禁止するには、[クライアント側ドライブへの読み取り専用アクセス]設定を有効にします。この設定項目をポリシーに追加するときは、[クライアントドライブリダイレクト]設定も追加されており、[許可]が選択されていることを確認してください。

Policies

Jul 07, 2016

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われます。

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と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

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Microsoft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](#)

ポリシーの使用

Jul 07, 2016

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る

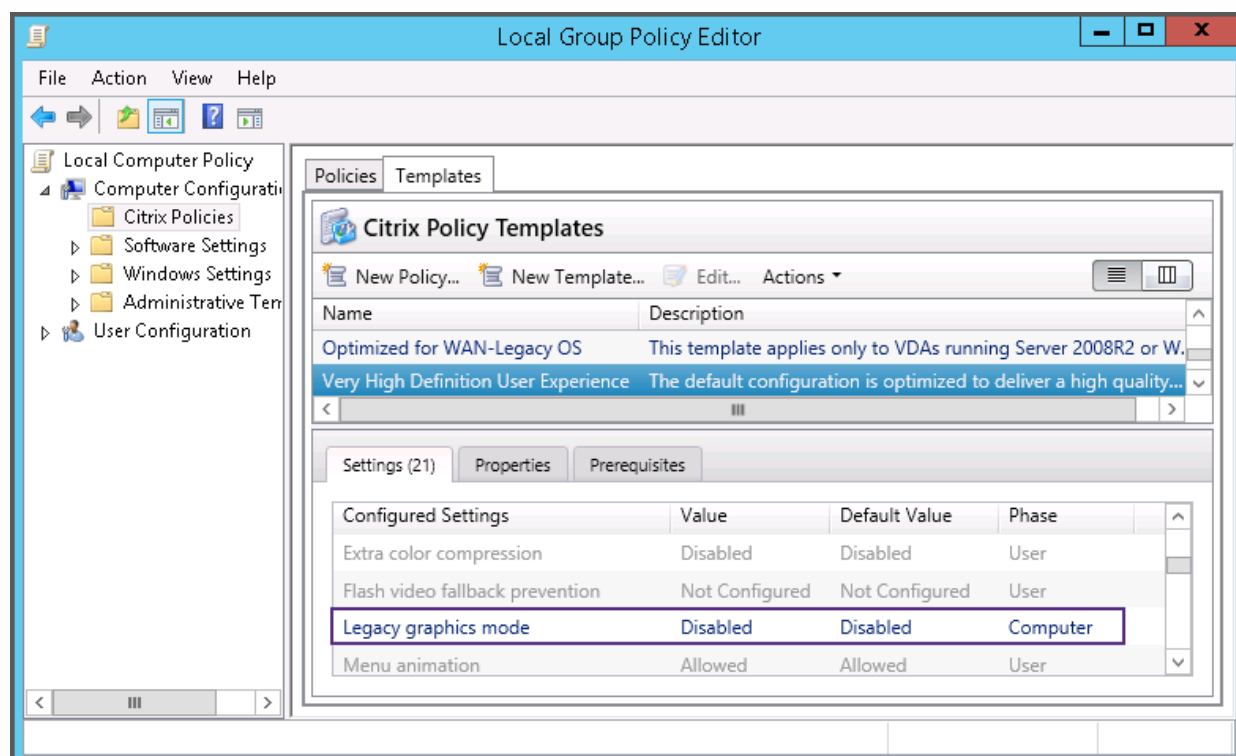
るには、[すべての設定]を選択します。

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。



ポリシーテンプレート

Jul 07, 2016

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。

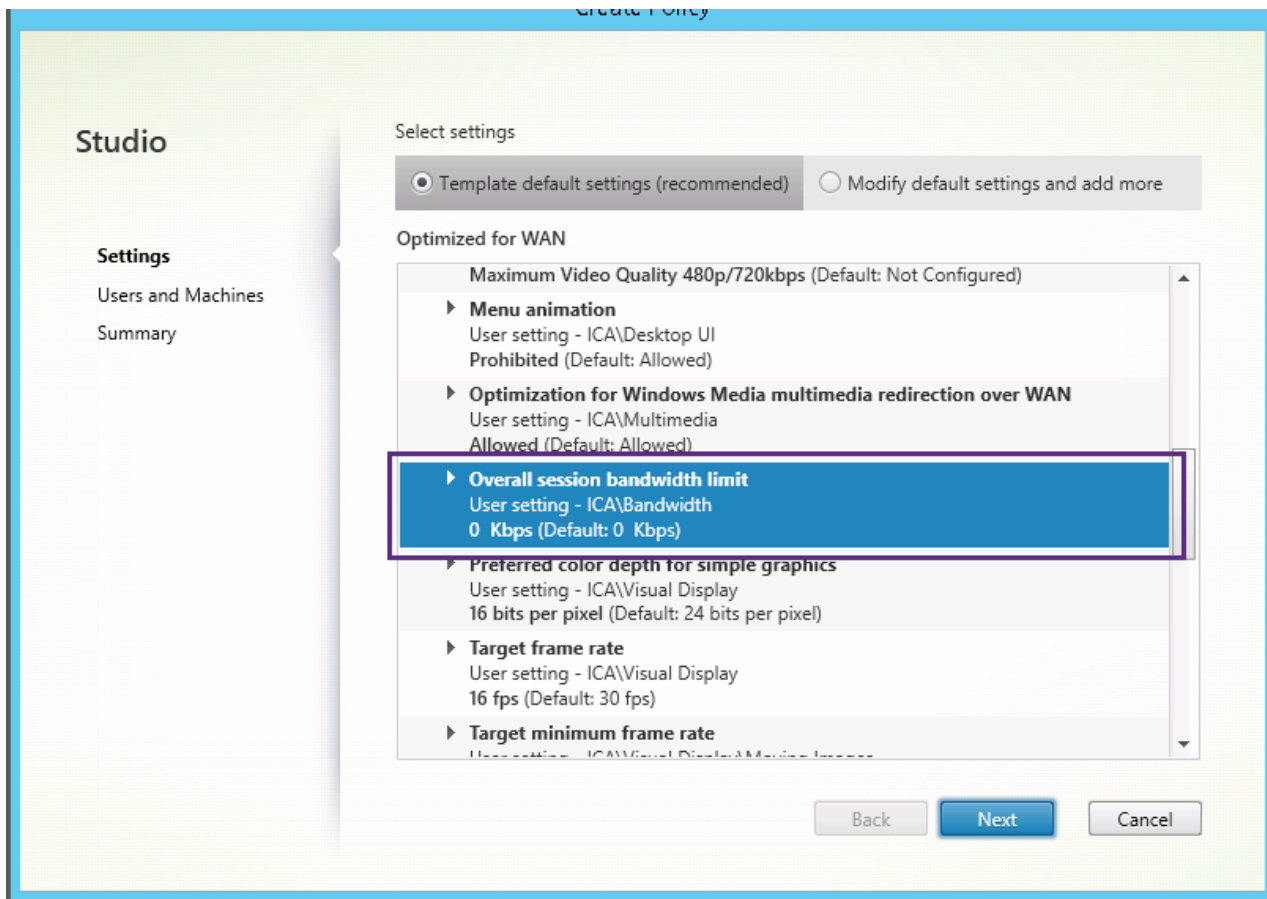
組み込みのCitrixテンプレート

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。
- **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おいて、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。

Create Policy



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：

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

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。

ポリシーの作成

Jul 07, 2016

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。

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
Delivery Group	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Hot fixを入手してインストールしてください。
ユーザーまたは	ユーザー名またはグループ名。

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は社内ネットワークのアドレス（10.8.169.*）に適用される「クライアントのIPアドレス」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、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。

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

既存のポリシーの優先度を変更する 目的	「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 手順
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

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

Jul 07, 2016

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：いわゆる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で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

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つの割り当てが追加されたポリシーは、[クライアントのIPアドレス] 割り当てで指定したアドレスのすべてのユーザーに適用されます。ただし、[ユーザーまたはグループ] 割り当てで指定したユーザーには、IPアドレスが指定した範囲内であっても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項目を基に、最終的に適用される設定項目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。

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、そのポリシーの割り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。

デフォルトのポリシー設定

Aug 26, 2016

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
ICAリスナー接続タイムアウト	120000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	禁止	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

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
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。

名前	デフォルト設定	VDA
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

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、VDA

名前	デフォルト設定	VDA
デスクトップコンポジションの画質	許可	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	Disabled	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
クライアント側フロッピードライブ	許可	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

名前	クライアント側リムーバブルドライブ	許可 デフォルト 設定	VDA 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	Disabled	Disabled	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	Disabled	Disabled	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	Disabled	Disabled	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	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	Disabled	Disabled	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	Disabled	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	Disabled	VDA for Server OS 7以降、VDA for 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	Disabled	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

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ディスプレイチャンネル	Disabled	VDA 7.6 FP2以降
Framehawkディスプレイチャンネルポートの範囲	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する	禁止	VDA for Server OS 7以降、VDA for Desktop OS 7以降
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 この設定はデフォルトで無効になっており、Windows 10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
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
ビデオ負荷管理ポリシー設定	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、VDA for Desktop OS 7以降
Windowsメディアリダイレクト	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サイズ使用	Disabled	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	Disabled	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	Disabled	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	Disabled	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	Disabled	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
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

名前	デフォルト設定	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）	Disabled	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	Disabled	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
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	Disabled	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のキャッシュ - 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	すべてのバージョンのVDA
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

名前	デフォルト設定	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	Disabled	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	1440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	Disabled	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	1440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	1440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

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	規則の指定なし	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
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	Disabled	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	Disabled	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
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	Disabled	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	Disabled	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	Disabled	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	Disabled	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	Disabled	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
ログオフ時のインターネットCookieファイルの処理	Disabled	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	Disabled	すべてのバージョンのVDA
Profile managementの有効化	Disabled	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	Disabled	すべてのバージョンの

名前	デフォルト設定	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	Disabled	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	Disabled	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	Disabled	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
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
名前	デフォルト設定	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	Disabled	すべてのバージョンのVDA
ドメイン名を包含	Disabled	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

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

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

名前	デフォルト設定	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

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	Disabled	すべてのバージョンのVDA
一般的な情報	Disabled	すべてのバージョン

名前	デフォルト設定	VDA
一般的な警告	Disabled	すべてのバージョンのVDA
ログの有効化	Disabled	すべてのバージョンのVDA
ファイルシステム操作	Disabled	すべてのバージョンのVDA
ファイルシステム通知	Disabled	すべてのバージョンのVDA
ログオフ	Disabled	すべてのバージョンのVDA
Logon	Disabled	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	Disabled	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	Disabled	すべてのバージョンのVDA
レジストリ操作	Disabled	すべてのバージョンのVDA
ログオフ時のレジストリ差分	Disabled	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	Disabled	すべてのバージョンのVDA

名前	デフォルト設定	VDA
カルプロファイル競合の制御	デフォルト設定ファイルを使用	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	Disabled	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	Disabled	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	Disabled	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

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	Disabled	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	Disabled	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 デフォルト設定	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	Disabled	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

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	Disabled	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

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 名前	デフォルト設定	VDA 5.5、5.6 FP1 VDA

ポリシー設定リファレンス

Jul 07, 2016

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

目的	使用するポリシー設定
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

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、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

目的	使用するポリシー設定
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 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アクセルレーションのデフォルトの動作 - 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

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 - 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
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

- o 負荷分散のためのユニバーサルプリントサーバー
- o 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

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。

ICAのポリシー設定

Jul 07, 2016

[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。

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。

デフォルトでは許可されます。

これを禁止すると、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ができなくなります。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
- 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形式を有効にすると、クリップボードコピーのサポート（HTML形式）により、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、形式名の太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]または[無効]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。

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に接続できます。

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プロトコルで使用する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、ほかの既知のポート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機能は許可されません。

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、無効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、無効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

[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が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形式を有効にすると、クリップボードコピーのサポート（HTML形式）により、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[セッションクリップボードの書き込み制限]設定で[禁止]または[無効]が設定されている場合、この設定項目は無視されます。

クライアントの自動再接続のポリシー設定

Jul 07, 2016

「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。

デフォルトでは許可されます。

自動再接続を許可すると、ユーザーはセッション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。

ただし、ユーザーのセッションIDと資格情報を保持するCookieが使用されない場合は、既存のセッションに再接続できず、新しいセッションが開始されることがあります。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、ユーザーが意図的に切断したセッションには再接続されません。

アプリケーションセッションでは、自動再接続が許可される場合、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、自動再接続が許可される場合、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。

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>

<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。

デフォルトでは、認証は要求されません。

ユーザーが最初にセッションにログオンすると、そのユーザーの資格情報は暗号化されてメモリ上に格納され、その暗号キーを含んだCookieが作成され、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。

クライアントの自動再接続のログ

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。

デフォルトでは、ログは無効になっています。

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。

オーディオのポリシー設定

Jul 07, 2016

【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と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。

- 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デ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え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、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。

帯域幅のポリシー設定

Jul 07, 2016

「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。

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) 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

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

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。

クライアントセンサーのポリシー設定

Jul 07, 2016

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。

デスクトップUIのポリシー設定

Aug 26, 2016

【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個人優先設定の変更は、デスクトップの変更です。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。

エンドユーザーモニタリングのポリシー設定

Jul 07, 2016

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。

デスクトップエクスペリエンス拡張のポリシー設定

Jul 07, 2016

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、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ほか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。

ファイルリダイレクトのポリシー設定

Jul 07, 2016

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。

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、すべてのクライアント側ドライブにファイルを保存できなくなります。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ブ

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。

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。

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。

Flashリダイレクトのポリシー設定

Jul 07, 2016

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。

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
```

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。

- 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。

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す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。
- **【サーバー側のコンテンツなし】**：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。ユーザーデバイス側でWebサイトからFlashコンテンツを取得できず、Webサイトが [Flashサーバー側でのコンテンツ

取得URLリスト]で指定されている場合、サーバー側コンテンツの取得が自動的に行われます。

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。

グラフィックのポリシー設定

Jul 07, 2016

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。

デフォルトでは、65536キロバイトに設定されます。

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 $(32\text{bpp} \div 8) \times (600\text{ピクセル}) \times (800\text{ピクセル}) = 1920000\text{バイト}$ 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。

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を無効にして、従来の表示モードにフォールバックします。これにより、WANやモバイル接続時のスケーラビリティが向上します。

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。このモードはWindows 2012および2012 R2でもサポートされますが、推奨はされません。

従来のグラフィックモードは、Windows 10、8.1、8ではサポートされません。

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。

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

Windows 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を使用できます。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[ビデオコーデックを使用しない]に指定すると、静止画像圧縮とビットマップ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。

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。

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、[可能な場合はビデオコーデックを使用する]を選択します。

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。

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。

キャッシュのポリシー設定

Jul 07, 2016

【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ず。

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。

Framehawkのポリシー設定

Jul 07, 2016

Framehawkセクションには、サーバーでFramehawkディスプレイチャンネルを有効化し、構成するためのポリシー設定が含まれます。

Framehawkディスプレイチャンネル

この機能を有効にすると、サーバーはFramehawkディスプレイチャンネルを使用して、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。この表示チャンネルは、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も多くなります。

デフォルトでは、Framehawkディスプレイチャンネルは無効になっています。

Framehawkディスプレイチャンネルポートの範囲

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ディスプレイチャン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。

Keep-Aliveのポリシー設定

Jul 07, 2016

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。

ローカルアプリケーションアクセスのポリシー設定

Jul 07, 2016

〔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。

モバイルデバイスでの動作のポリシー設定

Jul 07, 2016

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

この設定はデフォルトで無効になっており、Windows 10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。

マルチメディアのポリシー設定

Jul 07, 2016

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。

ビデオ品質の制限

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

注：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とがあります。

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メディアリダイレクト] 設定で [許可] が選択されていることを確認してください。

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インストール済みである。
- ビデオ会議セッションを始める前に、Webカメラがユーザーデバイスに接続済みである。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、最初に検出されたものから接続が試行されます。

WAN接続でのWindows Mediaマルチメディアリダイレクトの最適化

この設定を許可すると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、オーディオやビデオのメディアコンテンツをモバイルデバイスにストリーム配信したり、WAN上でのWindows Mediaコンテンツの配信を最適化してユーザーエクスペリエンスを向上させたりします。

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メディアリダイレクト] 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じ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

この設定項目では、リアルタイムマルチメディアトランスコードの処理をVirtual Delivery Agent (VDA) 側のGPU (Graphics Processing Unit) で行い、サーバーのスケーラビリティを向上させる機能を許可または禁止します。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が搭載されてい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コンテンツ配信を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。

ビデオフォールバック防止

管理者はビデオフォールバック防止ポリシー設定を使って、ストリーム配信されたコンテンツをユーザーに配信する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。これにより、サーバー側でのフォールバックへのRAVEに対するクライアント側での取得を可能にします。

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。

- **Server Fetched - Server Rendered**。サーバー側でのフォールバックへのRAVEに対するクライアント側での取得を可能にします。
- **Server Fetched - Client Rendered**。RAVEフォールバックに対するクライアント側での取得を可能にしますが、サーバー側でのレンダリングフォールバックへのRAVEをブロックします。
- **Client Fetched - Client Rendered**。サーバー側でのレンダリングフォールバックへのRAVEに対するクライアント側での取得をブロックします。

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。

Windows Mediaのクライアント側でのコンテンツ取得

この設定では、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。

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側で処理されるため、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、マルチメディアをURLから再生する機能だけが使用されます。

この設定をポリシーに追加するときは、[Windowsメディアリダイレクト] 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] 設定で [禁止] を選択すると、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メディアリダイレクト

この設定では、サーバーでのストリーミングオーディオとビデオの配信方法を制御および最適化します。

デフォルトでは、ストリーミングオーディオとビデオのユーザーデバイスへのストリーム配信が許可されます。

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 Direct 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。

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 Direct 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 Direct のバッファースize

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スize を 1~10 秒の間で指定します。

デフォルトのバッファースize は 5 秒です。

Windows Media Direct のバッファースize 使用

この設定では、[Windows Media Direct バッファースize] 設定で指定したバッファースize 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スize が使用されません。

この設定が無効の場合、または Windows Media Direct バッファースize 設定が構成されていない場合、サーバーはデフォルトのバッファースize 値 (5 秒) を使用します。

マルチストリーム接続のポリシー設定

Jul 07, 2016

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「,」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する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 CloudBridge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。

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：この設定項目を、帯域幅を制限する設定項目（[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。

ポートリダイレクトのポリシー設定

Jul 07, 2016

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が送信されます。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 (%)

印刷のポリシー設定

Jul 07, 2016

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。この場合、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

使用する場合は、[変更しない]を選択します。この場合、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。

クライアントプリンターのポリシー設定

Jul 07, 2016

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めます。

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。

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。ただし、セキュリティ上の理由から、やむを得ない場合を除きこのオプションを使用しないことをお勧めします。

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を転送されるため、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。

デフォルトでは、規則は指定されていません。

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。
- [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

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。

ドライバーのポリシー設定

Jul 07, 2016

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。

Universal Print Serverのポリシー設定

Jul 07, 2016

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）リスナーで使用する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、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Universal Print Server

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。

ユニバーサル印刷のポリシー設定

Jul 07, 2016

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す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] により、イメージ品質を低下させることなく、[必要なイメージ品質] で設定される圧縮レベルで必要な帯域幅の削減を有効または無効にします。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。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利用できる最大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、ユーザーが利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

セキュリティのポリシー設定

Jul 07, 2016

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。

サーバーの制限のポリシー設定

Jul 07, 2016

「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。

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。これはCitrixポリシー設定によって制御されるものではなく、Microsoftのダイアログボックスです。詳しくは、<http://support.citrix.com/article/CTX118618>を参照してください。

セッションの制限のポリシー設定

Jul 07, 2016

〔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。

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。

セッション画面の保持のポリシー設定

Jul 07, 2016

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。

デフォルトでは、許可されます。

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。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。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時の認証]設定を使用します。これにより、ユーザーが再接続するときに資格情報を入力するための画面が表示されます。

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。

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する、受信TCPポートを指定します。

デフォルトのポート番号は、2598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

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。

デフォルトでは、180秒（3分）に設定されています。

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ます。

タイムゾーン制御のポリシー設定

Jul 07, 2016

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掛にしています。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。

TWAINデバイスのポリシー設定

Jul 07, 2016

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

現在、TWAIN 2.0 はサポートされていません。

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。

USBデバイスのポリシー設定

Jul 07, 2016

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、デバイスはインタラクティブモード（02）で制御されます。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。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。
- WacomSTU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

Class	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイ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 #Input device operating in capture mode

Mode=00000002 VID=1230 PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=1230 PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=1230 PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=1230 PID=1230 # Device setup optimization enabled

レジストリ設定を使った最適化モードの無効化

レジストリフラグを使って、システム全体で最適化モードを無効にできます。

HKLM\System\CurrentControlSet\Services\Icausb\Parameters

DisableInputOptimization DWORD - 値を**1**に設定します

このレジストリの変更を適用するため、システムの再起動が必要です。

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. **[Control Panel]**、**[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止します。

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。

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
Class	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイ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。

視覚表示のポリシー設定

Jul 07, 2016

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

シンプルなグラフィックをピクセルあたり**16ビット**に設定して色深度を低下させ、画質をわずかに犠牲にすることで、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。このオプションは、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にのみサポートされます。

デフォルトでは、これはピクセルあたり24ビットに設定されています。

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、サーバーのスケール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。

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に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。

[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。

動画のポリシー設定

Aug 26, 2016

動画セクションには、動画の圧縮機能が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。

注意

VDAバージョン7.0～7.6では、動画圧縮と保持する最低フレーム数の各ポリシー設定は、**従来のグラフィックモード**が有効の場合のみ適用されます。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、これらの設定が適用されます。

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されます。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。

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。

注意

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次の設定項目が適用されます。

画質の下限レベル

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。

プログレッシブ圧縮のレベル

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

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

静止画のポリシー設定

Aug 26, 2016

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。

注意

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れらの設定項目が適用されます。

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

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

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

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

非可逆圧縮のしきい値

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

WebSocketのポリシー設定

Jul 07, 2016

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。

デフォルト値、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>://<hostFQDN>[:<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）。

負荷管理のポリシー設定

Jul 07, 2016

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。

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。

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、768 MBに設定されています。

プロファイル管理のポリシー設定

Jul 07, 2016

「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。

上級設定のポリシー設定

Jul 07, 2016

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、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、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、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、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み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。

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、Index.datの処理は実行されません。

基本設定のポリシー設定

Jul 07, 2016

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。

ドメイングループは、「<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せんが、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。

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。

ドメイングループは、「<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。

クロスプラットフォームのポリシー設定

Jul 07, 2016

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。

この設定はデフォルトで無効になっており、[処理済みグループ] ポリシー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。

この設定をここまたは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。

この設定をここまたは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。

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。

ファイルシステムのポリシー設定

Jul 07, 2016

〔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。

除外のポリシー設定

Jul 07, 2016

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」と指定した場合、ユーザープロファイルのデスクトップフォルダーは同期されません。

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：「Desktop\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。

同期のポリシー設定

Jul 07, 2016

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

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、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。

フォルダーリダイレクトのポリシー設定

Jul 07, 2016

〔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。

AppData (Roaming) のポリシー設定

Jul 07, 2016

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。

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。

アドレス帳のポリシー設定

Jul 07, 2016

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。

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。

デスクトップのポリシー設定

Jul 07, 2016

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。

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。

ドキュメントのポリシー設定

Jul 07, 2016

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。

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] 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。
- 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。

ダウンロードのポリシー設定

Jul 07, 2016

〔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。

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。

お気に入りのポリシー設定

Jul 07, 2016

〔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。

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。

リンクのポリシー設定

Jul 07, 2016

〔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。

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。

ミュージックのポリシー設定

Jul 07, 2016

【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。

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梨諾冷雨とするには、[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。

ピクチャのポリシー設定

Jul 07, 2016

「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。

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梨諾冷雨とするには、「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。

保存したゲームのポリシー設定

Jul 07, 2016

「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。

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。

検索のポリシー設定

Jul 07, 2016

〔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。

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。

スタートメニューのポリシー設定

Jul 07, 2016

〔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。

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。

ビデオのポリシー設定

Jul 07, 2016

【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梨諾冷雨とするには、【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。

ログのポリシー設定

Jul 07, 2016

「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、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、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、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、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、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、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、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、エラーのみが記録されます。

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、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、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、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、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、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、エラーおよび一般的な情報のみがログに記録されます。

Logon

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、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、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。

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、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のみがログファイルにアクセスできるよう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、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、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。

この設定をここまたはINIファイルで構成しない場合、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。

この設定をここまたはINIファイルで構成しない場合、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

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。

この設定をここまたはINIファイルで構成しない場合、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。

この設定をここまたはINIファイルで構成しない場合、エラーおよび一般的な情報のみがログに記録されます。

プロファイル制御のポリシー設定

Jul 07, 2016

「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並んでいます。

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ち時間を指定します。

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ブにアクセスするプロセスがある場合は、ここで待ち時間を延ばすことができます。また、プロファイルのサイズが大きい場合、待ち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、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、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、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、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。

- 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として保持し、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、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
- [Local
- 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、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他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。

注意：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、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

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、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、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、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。

レジストリのポリシー設定

Jul 07, 2016

「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。

ストリーム配信ユーザープロファイルのポリシー設定

Jul 07, 2016

「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、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では、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、直ちに取得されません。

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。

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。

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。

Receiverのポリシー設定

Jul 07, 2016

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で使用する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。

- Store name。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。

Virtual Delivery Agentのポリシー設定

Jul 07, 2016

「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：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

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。この設定を使用する場合は、[IPv6コントローラー登録のみを使用する] ポリシー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。

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に設定されています。

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。

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も

できます。

デフォルトでは、空白になっています。

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。

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。

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。

HDX 3D Proのポリシー設定

Jul 07, 2016

[HDX3DPro] 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。

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。

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。

仮想IPのポリシー設定

Jul 07, 2016

〔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。

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。

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。

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

Jul 07, 2016

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。

Connector for Configuration Manager 2012のポリシー設定

Jul 07, 2016

[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は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。

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。

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} Please save your work. 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。

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、「Upcoming Maintenance」というタイトルが設定されています。

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、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ジが表示されます。

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、「The server is currently going offline for maintenance」というメッセージが設定されています。

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、「Notification From IT Staff」というタイトルが設定されています。

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、00:05:00（5分）が設定されています。

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} Please save your work and log off. 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。

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、「Notification From IT Staff」というタイトルが設定されています。

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。

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、「The server is currently going offline for maintenance」というメッセージが設定されています。

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、00:05:00（5分）が設定されています。

アプリケーションの

Jul 07, 2016

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。

接続リース

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。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、この記事では、Controllerがリース接続モードのときの、そのほかの機能の可用性、操作、およびパフォーマンスに関連する注意事項を説明します。

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

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のアドレスは、VDAをインストールするときに、Citrixのポリシー設定やレジストリ設定など数種類の方法で指定できます。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。この記事では、VDAの登録のタイミングと方法、Controller情報の更新方法、Controllerの追加、削除、および移動方法を説明します。

Sessions

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/ipv6

XenAppおよびXenDesktopのこのリリースでは、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。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の仕様を決定するCitrixポリシー設定についても説明します。

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。

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。

ライセンス管理

Jul 07, 2016

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）。その他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 - Enterprise - 詳細設定	同時使用
XenDesktop	- Platinum - Enterprise - 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。

- 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。
- [操作] ペインの **[ライセンスの割り当て]** を選択します。
- 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。
- 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にログインしてください。

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。

- 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。
- [操作] ペインの **[ライセンスの追加]** を選択します。
- 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。

- 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。
- [操作] ペインの **[ライセンスサーバーの変更]** を選択します。
- ライセンスサーバーのアドレスを「:」形式で入力します。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。コ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。
3. [操作] ペインの **[ライセンス管理者グループの編集]** または **[ライセンス管理者グループの削除]** を選択します。

アプリケーション

Jul 07, 2016

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（おそらく異なるグループから）同じ名前と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。

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。

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合は、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ますが、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。

[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け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。
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。

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、新しい名前「app_1」が提案されます。

追加するアプリケーションが10個以下の場合、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せん。

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、そのグループが以前のXenDesktop 7.xバージョンで作成され、（2）デリバリーグループの編集権限がある場合は、デスクトップのみを配信する共有マシンを含む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け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。

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	Location
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
実行可能ファイルのパス	Location
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	Location

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多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。

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から1つを選択します。完了したら、[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

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、フォルダーを選択し、次に[操作] ペインで[**フォルダーの削除**]を選択します。アプリケーションや他のフォルダーを含んでいるフォルダーを削除すると、それらのオブジェクトも削除されます。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。）

ゾーン

Jul 07, 2016

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。

このアートを通じ、「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。

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。

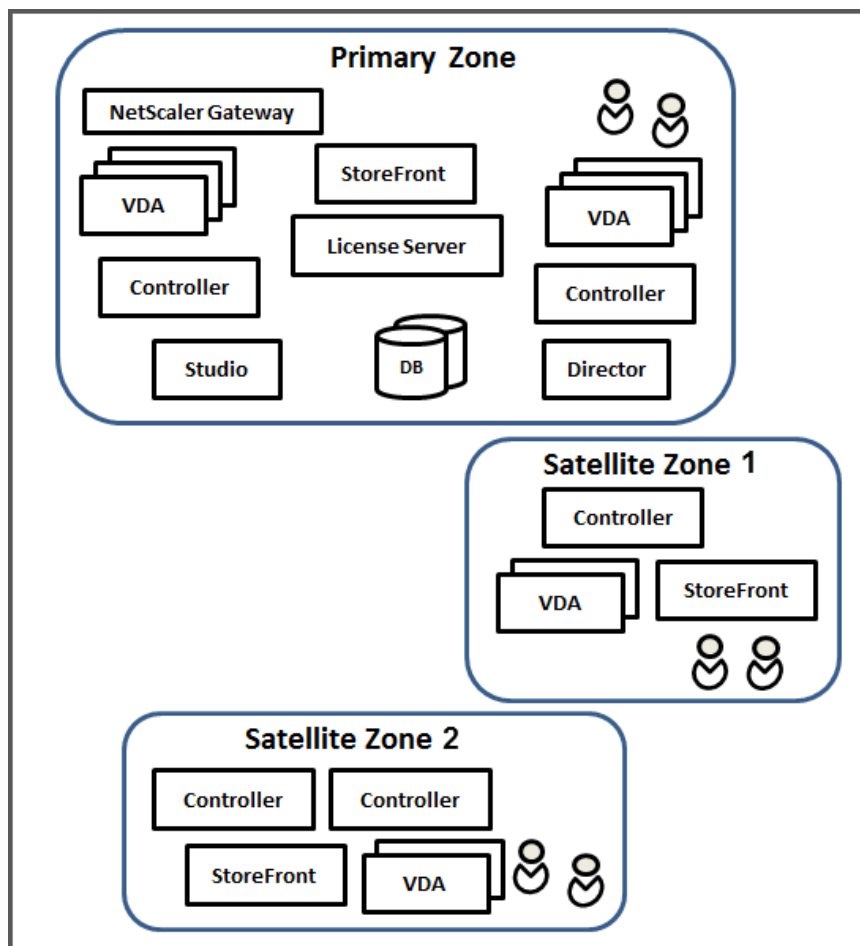
サテライトゾーン

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）。

それぞれのニーズと環境に応じて、1つのサイトに異なる種類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、接続リソ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

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（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（カタログの移動時には、関連する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。

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）。

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、およびホスト接続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。
- 実稼働サイトを作成してから、最初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

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可能性があります。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、カタログで使用されるホスト接続は、同じゾーン内に保持します。
- 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。

ゾーンの作成と管理

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、ゾーンに関連の権限（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）。

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. **[Save]** 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。

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. ゾーンを選択し、**[操作]** ペインの **[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。

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. 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を確認されます。

注意：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. 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。

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。

接続とリソース

Aug 26, 2016

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](#)
- [Host storage](#)
- [接続とリソースの作成](#)
- [既存の接続を使用した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。

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。

VMware

- 「[VMware仮想化環境](#)」
- VMware製品ドキュメント：

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

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。

Citrix CloudPlatform

- Citrix 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す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）。プールマスターで障害が発生した場合は、（[高可用性の編集] から）プール内のすべてのサーバーを選択してXenServerとの通信を許可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

Host storage

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。
- 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、ユーザープロフィールデータ、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す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的の名を持っていることを確認してください。（XenCenterで名前を変えるには、ストレージを右クリックして、名前プロパティを編集します。）

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が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ッシュと呼ばれます。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ーを提供します（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。

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

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。

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、[こちらの手順](#)を使用してください。

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。

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 **[接続およびリソースの追加]** を選択します。
3. **[新しい接続を作成する]** をクリックします。
4. 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、最後のページに到達するまで **[次へ]** をクリックします。

Add Connection and Resources

Studio

- Connection
- Storage Management
- Storage Selection
- Network
- Summary

Connection

☐ Use an existing Connection

vmwvc5u2

☒ Create a new Connection

Connection type: Citrix XenServer®

Connection address: Example: http://xenserver.example.com

User name: Example: root

Password:

Connection name: Example: MyConnection

Create virtual machines using:

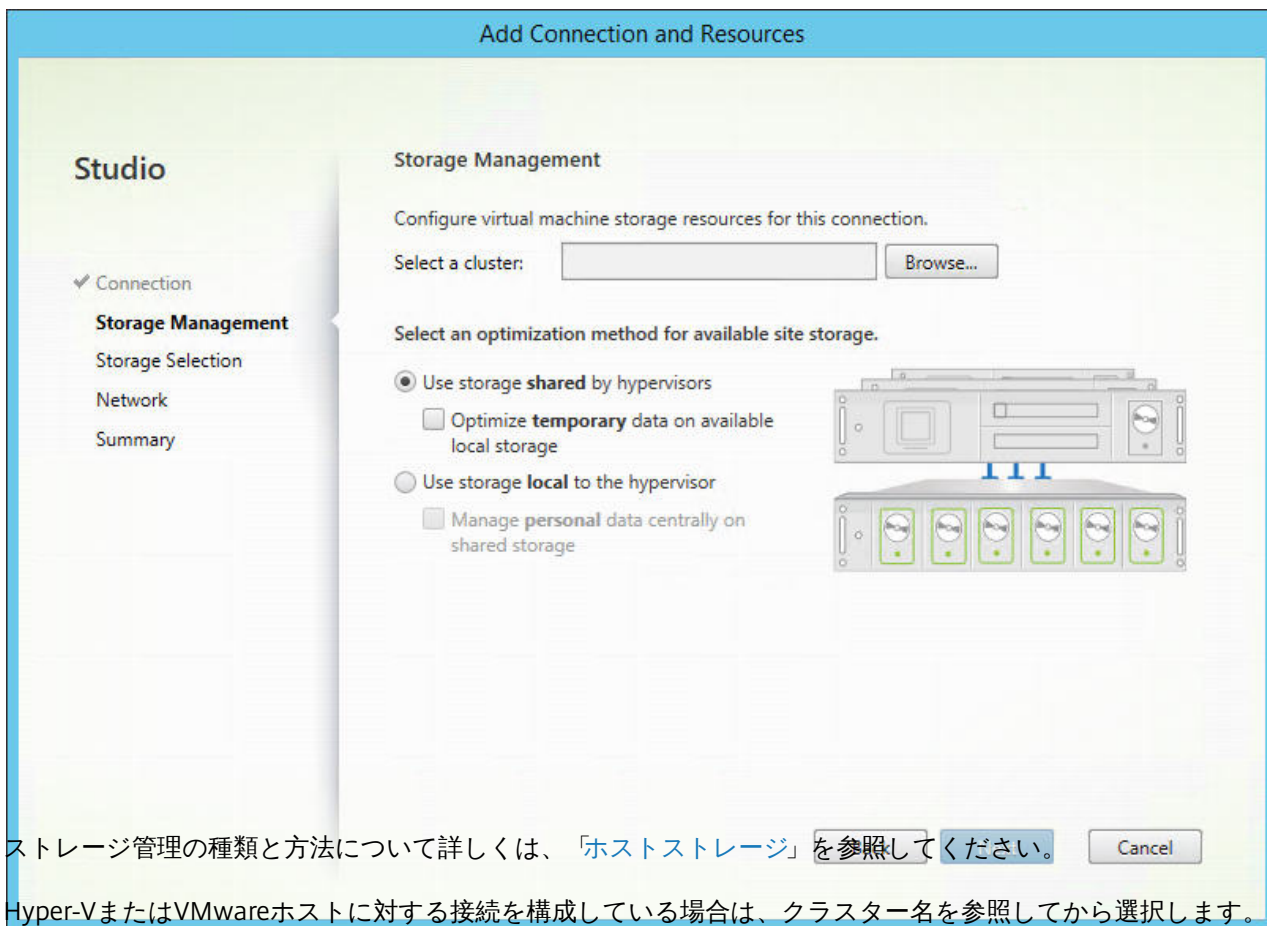
☒ Studio tools (Machine Creation Services)

☐ Other tools

Back Next Cancel

[接続] ページで、以下の情報を指定します。

- [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。



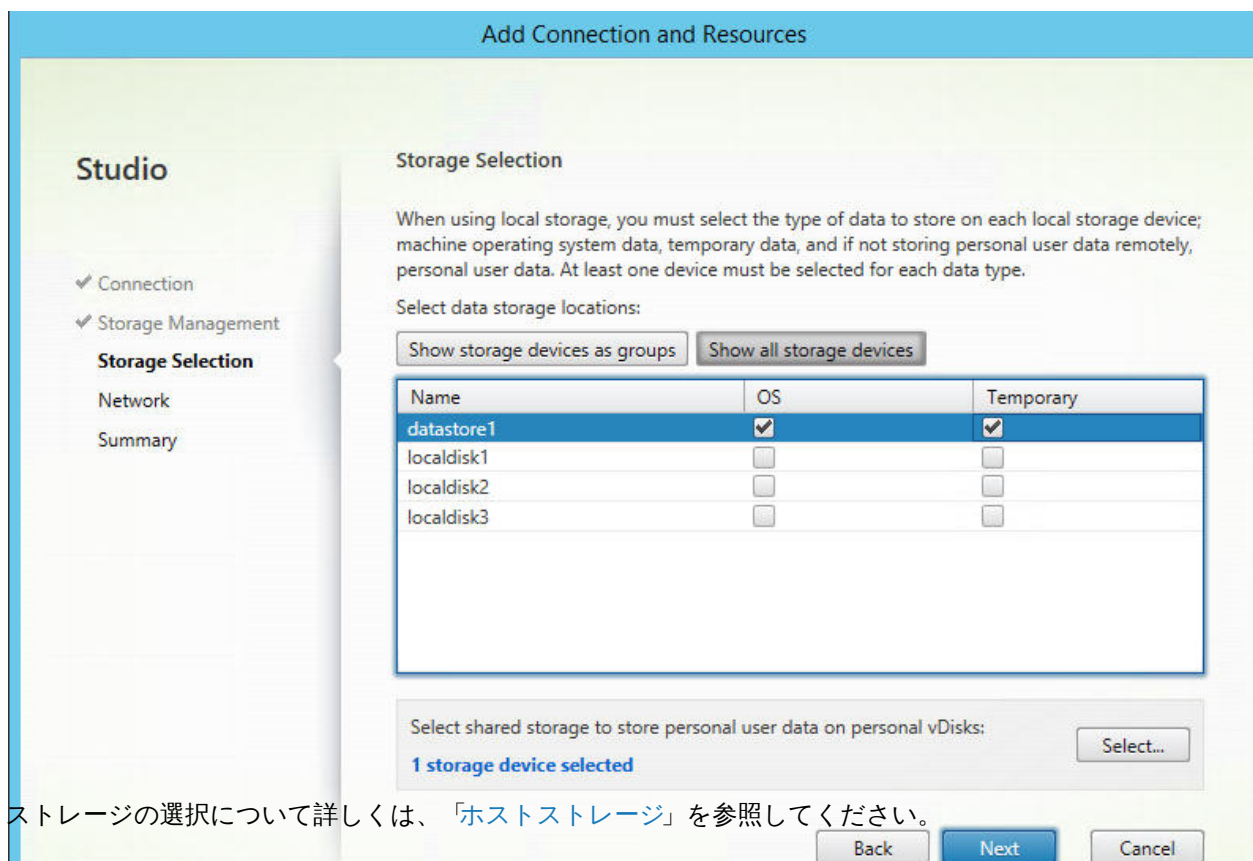
ストレージ管理の種類と方法について詳しくは、「[ホストストレージ](#)」を参照してください。

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のごとに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別は変化します。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別に対して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。

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。

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。

注意：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。

既存の接続を使用した接続とリソースの作成

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 **[接続およびリソースの追加]** を選択します。
3. **[既存の接続を使用する]** を選択し、使用する接続を選択します。
4. ウィザードの指示に従って、「[接続とリソースの作成](#)」に記載のページの操作を行います。

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. 作業が完了したら、行った変更を適用してウィンドウを開いたままにするには **[適用]** を、変更を適用してウィンドウを閉じるには **[OK]** をクリックします。

[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。これらの設定は、電源管理設定で同時起動が許可されたマシンの数が多すぎたり少なすぎたりする場合に役立ちます。接続の種類のそれぞれには多くのケースで適切な固有のデフォルト値があります。これらの値は、通常は変更しないでください。

[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、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] 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。

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の有効化**：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**：マシンをデリバリーグループから削除しても、そのデリバリーグループが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】**ペインの**【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】**を選択します。

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る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**：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。

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。

接続リース

Jul 07, 2016

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。

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。
- 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を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> 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。

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。

接続リース機能は、デフォルトで有効になっています。

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。
- 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。

仮想IPおよび仮想ループバック

Jul 07, 2016

注：これらの機能は、Windows Server 2008 R2マシンおよびWindows Server 2012 R2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、またはその他の目的で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。

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。
- 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。これにより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。

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.X.X.X（X.X.XはセッションIDに1を加えた値）に置き換えられます。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。

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 2008 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ます、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
- 値の名前：PreferLoopbackProcesses、種類：REG_MULTI_SZ、値のデータ：<list of processes>。ここで、はプロセスの一覧です。

Delivery Controller

Aug 26, 2016

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 — 実務サイトでのベストプラクティスとして、物理サーバー上で動作するControllerを2台以上配置します。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。

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。

VDAによるControllerの検出方法

VDAを使用するには、そのサイトのControllerに登録（接続を確立）する必要があります。VDAはListOfDDCsと呼ばれるControllerの一覧をチェックしてControllerを見つけます。ListOfDDCsは、そのサイトのControllerのDNSエントリまたはIPアドレスで構成されています。負荷分散のため、VDAは一覧のすべてのControllerで接続を自動的に分散させます。

ListOfDDCsに加えて、ListOfSIDsと呼ばれるControllerのマシンセキュリティID（SID）一覧により、VDAがアクセスできるController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。

サイト内でControllerの追加や削除に伴って、すべてのVDA上のListOfDDCsおよびListOfSIDsが確実に更新されるようにすることが重要です。これらの一覧を正しく更新しない場合、一覧にないControllerで仲介されたセッションがVDAで拒否される可能性があります。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。これらの一覧は、以下の方法で更新できます。

- 自動更新 — Controllerが追加または削除されたときに、ListOfDDCsおよびListOfSIDsを自動的に更新します。デフォルトでは、自動更新が有効になっています。
- 自己管理 — Controllerを識別するためのポリシーやレジストリ設定を手動で更新します。

ListOfDDCsおよびListOfSIDsに含まれている情報は、展開内の複数の場所で参照されます。VDAは以下の場所を順にチェックして、最初に見つかった一覧を使用します。

1. 自動更新機能により維持される永続的なストレージ。自動更新が有効な場合、VDAのインストール直後の初回登録以降では、ここにController情報が格納されます（このストレージには、マシンのポリシー情報も格納されています。これにより、再起動しても、ポリシー設定が保持されます）。インストール直後の初回登録時、または自動更新が無効な場合、VDAは以下の場所をチェックします。
2. ポリシー設定（Controller、Controller SID）。
3. レジストリのVirtual Desktop Agentキーの下のController情報。これらの値は、VDAのインストール時に指定するController

情報に基づいて、VDAのインストーラーにより設定されます。

4. 組織単位ベースのController検出。これは、後方互換性を維持するための従来の方法です。
5. Machine Creation Servicesにより作成されるPersonality.iniファイル。

ListOfDDCsに複数のController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。ListOfDDCsには、複数のControllerのエントリを角かっこで囲んだController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。

Version 7.0より前のXenDesktopをアップグレードした場合は、従来のCNAME機能が自動更新機能に置き換えられます。必要な場合は手動でCNAME機能を再度有効にすることができますが、DNSエイリアスの整合性に問題が生じるため、自動更新機能とCNAME機能の両方を使用することはできません。CNAME機能の再有効化について詳しくは、[CTX137960](#)を参照してください。

複数のゾーンを持つサイトでVDAがどこに登録を試行するかについて、詳しくは、「ゾーン」の記事を参照してください。

自動更新または自己管理を選択する場合の考慮事項

自動更新機能は、ポリシー設定によりデフォルトで有効になっています。

以下の様なサイトでは自動更新を使用できないため、自己管理を行う必要があります。

- Controllerグループを使用する展開。
- セキュリティ上の理由によりListOfSIDsを使用する展開（Active Directoryの負荷軽減のためにListOfSIDsを使用する場合は自動更新を使用できます）。
- ライトバックディスクなしでProvisioning Servicesを使用する展開。
- [Controller] または [コントローラーSID] ポリシー設定を使用する展開。

自動更新

[コントローラーの自動更新を有効にする] ポリシー設定は、Virtual Delivery Agent カテゴリにあります。自動更新を有効にするには、このポリシー設定を有効にします。これはデフォルトです。自動更新を無効にするには、このポリシー設定を無効にします。

自動更新が有効な環境でVDAをインストールする場合、VDAのインストール時に指定したいいずれかのControllerにVDAが登録されます。VDAのインストール時に指定したController情報は、インストーラーによりListOfDDCsレジストリ値に書き込まれます。

VDAをControllerに登録すると、登録先のControllerにより環境内のControllerの完全修飾ドメイン名（FQDN）およびセキュリティID（SID）の一覧がVDAに送信されます。この一覧の内容は、VDAにより自動更新用の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、およびポリシーの更新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。

VDAが受信した一覧に登録先のControllerが含まれていない場合（つまりそのControllerがサイトから削除された場合）、一覧のいずれかのControllerにVDAが再登録されます。VDAの登録または再登録が完了すると、新しい一覧を受信します。

次に例を示します。

1. 環境内に3つのControllerであるA、B、Cがあります。VDAをインストールしたときに、そのVDAが（インストール時に指

- した) Controller Bに登録されます。
2. サイトに2つのController (DおよびE) を追加します。90分以内に、更新された一覧が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)。
 3. サイトからController Bを削除します。前回のチェック以降にサイトのControllerに変更があったため、90分以内にVDAは更新済みの一覧を受信します。手順1.でインストールしたVDAはController Bに登録されていましたが、このControllerは一覧から削除されているため現在のController (A、C、D、E) のいずれかに再登録されます。

自己管理

自動更新機能を使用しない場合は、サイトのDelivery Controllerを追加、移動、または削除した後で、そのサイトにある各VDAのCitrixポリシー設定またはレジストリ値を管理者が更新する必要があります。レジストリの変更は、グループポリシーオブジェクトを使って更新することもできます。

Citrixポリシー設定を使って自己管理するには

1. [Controller] ポリシー設定で指定した完全修飾ドメイン名値を更新します。このポリシー設定は、[Virtual Delivery Agent設定] カテゴリにあります。
2. ListOfSIDsを併用している環境では、[コントローラーSID] ポリシー設定で指定したSID値を更新します。

レジストリを使って自己管理するには

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. サイトのすべてのController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)。スペースで区切って複数の値を入力できます。Controllerグループは角かっこで囲みます。

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgentにListOfDDCsとFarmGUIDキーの両方がある場合は、ListOfDDCsがController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。

2. 必要に応じて、ListOfSIDsレジストリキーを更新します。

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

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。

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働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予定の場合は、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を削除すると、Citrixソフトウェアやその他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他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す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。

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。
3. Controllerの移動先ゾーンを指定します。

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を指定します。

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。

Active Directory OUベースのController検出

このDelivery Controller検出方法は主に後方互換性のためにサポートされており、VDA for Windows Desktop OSでのみ有効です（VDA for Windows Server OSでは使用できません）。この検出方法では、サイト内のすべてのコンピューターが同じActive Directoryドメインに属しており、Controllerとデスクトップで使用されるドメイン間に相互信頼関係が設定されている必要があります。この検出方法を使用する場合、各デスクトップのレジストリで組織単位（OU）のGUIDを構成する必要があります。

OUベースのController検出を実行するには、Controller上でPowerShellスクリプトのSet-ADControllerDiscovery.ps1を実行します（このスクリプトは各Controllerの\$Env:ProgramFiles\Citrix\Broker\Service\Setup Scriptsフォルダーにあります）。スクリプトを実行するには、すべての管理タスクを実行できる権限に加えて、親OUでのCreateChild権限が必要です。

Active Directoryを使用してControllerが検出されるように構成する場合は、サイトを作成するときに、対応する組織単位（OU）をActive Directory内に作成する必要があります。このOUは、環境内のコンピューターが属しているフォレスト内のどのドメインにも作成できます。ベストプラクティスとしては、サイト内のControllerもこのOUに含まれている方が望ましいですが、これは必須ではありません。適切な権限を持つドメイン管理者はOUを空のコンテナとして作成して、そのOUの管理権限をほかのCitrix管理者に委任できます。

スクリプトを実行すると、以下の重要なオブジェクトが作成されます。これらのオブジェクトは、標準的なActive Directoryオブジェクトです。スキーマを拡張する必要はありません。

- Controllerのセキュリティグループ。サイト内のすべてのControllerのコンピューターアカウントは、このセキュリティグループに属している必要があります。サイト内のデスクトップは、このセキュリティグループに属しているControllerからのみデータを受け入れます。
すべてのControllerで、VDAを実行するすべての仮想デスクトップに対する「ネットワーク経由でコンピューターへアクセス」権限が必要です。このため、Controllerのセキュリティグループにこの権限を追加します。Controllerにこの権限がない場合、VDAは登録されません。
- サイトの名前など、サイトに関する情報を含むサービス接続ポイント（SCP）オブジェクト。[Active Directoryユーザーとコンピューター] 管理ツールでサイトOUを確認する場合、SCPオブジェクトを表示するには[表示]メニューの[拡張機能]を有効にする必要があります。
- サイトのOU内に作成されるRegistrationServicesという名前のコンテナ。このコンテナには、サイトの各Controllerについて1つのSCPオブジェクトが含まれます。Controllerが起動すると、そのSCPの内容が検証され、必要な場合は更新されます。

初回インストール後に複数の管理者でControllerを追加したり削除したりする必要がある場合は、RegistrationServicesコンテナで子オブジェクトを作成および削除する権限とControllerセキュリティグループでプロパティを書き込む権限が必要です（これらの権限は、Set-ADControllerDiscovery.ps1スクリプトを実行する管理者に自動的に付与されます。）。これらの権限はドメイン管理者または初回インストール時の管理者が付与できます。また、これを行うためのセキュリティグループを設定することをお勧めします。

サイトOUを使用する場合、以下の項目が適用されます。

- Active Directoryに情報が書き込まれるのは、この製品をインストールまたはアンインストールするときや、起動したControllerのSCPの情報を更新するとき（Controllerの名前や通信ポートを変更した後など）のみです。デフォルトでは、Set-ADControllerDiscovery.ps1スクリプトによってサイトOU内のオブジェクトに関する権限が適切にセットアップされ、各ControllerにSCPへの書き込み権限が付与されます。サイトOU内のオブジェクトの内容は、デスクトップとControllerの間の信頼を確立するために使用されます。以下の点を確認してください。
 - 許可された管理者のみが、セキュリティグループのアクセス制御リスト（ACL）を使用してControllerのセキュリティグループにコンピューターを追加したり削除したりできること。
 - 許可された管理者と各Controllerのみが、ControllerのSCP内の情報を変更できること。
- 展開で複製機能を使用する場合、潜在的な遅延による影響について考慮してください。詳しくは、Microsoftのドキュメントを参照してください。複数のActive Directoryサイトにドメインコントローラーがあるドメイン内でサイトOUを作成する場合は、特に重要になります。デスクトップやController、ドメインコントローラーの場所によっては、サイトOUを最初に作成したり、Controllerをインストールまたはアンインストールしたり、Controller名や通信ポートを変更したりしたときのActive Directoryの変更内容が、適切なドメインコントローラーに複製されるまでデスクトップ側に反映されない場合があります。このような遅延が発生するときは、デスクトップがControllerとの接続を確立できないためにユーザーが仮想デスクトップに接続できないなどの問題が発生します。

- この製品では、Active Directoryの標準のコンピューターオブジェクトの属性を複数使用して、デスクトップを管理します。環境によっては、デスクトップのActive Directoryレコードに格納されるコンピューターオブジェクトの完全修飾ドメイン名 (FQDN) が、接続を行うユーザーに返される接続設定の一部として含まれている場合があります。この情報がDNS環境の情報と一致していることを確認してください。

OUベースのController検出を使用してControllerをほかのサイトに移動するには、前述のControllerの移動に関する指示に従って操作します。古いサイトからControllerを削除した後 (手順2)、PowerShellスクリプトSet-ADControllerDiscovery -syncを実行します。このスクリプトにより、OUが現在のControllerの一覧と同期されます。移動先のサイトに参加した後 (手順3)、そのサイトの任意のController上で同じスクリプトを実行します。

必要な権限は、誰が、何を操作する必要があるかによって変わります。

サイトの作成中

Set-ADControllerDiscovery.ps1スクリプトを実行するCitrixサイト管理者が、サブOUとオブジェクトを作成するには、サイトOUの権限が必要です。(サイトOUがない場合、管理者はこれを作成する権限も必要です。ADドメイン管理者は、事前にサイトOUを作成して、Citrixサイト管理者IDに権限を割り当てることをお勧めします)。(OU内のみで) 必要な権限は、以下のとおりです。

- SCPの作成
- コンテナの作成
- セキュリティグループの作成

必要な場合、このスクリプトはサイトOUも作成できます。このためには、管理者IDは、新しいOUの親OUに対する権限を作成する必要があります。ただし、上記のとおり、これはお勧めしません。

この時点で、ユーザーは作成されたアイテムの暗黙的な所有者であり、これらのアイテムに関する追加のサブ権限は必要ありません。ここで、すべての追加のプロパティを新しく作成されたセキュリティグループに設定する必要があります。

Controllerの追加または削除

Citrixサイト管理者は、後からADControllerDiscovery.ps1スクリプトを実行して、サイトにControllerを追加したり、サイトから削除できます。これは、最初にOUコンテンツを作成したIDとは、違う管理者IDでも実行できます。必要な権限は以下のとおりです。

- 「Controllerの」セキュリティグループに対してマシンを追加または削除する
- 「RegistrationServices」コンテナでSCPを作成または削除する

通常操作中

通常操作中、ControllerマシンおよびVDAマシンには、次の権限が必要です。

- Controllerには、(「RegistrationServices」コンテナで) 現在のSCPオブジェクトにプロパティを設定する権限が必要です。
- ControllerおよびVDAは、OUおよびその下部で、すべてのオブジェクトに対する読み取り権限が必要です。

Sessions

Jul 07, 2016

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によるセッションの管理](#)」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ます。

- 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。セッション画面の保持機能により、[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、ユーザー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、ユーザーは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。

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

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な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、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他のリソースも引き継がれます。

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 SDK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他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他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>は、次のうちいずれかになります。

- **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。

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す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：REG_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

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。

Studioでの検索の使用

Jul 07, 2016

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できます。

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] ノードや[デリバリーグループ] ノードでは[検索] ボックスを使用できません。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一覧を表示します。この一覧のプロパティで詳細な検索式を定義できます。

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。

タグ

Jul 07, 2016

タグは、マシン、アプリケーション、デリバリーグループ、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場合、それらのアプリケーションに「テスト」という名前のタグを追加します。次に、Studioの検索結果を「テスト」タグでフィルタリングします。同様に、テストチームメンバーを含むデリバリーグループのみを表示する場合は、「テスター」タグをテストチームメンバーを含むデリバリーグループに追加し、Studioの検索結果を「テスター」タグでフィルタリングします。

- 指定されたタグを持つ（または持たない）アプリケーション、マシン、またはデリバリーグループに、Citrixポリシーを適用する（割り当てる）。

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。

タグの管理

Studioでマシン、アプリケーション、またはデリバリーグループを選択し、[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。

- オンになっ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。
- デリバリーグループを選択した場合、ハイフンを含むチェックボックスは、そのデリバリーグループの一部の項目（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。

- タグを追加または削除するには、追加または削除するタグの隣のチェックボックスをオンまたはオフにします。
- タグを作成するには、[タグの作成] を選択し、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れません。[OK] をクリックします。
- タグを編集するには、タグを選択して[タグを編集] をクリックします。新しい名前、および/または説明を入力して、[保存] をクリックします。同時に編集できるタグは1つのみです。
- タグを削除するには、タグを選択してから[タグの削除] 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。詳細な情報を表示するには、項目をクリックします。たとえば、2つのマシンが削除の影響を受ける場合、項目をクリックするとその2つのマシン名が表示されます。どの項目が影響を受けるかを確認したら、タグを削除するかどうかを確定します。

IPv4/IPv6サポート

Jul 07, 2016

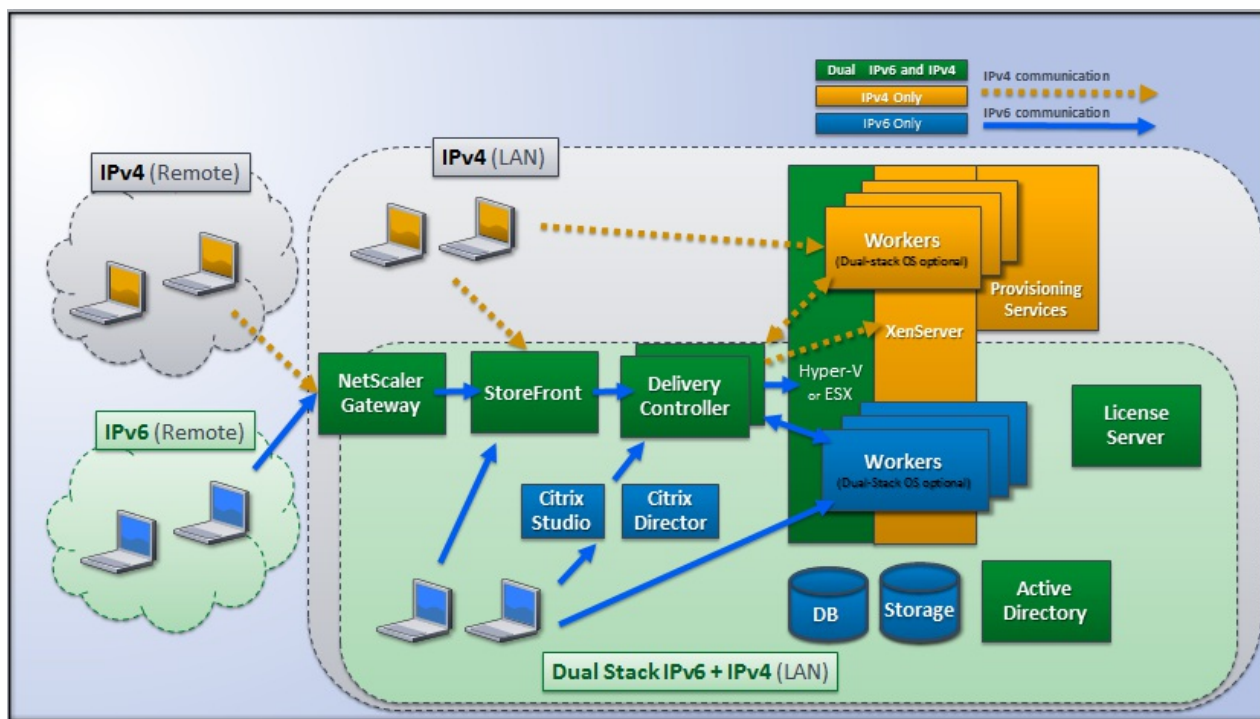
このリリースでは、IPv4のみまたはIPv6のみ（ピュアIPv4またはピュアIPv6）の環境がサポートされ、重複するIPv4とIPv6のネットワークを使用した「デュアルスタック」環境がサポートされます。

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 Controller登録のみを使用する。
- 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。

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コントローラー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

この展開は、以下のように管理されます。

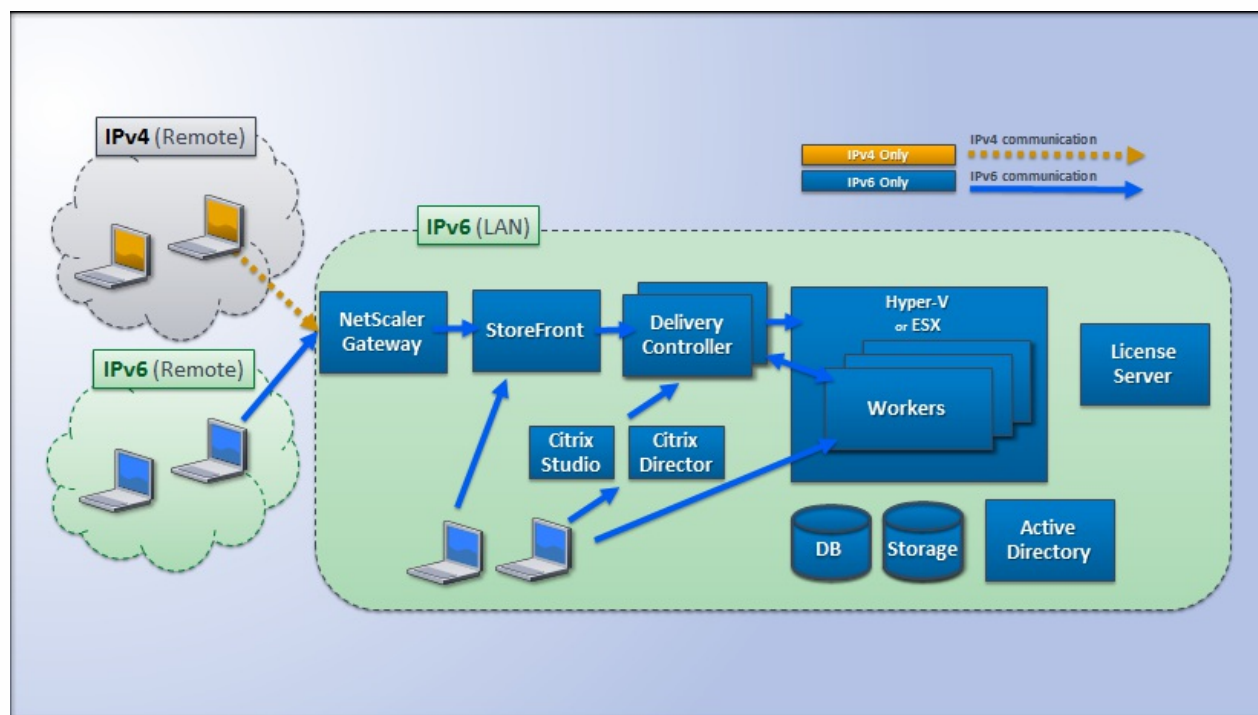
- ユーザーによるIPv6ネットワークの使用頻度が高く、管理者がユーザーにIPv6トラフィックの使用を求める場合、管理者にプライマリのIPv6ポリシー設定（つまり「IPv6 Controller登録のみを使用する」）が有効な組織単位（OU）またはワーカー

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。

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。



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 Controller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、VDAでIPv6アドレスが使用されるようにするには、[IPv6コントローラー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。

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。

クライアントフォルダーのリダイレクト

Jul 07, 2016

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
 - 値のデータ：1
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。

ユーザープロファイル

Jul 07, 2016

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わけではありません。

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。

いずれのプロファイル処理でも、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。

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ーを使用します。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ーとは、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。

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	Disabled	有効
プロファイルストリーム配信	Disabled	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	Disabled	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)	Disabled
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)

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。

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。

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。通常、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
Desktop	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
Links	はい	いいえ
My Music	はい	はい
My Pictures	はい	はい
My Videos	はい	はい
検索	はい	いいえ
保存したゲーム	いいえ	いいえ

フォルダー スタートメニュー	Windows 8でのリダイレクト はい	Windows Server 2008でのリダイレクト 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](http://technet.microsoft.com/ja-jp/library/cc766489(v=ws.10).aspx)を参照してください。

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。

Citrix Insight Services

Jul 07, 2016

Citrix Insight Services (CIS) は、診断およびトラブルシューティングのための、Citrixが提供する主要なプラットフォームです。CIS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。

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。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を目的として、この情報のアップロードが求められることがあります。

この情報は、ローカルの%ProgramData%\Citrix\に保存されます。

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。

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。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。

CEIPへは、関連するCitrix製品、コンポーネント、テクノロジー (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。

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。

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。

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。

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。このテクノロジーは、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
- 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、圧縮されたトレース情報を約20MB保持します。通常、Citrix Telemetry Serviceには過去24～48時間の情報が、この間隔の間に生成されたトレースの量に応じて含まれます。

- 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。

全製品インストーラーでグラフィックインターフェイスを使用してDelivery ControllerやVDAをインストールするときに、Call Homeに参加するかどうかを指定することができます。

コンポーネントをインストールすると、PowerShellコマンドレットを使用して、以下を行うことができますようになります。

- Call Homeのスケジュールによるアップロードを有効にするか、現在のスケジュールを変更する。これには、マシンカタログで使用する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が含まれ、これによって、作成済みの各仮想マシンでCall Homeを設定する必要がなくなります。
- 手動でデータを収集し、CISにアップロードする。
- 手動でデータを収集してローカルに保存し、後からデータをCISにアップロードする。

PowerShellコマンドレット構文に関する説明については、コマンドレットのヘルプを参照してください。

Call Homeのスケジュールによるアップロードに登録する場合、および手動で診断情報をCISにアップロードする場合は、Citrixのアカウント資格情報を入力する必要があります。CIS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。

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へのスケジュールによるアップロードに登録できます。デフォルトでは、データは現地時間の毎週日曜日の午前3時頃に収集され、CISにアップロードされます。アップロードの時間は、指定された時間の前後2時間以内になります。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は、PowerShellコマンドレットを使用して、手動でCall Homeデータを収集してアップロードしてください。

コンポーネントのインストール時におけるスケジュールによるアップロードの有効化

XenAppおよびXenDesktopの全製品インストーラーのグラフィックインターフェイスを使用してControllerやVDAをインストールする場合、Call Homeへのスケジュールによるアップロードに参加するかどうかを指定することができます。デフォルトでは、参加が選択されています。

- 参加する場合は、CISにCitrixのアカウント資格情報でサインインします。
- 参加しない場合（または参加しようとしたがCitrixのアカウント資格情報が検証されなかった場合）は、ウィザードのページで参加を拒否します。サイトのセットアップ後に、PowerShellコマンドレットを使用して登録することもできます。

PowerShellコマンドレットを使用したスケジュールによるアップロードの有効化

以下のコマンドレットを使用して、CISへのCall Home診断情報のスケジュールによるアップロードを有効にします。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-Credentials  
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

カスタムの日次または週次スケジュールを作成できます。

```
$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

スケジュールによるアップロードをキャンセルするには、以下のコマンドレットを入力します（キャンセル後も、PowerShellコマンドレットを使用した診断データのアップロードは実行できます）。

```
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。

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、2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
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' このパラメーターを省略すると、すべてのコレクターからのデータが収集されます。
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。

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
```


監視

Jul 07, 2016

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、エンドユーザーに提供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。

Session Recording

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、どのように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

- 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。

ODataプロトコルを使用したMonitor Service API

管理者は、サイトのMonitor Service APIでODataプロトコルを使用して履歴データを検索できます。これにより、IT担当者は履歴傾向を分析して、プランニングやトラブルシューティングを行えます。また、データを抽出してほかのツールやプロセスで処理することもできます。

Monitor Serviceスキーマでは、以下の種類のデータが提供されます。

- 接続エラーに関するデータ
- エラー状態のマシン
- セッションの使用
- ログオン処理時間
- 負荷分散データ

詳しくは、「[Monitor Service OData API](#)」を参照してください。

Personal vDisk診断ツール

インストールしたアプリケーションや変更したファイルなど、Personal vDiskのユーザーパーツやアプリケーションパーツに対してユーザーが行った変更をモニターするには、PVD診断ツールを使用します。

詳しくは、「[Personal vDiskモニタリング](#)」の記事を参照してください。

Session Recording

Jul 07, 2016

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、サーバーOSのVDIマシン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。

Session Recordingの導入

Jul 07, 2016

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。

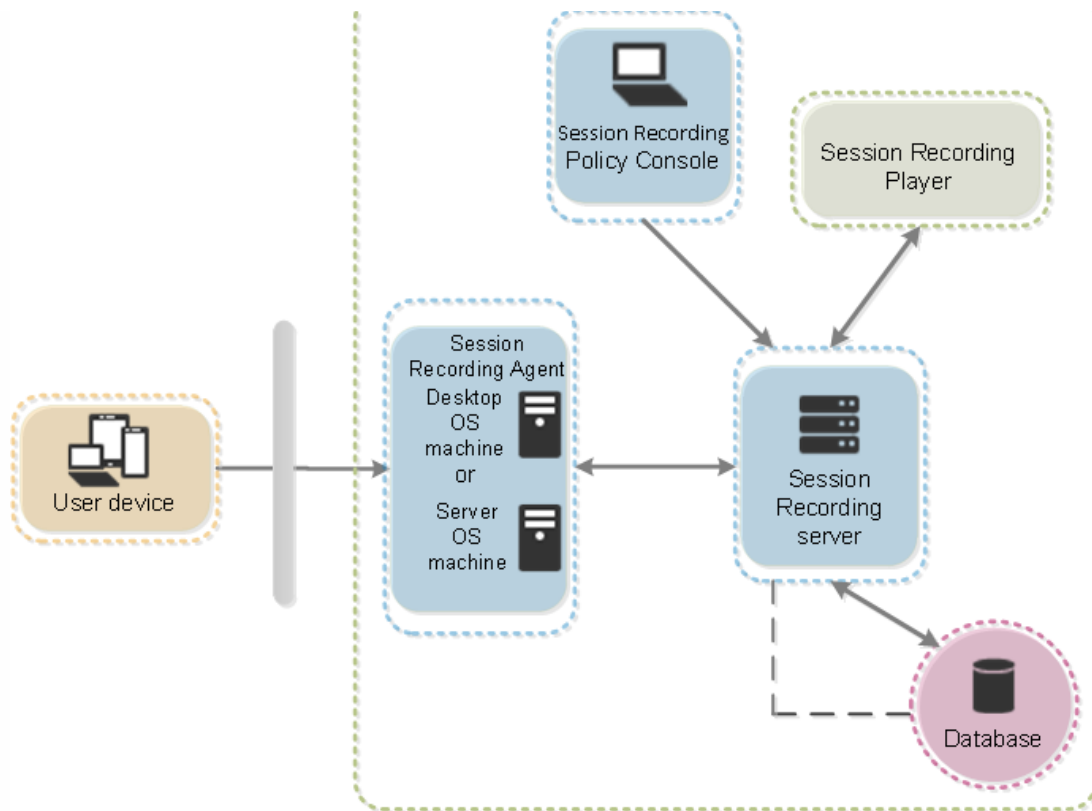
Session Recordingは5つのコンポーネントから構成されます。

- **Session Recording Agent**。各サーバーOSおよびVDIマシン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 Server**。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 Policy Console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。
- **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 Server、Session Recordingデータベース、Session Recording Policy Console、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はサーバーOSマシンにインストールされます。第2のサーバーはSession Recording Policy Consoleをホストし、第3のサーバーはSession Recording Server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サーバーOSマシンに接続します。ファイアウォール内では、Session Recording Agent、Session Recording Policy Console、Session Recording Player、およびSession RecordingデータベースはすべてSession Recording Serverに接続します。





導入計画

Jul 07, 2016

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。たとえば、複数のサイトで単一のSession Recording Server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。

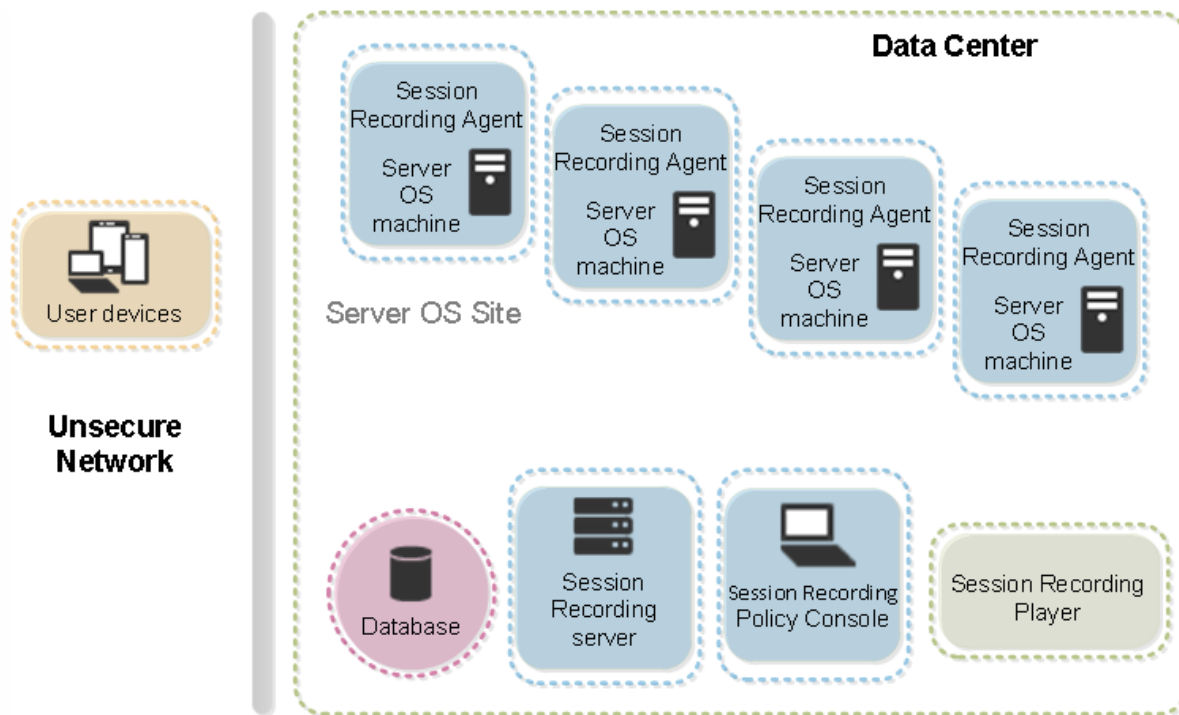
展開シナリオの例

ここでは、Session Recordingを展開する場合の2種類の構成例について説明します。

- 単一のサーバーOSマシンにSession Recording Agentを展開する。
- サイトの複数のサーバーOSマシンまたはワークステーションOSマシンにSession Recording Agentを展開する。

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はサイト内の各サーバーOSマシン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 Server、Session Recording Policy Console) 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。



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。
- Session Recordingでは、単一の構成内で複数のSession Recording Serverをクラスター化することはサポートされていません。
- 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に証明書を実インストールし、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 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。

セキュリティの推奨事項

Jul 07, 2016

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 Server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。

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マシン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] 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。

Microsoft社の<https://support.microsoft.com/en-us/kb/307973>を参照してください。

+ ログオン資格情報またはセキュリティ情報が、社内でも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。

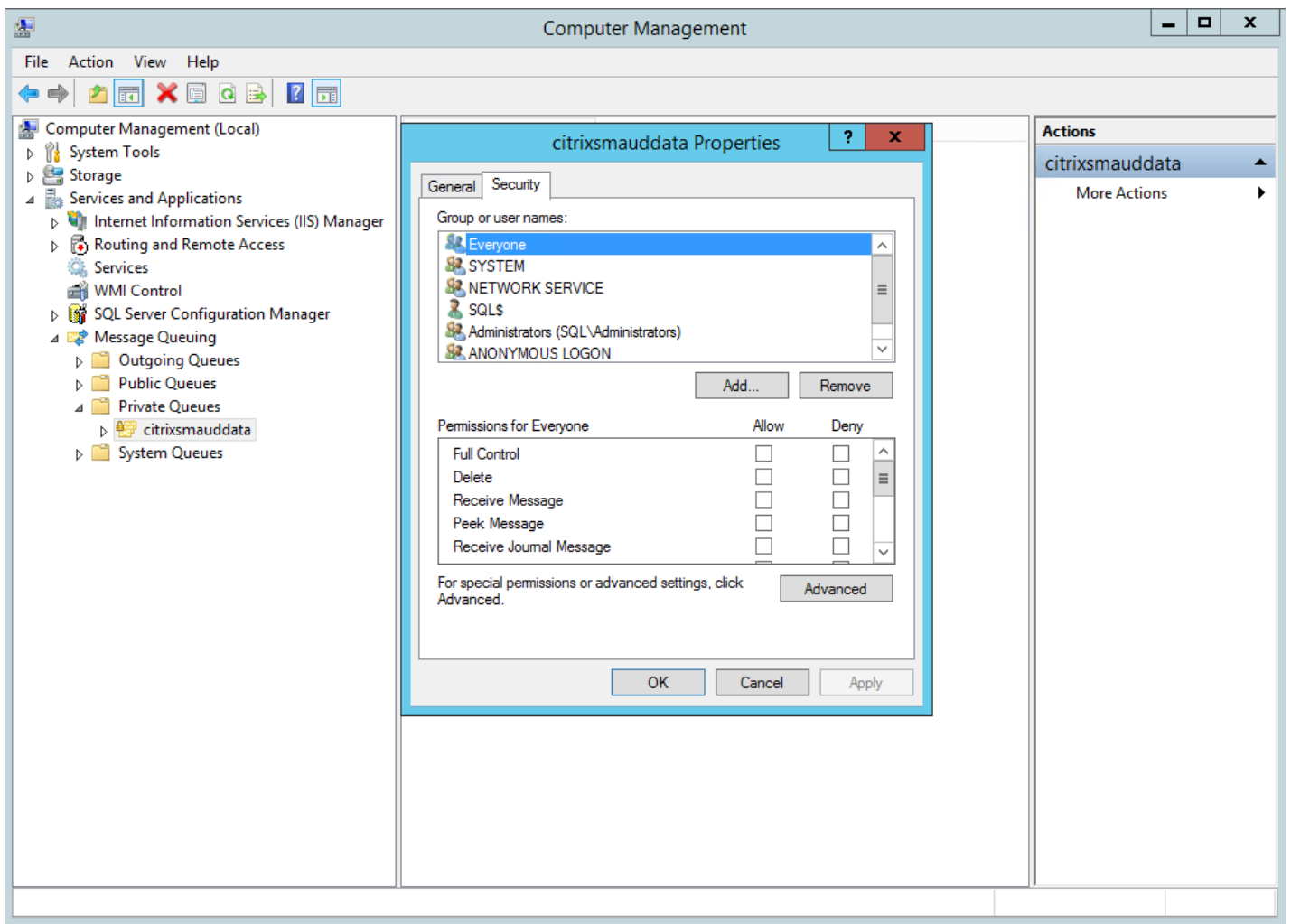
+ ユーザーは、リモートICAセッションに切り替える前に、機密情報を公開する可能性のあるアプリケーションをすべて

閉じる必要があります。

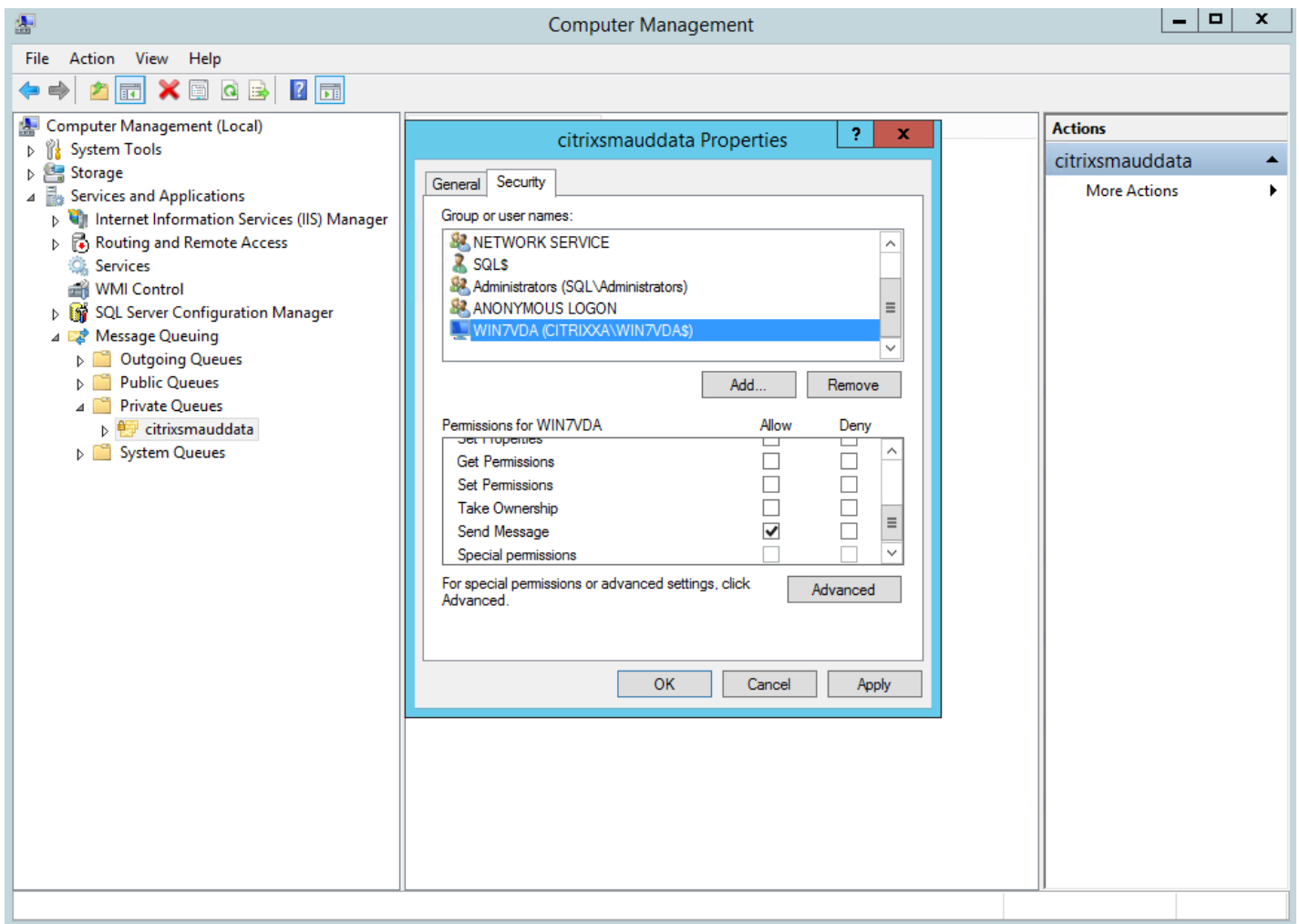
+ セッションの所有者は、デスクトップセッションが録画されている場合は、オンライン会議とMicrosoft Remote Assistanceソフトウェアが録画される可能性があることを出席者に知らせる必要があります。

+ 公開デスクトップまたは公開アプリケーションへのアクセスに対して、自動認証方法（シングルサインオン、スマートカードなど）のみを許可します。

- 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
 - HKLM\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
 - HKLM\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。



5) MSMQデータをこのサーバーに送信するVDAマシン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。



- 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 Server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] ダイアログボックスに表示される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 1.0を使いSSLv2、SSLv3、およびRC4 暗号をSession Recording ServerとSession Recordingデータベースで無効にします。詳しくは、Microsoftアーティクル<http://support.microsoft.com/default.aspx?scid=kb:ja-jp;187498>および<http://support.microsoft.com/kb/245030/en-us>を参照してください。
- 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 Properties] にあり、デフォルトで有効に設定されます。

- Amazon Web Services (AWS) などのパブリッククラウドにSession Recordingを展開しないでください。
- 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。

Session Recording機能の構成については、<http://support.citrix.com/article/CTX200868>を参照してください。

スケーラビリティに関する注意事項

Jul 07, 2016

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の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、<http://support.citrix.com/article/CTX200869>」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。

ハードウェアの推奨事項

ディスクとストレージ

ネットワークの性能

コンピューターの処理性能

複数のSession Recording Serverの展開

データベースのスケーラビリティ

ハードウェアの推奨事項

各Session Recording Server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えます。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 Serverのパフォーマンスを最適化するか、複数のコンピューターにSession Recording Server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は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 Server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 Server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

Session Recording Server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。
- 2GBから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 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 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秒当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。

Session Recordingのインストール

Jul 07, 2016

この記事には、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](#)

[スクリプトを使用してWindowsの役割および機能の前提条件を追加する](#)

[Session Recording Administrationコンポーネントのインストール](#)

[Session Recording データベースのインストール](#)

[Session Recording Server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](#)

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
	インストールを開始する前に、前提条件をインストールします。「システム要件」および「スクリプトを使用してWindowsの役割および機能の前提条件を追加する」を参照してください。
	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。
	以下のCitrixダウンロードページからSession Recordingをダウンロードします。 [XenApp] > https://www.citrix.com/downloads/xenapp.html または [XenDesktop] > https://www.citrix.com/downloads/xendesktop.html
	Session Recordingコンポーネント間の通信にSSLプロトコルを使用する場合は、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を構成してSession Recording Server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XenAppと共に使用する計画がある場合は、一意なQMIdのサーバーを準備します。「既知の問題」の説明を参照してください。この手順の実行に失敗すると、記録データが損失することがあります。
- 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を使用する場合は、TLS/HTTPSのサーバー証明書を構成します。

Session Recordingインストールファイル

- **Session Recording Administrationファイル**
 - Broker_PowerShellSnapIn_x64.msi
 - SessionRecordingAdministrationx64.msiと置き換え
- **Session Recording Agentファイル**
 - SessionRecordingAgentx64.msiと置き換え
- **Session Recording Playerファイル**
 - SessionRecordingPlayer.msiと置き換え

スクリプトを使用してWindowsの役割および機能の前提条件を追加する

Session Recordingを正常に機能させるには、Session Recordingコンポーネントをインストールする前に、Windowsの役割と機能を前提条件として追加する必要があります。役割と機能によっては、見つけ出してインストールするのが困難なものもあるため、この文書では、Citrixの提供するスクリプトを使用した手順を紹介しています。Session Recordingのコンポーネントをインストールする前に、スクリプトを実行してWindowsの役割および機能の前提条件をインストールします。

Windowsの役割および機能の前提条件をインストールするには、以下の手順に従います。

1. Citrixのスクリプトを使用する場合は、「[Windowsの役割および機能の前提条件用スクリプト](#)」を参照してください。
2. Session Recording Administrationコンポーネントをインストールする予定のマシンで以下を行います。
 - a) 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。

Set-ExecutionPolicy RemoteSigned

- b) Windowsコマンドプロンプトを管理者として起動し、次のコマンドを実行します。

powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1

正常に追加されている機能が表示され、スクリプトは停止します。

c) スクリプトの実行後、実行ポリシーが社内ポリシーに基づく適切な値に設定されていることを確認します。

3. Session Recording Agentコンポーネントをインストールする予定のマシンで以下を行います。

a) 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。

Set-ExecutionPolicy RemoteSigned

b) Windowsコマンドプロンプトを管理者として起動し、次のコマンドを実行します。

powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1

正常に追加されている機能が表示され、スクリプトは停止します。

c) スクリプトの実行後、実行ポリシーが社内ポリシーに基づく適切な値に設定されていることを確認します。

4. Windowsの役割と機能がインストールされたら、Session Recordingのインストールに進みます。

Session Recording Administrationコンポーネントのインストール

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です。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。

Session Recording Administrationコンポーネントをインストールする前に、すべての前提条件をインストールしているか確認します。詳しくは、「[Session Recordingのシステム要件](#)」を参照してください。

セキュリティ向上のため、データベースのインストール後にこれらの権限を削除できます。

1. **Broker_PowerShellSnapIn_x64.msi**を実行して、手順に従ってインストールを完了します。
2. Windowsコマンドプロンプトを管理者として起動し、**msiexec /i SessionRecordingAdministrationx64.msi**コマンドを実行するか、この.msiファイルをダブルクリックします。
3. インストールUIで[次へ]を選択して、ライセンス契約に同意します。
4. Session Recording Administration Setup画面で、インストールするSession Recording Administrationコンポーネントを選択します。

Session Recordingデータベースのインストール

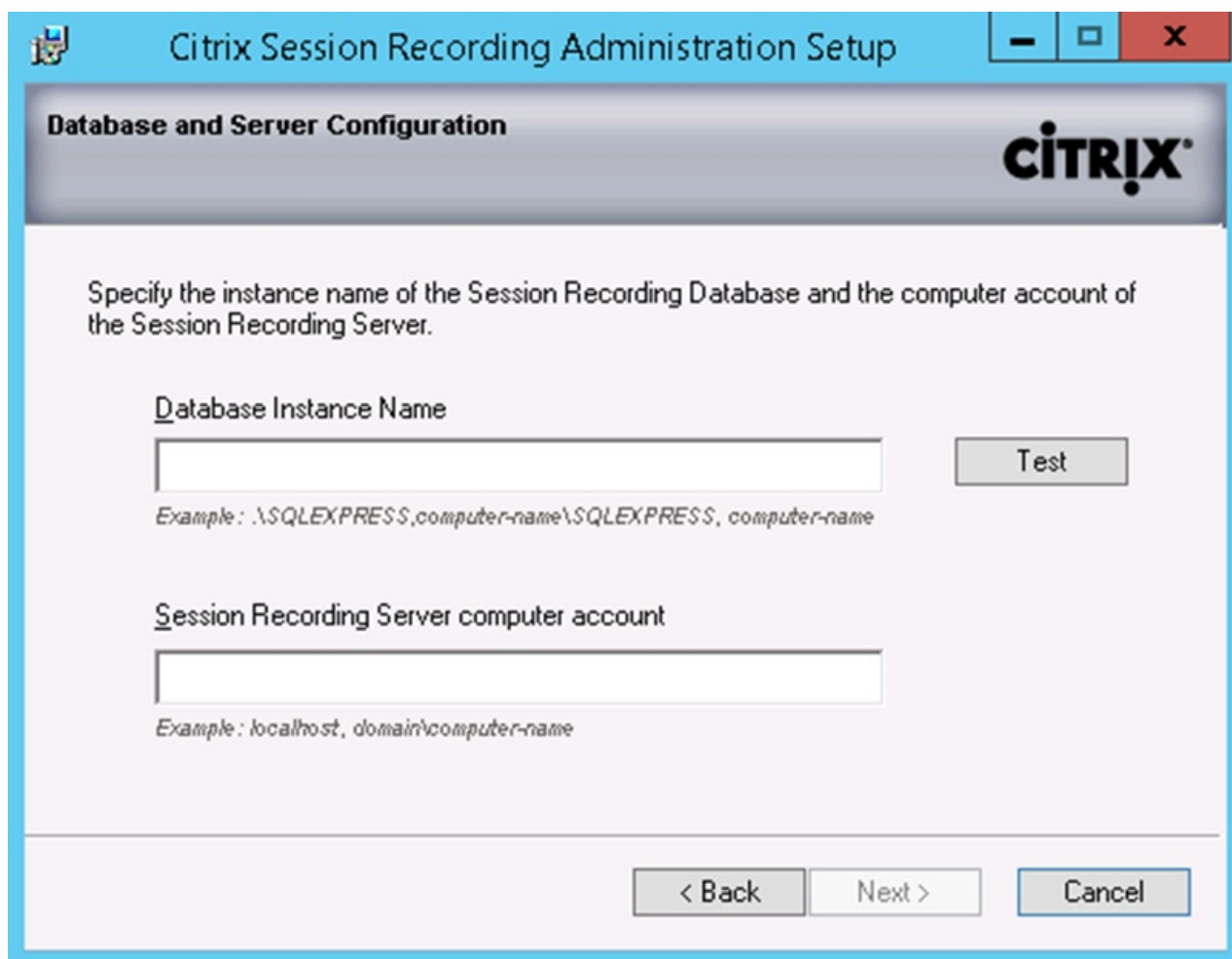
Session Recordingデータベースをインストールする前に、すべての前提条件をインストールしているか確認します。詳しくは、「[Session Recordingのシステム要件](#)」を参照してください。

Session Recordingデータベースコンポーネントと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サーバーにインストールし、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トールする。
 - 展開3：Session Recordingサーバーをあるサーバーにインストールし、Session RecordingデータベースとMicrosoft SQL Serverの両方を、Session Recordingサーバーをインストールしたマシンとは別のマシンにインストールする（推奨されません）。
1. [データベースの設定] ページで、次の作業を行います。
 - 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、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。



The image shows a screenshot of the 'Citrix Session Recording Administration Setup' window, specifically the 'Database and Server Configuration' tab. The window has a blue title bar with the Citrix logo and standard window controls. The main content area is white with a blue border. It contains the following elements:

- Title Bar:** 'Citrix Session Recording Administration Setup' with minimize, maximize, and close buttons.
- Tab:** 'Database and Server Configuration' with the Citrix logo on the right.
- Instructions:** 'Specify the instance name of the Session Recording Database and the computer account of the Session Recording Server.'
- Database Instance Name:** A text input field with a 'Test' button to its right. Below the field is an example: 'Example: \SQLEXPRESS,computer-name\SQLEXPRESS, computer-name'.
- Session Recording Server computer account:** A text input field. Below the field is an example: 'Example: localhost, domain\computer-name'.
- Navigation Buttons:** '< Back', 'Next >', and 'Cancel' buttons at the bottom right.

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。

【テスト】をクリックして、SQL Serverへの接続をテストします。現在のユーザーがSQL Serverのパブリックな役割権限を持っていることを確認します。権限がなければ、権限の制約によりテストは失敗します。【次へ】をクリックしてインストールを続行します。

2.手順に従ってインストールを完了します。インストール中、現在のユーザーがデータベース管理者ではない場合、sysadmin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。適切な資格情報を入力し、【OK】をクリックして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。

インストールの完了後は、sysadminサーバーロール権限は不要になり、現在のユーザーに対して安全に削除できます。

Important

CitrixSessionRecordingというデータベース名は変更できません。

Session Recording Serverのインストール

Session Recording Serverをインストールする前に、すべての前提条件をインストールしているか確認します。詳しくは、「[Session Recordingのシステム要件](#)」を参照してください。

1. [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。
2. [テスト]をクリックして、SQL Serverへの接続をテストします。現在のユーザーがSQL Serverのパブリックな役割権限を持っていることを確認します。権限がなければ、権限の制約によりテストは失敗します。[次へ]をクリックし、ウィザードの指示に従ってインストールを完了します。
3. インストールウィザードの最後に、Citrixのカスタマーエクスペリエンス向上プログラムに参加するかどうかを選択します。このプログラムに参加すると、統計情報や使用状況が匿名でCitrixに送信されます。詳しくは、「[Citrixカスタマーエクスペリエンス向上プログラム \(CEIP\) について](#)」を参照してください。

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機関]でSession Recording Serverを信頼します。
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およびFQDN、ポート番号、およびSession Recording AgentからSession Recording Brokerへの接続の種類 (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。

1. サーバーマネージャーを使用して、.NET Framework 3.5、およびHTTPをサポートするMicrosoft Message Queuing (MSMQ) を、XenApp 7.8 Server OS VDAまたはXenDesktop 7.8 VDIにインストールします。
2. Windowsコマンドプロンプトを管理者として起動し、次のコマンドを実行します。

msiexec /i SessionRecordingAgentx64.msi

または

msiexec /i SessionRecordingAgent.msi

または、.msiファイルをダブルクリックします。

32ビットシステムの場合は**SessionRecordingAgent.msi**、64ビットシステムの場合

は**SessionRecordingAgentx64.msi**と、プラットフォームの種類に応じた適切な.msiファイルを使用します。

3. インストールUIで[次へ]を選択して、ライセンス契約に同意します。
4. [Session Recording Agent構成] ページで、Session Recording Serverをインストールしたコンピューターの名前と、Session Recording Serverとの接続のプロトコルとポート情報を入力します。

The image shows a Windows-style window titled "Citrix Session Recording Agent Setup". The window has a header bar with the Citrix logo and the title "Session Recording Agent Configuration". Below the header, there is a text instruction: "Enter the Session Recording Server connection information below. Note that you can modify these values at a later date by running the Session Recording Agent properties." The main area contains three input fields: "Session Recording Server Name" (a text box), "Protocol" (a dropdown menu with "HTTP" and "HTTPS" options, where "HTTPS" is selected), and "Port" (a text box containing "443"). Below these fields is a "Test" button. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Session Recording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。 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を選択解除します。 SSL設定を開き、[SSLを必要とする]チェックボックスをオフにします。

5.手順に従ってインストールを完了します。

Session Recording Playerのインストール

Session Recording Server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。

SessionRecordingPlayer.msiを実行して、手順に従って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  
sessionrecordingservername=yourservername sessionrecordingbrokerprotoco=yourbrokerprotocol  
sessionrecordingbrokerport=yourbrokerport /!*v yourinstallationlog /q
```

32ビットシステム：

```
msiexec /i SessionRecordingAgent.msi sessionrecordingservername=yourservername  
sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /!*v yourinstallationlog /q
```

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。

*yourbrokerprotocol*は、HTTPまたはHTTPSで、Session Recording Brokerとの通信にSession Recording Agentで使用されるプロトコルです。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、つまりHTTPでは80、HTTPSでは443がSession Recording Agentで使用されます。

*!/!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 7.6.0（またはそれ以降のバージョン）を、最新リリース（現行）のSession Recordingのバージョンにアップグレードすることができます。

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、対応するSession Recording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サーバーと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sysadmin役割権限が必要です。この権限がない場合、アップグレード中にsysadmin役割資格情報を求められます。
- 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（またはそれ以降のバージョン）を、最新リリース（現行）のSession Recordingサーバーとともに使用できます。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サーバー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。

- 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、わずかですが録画を完了できない可能性があります。
- サイトの停止の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サーバーが別々のサーバーにインストールされている場合、Session Recordingサーバーで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サービスとともに実行されていることを確認します。Session Recordingサーバーをアップグレードします。Session RecordingデータベースとSession Recordingサーバー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サーバー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。

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機能を使用します。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sysadminが必要です。

Windowsの役割および機能の前提条件を追加するスクリプト

Jul 07, 2016

以下のスクリプトを使用して、Session Recordingが正しく動作するために必要なWindowsの役割および機能の前提条件をインストールできます。詳しくは、「[スクリプトを使用してWindowsの役割および機能の前提条件を追加する](#)」を参照してください。

Session Recording Administrationの前提条件のインストール

コピー

```
<#

.Synopsis

    Installs Prereqs for Session Recording Administration

.Description

    Supports Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.

    Install below windows feature on this machine:

    -Application Development - ASP.NET 4.5 on Server 2012 and Server 2012 R2, Application Development - ASP.NET on Server 2008 R2

    -Security - Windows Authentication

    -Management Tools - IIS 6 Management Compatibility

        IIS 6 Metabase Compatibility

        IIS 6 WMI Compatibility

        IIS 6 Scripting Tools

        IIS 6 Management Console

    -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)

{

    try

    {

        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}
```

```

        Add-WindowsFeature $feature

    }

    catch

    {

        Write-Host "Addition of Windows feature $featurename failed"

        Exit 1

    }

    Write-Host "Addition of Windows feature $featurename succeeded"

}

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like "**Microsoft Windows Server 2012*") -or ($system -Like "**Microsoft Windows Server 2008 R2*")))

{

    Write-Host("This is not a supported server platform. Installation aborted.")

    Exit

}

# Start to install Windows feature

Import-Module ServerManager

if ($system -Like "**Microsoft Windows Server 2012*")

{

    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5

}

if($system -like "**Microsoft Windows Server 2008 R2*")
{

```

```
{
    AddFeatures('Web-Asp-Net') #ASP.NET
}

AddFeatures('Web-Mgmt-Console') #IIS Management Console

AddFeatures('Web-Windows-Auth') # Windows Authentication

AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility

AddFeatures('Web-WMI') #IIS 6 WMI Compatibility

AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools

AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console

AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
```

Session Recording Agentの前提条件のインストール

コピー

```
<#

.Synopsis

    Installs Prereqs for Session Recording Administration

.Description

    Supports Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8, Windows 8.1 and Windows 10.

    Install below windows feature on this machine:

    -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)
{
    try
    {
        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}

        Add-WindowsFeature $feature
    }
    catch
    {
    }
}
```

```

    }

    catch

    {

        Write-Host "Addition of Windows feature $featurename failed"

        Exit 1

    }

    Write-Host "Addition of Windows feature $featurename succeeded"

}

# Start to install Windows feature

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like "*Microsoft Windows Server 2012*") -or ($system -Like "*Microsoft Windows Server 2008 R2*")-or ($system -Like "*N

{

    Write-Host("This is not a supported platform. Installation aborted.")

    Exit

}

if ($system -Like "*Microsoft Windows Server*")

{

    Import-Module ServerManager

    AddFeatures('MSMQ') #Message Queuing

    AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support

}

else

{

    try

```



```
{  
  
if($system -Like "*Microsoft Windows 7")  
  
{  
  
    dism /online /enable-feature /featurename:IIS-WebServerRole /featurename:IIS-WebServer /featurename:IIS-IIS6ManagementCon  
  
    dism /online /enable-feature /featurename:MSMQ-Container  
  
    dism /online /enable-feature /featurename:MSMQ-Server  
  
    dism /online /enable-feature /featurename:MSMQ-HTTP  
  
}  
  
else  
  
{  
  
    dism /online /enable-feature /featurename:MSMQ-HTTP /all  
  
}  
  
}  
  
catch  
  
{  
  
    Write-Host "Addition of Windows feature MSMQ HTTP Support failed"  
  
    Exit 1  
  
}  
  
write-Host "Addition of Windows feature MSMQ HTTP Support succeeded"  
  
}
```

Session Recordingの構成

Jul 07, 2016

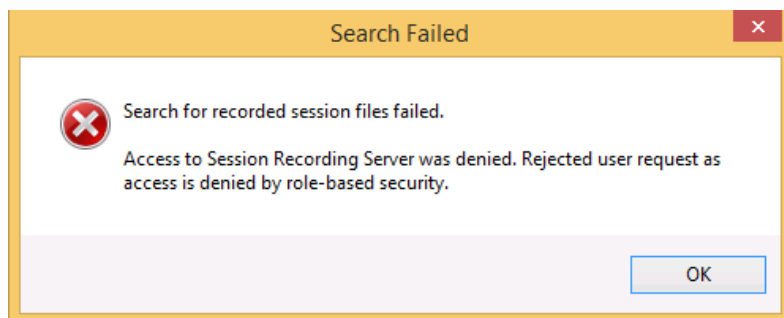
セッションの再生と録画のためのSession Recordingの構成

Session Recordingコンポーネントをインストールしたら、次の作業を行いSession Recordingを設定して、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。

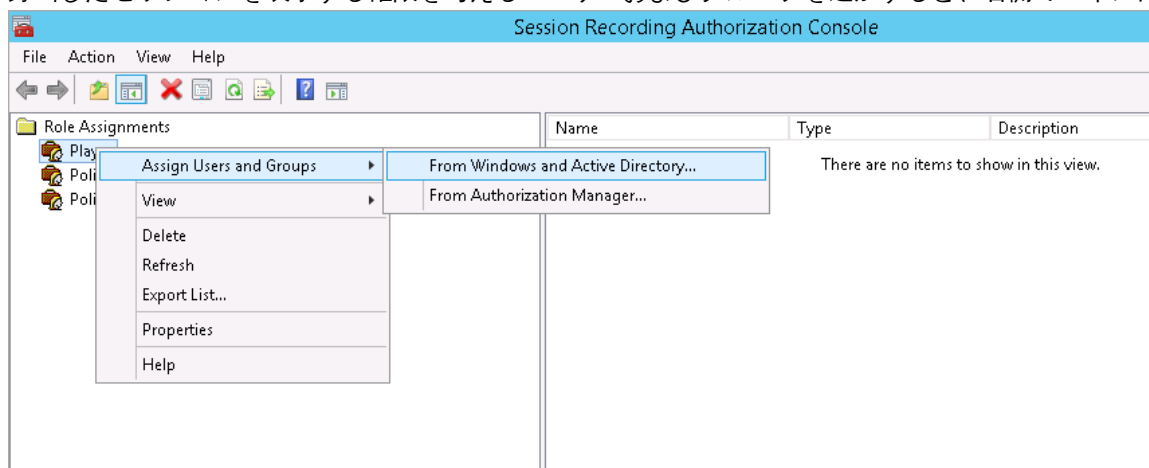
- ユーザーに録画を再生する権限を与える。
- ユーザーに録画ポリシーを管理する権限を与える。
- セッションを録画する録画ポリシーをアクティブにする。
- カスタムポリシーの構成
- Session Recording Playerを構成してSession Recording Serverと接続する。

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。



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。

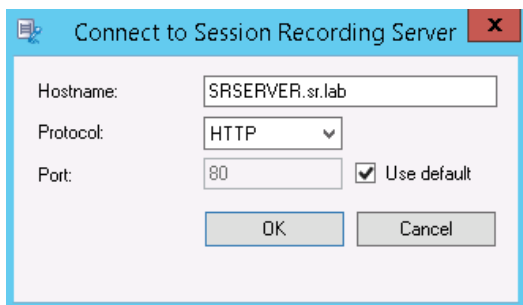
1. Session Recording Serverをホストするマシンに管理者としてログオンします。
2. Session Recording承認コンソールを起動して、PolicyAdministratorsを選択します。
3. 録画ポリシーを管理できるユーザーとグループを追加します。

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、一度にアクティブにできるポリシーは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. [Connect to Session Recording Server] ポップアップウィンドウが開いたら、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ポップアップウィンドウがエンドユーザーに表示されます。
 - 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ポップアップウィンドウが開くことはありません。
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。

注：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、「[カスタム録画ポリシーの作成](#)」を参照してください。

Session Recording Playerの構成

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 Serverとの接続を設定できますが、同時に複数のSession Recording Server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インします。
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 Server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 Serverと接続できるように構成する場合は、Session Recording Server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インします。
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7200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たら、Session Recording Agentサービスを再起動して変更を受け入れます。

ユーザーへのアクセス権の付与

Jul 07, 2016

注：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。

ユーザーに役割を割り当てるには

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。

録画ポリシーの作成とアクティブ化

Jul 07, 2016

Session Recording Policy Console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。

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。

システムポリシーの使用

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。** このポリシーを選択すると、セッションは録画されません。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ポップアップウィンドウがエンドユーザーに表示されます。
- **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ポップアップウィンドウが開くことはありません。

システムポリシーは変更したり削除したりできません。

ポリシーをアクティブにするには

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. Session Recording Policy Consoleを起動します。
3. [Connect to Session Recording Server] 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 Policy Console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] の [ポリシーのアクティブ化] を選択します。

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 Policy Console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。

- **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。録画されていることを通知するポップアップウィンドウがエンドユーザーに表示されます。

- 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が付きません。

規則ごとに次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がある場所を選択します。

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。

カスタムポリシーの構成

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、ダイアログボックス左側の「録画ポリシー」を選択し、メニューバーから「操作」>「新しいポリシーの追加」の順に選択します。
3. 「新しいポリシー」を右クリックして「規則の追加」を選択します。
4. 録画オプションの選択 - 規則ウィザードで、「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 - 以下の3つのオプションのいずれか、またはあらゆる組み合わせを選択できます。
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
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。
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。

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 Policy Consoleを起動します。
3. [Connect to Session Recording Server] 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 Policy Consoleで、[録画ポリシー] を選択します。
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] を選択します。
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] を選択し、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

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 Policy Consoleを起動します。
3. [Connect to Session Recording Server] 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 Policy Console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. 新しい規則を追加したり、規則を変更または削除したりします。
 - 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] を選択します。 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] を選択します。

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 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. [Connect to Session Recording Server] 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 Policy Console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。

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、ファイルがロールオーバーするときに新しいポリシーが有効になる場合があります。ファイルサイズが上限に達するとロールオーバーが実行されます。録画ファイルのサイズの上限については、「[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
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。

通知メッセージの作成

Jul 07, 2016

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。

必要な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ケール設定に対応する通知メッセージが表示されます。

新しい通知メッセージを作成するには

1. 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. [スタート] ボタンをクリックし、[Session Recording Server Properties] を選択します。
3. [Session Recording Server Properties] で、[通知] タブをクリックします。
4. [Add] 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。

録画の無効化または有効化

Jul 07, 2016

Session Recording Agentは、セッションを録画する各サーバーOSマシン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。

サーバーで録画を無効または有効にするには

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. [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. [セッションの録画] 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 Policy Console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。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ブラウザを開いた回数わかります。

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。各サーバーをそれぞれ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。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

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、[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。

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

Jul 07, 2016

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、実際には1、2秒の遅れが生じます。XenAppまたはXenDesktopサーバーからデータが伝達されるためです。

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 Server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 Properties] 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 Server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] メニューから[**Session Recordingサーバーのプロパティ**]を選択します。
3. [**Session Recordingサーバーのプロパティ**] 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。

デジタル署名を有効および無効にする

Jul 07, 2016

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済みである場合は、デジタル署名をセッションの録画に割り当てることにより、Session Recording環境のセキュリティを高めることができます。

デフォルトでは、デジタル署名は無効化されています。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。

デジタル署名を有効にするには

1. 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. [スタート] ボタンをクリックし、[Session Recording Server Properties] を選択します。
3. [Session Recording Server Properties] 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。

デジタル署名を無効にするには

1. 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. [スタート] ボタンをクリックし、[Session Recording Server Properties] を選択します。
3. [Session Recording Server Properties] で、[署名] タブをクリックします。
4. [消去] をクリックします。

録画の格納先の指定

Jul 07, 2016

[Session Recording Server Properties] を使用して、録画の格納先とアーカイブされた録画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。

録画ファイルの場所を指定するには

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。録画を格納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 Server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 Properties] を選択します。
3. [Session Recording Server Properties] 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。

アーカイブ済みファイルの復元フォルダーを指定するには

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。アーカイブされた録画を復元するフォルダーは変更できません。

1. 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. [スタート] ボタンをクリックし、[Session Recording Server Properties] を選択します。
3. [Session Recording Server Properties] 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ファイルを復元するフォルダーを入力します。

録画ファイルのサイズの指定

Jul 07, 2016

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は適用されません。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。

ファイルの限界値を指定するには

1. 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. [スタート] ボタンをクリックし、[Session Recording Server Properties] を選択します。
3. [Session Recording Server Properties] で、[ロールオーバー] タブをクリックします。
4. 10から1024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。

録画の表示

Jul 07, 2016

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。

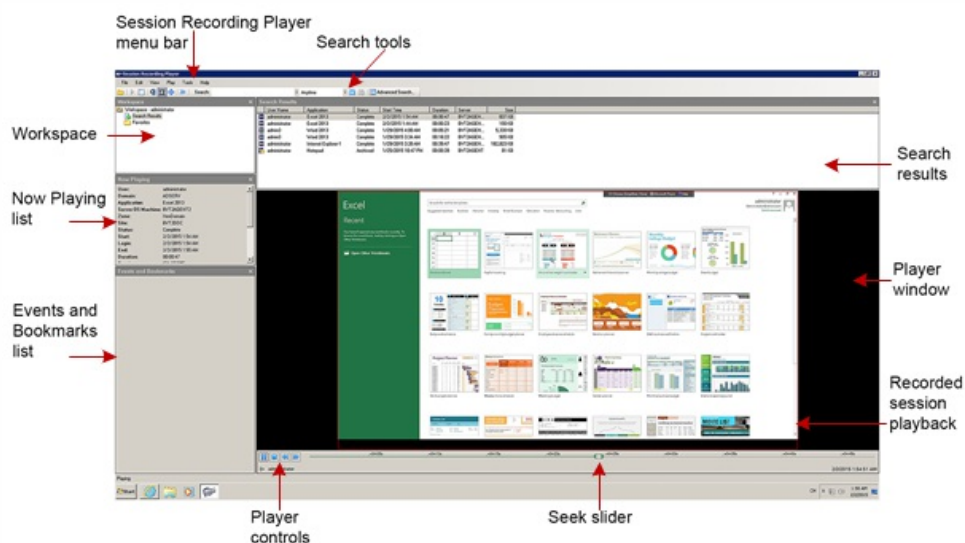
注：Session Recording管理者が、録画されたサーバーOSマシンセッションへのアクセス権をユーザーに付与する必要があります。セッションを表示できない場合は、Session Recording管理者に連絡してください。

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を起動するには

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。
Session Recording Playerが表示されます。

この図はSession Recording Playerとその主要要素を示します。これらの要素の機能について、以下で説明します。



ウィンドウ要素を表示または非表示にするには

Session Recording Playerには、表示するかどうかを切り換えるためのウィンドウ要素があります。

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、[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を変更するには

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インします。
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 Serverを選択します。

録画の再生

Jul 07, 2016

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。

検索結果の領域にある録画を開いて再生するには

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. 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には

セッションの録画ファイルの名前は、冒頭が付く一意な英数字のファイルIDで、拡張子は、再生データの保護機能が無効な録画の場合は.icl、有効な録画の場合は.icleになります。セッションの録画ファイルが保存されるディレクトリ構造には、セッションを録画した日付が反映されます。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、フォルダーパス2014\12\22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。
 - 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インします。
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 [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。

セッションの録画の検索

Jul 07, 2016

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：使用できる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。

クイック検索を実行するには

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. 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。

高度な検索を実行するには

ヒント：高度な検索では、150,000個を超えるエンティティが含まれる結果が返されるのに最大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マシン、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。[高度な検索] ダイアログボックスの[開く] をクリックして、保存したクエリを取得します。保存したクエリファイルの拡張子は.isqです。

検索オプションを設定するには

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。
2. [スタート] ボタンをクリックし、[Session Recording Player] を選択します。
3. 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。

セッションの録画の再生

Jul 07, 2016

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。セッション内では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。

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、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。

シークスライダーの使い方

プレーヤーウィンドウ下部の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：

Home キー:	冒頭へシークします。
End	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+ 右矢印	30秒先へシークします。
Ctrl+ 左矢印	30秒前へシークします。
Page Down	1分先へシークします。
Page Up	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+ Page Down	6分先へシークします。
Ctrl+ Page Up	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、メニューバーで、[ツール] > [オプション] > [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。

再生速度を変更するには

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. メニューバーで、[再生] > [再生速度] 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。

操作のない空白期間を省略するには

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。

イベントとブックマークの使用

Jul 07, 2016

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。

一覧にイベントとブックマークを表示するには

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。

ブックマークを挿入するには

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. 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。

コメントを追加または変更するには

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。

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。

ブックマークを削除するには

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. 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に移動するには

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。

再生の表示形式の変更

Jul 07, 2016

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を全画面で表示するには

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。

プレーヤーウィンドウを独立ウィンドウで表示するには

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。

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。

セッションの録画ファイルのキャッシュ

Jul 07, 2016

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。

キャッシュを有効にするには

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。

Session Recordingのトラブルシューティング

Jul 07, 2016

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。

Session Recording Agentが接続できない

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。次のような状況で、データの移行が必要です。

- 「基になる接続が閉じられました。SSL/TLSの安全なチャンネルを確立できませんでした。」この例外は、Session Recording Server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 Server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：[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 Serverで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。

「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 Server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をインストールできない

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がSession Recordingデータベースに接続できない

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 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 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 Policy Console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、またはMicrosoft SQL Server 2014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 Server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。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。

セッションが録画されない

アプリケーションセッションが録画されない場合は、まずSession Recording AgentとSession Recording Serverが動作するサーバーOSマシン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サーバーOSマシンで公開します。
- 録画が有効になっていない。サーバーOSマシンに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、サーバーOSマシンでSession Recording Agentサービスが実行されており、Session Recording ServerをホストするコンピューターでSession Recording Storage Manager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 Server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。

ライブセッションを再生できない

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 Properties] ダイアログボックスで[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。

録画が破損または不完全

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、MCS (Machine Creation Services) またはProvisioning Services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。

解決策：各VDAに対し、一意のQMIDを作成します。「[既知の問題](#)」で、回避策が紹介されています。

Session RecordingデータベースまたはSession Recording Serverのインストール時におけるデータベースインスタンスの接続テストの失敗

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。

解決策：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。

コンポーネント間の接続の確認

Jul 07, 2016

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 Server (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 Server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。

Session Recording Agentが接続されていることの確認

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 Server Properties] で、[接続] をクリックします。
4. [Session Recording Server] の値が、Session Recording Server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サーバーOSマシン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。

Session Recording Serverが接続されていることの確認

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。

1. 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. 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Session Recording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。

Session Recordingデータベースが接続されていることの確認

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。

IISの接続のテスト

Session Recordingコンポーネントで通信に問題が起きたときは、WebブラウザでSession Recording BrokerのWebページにアクセスしてSession Recording Server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。

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。

Webブラウザに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 Agentが動作するコンピューターがSession Recording Server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。

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?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/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。

Webブラウザに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 Playerが動作するコンピューターがSession Recording Server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。

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 Policy Consoleが動作するコンピューターがSession Recording Server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。

証明書の問題のトラブルシューティング

通信プロトコルにHTTPSを使用する場合は、Session Recording Server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 Server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 Serverを信頼できず、接続できません。

Session Recording Server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 Server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 Serverに接続するとき、接続するすべてのコンポーネント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 Server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 Serverへの接続は失敗します。Session Recording Server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 Server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。

Session Recording Playerに障害が発生した場合の録画の検索

Jul 07, 2016

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 Server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： [ツール] > [オプション] > [接続] を選択し、 [Session Recording Servers] 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 Server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 Server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 Serverが接続していることを確かめます。
- 「Access denied error.」 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。
- 「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の安全なチャンネルを確立できませんでした。」この例外は、Session Recording Server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] の順に選択します。
[Session Recordings Servers] 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。

MSMQのトラブルシューティング

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 Server (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 Server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。

- 接続待ちの状態、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] ダイアログボックスの [接続] タブで選択されているプロトコルに対応）、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 Server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 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/msmq/private\$/CitrixSmAudData**（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）
- 「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] ダイアログボックスで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 Server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。citrixmauddata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。

通信プロトコルの変更

Jul 07, 2016

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。

HTTPを通信プロトコルに使用するには

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. 各サーバーの [Session Recording Agentのプロパティ] ダイアログボックスで、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] を選択します。
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。

通信プロトコルをHTTPSに戻すには

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. 各サーバーの [Session Recording Agentのプロパティ] ダイアログボックスで、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] を選択します。
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。

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。

リファレンス：データベースレコードの管理

Jul 07, 2016

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%ProgramFiles%\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。

クイックリファレンス

次の表に、ICLDBユーティリティで使え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> [/i] [/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」と入力してフォルダーを移動し、「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。
remove	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。

removeall コマンド	説明 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。

サードパーティ製品についての通知

Jul 07, 2016

Session Recordingには、以下の条件でライセンスが有効になったサードパーティソフトウェアが含まれている可能性があります。この一覧は、一覧の作成日時時点のサードパーティソフトウェアを使用して生成されています。この一覧は製品のバージョンに応じて変更されることがあります。この一覧は「現状のまま」提供されるものであり、適用法令により許容される限度において、CITRIXおよびその製品供給者は、一覧または一覧の正確性もしくは完全性について、あるいは一覧の使用または配布によって生じる結果について、明示または黙示を問わず、法令上その他いかなる保証または条件もお客様に付与するものではありません。この一覧を使用した配布することにより、お客様は、いかなる場合においても、一覧の使用または配布によって生じる特別、直接的、間接的、または付随的損害、あるいはその他の損害について、CITRIXが責任を負わないことに同意するものとします。

MMC.NETライブラリ

Common Public License、Version 1.0によるライセンス

構成ログ

Jul 07, 2016

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他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 2.0 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。ただし、サイトを作成した後で、構成ログで使用するデータベースの場所をできるだけ早く変更することを強く推奨します。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。

- 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ても構成変更を許可する」チェックボックスをオフにします。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「構成ログを有効にする」がクリック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」チェックボックスをオンにします。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他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。
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了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。

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、「その他の権限」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があります。
- **SQL Serverデータベース** - データベースから記録を削除するための権限を持つ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。

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記述されます。

Personal vDiskの監視

Jul 07, 2016

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：このレポートでは、Software.Dat.Report.txtとSoftware.Dat.delta.txtの2つのファイルが生成されます。

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。

SYSTEM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Pvd-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。
- Setupapiapp.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に追加されたその他のファイル（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。

Director

Aug 26, 2016

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](#)

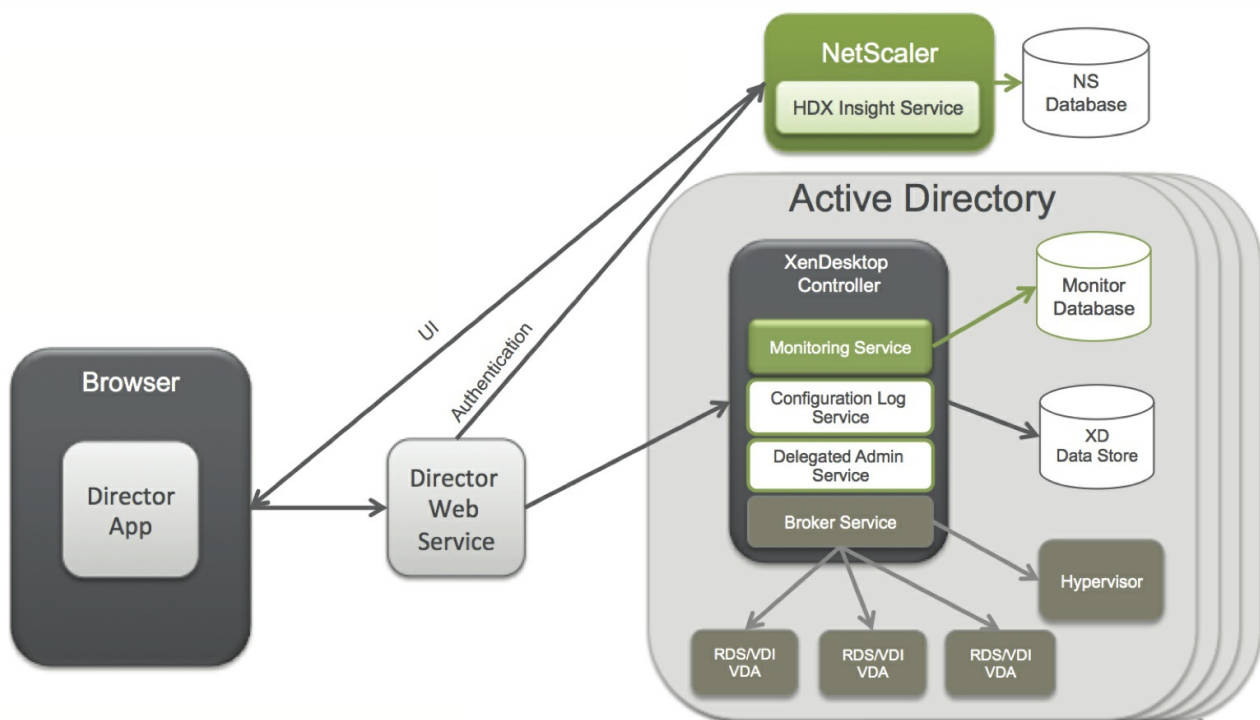
[XenApp 6.5用のDirectorのインストール](#)

[Directorへのログイン](#)

[Directorでの統合Windows認証の使用](#)

Directorについて

リアルタイムWebツールであるDirectorを使用すると、管理者はエンドユーザーのセッションを監視したり、トラブルシューティングを施したり、そのほかのサポートタスクを実行したりできます。



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 HDX Insight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できます。
- 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。HDX Insight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IT担当者による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、管理者が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かを判断できるようになります。

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、展開の主要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の展開と構成

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Directorは、Version 6.5よりも前のXenApp展開やVersion 7よりも前のXenDesktop展開をサポートしません。

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（「[管理権限の委任と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、「[CTX127389 : 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のインストール

DirectorはXenAppおよびDesktopに対応した全製品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。インストーラーによるデフォルトの構成のままだと、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、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、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。インストーラーの使用については、詳しくは、インストールに関するドキュメントで「[グラフィカルインターフェイスを使ったインストール](#)」を参照してください。個々のMSIファイルではなく、製品のメイン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上にインストールされたDirectorでは、サーバーアドレスとしてlocalhostが自動的に構成され、DirectorはデフォルトでローカルのControllerと通信します。

Controllerとは別の専用サーバー上にDirectorをインストールする場合は、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。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用のDirectorのインストール

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コントローラー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。

各XenAppサイトについて1つのコントローラーのサーバーアドレスを指定します。XenAppサイトのほかのコントローラーは

自動的にフェールオーバー用に使用されます。Directorは、コントローラー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がDVDの**Support\DirectorWMIProvider**フォルダーに収録されています。適切なすべてのXenAppサーバー（コントローラー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。TLSを有効にするためにDirectorを構成する必要はありません。

注意

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へのログオン

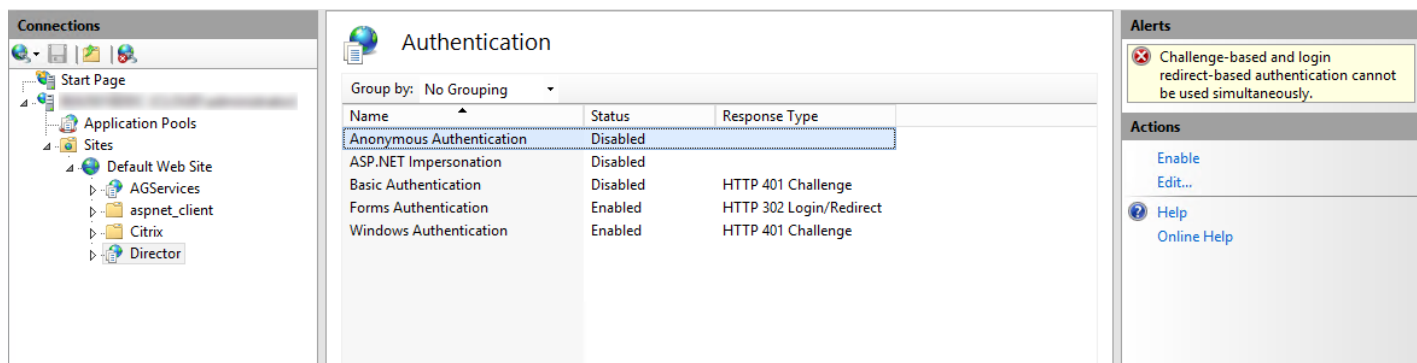
Directorにログオンするには、Webブラウザでhttps:///Directorまたはhttp:///Directorにアクセスします。

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。

Directorでの統合Windows認証の使用

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管理コンソールが開いたら、【ドメイン名】 > 【コンピューター】の順に移動し、委任アクセス許可を与える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、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。

詳細構成

Jul 07, 2016

ここでは次のことについて説明します。

複数のActive Directoryドメインとフォレストでのユーザーのサポート

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

複数のサイトまたは複数のActive Directoryフォレストのサポートなど、一部の詳細なDirector構成は、インターネットインフォメーションサービス (IIS) マネージャーの設定を介して制御します。

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。

複数のActive Directoryドメインとフォレストでのユーザーのサポート

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),

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。

注意

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へのサイトの追加

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ファームのコントローラー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コントローラーのアドレスです。

次の方法でXenApp 6.5ファームのコントローラーを追加することもできます。

`DirectorConfig.exe /xenapp FarmControllerName`

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、およびヘルプデスク管理者です。

ユーザーのプライバシーと使用しているアプリケーションを保護するため、「アプリケーション」タブでアプリケーションの一覧を非表示にできます。

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. 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。

次の設定の値を変更します。

`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。

展開環境の監視

Jul 15, 2016

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](#)

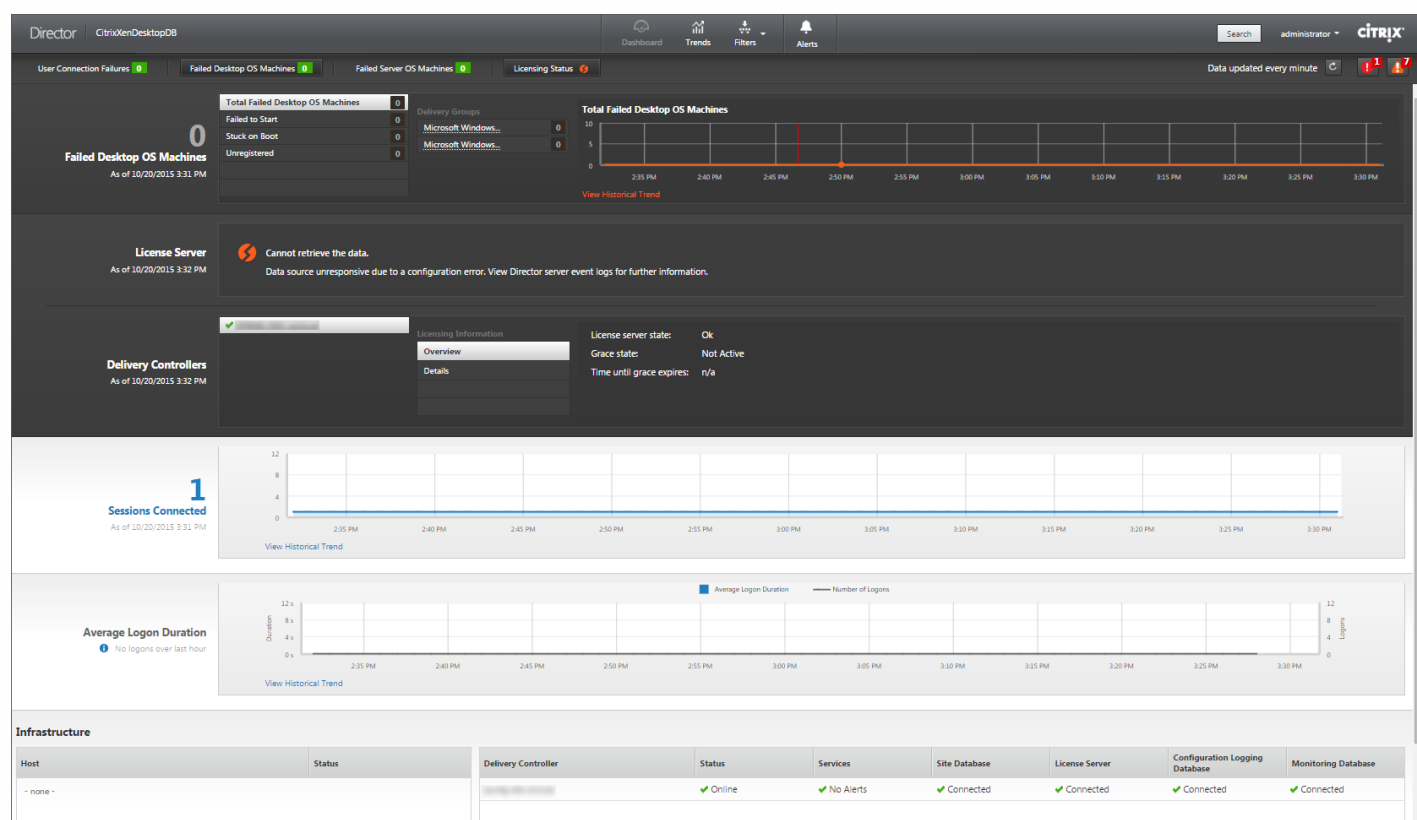
[Hotfixの監視](#)

[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](#)

サイトの監視

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。

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。 - Delivery Controllerアラートには、Delivery 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。 アラートのしきい値は、Studioで設定できます。 ライセンスサーバーのバージョンが11.12.1よりも前の場合や、Delivery ControllerがXenApp 7.6またはXenDesktop 7.6よりも古い場合、ライセンスサーバーアラートとDelivery Controllerアラートは表示されません。
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	サイトのホスト、Controller、およびインフラストラクチャのヘルス状態が表示されます。パフォーマンスに関するアラートを確認できます。 ホストの場合、接続状態、CPU、メモリ、帯域幅（ネットワーク使用）、およびストレージ（ディスク使用）のヘルス状態がXenServerまたはVMwareからの情報を使って監視されます。 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、XenServerのドキュメントで パフォーマンスアラートの設定 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

セッションの監視

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。

操作	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の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。「 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。
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。

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

「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、およびセッション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：セッション数が表示されます。「マシン」ビューでセッション数を表示することもできます。
- 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。

2. 「フィルター基準」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。

後でフィルターを開くには、「フィルター」メニューでエラーの種類（マシン、セッション、または接続）を選択し、保存済みのフィルターを選択します。

6. [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。

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

サイト全体の履歴傾向の監視

[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、および負荷評価についての履歴傾向情報が表示されます。 これらの情報を表示するには、[ダッシュボード] または [フィルター] ビューで [傾向] 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。

操作	説明
グラフデータのエクスポート	エクスポートするデータを含むタブを選択します。 [エクスポート] をクリックして、エクスポート形式 (PDF、Excel、またはCSV) を選択します。
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	[接続エラー] タブで、接続エラー情報を表示するマシンの種類、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。 管理者は、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。
HDX Insightを使用したネットワーク分析データの表示	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。 〔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。

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、発生したイベントま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。

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

Hotfixの監視

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。

ユーザーマシンの電源状態の制御

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。

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。
開始	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。

マシンへの接続の無効化

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。

アラートおよび通知

Jul 27, 2016

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](#)

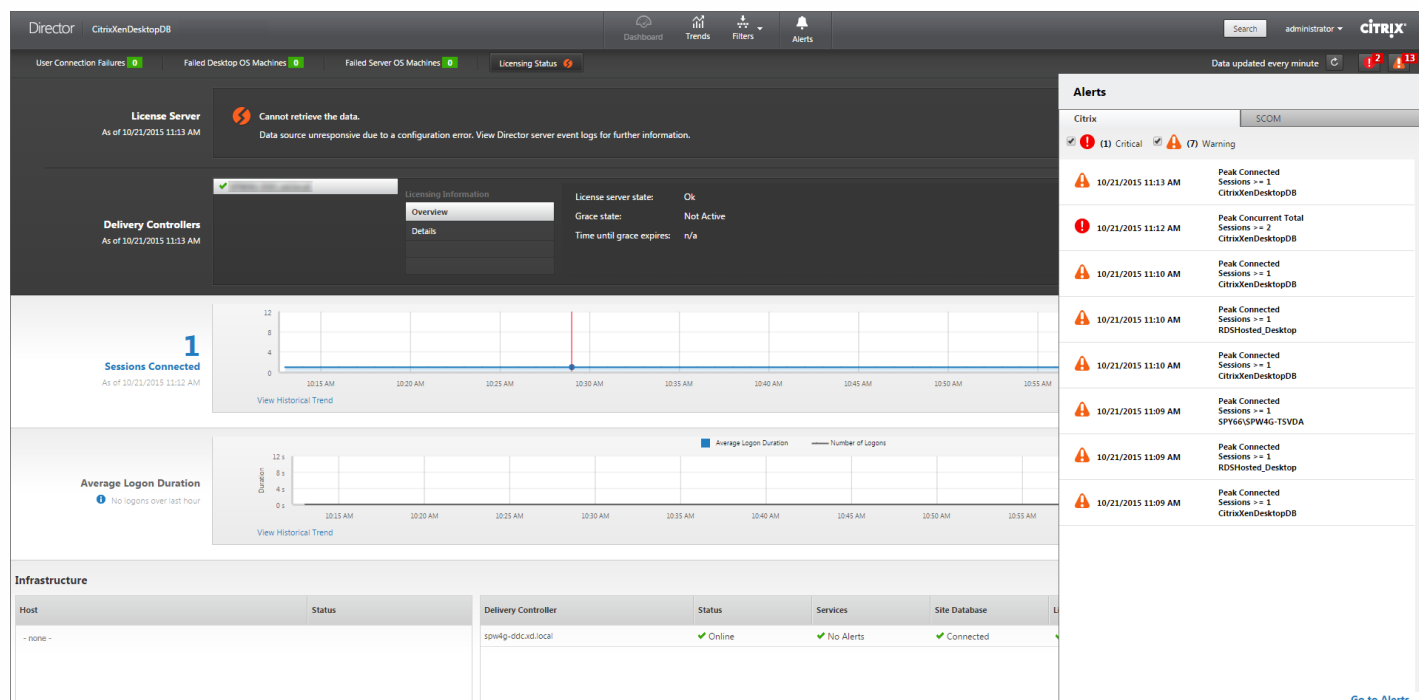
[アラートポリシーの条件](#)

[SCOMアラート](#)

[SCOM統合の構成](#)

[アラートの監視](#)

アラートは、Directorのダッシュボードおよびその他の概要ビューに、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、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、条件の最小しきい値に達したことを示します。

重大アラート（赤の円）は、条件の最大しきい値を超過したことを示します。

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。

[\[アラート\]](#) 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マシンを特定することができます。

Director CitrixXenDesktopDB

Dashboard Trends Filters Alerts

Citrix Alerts SCOM Alerts Citrix Alerts Policy Email Server Configuration

Citrix Alerts

Source:

Category:

State:

Time period: Ending

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アラートポリシーは、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できます。アラートの条件をしきい値違反に設定した結果として生成され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することができます。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」および「SCOM統合の構成」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アラートの合計です。

アラートポリシーの作成

Director CitrixXenDesktopDB

Dashboard Trends Filters Alerts

Search administrator CITRIX

Citrix Alerts SCOM Alerts Citrix Alerts Policy Email Server Configuration

Site Policy Delivery Group Policy Server OS Policy

[Back to Alert Policies](#)

Name of Alert:

Description:

Conditions:

- Peak Connected Sessions
- Peak Disconnected Sessions
- Peak Concurrent Total Sessions
- Connection Failure Rate
- Connection Failure Count
- Average Logon Duration
- Load Evaluator Index

Number of peak connected sessions

Warning Critical [Reset Values](#)

Peak connected sessions: mins mins

Re-alert interval: mins mins

Scope: No Server OS Machines assigned

Notifications preferences: No email addresses added

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SMTPサーバーを指定する必要があります。
7. [Save] をクリックします。

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の一意なデリバリーグループに対して、デリバリーグループごとに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）。

アラートポリシーの条件

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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 • 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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 • 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。 アラートが表示された場合に推奨される操作は、以下のとおりです。

	● 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。
Connection Failure Rate	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。
Connection Failure Count	過去1時間の接続エラー数。 アラートが表示された場合に推奨される操作は、以下のとおりです。 ● 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。
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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 ● 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。
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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 ● 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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 ● 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、ログオンに時間がかかる場合があります。 ● 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。

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。 アラートが表示された場合に推奨される操作は、以下のとおりです。 • 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。

SCOMアラート

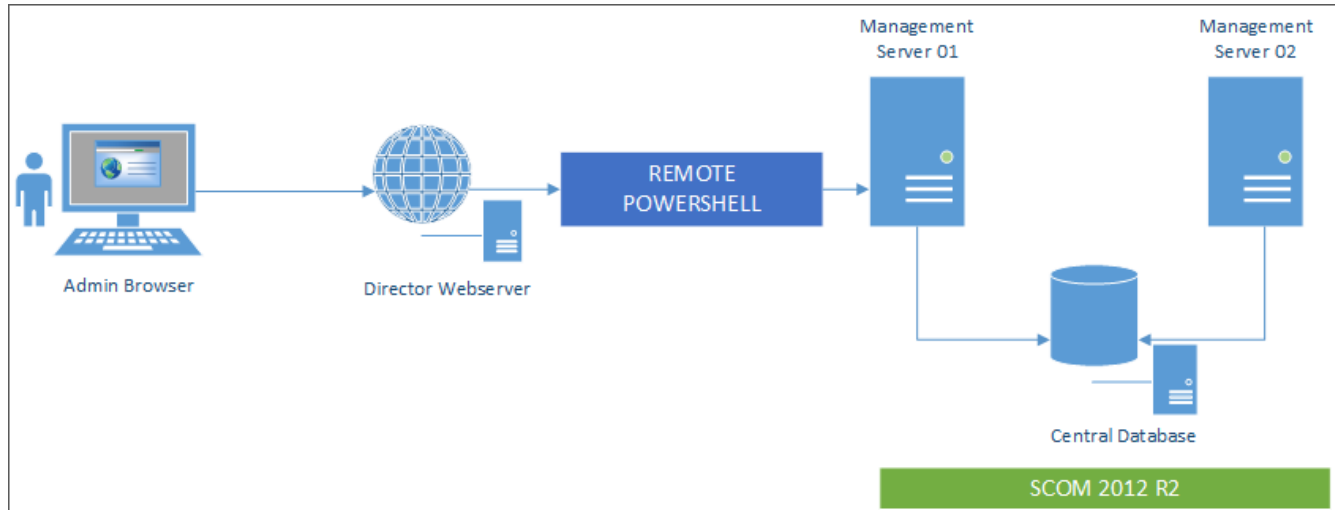
DirectorとのSCOM統合により、Microsoft System Center 2012 Operations Manager（SCOM）からのアラート情報を、Directorのダッシュボードおよびその他の概要ビューで表示できるようになります。

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。

SCOM統合の構成

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。



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。

- 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、SCOM管理者アカウントをweb.configファイルでDirectorConfigツールを使用して構成できますが、これは推奨されません。
- 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。これにより、SCOM管理サーバーに対する負荷を軽減し、パフォーマンスを最適化することができます。

Directorサーバーで、以下を実行します。

1. Directorサーバーでコマンド**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。管理者権限のPowerShellコマンドラインから管理者権限でPowerShellプロンプトを開き、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。

-command

Get-Item WSMAN:\localhost\Client\TrustedHosts

コピー

- 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る既存のエントリセットを表しています。

-command

Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"

コピー

3. DirectorConfigツールを使用して、SCOMを構成します。

-command

C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscm

コピー

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オペレーターには、4つのカテゴリがあります。これらの役割に基づいて、SCOMデータへのアクセスの種類が定義されます。たとえば、読み取り専用SCOMオペレーターには、[管理] ペインが表示されず、このオペレー

ターは規則、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。SCOM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、Director管理者は以下の処理を実行できません。

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ツールを使用して指定されたサーバーと同じです。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：

CLI

-command

コピー

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

PS

-command

コピー

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. MaxShellsPerUserの変更：

CLI

-command

コピー

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

PS

-command

コピー

```
Set-Item WSMAN:\localhost\Shell\MaxShellsPerUser 20
```

c. MaxMemoryPerShellMBの変更 :

CLI

-command

コピー

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

PS

-command

コピー

```
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

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

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。

管理権限の委任と Director

Jul 07, 2016

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。
ヘルプデスク管理者	[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。
マシンカタログ管理者	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。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	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。

管理者の役割	Directorでの権限

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。たとえば、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。

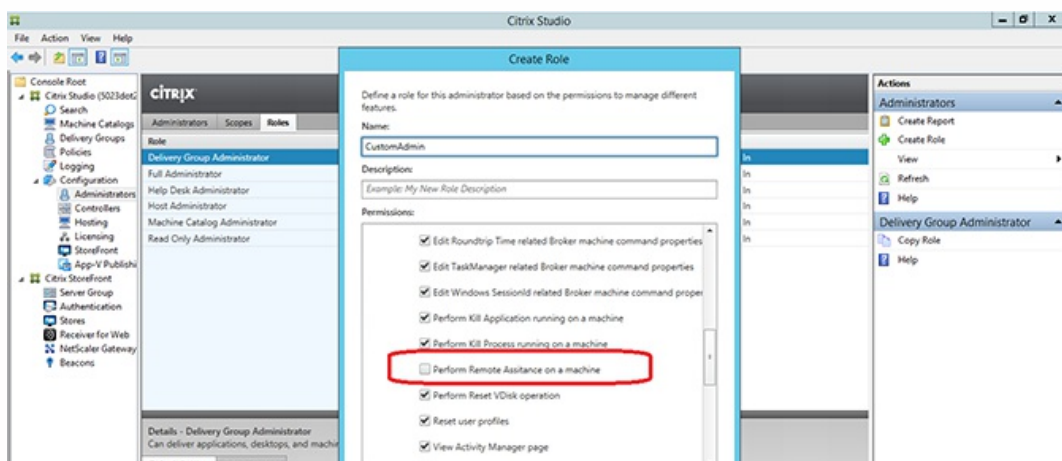
- DirectorにログオンするためのDelivery Controller権限。
- デリバリーグループのデータをDirectorで閲覧するための権限。

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。



さらに、ほかのコンポーネントの権限の一覧から、次の権限の追加を検討します。

- デリバリーグループの権限：
 - 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

Director展開環境の保護

Jul 07, 2016

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。

Microsoftインターネットインフォメーションサービス (IIS) の構成

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

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
- HEAD

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

Important

- 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。

ユーザー権利の構成

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 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。

Directorの証明書：

- HTTPSを使用するために、信頼される証明書が構成され使用されます。

Directorの通信

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、SSL (Secure Sockets Layer) および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。

DirectorとXenApp/XenDesktopサーバー間のデータトラフィックを保護するには、TLS Relayを使用します。詳しくは、「[Securing Citrix Director: OData Interface through TLS](#)」のブログの記事を参照してください。

Directorとユーザーデバイスの間の通信は、NetScaler GatewayおよびHTTPSで保護することをお勧めします。DirectorでHTTPSを使用するには、認証サービスを提供するMicrosoftインターネットインフォメーションサービス (IIS) インスタンスでHTTPSを構成する必要があります。IISが適切に構成されていない場合、Directorの通信にHTTPが使用されます。実稼働環境では、Directorへのすべてのユーザー接続が保護されるようにしてください。

Directorのセキュリティ境界による分離

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展開環境全体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異なるWebドメインにDirectorを展開することをお勧めします。

XenDesktop 7よりも前のVDAに対する権限の構成

Jul 07, 2016

ユーザーデバイス上にXenDesktop 7よりも前のバージョンのVDAがインストールされている場合、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他のユーザー) 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。たとえば、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、このサービス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するだけです。

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

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：
 - Performance Monitor Users
 - Event Log Readers

これらの権限を自動的に付与するには、インストールメディアのx86\Virtual Desktop Agentおよびx64\Virtual Desktop Agentフォルダーおよび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`

HDX Insightの構成

Jul 07, 2016

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。

HDX Insightにより、ネットワーク分析およびパフォーマンス管理機能がDirectorに統合されます。

- ネットワーク分析機能では、HDX Insight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。これにより、環境内のICAトラフィックをDirectorで詳細に分析できます。
- 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により以下の追加情報がDirectorに提供されます。

- [傾向] ページには、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。
- [ユーザーの詳細] 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。

Director上でネットワーク分析機能を構成するには

Directorでは、NetScaler HDX Insightによるネットワーク分析が実行されます。これにより、Citrixアプリケーションおよびデスクトップの管理者は、ネットワークパフォーマンスを低下させる問題のトラブルシューティングおよび関連付けを行います。

NetScaler Insight CenterをインストールしてDirectorで構成し、ネットワーク分析を有効にする必要があります。NetScaler Insight Centerは、Citrix.comからダウンロード可能な仮想マシン（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。この情報に基づいて、HDX InsightはクライアントとバックエンドのCitrix-インフラストラクチャ間のICAプロトコルの高精度な分析機能を提供します。

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）を構成します。
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。

ユーザーの問題のトラブルシューティング

Jul 07, 2016

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。
- 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	参照先
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
接続できない	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
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。

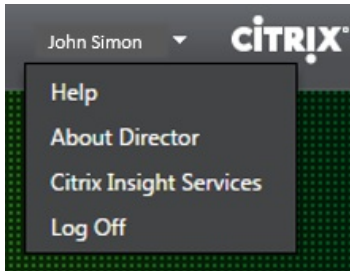
検索結果には、現在マシンを使用していないユーザーや、マシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 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 Diagnosis Facility (CDF) トレースをキャプチャします。Scoutは、Citrix Insight Services (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。

ユーザーのシャドウ

Jul 07, 2016

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Microsoft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。

ユーザーへのメッセージの送信

Jul 07, 2016

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。

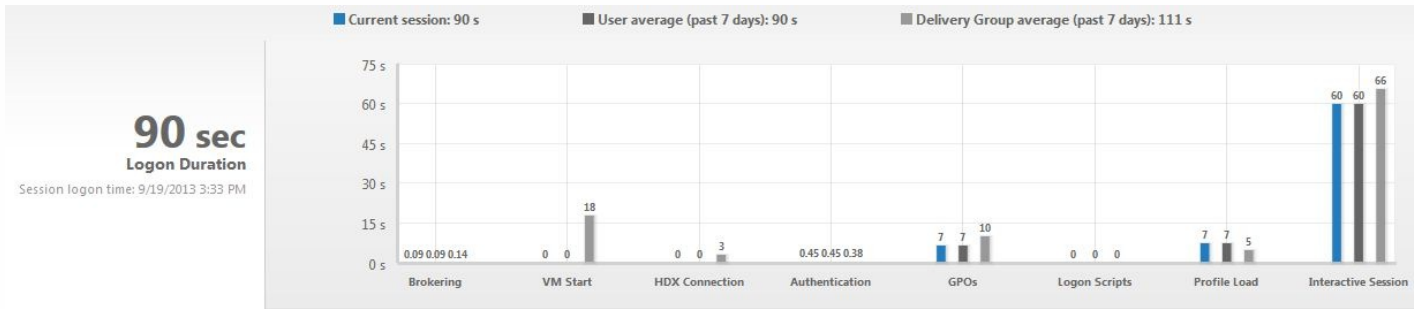
メッセージが正しく送信されると、Directorに確認メッセージが表示されます。マシンに接続しているユーザーにメッセージが表示されます。

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。

ユーザーログオンの問題の診断

Jul 15, 2016

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。

- [ユーザーの詳細] ビューで、[ログオン処理時間] パネルを使用してログオン状態のトラブルシューティングを行います。
 - 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。
- 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。
Authentication	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

	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場合があります。

注意

〔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設計されています。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。
- 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。

アプリケーションエラーの解決

Jul 07, 2016

「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。

操作	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	パッチまたはその他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て、担当の管理者に問題を報告します。「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。

デスクトップ接続の復元

Jul 07, 2016

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。

操作	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。

セッションの復元

Jul 07, 2016

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。

操作	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Virtual Delivery Agent (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。

HDXチャネルシステムレポートの生成

Jul 07, 2016

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。

Personal vDiskのリセット

Jul 07, 2016

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。

ユーザープロファイルのリセット

Jul 07, 2016

注意：プロファイルのリセットすると、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、プロファイルの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ただければなりません。

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。

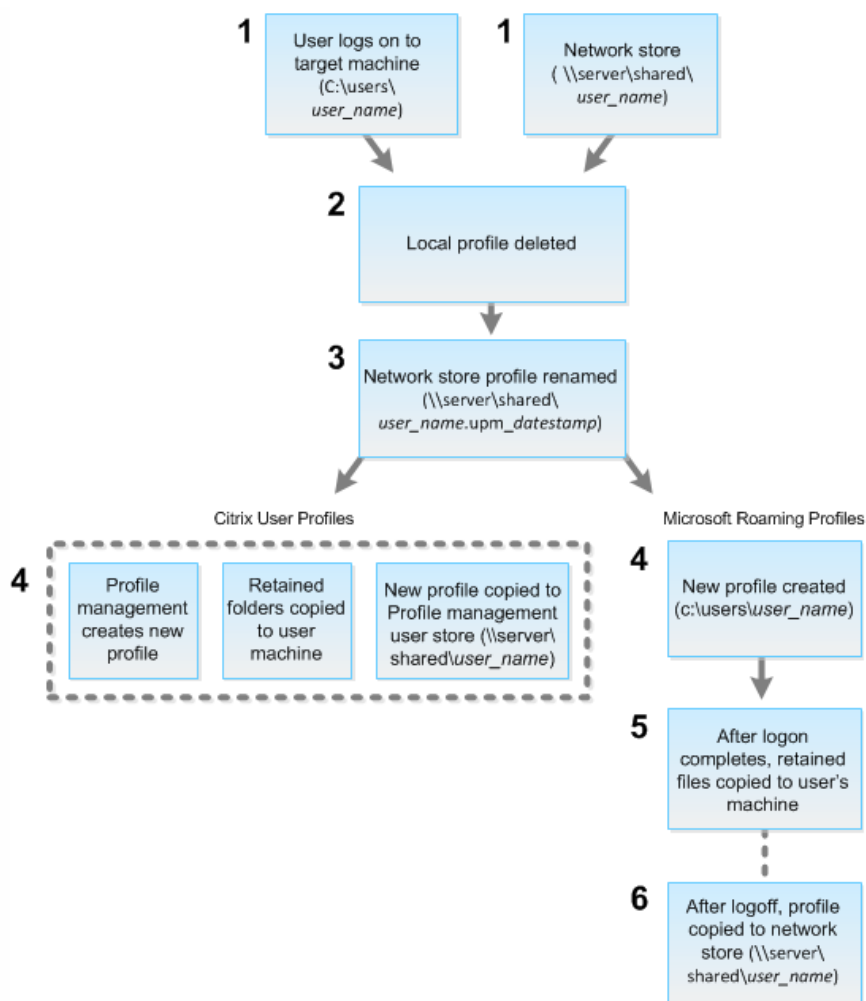
ユーザーのプロファイルのフォルダーやファイルが保存され、新しいプロファイルにコピーされます。これらのフォルダーは、以下の順番でコピーされます。

- Desktop
- 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。

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。

次にユーザーがログオンしたときに、下図の処理が実行されます。



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、ユーザーのログオンが通常どおりに処理されます。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。

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。

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、拡張子として日時が含まれます (.upm_)。
4. 現在のプロファイルのフォルダー（拡張子upm_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。

SDKおよびAPI

Aug 26, 2016

このリリースでは、複数のSDKおよびAPIを使用できます。

XenAppおよびXenDesktop SDK : XenAppおよびXenDesktop SDKは、多くのMicrosoft Windows PowerShell Version 3.0スナップインに基づいています。これにより、Citrix Studioと同じタスクだけでなく、Studioでサポートされないタスクを実行できます。

詳しくは、[Citrix Developer](#)を参照してください。

CitrixグループポリシーSDK : Citrixグループポリシー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、後述の「[グループポリシーSDK](#)」セクションを参照してください。

Monitor Service OData API : Monitor Service OData APIを使用して、以下を実行できます。

- 将来の計画のために履歴傾向を分析する。
- 接続やマシンの障害に対する詳細なトラブルシューティングを実行する。
- ほかのツールおよびプロセスに情報をインポートする（Microsoft ExcelのPowerPivotテーブルを使って別の方法でデータを表示するなど）。
- APIで提供されるデータ上にカスタムユーザーインターフェイスを構築する。

詳しくは、「[Monitor Service OData API](#)」を参照してください。

XenAppおよびXenDesktop SDK

Version 7.x以降、XenAppとXenDesktopでは「FlexCast Management Architecture」と呼ばれる共通の統合アーキテクチャが使用されています。これにより、従来XenDesktopでのみ提供されていた多くの機能がXenAppでも提供されるようになりました。このため、これらの機能に関するSDK要素は、XenDesktopについてのみ説明されていても、XenAppとXenDesktopの両方に適用されます。

XenDesktop 5 SDKを使い慣れている場合、XenAppおよびXenDesktop SDKの7.xバージョンとの主な違いは以下の一覧のとおりです。

- **新しい高レベルのSDK** — XenDesktop 7 SDKでは、サイトの作成や管理を自動化するためのスクリプトを簡単に作成できます。高レベルのSDKにより、複雑な低レベルSDKを使用しなくても、たとえば2つのコマンドレットを実行するだけで新しいサイトを作成できます。
- **新しい低レベルSDK** — XenDesktop 5のBroker SDKに含まれていた、Delegated Administration Service (DAS) 用に拡張されたSDKなど、個々の低レベルSDKが新しいXenDesktop 7サービス用に提供されています。また、Monitor Service、環境テスト、構成ログなどの新しい機能用のSDKもあります。
- **WindowsサーバーOSマシンカタログおよびデリバリーグループ** -XenDesktop 7 SDKを使って、サーバーOS上でホストされるコスト効率の良いアプリケーションやデスクトップを配信できます。
- **デスクトップOSマシンアプリケーション** — デスクトップOSマシンアプリケーションは、SDKレベルで大幅に変更されて

います。デスクトップOS上でアプリケーションを実行する既存のスクリプトを使用している場合は、後方互換性がほとんどないため、そのスクリプトをXenDesktop 7用に更新する必要があります。

- **デリバリーグループのマシンに対する設定の適用** — XenDesktop 7では、構成スロットを使用して、サイト内のすべてのマシンにではなく、特定のデリバリーグループのマシンに設定を適用できます。これにより、各デリバリーグループに異なる設定を適用できます。ReceiverやApp-V公開サーバーで使用するStoreFrontアドレスの設定など、さまざまな種類の設定を含む多くの定義済み構成スロットが提供されます。スロットの一連の設定を特定のデリバリーグループに適用して、別の設定セットを別のデリバリーグループに適用することができます。これらの設定セットには、「営業部ポリシー」など、わかりやすい名前を付けることができます。

- **カタログの種類の置き換え** — XenDesktop 7では、カタログの種類が個々のプロパティを持つカタログに置き換えられています。後方互換性のため、single image（プール）やthin clone（専用）などのカタログの種類を使用した既存のスクリプトも引き続きサポートされますが、内部的にはこれらはプロパティのセットに変換されます。

注意：XenDesktop 5のカタログの種類との後方互換性は、可能な限り保持されています。ただし、新しいスクリプトを作成する場合はカタログの種類を使用せずに、個々のプロパティを備えたカタログを指定してください。

- **Desktopオブジェクトの置き換え** — XenDesktop 5のBroker SDKスクリプトで使用される主なSDKオブジェクトの1つとして、Desktopオブジェクトがありました。Desktopオブジェクトを使用して、マシン、およびマシン上のセッションの両方を参照できます。XenDesktop 7では、このオブジェクトはSessionオブジェクトとMachineオブジェクトに置き換えられています。どちらもDesktopオブジェクトと同じように動作するよう拡張されています。ただし後方互換性のため、Desktopオブジェクトを使用した既存のスクリプトを引き続きサポートされます。

注意：XenDesktop 5との後方互換性は、可能な限り保持されています。ただし、新しいスクリプトを作成する場合はDesktopオブジェクトを使用せずに、SessionオブジェクトとMachineオブジェクトを指定してください。

SDKとStudioでは、ポリシー規則の扱い方に違いがあります。SDKでは、ポリシー規則の entitlement（EntitlementPolicyRule）およびassignment（AssignmentPolicyRule）はそれぞれ独立したエンティティです。Studioでは、これらのエンティティはデリバリーグループ内に統合されているため表示されません。また、SDKでのaccess（AccessPolicyRule）による制限は、Studioよりも緩いものになっています。

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 3.0のシェルを開きます。Studioを開き、[PowerShell] タブを選択し、[PowerShellを起動] 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表示するには：

1. PowerShellコンソールからCitrixスナップインを追加します。Add-PSSnapin Citrix.*.Admin.V*。
2. 『[PowerShell Integrated Scripting Environment \(ISE\)](#)』の説明に従います。

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、コマンドhelp New-PSDrive -path localgpo:/を実行します）。

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 <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string> 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。

Monitor Service OData API

Jul 07, 2016

管理者は、Citrix Directorのコンソールで表示した履歴データを、Monitor ServiceのAPIを使って照会できます。このAPIを使用すると、次の操作を行えます。

- 将来の計画のために履歴傾向を分析する。
- 接続やマシンの障害に対する詳細なトラブルシューティングを実行する。
- ほかのツールおよびプロセスに情報をインポートする（Microsoft ExcelのPowerPivotテーブルを使って別の方法でデータを表示するなど）。
- APIで提供されるデータ上にカスタムユーザーインターフェイスを構築する。

Monitor Service APIではOpen Data（OData）プロトコルが使用されます。これはデータを照会および更新するためのWebプロトコルで、HTTPなどのWebテクノロジーに基づいています。ODataプロトコルについて詳しくは、<http://www.odata.org>を参照してください。

Monitor Service APIは、処理および統合時に読み込まれるWindows Communication Foundation（WCF）Data Servicesを使用して、SQL Serverデータベース上に構築されます。WCFを使用して2つのエンドポイントがwsHttpBindingで公開されます。ベースアドレスは「<http://{dc-host}/Citrix/Monitor/OData/v2>」です。また、TLSを使ってエンドポイントを保護することもできます。詳しくは、「[TLSを使ったエンドポイントのセキュリティ保護](#)」を参照してください。

1. Dataエンドポイントは、データベースエンティティへの直接読み取り専用アクセスを公開し、ODataクエリ言語を使用してアクセスすることができます。このエンドポイントは、フィルタリングおよび列の選択により高度に柔軟なアクセスを実行できます。Data APIのURIは「<http://{dc-host}/Citrix/Monitor/OData/v2/Data>」です。Monitor Serviceデータへのアクセスについて詳しくは、「[APIを使ったデータアクセス](#)」を参照してください。
2. Methodsエンドポイントは、[ダッシュボード] ページや [傾向] ページでの照会など、Citrix Directorで複雑なグループ化や高性能な標準を必要とするデータを取得するためのサービス操作を公開します。Methods APIのURIは「<http://{dc-host}/Citrix/Monitor/OData/v2/Methods>」です。MethodsはDirectorでのみ使用され、通常Citrix製品の管理者やユーザーが使用することはありません。したがって、ここでは説明しません。

XenApp/XenDesktop 7.6に付属のAPIにより、以下の新機能が提供されます。

- **Hotfixインベントリ**。Directorの [ユーザーの詳細] ビューまたは [マシン] ビューを使用すると、マシンにインストールされているCitrix Hotfixの一覧を表示できます。このAPIを使用すると、このデータを抽出してカスタムレポート（サイト全体でインストールされているHotfixの状態など）を作成したり、分析エンジンに取り込んだりできます。いくつかのクラスが追加され、MachineクラスにControllerやVDAにインストールされたCitrix Hotfixの追跡機能が追加されました。
- **匿名セッションのトラブルシューティング**。プールされたローカルユーザーアカウントのセットを使用してセッションを実行できます。このAPIでは、Sessionクラスに新しいIsAnonymousプロパティ（デフォルト値：FALSE）が追加されています。
- **ホストされるアプリケーションの使用量レポート**。Directorでは、ホストされるアプリケーションの経時的な使用状況を示すキャパシティレポートが提供されます。このAPIを使用すると、ユーザーセッションで実行されている各アプリケーションインスタンスの詳細をレポートできます。

このAPIの新機能について詳しくは、<http://support.citrix.com/help/monitorserviceapi/7.6/>のAPIリファレンスを参照してください。

GetSessionSummaryメソッドは、このリリースでは廃止されました。

APIを使ったデータアクセス

Jul 07, 2016

以下の種類のデータは、Monitor Service APIを介して使用できます。

- 接続エラーに関するデータ
- エラー状態のマシン
- セッションの使用
- ログオン処理時間
- 負荷分散データ
- マシンに適用されたHotfix
- ホストされたアプリケーションの使用

データオブジェクトの説明について詳しくは、<http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/>を参照してください。

Monitor Service OData APIを使用するには、XenAppまたはXenDesktopの管理者である必要があります。APIを呼び出すには、読み取り専用の特権が必要です。ただし、返されるデータは、その管理者の役割と権限によって異なる場合があります。たとえば、デリバリーグループ管理者はMonitor Service APIを呼び出すことができますが、取得可能なデータはCitrix Studioでセットアップされるデリバリーグループアクセスにより制御されます。XenApp/XenDesktop管理者の役割と権限について詳しくは、「[管理権限の委任](#)」を参照してください。

データのクエリ

Monitor Service APIは、ODataコンシューマーでアクセスできるRESTベースのAPIです。ODataコンシューマーは、ODataプロトコルで公開されたデータを消費するアプリケーションを指します。シンプルなWebブラウザからODataプロトコルのすべての機能を実行できるカスタムアプリケーションまでさまざまなODataコンシューマーがあります。ODataコンシューマーについて詳しくは、<http://www.odata.org/ecosystem#consumers>を参照してください（英文）。

Monitor Serviceデータモデルのすべての部分はアクセス可能で、URL上でフィルタリングできます。ODataでは、URL形式のクエリ言語を使用してサービスからエントリを抽出できます。詳しくは、<http://msdn.microsoft.com/ja-jp/library/ff478141.aspx>を参照してください。

クエリはサーバー側で処理され、クライアント側でODataプロトコルを使ってさらに詳細にフィルタリングできます。

取得されるデータは、集計データ（サマリーテーブル）、オブジェクト（マシン、セッションなど）の現在の状態、およびログデータ（接続イベントなどの履歴）の3つのカテゴリに分類されます。

注：ODataプロトコルでは列挙（enum）はサポートされず、整数（integer）が使用されます。Monitor Service OData APIによって返される値については、<http://support.citrix.com/help/monitorserviceapi/7.6/>を参照してください。

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）やマシン障害（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。
- ログオン処理時間（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する必要があります。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、およびその他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の長さの長さを示します。
- **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。

- $0 < T \leq 1$ 時間の場合は分単位の粒度
- $0 < T \leq 30$ 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以外のエディションでは、8日目からクリーンアップが開始されます。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。

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 (日数)	アクセス方法
GroomSessionsRetentionDays	Sessionレコードおよび SessionDetailレコード	非 Platinum ユーザーは7 日、 Platinum ユーザーは 90日	コマンドレット (set/get- monitorconfiguration)
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）	非 Platinum ユーザーは7 日、 Platinum ユーザーは 90日	コマンドレット (set/get- monitorconfiguration)
GroomHourlyRetentionDays	集計データ（時間単位）	32日	Monitor.Configuration Database Table。下記 注を参照
GroomMinuteRetentionDays	集計データ（分単位）	3日	Monitor.Configuration Database Table。下記 注を参照
GroomFailuresRetentionDays	MachineFailureLogレコードおよび ConnectionFailureLogレコード	非 Platinum ユーザーは7 日、 Platinum ユーザーは 90日	コマンドレット (set/get- monitorconfiguration)

設定名	対象データ	デフォルト値 (目数)	アクセス方法
GroomLoadIndexesRetentionDays	LoadIndexレコード	Platinum ユーザーは7日、Platinumユーザーは90日	(set/get-monitorconfiguration)
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る	非Platinumユーザーは7日、Platinumユーザーは90日	コマンドレット (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	VDAマシンおよびControllerマシンに適用されたHotfix	非PlatinumユーザーおよびPlatinumユーザーの両方で90日	コマンドレット (set/get-monitorconfiguration)

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。

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。

TLSを使ったエンドポイントのセキュリティ保護

Jul 07, 2016

ここでは、Monitor Service OData APIエンドポイントを保護するためのTLSの使用方法について説明します。TLSを使用する場合、サイトのすべてのDelivery Controller上でTLSを構成する必要があります。TLSを構成したControllerと構成していないControllerを混在させることはできません。

Monitor ServiceエンドポイントをTLSで保護するには、以下の構成を行います。このための手順には、各サイトで1回のみ必要なものと、サイト内でMonitor Serviceをホストするすべてのマシン上で行うものがあります。次の手順に従います。

パート1：システムへの証明書の登録

- 信頼された証明書マネージャーを使用して証明書を作成します。証明書は、OData TLSで使用するマシン上のポートに関連付ける必要があります。
 - Monitor ServiceのTLS通信用のポートとしてこのポートを構成します。このための手順は、使用している環境とこれが証明書でどのように機能するかにより異なります。次の例では、ポート449を構成しています。
- 証明書をポートに関連付けます。
`netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9appid='{00000000-0000-0000-0000-000000000000}'`
ヒント：PowerShellのコマンドウィンドウでは、上記のようにappIdのGUIDを一重引用符で囲む必要があります。一重引用符で囲まないと、コマンドが正しく動作しません。この例では、コマンドを読みやすくするために改行が追加されています。

パート2：Monitor Service構成設定の変更

- サイト内の任意のDelivery Controller上で、次のPowerShellコマンドを1回実行します。これにより、Monitor ServiceがConfiguration Serviceから登録解除されます。
`asnp citrix.* $serviceGroup = get-configregisteredinstance -servicetype Monitor | Select -First 1 ServiceGroupUid remove-configservicegroup -ServiceGroupUid $serviceGroup.ServiceGroupU`
- サイト内のすべてのController上で、以下の操作を行います。
 - cmdプロンプトを開き、Citrix Monitorフォルダー（通常C:\Program Files\Citrix\Monitor\Service）に移動します。次のコマンドを実行します。
`Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl`
 - 次のPowerShellコマンドを実行します。
`asnp citrix.* (if not already run within this window) get-MonitorServiceInstance | register-ConfigServiceInstance Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGro`

例

Jul 07, 2016

ここでは、OData APIを使用してMonitor Serviceデータをエクスポートする方法について例を挙げて説明します。

例1 - Raw XML

1. XenApp/XenDesktopサイトに対する適切な管理権限で実行しているWebブラウザで、各データセットのURLを開きます。Advanced Rest ClientアプリをインストールしたChromeブラウザの使用を推奨します。
2. ソースを表示します。

例2 - ExcelとPowerPivot

以下の手順は、Microsoft ExcelおよびPowerPivotがインストール済みであることを前提としています。

Excelを開きます（XenApp/XenDesktopサイトの適切な管理権限で実行します）。

Excel 2010では以下の操作を行います。

1. [PowerPivot] タブをクリックします。
2. [PowerPivotウィンドウ] をクリックします。
3. リボンの [データフィードから] をクリックします。
4. 接続の表示名としてわかりやすい名前（XenDesktop Monitoring Dataなど）を選択し、データフィードURLとして「<http://{dc-host}/Citrix/Monitor/OData/v2/Data>」（TLSを使用している場合は「https:~」）を入力します。
5. [次へ] をクリックします。
6. Excelにインポートするテーブルを選択し、[完了] をクリックします。データが取得されます。
7. これでPowerPivotのピボットテーブルやピボットグラフを使ってデータを表示および分析できるようになりました。詳細については、Learning Center (<http://www.microsoft.com/en-us/bi/LearningCenter.aspx>) を参照してください

Excel 2013では以下の操作を行います。

1. [データ] タブをクリックします。
2. [その他のソース]、[ODataデータフィード] の順に選択します。
3. データフィードURLとして「<http://{dc-host}/Citrix/Monitor/OData/v1/Data>」（TLSを使用している場合は「https:~」）を入力し、[次へ] をクリックします。
4. Excelにインポートするテーブルを選択し、[次へ] をクリックします。
5. デフォルトの名前を使用するか変更して、[完了] をクリックします。
6. [接続のみ] または [ピボットレポート] を選択します。データが取得されます。
7. これでPowerPivotのピボットテーブルやピボットグラフを使ってデータを表示および分析できるようになりました。詳細については、Learning Center (<http://www.microsoft.com/en-us/bi/LearningCenter.aspx>) を参照してください

例3 - LINQPad

以下の手順は、LINQPadがインストール済みであることを前提としています。

1. XenApp/XenDesktopサイトの適切な管理権限でLinqPadを実行します。
ヒント：Delivery Controllerの上でダウンロード、インストール、および実行すると簡単です。
2. Add接続リンクをクリックします。
3. WCF Data Services 5.1 (OData 3) を選択し、[Next] をクリックします。
4. データフィードURLとして「<http://{dc-host}/Citrix/Monitor/OData/v2/Data>」（TLSを使用している場合は「https:

～」)を入力します。必要な場合は、Delivery Controllerにアクセスするためのユーザー名とパスワードを入力します。
[OK] をクリックします。

5. これで、データフィードに対してLINQクエリを実行し、必要なデータをエクスポートできるようになりました。たとえば、カタログを右クリックして、[Catalogs.Take(100)] を選択します。これにより、データベースの最初の100のカタログが取得されます。[Export]、[Export to Excel with formatting] の順に選択します。

APIでLINQPadを使用する方法に関する事例については、<http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/>を参照してください。