XenApp and XenDesktop 7.15 LTSR

Contents

新機能

August 24, 2021

このリリースについて

累積更新プログラム 8（CU8） について

累積更新プログラム 7（CU7） について

累積更新プログラム 6（CU6） について

累積更新プログラム 5（CU5） について

累積更新プログラム 4（CU4） について

累積更新プログラム 3（CU3） について

累積更新プログラム 2（CU2）について

累積更新プログラム 1（CU1）について

7.15 LTSR（初期リリース）について

累積更新プログラム **8**（**CU8**）

September 16, 2021

リリース日：2021 年 8 月 11 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 8（CU8）では、7.15 LTSR CU7 リリース以降に報告された 40 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU7 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU8 をダウンロード

> 重要:
>
> このリリースでは、StoreFront のインストールおよびアップグレード方法が変更されています。以前のリリースでは、全製品インストーラーのメインページで ［はじめに］タイルをクリックすると、［コアコンポーネント］ページには StoreFront が含まれていました。StoreFront とその他のコアコンポーネントを選択して、同じマシンにインストールできます。
>
> このリリースでは、［コアコンポーネント］ページに StoreFront チェックボックスは含まれなくなりました。StoreFront をインストールまたはアップグレードするには、メインページの ［拡張展開］で ［**Citrix StoreFront**］をクリックします。これによって、インストールメディアから`CitrixStoreFront-x64.exe`が起動されます。
>
> `XenDesktopServerSetup.exe`コマンドでは、`/components storefront`を指定することができなくなりました。指定しようとすると、コマンドは失敗します。コマンドラインで StoreFront をインストールするには、Citrix Virtual Apps and Desktops インストールメディアの`x64`フォルダーから`CitrixStoreFront-x64.exe`を実行します。
>
> 重要:
>
> Citrix ライセンス管理コンソールは製品終了となり、ライセンスサーバー 11.16.3.0 ビルド 30000 でのサポートが終了しました。Citrix Licensing Managerを使用します。

新しい展開環境

新しく CU8 を展開するには

CU8 メタインストーラーを使用して、CU8 に基づく新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU8 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべての LTSR コンポーネントを CU8 に更新することをお勧めします。例：Citrix Provisioning が LTSR 展開環境に含まれる場合、Citrix Provisioning コンポーネントを CU8 に更新します。Citrix Provisioning が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU8** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.8000	
VDA for Server OS	7.15.8000	
Citrix Studio	7.15.8000	
Citrix Director	7.15.8000	
Delivery Controller	7.15.8000	
Citrix フェデレーション認証サービス	7.15.8000	
Citrix グループポリシー管理	3.1.8000	
Citrix グループポリシークライアント側拡張	3.1.8000	
Linux VDA	7.15.6000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.8000	
Provisioning Services	7.15.39	
Session Recording	7.15.8000	Premium Edition のみ
StoreFront	3.12.8000	
ユニバーサルプリントサーバー	7.15.8000	

Citrix XenApp および **XenDesktop 7.15 LTSR CU8** の互換性のあるコンポーネント

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

7.15 LTSR CU8 と互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	2011
* ブラウザーコンテンツのリダイレクト	15.19.2000
ライセンスサーバー用 Citrix SCOM Management Pack	1.2

7.15 LTSR CU8 と互換性のあるコンポーネントおよびプラットフォーム	バージョン
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.3000
ライセンスサーバー	11.16.6.0 ビルド 33000
セルフサービスパスワードリセット	1.1.20.0
Workspace Environment Management	2012

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU8 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーションと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU8 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します：

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU8 インストーラーを実行します。これにより、新しいサイトで使用する新しい Virtual Delivery Agent for Server OS に自動アップグレードされます。

- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。
- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU8 サイトにインポートできます：一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU8 Controller 上で PowerShell インポートコマンドレットを実行して、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

October 22, 2021

Citrix Director

- Citrix Director が誤ったユーザーセッション数を表示することがあります。[CVADHELP-14849]

Citrix ポリシー

- ［ポリシー］**>**［割り当て先］タブには、1 つまたは複数のデリバリーグループに割り当てた Citrix ポリシーが誤って表示される場合があります。たとえば、2 つのデリバリーグループに 1 つのポリシーを割り当て、そのうちの 1 つの割り当てだけを有効にします。［割り当て先］タブに移動すると、両方のデリバリーグループが表示されます。ポリシーを無効にすると、割り当てが解除されます。ただし ［割り当て先］タブには、引き続きポリシーが割り当てられていると表示されます。[CVADHELP-15233]
- Citrix Cloud 環境でポリシーを作成し、ドメイン A の組織単位を使用してフィルターする場合に、ドメイン B のユーザーがログオンできないことがあります。この問題は、公開された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きに発生します。[[CVADHELP-17179]

Citrix Studio

- この修正により、承認された StoreFront サーバーおよび Citrix Gateway サーバーのみが Delivery Controller と通信できるようになり、セキュリティが向上します。詳しくは、「セキュリティキー」を参照してください。[CVADHELP-15729]
- 既存のカタログから仮想マシンを追加または削除しようとすると失敗することがあります。[CVADHELP-17316]

Delivery Controller

- この修正により、承認された StoreFront サーバーおよび Citrix Gateway サーバーのみが Delivery Controller と通信できるようになり、セキュリティが向上します。詳しくは、「セキュリティキー」を参照してください。[CVADHELP-15729]
- AWS ホスト接続に関連付けられているマシンまたはカタログを削除すると、EBS ルートデバイスが自動的に削除されない場合があります。この問題は、マシンカタログ作成中にこれらのカタログ用に作成されたディスクで基本イメージの **DeleteOnTermination** フラグが`$true`から`$false`に変化するため発生します。[CVADHELP-16096]
- Citrix Broker Service（Brokerservice.exe）が応答しなくなり、オフラインになることがあります。[CVADHELP-16352]
- XenApp および XenDesktop 7.15 CU6 を Citrix Virtual Apps and Desktops 1912 LTSR CU2 にアップグレードした後、データベースの更新時に問題が発生することがあります。この問題は、**AdminAccountName/AdminUpn** エントリが 64 文字を超えているときに発生します。[CVADHELP-17379]
- 更新されたマスターイメージが VDA に昇格されていない場合、&や`$`などの特殊文字を含む名前でカタログを更新しようとすると失敗することがあります。[CVADHELP-17686]
- マルチサイト集計機能が構成され、資格ポリシー規則で「SessionReconnection」プロパティが **SameEndPointOnly** に設定されている場合、アクティブなセッションに再接続する代わりに、新しいセッションが起動されることがあります。[CVADHELP-17692]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU8 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Profile Management

- Windows のユーザー資格情報は、Credential Manager から削除された後も残る場合があります。[CVADHELP-16083]
- ［除外されたファイルまたはフォルダーを削除］を有効にする前に［ログオン時の除外チェック］ポリシー経由で作成され、［除外の一覧 - ディレクトリ］または［デフォルトの除外一覧の有効化 - ディレクトリ］ポリシーで除外されたフォルダーは、削除されません。[CVADHELP-16439]
- ［大きなファイルの処理 **-** シンボリックリンクとして作成されるファイル］ポリシー設定で作成された新しいファイルは、ログオフ中に同期しないことがあります。[CVADHELP-16526]
- Citrix Profile Management がインストールされていると、リダイレクトされたフォルダーがローカルユーザープロファイルの下に再作成される場合があります。[CVADHELP-16861]

- この修正により、Citrix Profile Management WMI Plugin インストーラーのセキュリティの脆弱性が解決されます。詳しくは、Knowledge Center の記事CTX319750を参照してください。[CVADHELP-17728]
- この修正により、Citrix Profile Management インストーラーのセキュリティの脆弱性が解決されます。詳しくは、Knowledge Center の記事CTX319750を参照してください。[CVADHELP-17939]

Provisioning Services

Provisioning Services 7.15 LTSR CU8ドキュメントは、このリリースの更新に関する特定の情報を提供します。

StoreFront

- この修正により、承認された StoreFront サーバーおよび Citrix Gateway サーバーのみが Delivery Controller と通信できるようになり、セキュリティが向上します。詳しくは、「セキュリティキー」を参照してください。[CVADHELP-15729]
- ソケットプールが有効な状態で StoreFront にログオンしようとすると、次のエラーメッセージが表示されて失敗する場合があります:

  要求を完了できません

  この問題は、TCP 動的ポートを使い果たしている場合に発生します。

  [CVADHELP-16625]
- マルチサイト集計機能が構成され、資格ポリシー規則で **SessionReconnection** プロパティが **SameEndPointOnly** に設定されている場合、アクティブなセッションに再接続する代わりに、新しいセッションが起動されることがあります。[CVADHELP-16698]
- StoreFront をバージョン 7.15 LTSR CU4 からアップグレードした後、同じホスト名の VDI デスクトップがシリアル順ではなくランダムな順序で表示される場合があります。[CVADHELP-16723]
- Citrix StoreFront サービス API を使用してユーザーセッションを起動しようとすると、起動リクエストに渡されるパラメーターが正しくないことがあります。[CVADHELP-16834]

ユニバーサルプリントサーバー

サーバー

- ユニバーサルプリントサーバー（UPServer.exe）が予期せず終了することがあります。この問題は、prntvpt.dll モジュールに障害がある場合に発生します。[CVADHELP-12651]

User Profile Management VDA

- セッションにログオンすると、ユーザーデータが予期せず削除されることがあります。この問題は、Citrix のフォルダーリダイレクトパスポリシー設定（デスクトップパス設定など）でファイルサーバーのアドレスを

path1 から path2 に変更すると発生します。ただし、path1 と path2 は同じ物理的な場所を指します。この問題を回避するには、Microsoft グループポリシー設定［フォルダーリダイレクトの前に古いターゲットと新しいターゲットが同じ共有を指すことを確認する］を有効にします。詳しくは、Citrix フォルダーリダイレクトパスポリシー設定の「説明」の部分を参照してください。[CVADHELP-12439]

VDA for Desktop OS

印刷

- Chrome 向け Citrix Workspace アプリ経由で起動されたセッションから PDF ファイルを印刷しようとすると、失敗する場合があります。[CVADHELP-15318]
- リモート PC アクセス VDA を使用して Mac 向け Citrix Workspace アプリ経由で印刷する場合、プリンター設定が無視される場合があります。[CVADHELP-15320]
- Citrix ユニバーサルプリンタードライバー（UPD）を使用してファイルを印刷しようとすると、印刷されたファイルに誤った画像が表示される場合があります。この問題は、VDA をバージョン 7.15.5000 からバージョン 1912.1000 にアップグレードし、ヘビーウェイト圧縮を有効にした場合に発生します。[CVADHELP-15813]

セッション/接続

- Windows 向け Citrix Workspace アプリでセッションを記録すると、マウスポインターの動きが記録されないことがあります。この問題は、VDA バージョン 7.15.400 で発生します。[CVADHELP-13300]
- タスクバープレビューを使用してウィンドウに切り替えようとすると、そのウィンドウを開くのに時間がかかる場合があります。[CVADHELP-15422]
- 更新プログラム KB4586853 が適用された Microsoft Windows 10 20H2 で一般的な IME を使用すると、アプリケーションが予期せず終了する場合があります。[CVADHELP-16664]
- この修正により、高度なキーボード設定で使用可能なアプリケーションウィンドウごとに異なる入力方法を設定できるようになりました。[CVADHELP-16731]
- 特定のサードパーティアプリケーションを使用している場合、アプリケーションが別のウィンドウを開いたときに黒い画面が表示されることがあります。[CVADHELP-16956]

システムの例外

- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x93（INVALID_KERNEL_HANDLE）によるブルースクリーンが表示されることがあります。[CVADHELP-15326]
- 直接アクセス VPN トンネルを介して OU ベースの Controller 検出を実行すると、Citrix Desktop Service（BrokerAgent.exe）が多数の ID 1010 イベントを生成することがあります。[CVADHELP-16754]
- Citrix Desktop Service （BrokerAgent.exe）でアクセス違反が発生して、予期せず終了することがあります。[CVADHELP-17055]

ユーザーエクスペリエンス

- Explorer を使用すると、画面に黒いパッチが表示されることがあります。この問題は、特定の AMD GPU モデルを使用してエンドポイントに接続した場合に発生します。

  この修正を有効にするには、以下のレジストリキーを設定します:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  名前：MinTransientWidth

  種類：DWORD

  値：00000021

  [CVADHELP-17057]

VDA for Server OS

印刷

- Chrome 向け Citrix Workspace アプリ経由で起動されたセッションから PDF ファイルを印刷しようとすると、失敗する場合があります。[CVADHELP-15318]
- リモート PC アクセス VDA を使用して Mac 向け Citrix Workspace アプリ経由で印刷する場合、プリンター設定が無視される場合があります。[CVADHELP-15320]
- Citrix ユニバーサルプリンタードライバー（UPD）を使用してファイルを印刷しようとすると、印刷されたファイルに誤った画像が表示される場合があります。この問題は、VDA をバージョン 7.15.5000 からバージョン 1912.1000 にアップグレードし、ヘビーウェイト圧縮を有効にした場合に発生します。[CVADHELP-15813]

セッション/接続

- Windows 向け Citrix Workspace アプリでセッションを記録すると、マウスポインターの動きが記録されないことがあります。この問題は、VDA バージョン 7.15.400 で発生します。[CVADHELP-13300]
- HTML5 用の Citrix Workspace アプリを介してセッションを起動しようとすると、セッションが全画面モードではなくウィンドウモードで実行されることがあります。この問題は、Windows Server 2012 で実行されている VDA で発生します。[CVADHELP-14865]
- タスクバープレビューを使用してウィンドウに切り替えようとすると、そのウィンドウを開くのに時間がかかる場合があります。[CVADHELP-15422]
- Web カメラがレジストリに追加されない場合があります。シトリックスセッション内で、これにより他のアプリケーションが Web カメラを認識できなくなることがあります。

  次のレジストリキーを設定して、ユーザーが **WebcamArrivalEvent** の待機時間を調整できるようにします:

  - 32 ビットシステムの場合：

    HEKY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

    名前：RetryNumToWaitWebcamArrival

    種類：DWORD

    値：デフォルトでは、レジストリは存在しません。レジストリが存在しないか読み取られていない場合、デフォルト値の 1000 が使用されます。この値は、デフォルトの待機時間の長さである 20 秒を示します。値が 1000 未満の場合、デフォルト値（1000）が使用されます。

  - 64 ビットシステムの場合：

    HEKY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxRealTime

    名前：RetryNumToWaitWebcamArrival

    種類：DWORD

    値：デフォルトでは、レジストリは存在しません。レジストリが存在しないか読み取られていない場合、デフォルト値の 1000 が使用されます。この値は、デフォルトの待機時間の長さである 20 秒を示します。値が 1000 未満の場合、デフォルト値（1000）が使用されます。

    [CVADHELP-16318]

- この修正により、高度なキーボード設定で使用可能なアプリケーションウィンドウごとに異なる入力方法を設定できるようになりました。[CVADHELP-16731]
- 特定のサードパーティアプリケーションを使用している場合、アプリケーションが別のウィンドウを開いたときに黒い画面が表示されることがあります。[CVADHELP-16956]

システムの例外

- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x93（INVALID_KERNEL_HANDLE）によるブルースクリーンが表示されることがあります。[CVADHELP-15326]
- 直接アクセス VPN トンネルを介して OU ベースの Controller 検出を実行すると、Citrix Desktop Service（BrokerAgent.exe）が多数の ID 1010 イベントを生成することがあります。[CVADHELP-16754]
- Citrix Desktop Service （BrokerAgent.exe）でアクセス違反が発生して、予期せず終了することがあります。[CVADHELP-17055]

ユーザーエクスペリエンス

- Explorer を使用すると、画面に黒いパッチが表示されることがあります。この問題は、特定の AMD GPU モデルを使用してエンドポイントに接続した場合に発生します。

  この修正を有効にするには、以下のレジストリキーを設定します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

名前：MinTransientWidth

種類：DWORD

値：00000021

[CVADHELP-17057]

仮想デスクトップコンポーネント - その他

- App-V アプリケーションの起動に時間がかかる場合があります。[CVADHELP-16732]

累積更新プログラム 7（CU7）

September 16, 2021

リリース日：2021 年 2 月 9 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 7（CU7）では、7.15 LTSR CU6 リリース以降に報告された 60 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU6 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

Download 7.15 LTSR CU7

> 重要：
>
> このリリースでは、StoreFront のインストールおよびアップグレード方法が変更されています。以前のリリースでは、全製品インストーラーのメインページで ［はじめに］タイルをクリックすると、［コアコンポーネント］ページには StoreFront が含まれていました。StoreFront とその他のコアコンポーネントを選択して、同じマシンにインストールできます。
>
> このリリースでは、［コアコンポーネント］ページに StoreFront チェックボックスは含まれなくなりまし

> た。StoreFront をインストールまたはアップグレードするには、メインページの ［拡張展開］で ［**Citrix StoreFront**］をクリックします。これによって、インストールメディアから`CitrixStoreFront-x64.exe`が起動されます。
>
> `XenDesktopServerSetup.exe`コマンドでは、`/components storefront`を指定することができなくなりました。指定しようとすると、コマンドは失敗します。コマンドラインで StoreFront をインストールするには、Citrix Virtual Apps and Desktops インストールメディアの`x64`フォルダーから`CitrixStoreFront-x64.exe`を実行します。
>
> 重要:
>
> Citrix ライセンス管理コンソールは製品終了となり、ライセンスサーバー 11.16.3.0 ビルド 30000 でのサポートが終了しました。Citrix Licensing Managerを使用します。

新しい展開環境

新しく CU7 を展開するには

CU7 メタインストーラーを使用して、CU7 に基づく新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU7 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべての LTSR コンポーネントを CU7 に更新することをお勧めします。例：Citrix Provisioning が LTSR 展開環境に含まれる場合、Citrix Provisioning コンポーネントを CU7 に更新します。Citrix Provisioning が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU7** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.7000	
VDA for Server OS	7.15.7000	
Citrix Studio	7.15.7000	
Citrix Director	7.15.7000	

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
Delivery Controller	7.15.7000	
Citrix フェデレーション認証サービス	7.15.7000	
Citrix グループポリシー管理	3.1.7000	
Citrix グループポリシークライアント側拡張	3.1.7000	
Linux VDA	7.15.6000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.7000	
Provisioning Services	7.15.33	
Session Recording	7.15.7000	Premium Edition のみ
StoreFront	3.12.7000	
ユニバーサルプリントサーバー	7.15.7000	

Citrix XenApp および **XenDesktop 7.15 LTSR CU7** の互換性のあるコンポーネント

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

7.15 LTSR CU7 と互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	2011
* ブラウザーコンテンツのリダイレクト	15.19.2000
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.3000

7.15 LTSR CU7 と互換性のあるコンポーネントおよびプラットフォーム	バージョン
ライセンスサーバー	11.16.6.0 ビルド 33000
セルフサービスパスワードリセット	1.1.20.0
Workspace Environment Management	2012

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU7 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーションと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU7 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します。

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU7 インストーラーを実行します。これにより、新しいサイトで使用する新しい Virtual Delivery Agent for Server OS に自動アップグレードされます。
- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。
- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU7 サイトにインポートできます：一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU7 Controller 上で PowerShell インポートコマンドレットを実行して、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- ネットワーク接続が不十分なシナリオでは、大規模なサイトを含む環境で Citrix Director を使用すると、IIS ワーカープロセス（w3wp.exe）が大量のメモリを消費する場合があります。Citrix Director ページの読み込みが停止します。[CVADHELP-14959]
- VDA をアンインストールした後、Citrix Windows Management Instrumentation（WMI）の名前空間が残る場合があります。[CVADHELP-14965]
- ［マシン使用率の履歴］ページの ［上位 **10** 位のプロセス］テーブルのデータが表示されない場合があります。次のメッセージが表示されます:

  このマシンではプロセスデータ収集が無効になっています。収集を開始するには、プロセス監視ポリシーを有効にしてください。

  [CVADHELP-15893]
- ［**Director**］**>** ［傾向］**>** ［ログオンパフォーマンス］**>** ［レポートのエクスポート］ページでレポートを生成してエクスポートすると、レポートに間違った仲介時間の値が表示されることがあります。この問題は、**.** が **,** に置き換えられるドイツ語のレポートで発生します。[CVADHELP-16097]

Citrix ポリシー

- Citrix Group Policy Engine をバージョン 1.7 からバージョン 7.15 にアップグレードすると、**Citrix** ユーザーポリシーの下のプリンター割り当てポリシーが表示されない場合があります。[CVADHELP-15608]

Citrix Studio

- Azure へのホスト接続を作成しているときに、サービスプリンシパルを作成しようとすると、ADSTS700016 エラーで失敗する場合があります。[CVADHELP-16219]

Delivery Controller

- 公開アプリケーションによっては、アプリケーションの列挙が失敗することがあります。この問題は、.exe ファイルに破損したアプリケーションアイコンが存在する場合に発生します。[CVADHELP-13133]

- 大規模な Citrix Virtual Apps and Desktops 環境では、監視データベースのクリーンアップ用のストアドプロシージャが機能しない場合があります。この問題は、監視データベースのサイズが大きい場合に発生します。[CVADHELP-13287]
- Delivery Controller がイベントログで次のローカルホストキャッシュエラー 505 を受け取ることがあります：不明なエラー。[CVADHELP-14428]
- メモリ使用量が高いことが原因で VDA が負荷限界を報告した後、メモリ使用量が低いレベルまで低下しても、読み込みインデックス値が 10,000 のままになることがあります。[CVADHELP-14563]
- PowerShell を使用して Azure で Machine Creation Services（MCS）カタログを作成しようとすると失敗し、次のエラーメッセージが表示されることがあります：

  パス「**Citrix.AzureRmPlugin.InventoryItemPath**」でアイテムを見つけることができませんでした。

  この問題は、Shared Azure サブスクリプションをスコープが狭いサービスプリンシパルと組み合わせて使用すると発生します。[CVADHELP-14640]
- Citrix Director を使用して新しいセッションにログオンすると、［傾向］にある ［ログオンパフォーマンス］タブの ［平均ログオン処理時間］グラフに、そのログオンが表示されないことがあります。ただし、そのログオンは ［ユーザーセッションごとのログオン処理時間］フォームに表示されます。[CVADHELP-14740]
- vSAN ストレージポリシーが、Machine Creation Services（MCS）を使用して作成された仮想マシンに適用されないことがあります。この問題は、マシンに接続されているディスクのバージョンが正しくない場合に発生します。[CVADHELP-14935]
- Studio のナビゲーションペインで［マシンカタログ］を選択すると、Studio がカタログのリストを表示できないことがあります。このエラーメッセージが表示されます：

  カタログを表示できません。

  この問題は、Studio では PowerShell コマンドの「**Get-ProvSchemeMasterVMImageHistory**」でオブジェクトのリストを取得できないために発生します。[CVADHELP-15211]
- VMware vSphere 7.0 を使用して Machine Creation Services（MCS）カタログを作成しようとすると失敗する場合があります。[CVADHELP-15237]
- この修正により、低速の Active Directory 環境において、Delivery Controller（XML サービス）で発生する可能性があるパフォーマンスの問題が解決します。

  この修正を有効にするには、以下のレジストリキーを設定します：

  HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

  または

  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\DesktopServer

  名前：DisableGetPasswordExpiryInfo

  種類：DWORD

値：1

[CVADHELP-15536]

- この修正には Microsoft System Center Virtual Machine Manager（SCVMM）2019 による Machine Creation Service（MCS）のサポートが含まれます。[CVADHELP-15779]

Metainstaller

- VDA のインストール時に、GUI で選択していなくても Personal vDisk などの追加コンポーネントがインストールされる場合があります。[CVADHELP-15572]
- VDA をアップグレードするとき、［機能］ページで ［パフォーマンス最適化］機能を無効にできません。また、そのページで他の機能を有効にできません。[CVADHELP-14560]

Profile Management

- Profile Management で ［プロファイルストリーミング］ポリシーが有効になっている場合、Internet Explorer 11 でファイルをダウンロードしようとすると失敗することがあります。[CVADHELP-12970]
- ［コントロールパネル］**>**［システムとセキュリティ］**>**［設定の変更］**>**［詳細設定］**>**［ユーザープロファイル］**>**［設定］の順に移動すると、ログインユーザーのプロファイルの［サイズ］フィールドに疑問符（?）マークが表示されます。他のユーザープロファイルは正しいサイズを表示しています。[CVADHELP-13993]
- Appdata\local\temp を［除外の一覧 **-** ディレクトリ］に追加すると、Profile Management はユーザープロファイルに Appdata\local\temp フォルダーを作成せず、Microsoft Outlook などの一部のアプリケーションでランタイムエラーが発生します。この問題は、［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］ポリシーが有効になっている場合に、2 回目以降のログオン中に発生します。[CVADHELP-14054]
- Profile Management が、［レジストリの包含の一覧］にあるレジストリキーのサブキーを同期しません。たとえば、［レジストリの包含の一覧］に Software\Citrix を追加するとき、ユーザーストアには HKEY_CURRENT_USER\SOFTWARE\Citrix のみが保存されます。サブキーが保存されません。[CVADHELP-14815]
- ［ミラーリングするフォルダー］一覧にあるフォルダーがログオン時にユーザーストアに存在しない場合、ローカルのユーザープロファイルが削除されます。[CVADHELP-15248]
- **Desktop** を ［除外の一覧**-**ディレクトリ］ポリシーに追加した場合、ユーザーが公開アプリケーションまたはデスクトップで変更を保存しようとすると、エラーが発生することがあります。[CVADHELP-15792]

Provisioning Services

Provisioning Services 7.15 LTSR CU7は、このリリースの更新に関する特定の情報を提供します。

StoreFront

- iPadOS 13 以降では、ユーザーがログオンしようとすると、StoreFront Web ページがフリーズすることがあります。この問題は、StoreFront 展開で［クラシックエクスペリエンスを有効にする］ポリシーが有効になっている場合に発生します。[CVADHELP-14905]
- ストアフォルダーにカスタム構成ファイルが存在する場合、ストアフォルダー内の web.config ファイルのコンテンツがカスタムファイルで置き換えられることがあります。この問題は、StoreFront をアップグレードするときに発生します。[CVADHELP-13485]

VDA for Desktop OS

セッション/接続

- 複数の USB デバイスがセッションにリダイレクトされると、そのうちの 1 つが正しく機能しない場合があります。[CVADHELP-12516]
- セッションのデフォルトのオーディオデバイスは、ユーザーデバイスのデフォルトのオーディオデバイスと異なる場合があります。セッションでは、オーディオデバイス一覧の一番上のデバイスがデフォルトになります。[CVADHELP-13324]
- XenApp および XenDesktop バージョン 7.15 LTSR CU4 が Microsoft Windows Server 2016 で実行されているサイトで、公開アプリケーションを起動しようとすると、アプリケーションセッションが応答しなくなることがあります。このエラーメッセージが表示されます:

  ローカルセッションマネージャーをお待ちください

  [CVADHELP-13967]
- **SAS** 通知が有効になっている場合、コンソールで既存のセッションに接続している複数のモニターを持つユーザーは、モニターのレイアウトが正しく復元されていないことを発見することがあります。たとえば、右側のモニターが 1 で、メインモニターとして選択され、左側のモニターが 2 の場合、ユーザーは再接続時に位置が入れ替わっていることに気付く可能性があります。この問題は、物理デスクトップを使用しているリモート PC ユーザーにのみ影響します。これは、2 つの機能間で互換性がないことによるものです。[CVADHELP-14249]
- IPv6 が有効になっていると、VDA が断続的に登録解除されることがあります。[CVADHELP-14847]
- この修正により、UDP 接続経由で小さなデータグラムを送信するタイマーが提供され、ホストとクライアント間の接続が維持されます。

  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:

  - *32* ビットシステム

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    名前：KeepAliveTimer

    種類：DWORD

値：Keep-Alive メッセージ間の待機時間間隔（秒単位）を示します。空のままにするか 0 に設定すると、Keep-Alive パケットは送信されず、Keep-Alive 機能は動作しません。推奨値は 15 です。

- *64* ビットシステム

  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

  名前：KeepAliveTimer

  種類：DWORD

  値：Keep-Alive メッセージ間の待機時間間隔（秒単位）を示します。空のままにするか 0 に設定すると、Keep-Alive パケットは送信されず、Keep-Alive 機能は動作しません。推奨値は 15 です。

  [CVADHELP-15122]

- CtxUvi Hooking ドライバーを無効にすると、イベントログが生成されない場合があります。この問題は、使用可能なシステムリソースが少ない場合に発生します。[CVADHELP-15241]
- この修正により、VDA で NTLM 認証を有効にせずに複数のフォレスト展開を構成できる新機能がサポートされます。ただし、NTLM 認証を有効にするための以前の機能は、その他の信頼を伴わない展開用に保持されます。VDA で NTLM 認証が不要に有効になることを回避するために、**SupportMultipleForestDdcLookup** という名前のレジストリエントリが追加されています（NTLM は Kerberos よりも安全性が低くなります）。**SupportMultipleForest** エントリの代わりに **SupportMultipleForestDdcLookup** を使用できます。**SupportMultipleForest** は、後方互換性のために引き続き使用できます。**SupportMultipleForestDdcLookup** レジストリキーは、VDA が Delivery Controller のルックアップを実行する方法を決定します。詳しくは、「複数の Active Directory フォレスト環境での展開」を参照してください。[CVADHELP-15467]
- VDA が Delivery Controller に登録しようとすると、Broker Agent はローカルドメインで最初の DNS ルックアップを実行します。このルックアップにより、Delivery Controller に到達できることを確認します。DNS ルックアップが失敗すると、Broker Agent は Active Directory でトップダウンクエリを実行するようにフォールバックし、すべてのドメインで検索を繰り返し実行します。Delivery Controller のアドレスが無効な場合（たとえば、管理者が VDA のインストール時に FQDN を誤って入力した場合）、クエリ操作によってドメインコントローラーで DDoS のような結果が発生する可能性があります。詳しくは、「VDA 登録中の Controller の検索」を参照してください。[CVADHELP-15484]
- タイムゾーンポリシーが ［サーバーのタイムゾーンを使用する］に設定されていても、ユーザーセッションを介してクライアント側のタイムゾーンが VDA にリダイレクトされることがあります。[CVADHELP-15628]
- 従来のグラフィックモードポリシーを有効にすると、セッションを起動したときに灰色の画面が表示される場合があります。この問題は、VDA バージョン 7.15.6000 で発生します。[CVADHELP-15841]
- サーバー VDI VDA で、［スタート］メニューの電源ボタンに［切断］オプションが表示されない場合があります。[CVADHELP-16595]

システムの例外

- VDA をバージョン 7.15 累積更新プログラム 5（CU5）から CU6 またはバージョン 2003 にアップグレードした後、グループポリシーエンジン（CseEngine.exe）サービスが予期せず終了することがあります。[CVADHELP-14515]
- Citrix Audio Redirection ServiceÂ（CTXAudioSvc）が、イベント ID 1000 と例外コード 0x0c0000005 で予期せず終了することがあります。この問題は、CtxVorbisDmo64.dll モジュールに障害がある場合に発生します。[CVADHELP-14898]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード APC_INDEX_MISMATCH (1) によるブルースクリーンが表示されることがあります。この問題は、マップされたクライアントドライブにアクセスしようとすると発生します。[CVADHELP-15003]
- VDA で tdica.sys の重大な例外が発生し、バグチェックコード 0x1000007e によるブルースクリーンが表示されることがあります。この問題は、HTML5 向け Citrix Workspace アプリ経由でセッションを起動したときに発生します。[CVADHELP-15220]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x93（INVALID_KERNEL_HANDLE）によるブルースクリーンが表示されることがあります。[CVADHELP-15326]
- Web アプリケーションで埋め込みの Windows Media ファイルを表示しようとすると、Internet Explorer が予期せず終了する場合があります。この問題は、HostMMTransport.dll モジュールに障害がある場合に発生します。[CVADHELP-15598]

VDA for Server OS

セッション/接続

- 複数の USB デバイスがセッションにリダイレクトされると、そのうちの 1 つが正しく機能しない場合があります。[CVADHELP-12516]
- XenApp および XenDesktop バージョン 7.15 LTSR CU4 が Microsoft Windows Server 2016 で実行されているサイトで、公開アプリケーションを起動しようとすると、アプリケーションセッションが応答しなくなることがあります。このエラーメッセージが表示されます:

  ローカルセッションマネージャーをお待ちください

  [CVADHELP-13967]
- 音声処理のサンドボックス化を許可するポリシーを有効にすると、Citrix Virtual Apps and Desktops から開いた Google Chrome でオーディオが機能しない場合があります。[CVADHELP-14784]
- ライセンス統計は、サイト間で一貫していない可能性があります。たとえば、Citrix 同時接続ユーザー（CCU）によって消費されるライセンスと、複数のサイトの一意のユーザーに割り当てられるライセンスとの間に明らかな不一致がある可能性があります。[CVADHELP-14950]

- この修正により、UDP 接続経由で小さなデータグラムを送信するタイマーが提供され、ホストとクライアント間の接続が維持されます。

  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:

  - *32* ビットシステム

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    名前：KeepAliveTimer

    種類：DWORD

    値：Keep-Alive メッセージ間の待機時間間隔（秒単位）を示します。空のままにするか 0 に設定すると、Keep-Alive パケットは送信されず、Keep-Alive 機能は動作しません。推奨値は 15 です。

  - *64* ビットシステム

    HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

    名前：KeepAliveTimer

    種類：DWORD

    値：Keep-Alive メッセージ間の待機時間間隔（秒単位）を示します。空のままにするか 0 に設定すると、Keep-Alive パケットは送信されず、Keep-Alive 機能は動作しません。推奨値は 15 です。

    [CVADHELP-15122]

- CtxUvi Hooking ドライバーを無効にすると、イベントログが生成されない場合があります。この問題は、使用可能なシステムリソースが少ない場合に発生します。[CVADHELP-15241]
- クロックドリフトが発生すると、Microsoft Teams は最適化モードでの読み込みに失敗する場合があります。このドリフトによって、Citrix 証明書が無効または期限切れであると見なされます。この問題を回避するには、HTML5 ビデオリダイレクトサービス（txHdxWebSocketService）のスタートアップの種類を、デフォルトの ［自動］ではなく ［自動（遅延開始)］に変更します。[CVADHELP-15298]
- この修正により、VDA で NTLM 認証を有効にせずに複数のフォレスト展開を構成できる新機能がサポートされます。ただし、NTLM 認証を有効にするための以前の機能は、その他の信頼を伴わない展開用に保持されます。VDA で NTLM 認証が不要に有効になることを回避するために、**SupportMultipleForestDdcLookup** という名前のレジストリエントリが追加されています（NTLM は Kerberos よりも安全性が低くなります)。**SupportMultipleForest** エントリの代わりに **SupportMultipleForestDdcLookup** を使用できます。**SupportMultipleForest** は、後方互換性のために引き続き使用できます。**SupportMultipleForestDdcLookup** レジストリキーは、VDA が Delivery Controller のルックアップを実行する方法を決定します。詳しくは、「複数の Active Directory フォレスト環境での展開」を参照してください。[CVADHELP-15467]
- VDA が Delivery Controller に登録しようとすると、Broker Agent はローカルドメインで最初の DNS ルックアップを実行します。このルックアップにより、Delivery Controller に到達できることを確認します。DNS ルックアップが失敗すると、Broker Agent は Active Directory でトップダウンクエリを実行するようにフォールバックし、すべてのドメインで検索を繰り返し実行します。Delivery Controller のアドレスが無

効な場合（たとえば、管理者が VDA のインストール時に FQDN を誤って入力した場合）、クエリ操作によってドメインコントローラーで DDoS のような結果が発生する可能性があります。[CVADHELP-15484]

- リモートデスクトップセッションを切断して再接続すると、VDA for Server OS で無効な XenApp セッションが開始されることがあります。無効なセッションは、VDA を再起動するまで残ります。[CVADHELP-16453]

システムの例外

- Windows オーディオサービスをホストするサービスホスト（svchost.exe）プロセスが、ユーザーセッション内で予期せず終了することがあります。この問題は、メモリリークが原因で発生します。[CVADHELP-13687]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード APC_INDEX_MISMATCH (1) によるブルースクリーンが表示されることがあります。この問題は、マップされたクライアントドライブにアクセスしようとすると発生します。[CVADHELP-15003]
- VDA で tdica.sys の重大な例外が発生し、バグチェックコード 0x1000007e によるブルースクリーンが表示されることがあります。この問題は、HTML5 向け Citrix Workspace アプリ経由でセッションを起動したときに発生します。[CVADHELP-15220]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x93（INVALID_KERNEL_HANDLE）によるブルースクリーンが表示されることがあります。[CVADHELP-15326]
- Web アプリケーションで埋め込みの Windows Media ファイルを表示しようとすると、Internet Explorer が予期せず終了する場合があります。この問題は、HostMMTransport.dll モジュールに障害がある場合に発生します。[CVADHELP-15598]
- Linux 向け Citrix Workspace アプリから起動されたマルチポート対応 TCP セッションに再接続しようとすると、VDA が予期せず終了する場合があります。[CVADHELP-15674]

仮想デスクトップコンポーネント - その他

- 多くの App-V アプリケーションをホストしている VDA から App-V アプリケーションを起動すると、VDA が登録解除されることがあります。この問題は、関連するポリシーファイルの処理に時間がかかる場合に発生します。[CVADHELP-12592]
- この修正により、基本コンポーネント内のセキュリティ上の脆弱性の問題が解決されます。詳しくは、Knowledge Center の記事CTX285059を参照してください。[CVADHELP-14755]

累積更新プログラム **6**（**CU6**）

September 16, 2021

リリース日：2020 年 6 月 30 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 6（CU6）では、7.15 LTSR CU5 リリース以降に報告された 94 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU5 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU6 をダウンロード

> 重要:
>
> このリリースでは、StoreFront のインストールおよびアップグレード方法が変更されています。以前のリリースでは、全製品インストーラーのメインページで ［はじめに］タイルをクリックすると、［コアコンポーネント］ページには StoreFront が含まれていました。StoreFront とその他のコアコンポーネントを選択して、同じマシンにインストールできます。
>
> このリリースでは、［コアコンポーネント］ページに StoreFront チェックボックスは含まれなくなりました。StoreFront をインストールまたはアップグレードするには、メインページの ［拡張展開］で ［**Citrix StoreFront**］をクリックします。これによって、インストールメディアから`CitrixStoreFront-x64.exe`が起動されます。
>
> `XenDesktopServerSetup.exe`コマンドでは、`/components storefront`を指定することができなくなりました。指定しようとすると、コマンドは失敗します。コマンドラインで StoreFront をインストールするには、Citrix Virtual Apps and Desktops インストールメディアの`x64`フォルダーから`CitrixStoreFront-x64.exe`を実行します。
>
> 重要:
>
> Citrix ライセンス管理コンソールは製品終了となり、ライセンスサーバー 11.16.3.0 ビルド 30000 でのサポートが終了しました。Citrix Licensing Managerを使用します。

新しい展開環境

新しく CU6 を展開するには

CU6 メタインストーラーを使用して、CU6 に基づく新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU6 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべての LTSR コンポーネントを CU6 に更新することをお勧めします。たとえば、Provisioning Services が LTSR 展開環境に含まれる場合、Provisioning Services コンポーネントを CU6 に更新します。Provisioning Services が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU6** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.6000	
VDA for Server OS	7.15.6000	
Citrix Studio	7.15.6000	
Citrix Director	7.15.6000	
Delivery Controller	7.15.6000	
Citrix フェデレーション認証サービス	7.15.6000	
Citrix グループポリシー管理	3.1.6000	
Citrix グループポリシークライアント側拡張	3.1.6000	
Linux VDA	7.15.5000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.6000	
Provisioning Services	7.15.27	
Session Recording	7.15.6000	Premium Edition のみ
StoreFront	3.12.6000	
ユニバーサルプリントサーバー	7.15.6000	

XenApp および **XenDesktop 7.15 LTSR CU6** の互換性のあるコンポーネント

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

7.15 LTSR CU6 互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	1903
* ブラウザーコンテンツのリダイレクト	15.15
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.3000
ライセンスサーバー	11.16.6.0 ビルド 31000
セルフサービスパスワードリセット	1.1.20.0
Workspace Environment Management	1906.0.1.1

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU6 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーシ

ョンと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU6 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します:

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU6 インストーラーを実行します。これにより、新しいサイトで使用する新しい Virtual Delivery Agent for Server OS に自動アップグレードされます。
- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。
- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU6 サイトにインポートできます: 一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU6 Controller 上で PowerShell インポートコマンドレットを実行し、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- インターネットインフォメーションサービス（IIS）の再起動後、最初に Citrix Director にログオンすると次のエラーメッセージが ［傾向］ページに表示されることがあります:

  使用できる詳細はありません。

  [CVADHELP-12426]

- 複数のユーザーへのメッセージの送信に失敗して、次のエラーメッセージが表示されることがありました:

  メッセージを送信できません。予期しないエラーです。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。

  [CVADHELP-12601]

- Citrix Director が SMTP サーバーを使用して電子メール構成を設定しようとすると、次のエラーメッセージが表示されることがあります:

  無効なメールサーバーです

  [CVADHELP-14449]

- Citrix Director を使用してスタンドアロンサーバー上にメールサーバーを構成しようとすると、次のエラーメッセージが表示されることがあります:

  無効なメールサーバーです。

  この問題は、警告と通知のメールサーバーを構成するときに発生します。[CVADHELP-14648]

Citrix ポリシー

- グループポリシーエンジン（CseEngine.exe）サービスを再起動しないと、サーバーが切断されるか応答しなくなることがあります。[CVADHELP-12987]

Citrix Studio

- App-V アプリケーションの起動に失敗して、次のエラーメッセージが表示されることがありました:

  起動できません

  この問題は、大量の App-V パッケージが完全に VDA にストリーミングされないときに発生します。[CVADHELP-12889]

- Citrix Studio をバージョン 7.6 から 7.15 にアップグレードすると、一部のウィザード（マシンカタログやデリバリーグループなど）を開くときに時間がかかることがあります。[CVADHELP-13267]

- App-V パッケージを Citrix Studio を追加すると、一部のパッケージはカスタマイズされたアイコンではなくデフォルトのアイコンを表示することがあります。[CVADHELP-13338]

- PVS コレクションからデバイスを Citrix Studio のカタログに追加しようとすると、既にカタログに存在するマシンも含めてすべてのターゲットデバイスが表示されることがあります。[CVADHELP-13403]

- 実行可能なパスまたはアプリケーショングループに割り当てられた既存アプリのアイコンの場所を変更しようとすると、次のエラーメッセージが表示されることがあります:

  デリバリーグループ内のマシンを参照できません。ローカルマシン上を参照しますか**?**

  [CVADHELP-14199]

- Studio を公開アプリとして実行すると、Studio が応答しなくなることがあります。[CVADHELP-14207]

Delivery Controller

- Citrix Director を使用して多くのユーザーにメッセージを送信しようとすると、失敗することがあります。このエラーメッセージが表示されます:

  メッセージを送信できません。データソースが応答しないか、エラーが報告されました。

  この修正は、この問題の発生を最小限に抑えることを意図しています。

  [CVADHELP-12066]

- Citrix Director からアプリケーションインスタンスのカスタムレポートを表示しようとすると、一部のフィールドにアプリケーションの終了時刻ではなく Null 値が表示されることがあります。[CVADHELP-12733]
- アプリケーションを列挙すると、サイトデータベースをホストしている SQL Server で CPU 使用率の大幅な上昇につながることがあります。[CVADHELP-13043]
- 監視データベースの表からリソース利用率データをグルーミングしようとするとタイムアウトで失敗することがあります。[CVADHELP-13075]
- マシンカタログで ［リモート **PC** アクセスの **Wake on LAN**］機能を有効にすると、ローカルホストキャッシュがデータの同期を停止することがあります。この問題は、Microsoft System Center Configuration Manager（SCCM）をホスティング接続として使用するときに発生します。[CVADHELP-13122]
- ユーザーセッションが実行されている仮想マシンが予期せずシャットダウンすることがあります。この問題は、クライアントの自動再接続機能がデータベースで保留中の［削除］電源操作のトリガーに失敗すると発生します。[CVADHELP-13165]
- 2019 年の夏時間の終了後、再起動スケジュールが構成されると、デリバリーグループでのみ予期しないスケジュールの再起動が発生します。[CVADHELP-13486]
- 他のドメインの管理者を Citrix Studio に追加すると、Studio に次のエラーメッセージが表示されることがあります:

  エラー**: Central Configuration Service** の場所を検証できませんでした。

  Studio を使用してこのサイトを管理する十分な権限がないか、委託管理サービスに問題があります。

  この問題は、いずれかのドメインのドメインコントローラーに到達できない場合に発生します。[CVADHELP-13651]
- **udadmin** コマンドを使用してライセンスサーバーレポートを生成すると、同じデバイスにライセンスが複数回発行されているという内容のレポートが表示されることがあります。この問題は、正しいハードウェア ID を持つ別のデバイスが、重複している名前に対して更新される場合に発生します。この問題は、ライセンスの消費には影響せず、レポートにのみ影響します。[CVADHELP-13763]
- ローカルホストキャッシュ（LHC）のファイルは、ダウンロードが開始された後、削除される可能性があります。その結果、古いファイルが残るか、LHC ファイルが C:\Windows\ServiceProfiles\NetworkService に表示されません。[CVADHELP-13980]
- 同期構成をローカルホストキャッシュデータベースにインポートしようとすると、エラー 505 で繰り返し失敗することがあります。[CVADHELP-14237]
- XenApp および XenDesktop 7.15 累積更新プログラム 1 を累積更新プログラム 3 にアップグレードした後、ローカルホストキャッシュ（LHC）をインポートしようとすると、エラー 505 で失敗することがあります。[CVADHELP-14429]

フェデレーション認証サービス

- GUI は、複数の認証機関（CA）サーバーをサポートしていません。[CVADHELP-11919]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU6 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Profile Management

- Microsoft Windows 10 バージョン 2004 でユーザープロファイルを作成しようとすると失敗する場合があります。[CVADHELP-14235]
- 一時プロファイルを使用してセッションにログオンすると、空のユーザープロファイルフォルダーが C:\Users の下に作成されることがあります。Profile Management によりログオフ時に一時プロファイルが削除され、空のユーザープロファイルフォルダーが残ります。[CVADHELP-14297]
- Profile Management で［AppData(Roaming) フォルダーをリダイレクト］ポリシーが有効になっている場合、［スタート］メニューに一部のタイルが表示されないことがあります。この問題は、Citrix Virtual Apps and Desktops 1912 以前を実行している Windows Server 2016 または 2019 マシンにログオンしたときに発生します。[CVADHELP-14336]
- ［ログオン時の除外チェック］ポリシーを有効にすると、Profile Management は除外されたフォルダーに含まれるファイルの同期に失敗する場合があります。そのため、ログオン時にこれらのファイルが削除または無視される場合があります。この問題は、［同期するファイルの一覧］ポリシーのワイルドカードが含まれるパスと一致するファイルで発生します。[CVADHELP-14347]

Provisioning Services

Provisioning Services 7.15 LTSR CU6は、このリリースの更新に関する特定の情報を提供します。

StoreFront

- StoreFront バージョン 3.12 累積更新プログラム 3 が、SAML 認証と複数のドメインを含む複雑な AD アーキテクチャを使用して構成されている場合、フェデレーション認証サービス（FAS）でアプリケーションを起動できないことがあります。このエラーメッセージが表示されます：

  アプリケーションを起動できません。

  この問題は、ストアで FAS が有効になっている場合に発生します。

  [CVADHELP-12865]

- StoreFront 管理コンソールに SAML 認証を構成し、アドレスフィールドに IdP URL（PingID 用）を入力すると、これらの変更が保存されないことがあります。このエラーメッセージが表示されます：

  表示されるエラー：変更の保存時にエラーが発生しました。

  [CVADHELP-13373]

- サードパーティ製アプリケーションを ID プロバイダー（IdP）として使用すると、セキュリティアサーションマークアップランゲージ（SAML）認証が失敗する場合があります。

  次のエラーメッセージが表示されます:

  マップされたアカウントでエラーが発生しました。

  [CVADHELP-13396]

- ストアフォルダーにカスタム構成ファイルが存在する場合、ストアフォルダー内の web.config ファイルのコンテンツがカスタムファイルで置き換えられることがあります。この問題は、StoreFront をアップグレードするときに発生します。[CVADHELP-13485]
- この修正により、基本コンポーネント内のセキュリティ上の脆弱性の問題が解決されます。[CVADHELP-13602]
- アップグレード履歴に 2.6、3.0.1、3.5、3.8 が含まれる場合、Citrix StoreFront Protocol Transition サービスが停止状態のときに 3.12 CU* 以降へのアップグレードが失敗することがあります。[CVADHELP-13626]
- StoreFront にログオンすると、アプリケーションの列挙が完了するまでに時間がかかる場合があります。この問題は、ユーザー名をドメイン\ユーザー名形式で入力し、ユーザー認証が Delivery Controller に委任されている場合に発生します。[CVADHELP-13891]
- StoreFront コンソールで、アンダースコア（_）を含むドメイン名を信頼済みドメインリストに追加しようとすると、失敗することがあります。[CVADHELP-14213]
- この修正により、基本コンポーネント内のセキュリティ上の脆弱性の問題が解決されます。詳しくは、Knowledge Center の記事CTX277455を参照してください。[LCM-7272]
- Delivery Controller をインストールすると、StoreFront がデフォルトでインストールされない場合があります。これをインストールするには、Citrix Virtual Apps and Desktops メタインストーラーから Citrix StoreFront オプションを使用します。[LCM-7335]

ユニバーサルプリントサーバー

クライアント

- アクセス違反のため、ユニバーサルプリントサーバー（UPServer.exe）が予期せず終了することがあります。[CVADHELP-10627]
- 印刷スプーラーサービス（spoolsv.exe）でデッドロックが発生することがあります。その結果、文書の印刷に失敗し、Microsoft Office アプリケーションは起動しません。[CVADHELP-13315]
- アプリケーションを起動しようとすると、Citrix Print Manager Service（CpSvc.exe）が予期せず終了することがあります。[CVADHELP-13945]
- 印刷スプーラーサービスが異常終了することがあります。[CVADHELP-13954]

サーバー

- アクセス違反のため、ユニバーサルプリントサーバー（UPServer.exe）が予期せず終了することがあります。[CVADHELP-10627]
- ユニバーサルプリントサーバー（UPServer.exe）が予期せず終了することがあります。この問題は、prntvpt.dll モジュールに障害がある場合に発生します。[CVADHELP-12651]

VDA for Desktop OS

キーボード

- Citrix の汎用クライアント入力システム（IME）機能を有効にした場合、中国語のクライアント IME を使用して特殊文字や数字を入力すると、アプリケーションが予期せず終了する場合があります。この問題は、Microsoft Windows 10 バージョン 1809 および Windows Server 2019 を実行中のデスクトップおよびアプリセッションで発生します。[CVADHELP-13961]

インストール、アンインストール、アップグレード

- VDA をアップグレードすると、**MaxVideoMemoryBytes** レジストリキーがデフォルト値に戻ることがあります。[CVADHELP-13629]
- VDA をアップグレードするとき、［機能］ページで ［パフォーマンス最適化］機能を無効にできません。また、そのページで他の機能を有効にできません。[CVADHELP-14560]

印刷

- VDA をバージョン 7.15 累積更新プログラム 4 にアップグレード後、Citrix Print Manager Service（CpSvc.exe）が予期せず終了することがあります。[CVADHELP-12888]
- アプリケーションを起動しようとすると、Citrix Print Manager Service（CpSvc.exe）が予期せず終了することがあります。[CVADHELP-13945]

セッション/接続

- 専用デスクトップセッションを開始すると、ログオンに失敗し、ログオフプロセスが停止することがあります。Citrix Studio ではセッションは接続済みと表示されますが、手動でマシンを再起動するまでログオフすることはできません。[CVADHELP-10931]
- Windows Media Player がプレイリストの現在のトラックから次のトラックに移動すると、次のトラックの先頭でオーディオが再生されないことがあります。この問題は、Windows Media リダイレクトが有効になっている場合に発生します。[CVADHELP-11639]

- オーディオデバイスをユーザーセッションに追加すると、Skype for Business のサウンド以外のデバイスからサウンドを聞くことはできません。このエラーメッセージが表示されます:

  エラー **-** 使用可能なデバイススロットがありません **-** デバイスを追加できませんでした。

  この問題は、8 つを超える数の再生デバイスまたは録音デバイスがエンドポイントに接続されている場合に発生します。[CVADHELP-12760]

- VDA でセッションローミングが機能しないことがあります。この問題は、Dell Wyse シンクライアントデバイスで発生します。[CVADHELP-13003]

- 別のマシンのアクティブセッションに再接続すると、リダイレクトされたプリンターとクライアントドライブが失われることがあります。この問題は、アクティブなユーザーセッションをロックまたは切断せずに、あるマシンから別のマシンに移動したときに発生します。[CVADHELP-13035]

- アプリケーションが Web カメラを使用してビデオをキャプチャしているときに ［キャンセル］ボタンをクリックすると、アプリケーションが応答しなくなることがあります。この問題は、MFDeviceSource.dll モジュールに障害がある場合に発生します。[CVADHELP-13062]

- VDA で次のレジストリキーの値を 1 に変更すると、クライアントドライブからのデータの読み取りに時間がかかることがあります。

  有効にするには、次のレジストリキーを追加します:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  名前：PacketIntegrityChecks

  種類：DWORD

  値：1

  [CVADHELP-13063]

- Windows 向け Citrix Workspace アプリでセッションを記録すると、マウスポインターの動きが記録されないことがあります。この問題は、VDA バージョン 7.15.400 で発生します。[CVADHELP-13300]

- サードパーティの脆弱性スキャナーを使用して VDA でセッションを起動しようとすると失敗することがあります。[CVADHELP-13306]

- 再起動後に VDA が応答しなくなることがあります。この問題は、Symantec SEP などのセキュリティソフトウェアがセキュリティスキャンを実行するときに発生します。[CVADHELP-13832]

- アプリケーションウィンドウの一部が透明になり、アプリケーションがフォアグラウンドではなくバックグラウンドで実行されることがあります。この問題は、シームレスモードで発生します。[CVADHELP-13903]

- マルチモニター環境で、アプリケーションが同じモニターに一貫性をもって表示されないことがあります。この問題は、新しいワークステーションに移行するときに発生します。[CVADHELP-13657]

スマートカード

- Windows 10 でスマートカード認証を構成した後、ユーザーセッションでデスクトップを起動すると、スマートカードパススルー認証が失敗することがあります。この問題は、シンクライアントからデスクトップを起動したときに発生します。[CVADHELP-11757]

システムの例外

- USB リダイレクトにより VDA に重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HAN**（**7e**）のブルースクリーンが表示されることがあります。また、USB リダイレクトのグローバルロックが解除されないことがあり、他のリダイレクトをブロックします。[CVADHELP-9237]
- VDA で ctxdvcs.sys の重大な例外が発生し、ブルースクリーンが表示されることがあります。[CVADHELP-13000]
- VDA で ctxdvcs.sys の重大な例外が発生し、バグチェックコード 0xc0000409 によるブルースクリーンが表示されることがあります。[CVADHELP-13102]
- Electron フレームワークを使用するアプリケーションは、次のエラーメッセージで予期せず終了することがあります:

  {例外**}** 不正な命令不正な命令を実行しようとしました。

  [CVADHELP-13440]

ユーザーインターフェイス

- **Citrix Workspace –** 基本設定ウィンドウで［デバイス］タブが見つからないことがあります（［**Desktop Viewer**］ツールバー > ［基本設定］）。この問題は、サーバー VDI スイッチ経由で VDI デスクトップを Microsoft Windows Server 上で実行している場合に発生します。[CVADHELP-14158]

VDA for Server OS

キーボード

- Citrix の汎用クライアント入力システム（IME）機能を有効にした場合、中国語のクライアント IME を使用して特殊文字や数字を入力すると、アプリケーションが予期せず終了する場合があります。この問題は、Microsoft Windows 10 バージョン 1809 および Windows Server 2019 を実行中のデスクトップおよびアプリセッションで発生します。[CVADHELP-13961]

印刷

- VDA をバージョン 7.15 累積更新プログラム 4 にアップグレード後、Citrix Print Manager Service（CpSvc.exe）が予期せず終了することがあります。[CVADHELP-12888]

- ドキュメントを別の出力プリンタートレイに印刷しようとすると失敗することがあります。印刷ダイアログボックスで別のトレイを選択した場合でも、印刷ジョブはデフォルトのトレイにドキュメントを出力します。[CVADHELP-13492]
- アプリケーションを起動しようとすると、Citrix Print Manager Service（CpSvc.exe）が予期せず終了することがあります。[CVADHELP-13945]

セッション/接続

- Windows Media Player がプレイリストの現在のトラックから次のトラックに移動すると、次のトラックの先頭でオーディオが再生されないことがあります。この問題は、Windows Media リダイレクトが有効になっている場合に発生します。[CVADHELP-11639]
- VDA for Server OS で公開アプリケーションを起動すると、Windows RunOnce レジストリキーが実行されないことがあります。[CVADHELP-11991]
- Delivery Controller に無効なセッション情報が表示されることがあります。この問題は、VDA が Delivery Controller に送信するセッション情報に IP アドレス 127.0.0.1 が含まれている場合に発生します。[CVADHELP-12767]
- アプリケーションを起動できないことがあります。その結果、［タスクマネージャー］下のセッションの詳細が見つからず、Citrix Studio に次のアプリケーションステータスが表示されます：アプリケーションが実行されていません。問題が発生すると、VDA が再登録され、次のエラーメッセージが表示されることがあります：

  イベント **ID 1048**：ブローカーによる **WCF** の失敗または拒否

  [CVADHELP-12856]
- ユーザーセッションでテキストをハイライトしようとすると、パフォーマンスの問題が発生することがあります。この問題は、公開デスクトップで実行されている Microsoft Outlook バージョン 2016 でそれを行う場合に発生します。

  有効にするには、次のレジストリキーを追加します：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\

  名前：CursorShapeChangeMinInterval

  種類：DWORD

  値：設定可能な値：10～100。推奨値：50。デフォルトは 0 で、これは無効を意味します。

  [CVADHELP-12886]
- アプリケーションが Web カメラを使用してビデオをキャプチャしているときに［キャンセル］ボタンをクリックすると、アプリケーションが応答しなくなることがあります。この問題は、MFDeviceSource.dll モジュールに障害がある場合に発生します。[CVADHELP-13062]

- VDA で次のレジストリキーの値を 1 に変更すると、クライアントドライブからのデータの読み取りに時間がかかることがあります。

  有効にするには、次のレジストリキーを追加します:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  名前：PacketIntegrityChecks

  種類：DWORD

  値：1

  [CVADHELP-13063]

- Windows 向け Citrix Workspace アプリでセッションを記録すると、マウスポインターの動きが記録されないことがあります。この問題は、VDA バージョン 7.15.400 で発生します。[CVADHELP-13300]
- Citrix Studio と Citrix Director を使用してユーザーセッションからログオフしようとすると、そのセッションで公開アプリケーションを起動するときに、失敗することがあります。[CVADHELP-13307]
- マルチモニター環境で、アプリケーションが同じモニターに一貫性をもって表示されないことがあります。この問題は、新しいワークステーションに移行するときに発生します。[CVADHELP-13657]
- 再起動後に VDA が応答しなくなることがあります。この問題は、Symantec SEP などのセキュリティソフトウェアがセキュリティスキャンを実行するときに発生します。[CVADHELP-13832]
- アプリケーションウィンドウの一部が透明になり、アプリケーションがフォアグラウンドではなくバックグラウンドで実行されることがあります。この問題は、シームレスモードで発生します。[CVADHELP-13903]
- ネットワークの切断後にクライアントの自動再接続（ACR）がセッションに再接続しようとすると、COM ポートリダイレクトが機能しないことがあります。[CVADHELP-13926]
- メモリ使用量が高いことが原因で VDA が負荷限界を報告した後、メモリ使用量が低いレベルまで低下しても、読み込みインデックス値が 10,000 のままになることがあります。[CVADHELP-14563]
- シームレスセッションをロックすると、セッションウィンドウのサイズに関係なく、ログオンウィンドウが全画面表示されることがあります。その結果、エンドポイントのデスクトップやその他のアプリケーションにアクセスできなくなります。[CVADHELP-14589]

スマートカード

- スマートカードを使用したパススルー認証が断続的に失敗することがあります。この問題は、Windows Server 2016 で HDX セッションを起動するときに発生します。[CVADHELP-13054]

システムの例外

- USB リダイレクトにより VDA に重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HAN**（**7e**）のブルースクリーンが表示されることがあります。また、USB リダイレクトのグローバルロックが解除されないことがあり、他のリダイレクトをブロックします。[CVADHELP-9237]

- VDA で ctxdvcs.sys の重大な例外が発生し、ブルースクリーンが表示されることがあります。[CVADHELP-13000]
- VDA で ctxdvcs.sys の重大な例外が発生し、バグチェックコード 0xc0000409 によるブルースクリーンが表示されることがあります。[CVADHELP-13102]
- サーバーで icardd.dll の重大な例外が発生し、バグチェックコード 0x0000003B によるブルースクリーンが表示されることがあります。[CVADHELP-13330]
- Electron フレームワークを使用するアプリケーションは、次のエラーメッセージで予期せず終了することがあります:

  {例外**}** 不正な命令不正な命令を実行しようとしました。

  [CVADHELP-13440]
- サービスホスト（svchost.exe）プロセスまたは wfshell.exe プロセスで、アクセス違反が発生して予期せず終了することがあります。この問題は、icaendpoint.dll モジュールに障害がある場合に発生します。[CVADHELP-14276]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x22 によるブルースクリーンが表示されることがあります。[CVADHELP-14332]
- 9 台を超える数のモニターを持つデバイスでは、ユーザーセッションの起動が致命的な例外で失敗し、バグチェックコード 0x3B によるブルースクリーンが表示されることがあります。[CVADHELP-14775]

仮想デスクトップコンポーネント - その他

- 多くの App-V アプリケーションをホストしている VDA から App-V アプリケーションを起動すると、VDA が登録解除されることがあります。この問題は、関連するポリシーファイルの処理に時間がかかる場合に発生します。[CVADHELP-12592]

累積更新プログラム **5**（**CU5**）

September 16, 2021

リリース日：2019 年 10 月 22 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 5（CU5）では、7.15 LTSR CU4 リリース以降に報告された 120 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU4 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU5 をダウンロード

新しい展開環境

新しく CU5 を展開するには

CU5 メタインストーラーを使用して、CU5 に基づく新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU5 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべての LTSR コンポーネントを CU5 に更新することをお勧めします。たとえば、Provisioning Services が LTSR 展開環境に含まれる場合、Provisioning Services コンポーネントを CU5 に更新します。Provisioning Services が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU5** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.5000	
VDA for Server OS	7.15.5000	
Citrix Studio	7.15.5000	
Citrix Director	7.15.5000	
Delivery Controller	7.15.5000	

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
フェデレーション認証サービス	7.15.5000	
グループポリシー管理のエクスペリエンス	3.1.5000	
Linux VDA	7.15.5000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.5000	
Provisioning Services	7.15.21	
Session Recording	7.15.5000	Premium Edition のみ
StoreFront	3.12.5000	
ユニバーサルプリントサーバー	7.15.5000	

Citrix XenApp および **XenDesktop 7.15 LTSR CU5** の互換性のあるコンポーネント

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

7.15 LTSR CU5 互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	1903
* ブラウザーコンテンツのリダイレクト	15.15
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.3000
ライセンスサーバー	11.16.3.0 ビルド 28000
セルフサービスパスワードリセット	1.1.10.0

7.15 LTSR CU5 互換性のあるコンポーネントおよびプラットフォーム	バージョン
Workspace Environment Management	1906.0.1.1

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

除外対象のコンポーネント
Personal vDisk：Windows 10 マシンでは除外されます。Windows 7 マシンの場合、2020 年 1 月 14 日まで LTSR は限定的にサポートされます（CU の要件が適用されます）

除外対象のコンポーネント
AppDisk

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU5 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーションと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU5 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します。

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU5 インストーラーを実行します。これにより、新しいサイトで使用する新しい Virtual Delivery Agent for Server OS に自動アップグレードされます。
- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。
- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU5 サイトにインポートできます：一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU5 Controller 上で PowerShell インポートコマンドレットを実行して、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- 同じ Active Directory フォレストに親ドメインと子ドメインの 2 つのドメインがあります。ユーザーは、XenDesktop デリバリーグループに自動的に属する子ドメインのドメインローカルグループに追加されます。親ドメインの管理者が Director にログオンすると、ダッシュボードにセッションの一覧が表示されます。管理者がセッションの詳細を表示しようとすると、次のエラーメッセージが表示されます:

  このユーザーには実行中のセッションや割り当てられたデスクトップがありません。

  ただし、子ドメインの管理者はこの問題に遭遇しません。[LD0178]

- Citrix Director コンソールで、アプリケーションインスタンスの公開名でフィルタリングされた複数のユーザーにメッセージを送信すると、次のエラーメッセージが表示される場合があります:

  メッセージを送信できません。予期しないエラーです。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。[LD1257]

- Citrix Director のユーザーデータセクションに個人設定データが表示されないことがあり、次のエラーメッセージが表示されます:

  予期しないエラーです。[LD1353]

- マルチセッション環境で［フィルター］>［セッション］>［すべて］に移動してセッションからログオフすると、セッションはログオフします。同じユーザー名の別のセッションを二度目に選択してログオフしようとすると、このエラーメッセージが開きます:

  データソースが応答しないか、エラーが報告されました。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。[LD1441]

- Citrix Director では、いくつかのテーブルレコードのみが表示され、その後に空白が表示される場合があります。残りのレコードは、テーブルを下にスクロールした場合のみ表示できます。[LD1706]

Citrix Studio

- **XenApp** エディションで［詳細］を選択すると、新しい Amazon Web Services（AWS）ホスト接続を作成できない場合があります。[LD1988]
- カタログから仮想マシンを削除しようとすると、［**System.ArgumentNullException** の値は **Null** にできません］という例外によって削除が失敗する場合があります。[LD2014]
- VDA に展開された App-V パッケージが、誤って VDA から削除される可能性があります。そのため、この修正では HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features にレジストリキーが導入され、このキー

で、クリーンアップを有効にするか無効にするかを制御できます。デフォルトでは、クリーンアップは無効になっています。[LD2025]

有効にするには、次のレジストリキーを追加します:

HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

名前: RedundantPackageCleanup

種類: REG_SZ

データ: True

- Citrix Studio を介してマシンカタログにマシンを追加しようとすると、次の例外が発生して失敗する場合があります: エラー **ID**: **XDDS:081419B3**。この問題が発生するのは、Provisioning Services データベースの`dbo.device`テーブルに NULL `domainObjectSID`属性が含まれる 1 つまたは複数のターゲットデバイスがある Provisioning Services デバイスコレクションからマシンが追加されたときです。[LD2029]

構成ログサービス

- ユーザーのセキュリティ識別子（SID）の解決中に、サイト構成テストレポートでエラーが生成されることがあります。この問題は、構成ログ SID ID が Active Directory から解決できるかを検証するチェック機能で発生します。[LD1569]

コントローラー

- Machine Creation Services（MCS）を使用してベースディスクイメージを削除しようとすると失敗することがあります。[LD2143]
- この修正により、VDA を再起動したときに Citrix High Availability Service で発生するメモリリークの問題が解決されます。[LD1121]
- Amazon Web Services（AWS）の使用中にマシンを再起動すると、数分の遅れが発生することがあります。[LD1220]
- SQL Server では、監視データベースの CPU 使用率が非常に高くなる場合があります。この問題により、全体的なパフォーマンスが低下します。[LD1478]
- Amazon Web Services を（AWS）利用している場合、Citrix Studio から手動で実行した電源操作やその他のスケジュールされた電源操作が失敗することがあります。この問題は、マシンの電源がオンの状態のときに仮想マシンをリセットすると発生します。[LD1548]
- Citrix Broker Service を停止しようとすると失敗する場合があります。[LD1753]
- この修正は、基本コンポーネント内の 1 件の問題に対応しています。[LD1808]
- Citrix Scout レポートを実行すると、Citrix Analytics Service が予期せず終了し、次のエラーメッセージが表示される場合があります:

Citrix Analytics サービスが停止しました。[LD1860]

- エラーメッセージや進行状況バーが表示されずに、カタログの更新が失敗することがあります。[LD1980]
- **XenApp** エディションで ［詳細］を選択すると、新しい Amazon Web Services（AWS）ホスト接続を作成できない場合があります。[LD1988]
- カタログから仮想マシンを削除しようとすると、[**System.ArgumentNullException** の値は **Null** にできません］という例外によって削除が失敗する場合があります。[LD2014]
- ［**Citrix Director**］>［傾向］>［容量管理］>［サーバー **OS** 使用量］にアクセスすると、［最大同時接続サーバー **OS** デスクトップインスタンス数］が実際の数より多いセッション数を表示することがあります。この問題は、セッションの再接続によって ［最大同時接続サーバー **OS** デスクトップインスタンス数］が単一のセッションを複数回として数えるために発生します。[LD2122]
- VMware 環境で Machine Creation Services（MCS）を使用してマシンカタログを作成しようとすると失敗し、次のエラーメッセージが表示されます:

  FailedToCreateImagePreparationVm [LD2158]
- Microsoft Azure で Machine Creation Services（MCS）カタログを作成または更新しようとすると失敗し、次のエラーメッセージが表示されることがあります:

  Error, exception of type: “System.OutOfMemoryExceotion” [LD2160]

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU5 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Profile Management

- Citrix Profile Management を使用すると、ユーザーのログオン時にレジストリキー「HKEY_LOCAL_MACHINE\SYSTEM\
で作成されるファイアウォール規則を削除するための Microsoft の修正プログラムが機能しないことがあります。この問題は、Citrix Profile Management がローカルプロファイルを削除するための Microsoft の標準 API を呼び出さないために発生します。この修正について詳しくは、Microsoft 社のナレッジベースの記事KB4467684を参照してください。[LD1074]
- セッションから削除したファイルが、UPM ストアから削除されないことがあります。[LD1270]
- VDA が提供するイベントログデータと比較すると、Citrix Director が記録するログオン期間がずれている場合があります。[LD1679]
- Profile Management は、破損したローカルプロファイルの読み込みに失敗した後、プロファイルストアへのコピー操作をキャンセルしませんNTUSER.DAT。代わりに、破損したレジストリハイブをプロファイルストアにコピーし、NTUSER.DATファイルとそのバックアップを上書きします。[LD1816]

- 除外の一覧にレジストリパスを追加しても、そのレジストリパスが引き続き保存される場合があります。この問題は、レジストリパスの末尾にバックスラッシュ（\）が存在する場合に発生します。[LD1862]
- Citrix Desktop Service（BrokerAgent.exe）が予期せず終了することがあり、Citrix Profile Management サービスを再起動するまで次の例外が発生します：

  System_Management_Instrumentation_ni!WmiNative.WbemProvider.WmiNative.IWbemServices.Cr
  [LD2223]

Provisioning Services

Provisioning Services 7.15 LTSR CU5は、このリリースの更新に関する特定の情報を提供します。

StoreFront

- 同じアイコンをクリックして以前に切断されたセッションに再接続しようとすると、セッションに再接続できない場合があります。この問題は、同じ名前を持つ複数のデスクトップがエンドユーザーに公開されている場合に発生します。[LD1367]
- ユーザーファームマッピングに割り当てられた Controller を編集して変更を保存しようとすると、Microsoft 管理コンソール（MMC）が予期せず終了する場合があります。この問題は、Microsoft .NET Framework 4.7 がインストールされているサーバーで発生します。[LD1668]

ユニバーサルプリントサーバー

クライアント

- 印刷スプーラーサービスが異常終了することがあります。この問題は、`CRawStreamHeaderWriter::EndPage`および`CRawStreamHeaderWriter::StartPage`が Null オブジェクトにアクセスしようとすると発生します。[LC7893]
- ユニバーサルプリントサーバーにより、印刷スプーラーサービスが応答しなくなることがあります。[LC9341]
- ドキュメントを印刷する前に、公開デスクトップセッションの印刷ダイアログボックスで使用可能なプリンターの一覧からプリンターを選択します。プリンターがドキュメントの印刷を開始するときに、遅延が発生することがあります。[LC9601]
- VDA のインストール後、プリンタープロパティのプリンターポートが、マップされたネットワークプリンターに表示されなくなることがあります。[LD0949]
- 一部のワークフローでは、ドキュメントの印刷に時間がかかる場合があります。[LD1256]
- ［ユニバーサル印刷の使用］設定を ［ユニバーサル印刷のみを使用する］に設定すると、クライアントプリンターがセッションで自動作成されてないことがあります。[LD1395]

User Profile Management VDA

- セッションにログオンすると、ユーザーデータが予期せず削除されることがあります。この問題は、**Citrix** のフォルダーリダイレクトパスポリシー設定（デスクトップパス設定など）でファイルサーバーのアドレスを path1 から path2 に変更すると発生します。ただし、path1 と path2 は同じ物理的な場所を指します。この問題を回避するには、Microsoft グループポリシー設定［フォルダーリダイレクトの前に古いターゲットと新しいターゲットが同じ共有を指すことを確認する］を有効にします。詳しくは、Citrix フォルダーリダイレクトパスポリシー設定の「説明」の部分を参照してください。[LD1500]

VDA for Desktop OS

キーボード

- 韓国語の IME（Input Method Editor）を使用してテキストを入力する場合、マウスをクリックするとテキストの最後の文字が消えることがあります。この問題は、Citrix Receiver で汎用クライアント IME が有効になっている場合に発生します。[LD1380]
- Web サイトに移動してキーボードを非表示に設定しても、Web サイトの編集領域外にキーボードが引き続き表示される場合があります。[LD1382]

印刷

- 一部のワークフローでは、ドキュメントの印刷に時間がかかる場合があります。[LD1256]
- ［ユニバーサル印刷の使用］設定を ［ユニバーサル印刷のみを使用する］に設定すると、クライアントプリンターがセッションで自動作成されてないことがあります。[LD1395]
- VDA for Desktop OS では、マップされたクライアントプリンターでファイルを印刷しようとすると失敗することがあります。この問題は、VDA が Windows 10 バージョン 1903 にインストールされている場合に発生します。[LD2370]

セッション/接続

- ユーザーセッションでオーディオを再生すると、ポンという音が聞こえる場合があります。この問題は、オーディオを再生するときに発生します。[LD0455]
- Citrix Receiver for Windows では、オーディオを再生すると断続的に音が聞こえることがあります。[LD0624]
- Adobe Acrobat Reader と Microsoft Outlook をシームレスモードで実行しているときに両方のプログラムを最大化すると、Acrobat Reader のメニューバー、最小化ボタン、元に戻すボタンおよび閉じるボタンが反応しなくなることがあります。[LD1006]
- USB マイクをユーザーデバイスに接続してセッションを起動すると、USB マイクがリダイレクトに失敗することがあります。USB デバイスは ［最適化］、［ポリシー制限］として表示されます。[LD1027]

- オーディオを再生または一時停止すると、一部のサードパーティ製アプリケーションでノイズが発生する場合があります。[LD1136]
- VDA でセッションを開始しようとすると失敗する場合があります。[LD1180]
- VDA をインストールすると、USB ルートハブもデバイスマネージャーにインストールされます。USB 2.0 ルートハブまたは USB 3.0 ルートハブが既にインストールされている場合でも、USB ルートハブはインストールされます。[LD1196]
- ［従来のグラフィックモード］ポリシーが有効なときに、VDA for Desktop OS に接続しようとして失敗することがあります。この問題は、VDA が Microsoft Windows Server 2008 R2 にサーバー VDI としてインストールされている場合に発生します。[LD1296]
- VDA を再起動した後の最初の接続で、［セッション画面の保持のタイムアウト］ポリシーが適用されないことがあります。ただし、その後の接続にポリシーを適用しようとするとうまくいく場合があります。[LD1397]
- Enlightened Data Transport(EDT)が有効な場合､VDA はバグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_ (0x1000007E)** により予期せず終了することがあります。この問題は、Zscaler 経由で外部からユーザーセッションにアクセスすると発生します。[LD1493]
- Citrix Studio などの特定のレガシアプリケーションは、クライアント側の解像度が変更されるとシームレスセッションで正しく再描画されないことがあります。[LD1554]
- セッションに再接続すると、ユーザーデバイスのシステムトレイに VDA 通知アイコンが表示されなくなることがあります。[LD1629]
- XenApp および XenDesktop 7.15 LTSR 累積更新プログラム（CU）2 を CU3 にアップグレード後、公開デスクトップセッションで一部の.Net アプリケーションが応答しなくなることがあります。この問題は、Windows Server 2008 R2 上の VDA で発生します。[LD1726]
- ユーザーセッション内で視覚効果を変更すると、レジストリキー HKEY_CURRENT_USER\Control Panel\Desktop の値`UserPreferencesMask`が新しい値に更新されないことがあります。[LD1827]

  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。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  名前：HookProcess

  種類：REG_DWORD

  データ：1
- Microsoft Windows オペレーティングシステムの日本語バージョンでは、［デバイスマネージャー］のデバイスの説明が破損している可能性があります。[LD1834]
- アクセス違反により、wfshell.exe プロセスが予期せず終了する場合があります。その結果、アプリケーションの起動に失敗します。[LD2050]

スマートカード

- スマートカードパススルー認証が Windows 8 または Windows 10 で失敗することがあります。VDA セッションをロックしてからロック解除すると、ユーザーはスマートカードユーザーからドメインユーザーに変更されます。[LD1365]

システムの例外

- 位置情報 API を実装する Web アプリケーションを実行すると、Internet Explorer（iexplore.exe）プロセスが予期せず終了する場合があります。[LD0677]
- AMD Opteron（TM）プロセッサ 6128 HE を搭載したマシンで Citrix ソフトウェアグラフィックプロセス（Ctxgfx.exe）が予期せず終了する場合があります。[LD0954]
- VDA で wfshell.exe プロセスが、予期せずに終了する場合があります。この問題は、CtxUiMon.dll モジュールに障害がある場合に発生します。[LD1359]
- XenApp および XenDesktop 7.15 LTSR が実行されている VDA では、ctxdvcs.sys で重大な例外が発生し、バグチェックコード 0x0000007E によりブルースクリーンが表示される場合があります。[LD1688]
- VDA で wfshell.exe プロセスが、予期せずに終了する場合があります。[LD1847]
- 修正 LD0624 を適用後、VDA for Desktop OS は ctxad.sys により重大な例外が発生しオーディオクライアントチェックコードでブルースクリーンを表示することがあります。[LD1995]
- wfshell.exe プロセスが予期せず終了すると、アプリケーションの起動に失敗することがあります。この問題は、cmpcom.dll モジュールに障害がある場合に発生します。[LD2107]

ユーザーインターフェイス

- 資格情報を手動で入力する必要があるときに、ログオンウィンドウが前面に表示されないことがあります。[LC9861]
- Citrix ［切断］ボタンがインストールされた状態で［開始］ボタンをクリックするとボタンが開かないか、開くのに時間がかかることがあります。[LD1149]
- 公開アプリケーションのコンテキストメニューを右クリックしたときに、カーソルのある場所にメニューが開かないことがあります。[LD1243]
- Surface Pro デバイスで VDA セッションを起動し、［ペンと **Windows** インク］ページで ［手書きパネルで指先を使って書く］機能を有効にすると、問題が発生する場合があります。入力したテキストまたはイメージのフォントサイズが、マウスを使用して入力したサイズより大きくなることがあります。[LD1472]
- ウィンドウが断続的に移動するか、**VDI** デスクトップ画面から消えることがあります。[LD1696]

VDA for Server OS

キーボード

- 韓国語の IME（Input Method Editor）を使用してテキストを入力する場合、マウスをクリックするとテキストの最後の文字が消えることがあります。この問題は、Citrix Receiver で汎用クライアント IME が有効になっている場合に発生します。[LD1380]
- Web サイトに移動してキーボードを非表示に設定しても、Web サイトの編集領域外にキーボードが引き続き表示される場合があります。[LD1382]

印刷

- ドキュメントを印刷する前に、公開デスクトップセッションの印刷ダイアログボックスで使用可能なプリンターの一覧からプリンターを選択します。プリンターがドキュメントの印刷を開始するときに、遅延が発生することがあります。[LC9601]
- 一部のワークフローでは、ドキュメントの印刷に時間がかかる場合があります。[LD1256]
- ［ユニバーサル印刷の使用］設定を ［ユニバーサル印刷のみを使用する］に設定すると、クライアントプリンターがセッションで自動作成されてないことがあります。[LD1395]

セッション/接続

- Adobe Acrobat Reader と Microsoft Outlook をシームレスモードで実行しているときに両方のプログラムを最大化すると、Acrobat Reader のメニューバー、最小化ボタン、元に戻すボタンおよび閉じるボタンが反応しなくなることがあります。[LD1006]
- USB マイクをユーザーデバイスに接続してセッションを起動すると、USB マイクがリダイレクトに失敗することがあります。USB デバイスは ［最適化］、［ポリシー制限］として表示されます。[LD1027]
- Citrix Broker Service は、イベントログに次のエラーを報告することがあります：

  Citrix Broker Service で、マシン’machine_name’ の Virtual Desktop Agent に必要な基本設定を特定できません。

  例外：System.ArgumentNullException

  パラメーター名：enumStr [LD1315]
- 複数の Active Directory セキュリティグループが表示を制限するように構成されると、起動時間が長くなることがあります。[LD1368]
- VDA を再起動した後の最初の接続で、［セッション画面の保持のタイムアウト］ポリシーが適用されないことがあります。ただし、その後の接続にポリシーを適用しようとするとうまくいく場合があります。[LD1397]
- Winlogon.exe プロセスが予期せず終了すると、サーバー OS 用の VDA が応答しなくなることがあります。[LD1480]

- Enlightened Data Transport(EDT)が有効な場合、VDA はバグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_ (0x1000007E)** により予期せず終了することがあります。この問題は、Zscaler 経由で外部からユーザーセッションにアクセスすると発生します。[LD1493]
- Citrix Studio などの特定のレガシアプリケーションは、クライアント側の解像度が変更されるとシームレスセッションで正しく再描画されないことがあります。[LD1554]
- セッションに再接続すると、ユーザーデバイスのシステムトレイに VDA 通知アイコンが表示されなくなることがあります。[LD1629]
- XenApp および XenDesktop 7.15 LTSR 累積更新プログラム（CU）2 を CU3 にアップグレード後、公開デスクトップセッションで一部の.Net アプリケーションが応答しなくなることがあります。この問題は、Windows Server 2008 R2 上の VDA で発生します。[LD1726]
- ユーザーセッション内で視覚効果を変更すると、レジストリキー HKEY_CURRENT_USER\Control Panel\Desktop の値`UserPreferencesMask`が新しい値に更新されないことがあります。[LD1827]

  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。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  名前：HookProcess

  種類：REG_DWORD

  データ：1
- Microsoft Windows オペレーティングシステムの日本語バージョンでは、［デバイスマネージャー］のデバイスの説明が破損している可能性があります。[LD1834]
- アクセス違反により、wfshell.exe プロセスが予期せず終了する場合があります。その結果、アプリケーションの起動に失敗します。[LD2050]

システムの例外

- 位置情報 API を実装する Web アプリケーションを実行すると、Internet Explorer（iexplore.exe）プロセスが予期せず終了する場合があります。[LD0677]
- AMD Opteron（TM）プロセッサ 6128 HE を搭載したマシンで Citrix ソフトウェアグラフィックプロセス（Ctxgfx.exe）が予期せず終了する場合があります。[LD0954]
- Microsoft Internet Explorer が予期せず終了する場合があります。この問題は、icaendpoint.dll モジュールに障害がある場合に発生します。[LD1266]
- VDA で wfshell.exe プロセスが、予期せずに終了する場合があります。この問題は、CtxUiMon.dll モジュールに障害がある場合に発生します。[LD1359]
- XenApp および XenDesktop 7.15 LTSR が実行されている VDA では、ctxdvcs.sys で重大な例外が発生し、バグチェックコード 0x0000007E によりブルースクリーンが表示される場合があります。[LD1688]

- VDA で wfshell.exe プロセスが、予期せずに終了する場合があります。[LD1847]
- wfshell.exe プロセスが予期せず終了すると、アプリケーションの起動に失敗することがあります。この問題は、cmpcom.dll モジュールに障害がある場合に発生します。[LD2107]

ユーザーエクスペリエンス

- マウスの左ボタンを使用してタスクバーのボリュームコントロールをクリックすると、ボリュームコントロールを開けない場合があります。この問題は、英語版以外の Microsoft Windows オペレーティングシステムで発生します。[LD0039]

ユーザーインターフェイス

- 資格情報を手動で入力する必要があるときに、ログオンウィンドウが前面に表示されないことがあります。[LC9861]
- 公開アプリケーションのコンテキストメニューを右クリックしたときに、カーソルのある場所にメニューが開かないことがあります。[LD1243]
- Surface Pro デバイスで VDA セッションを起動し、［ペンと **Windows** インク］ページで ［手書きパネルで指先を使って書く］機能を有効にすると、問題が発生する場合があります。入力したテキストまたはイメージのフォントサイズが、マウスを使用して入力したサイズより大きくなることがあります。[LD1472]

仮想デスクトップコンポーネント **-** その他

- Internet Explorer の公開インスタンスでアプリケーションを取得すると、アプリケーション名の不一致が起きることがあります。その結果、同じマシンに接続している別のユーザーに対して、同じアプリケーション名が表示されます。[LD0351]
- ユーザープリンシパル名（UPN）（user@domain）を使用してセッションにログオンすると、問題が発生することがあります。画面をロックすると、ロックされたデスクトップ上で UPN（ユーザー @ ドメイン）ではなく SAM アカウント（ドメイン\ユーザー名）が表示されます。[LD1141]
- VDA でセッションを開始しようとすると失敗する場合があります。[LD1180]
- Citrix Broker Service は、イベントログに次のエラーを報告することがあります：

  Citrix Broker Service で、マシン’machine_name’ の Virtual Desktop Agent に必要な基本設定を特定できません。

  例外：System.ArgumentNullException

  パラメーター名：enumStr [LD1315]
- System Center Virtual Machine Manager をテンプレートとして作成した VM を使用してカタログを作成しようとすると、失敗することがあります。この問題は、VM に Windows 10 バージョン 1803 以降がインストールされていて、VM でセキュアブートが有効になっている場合に発生します。[LD1608]

- VDA が提供するイベントログデータと比較すると、Citrix Director が記録するログオン期間がずれている場合があります。[LD1679]
- Broker Agent は、持続的なデータの場所に.gpf ファイルを書き込みません。[LD1691]
- VDA に展開された App-V パッケージが、誤って VDA から削除される可能性があります。そのため、この修正では HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features にレジストリキーが導入され、このキーで、クリーンアップを有効にするか無効にするかを制御できます。デフォルトでは、クリーンアップは無効になっています。[LD2025]

  有効にするには、次のレジストリキーを追加します:

  HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

  名前：RedundantPackageCleanup

  種類：REG_SZ

  データ：True

累積更新プログラム 4（CU4）

September 16, 2021

リリース日：2019 年 4 月 23 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 4（CU4）では、7.15 LTSR CU3 リリース以降に報告された 140 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU3 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU4 をダウンロード

この累積更新プログラムの新機能

- Delivery Controllers およびサイトを 7.15 CU4 にアップグレードする場合は、実際のアップグレードが開始される前に事前サイトテストが実行されます。そのテストには、不可欠な Citrix サービスが適切に実行されていること、およびサイトデータベースが正しく動作していて最近バックアップが行われていることの確認が含まれています。このテストが実行されると、レポートを表示できます。検出された問題を修正し、必要に応じてテストを再実行できます。このテストは、アップグレードを正常に続行するのに役立ちます。
- このリリースでは、Citrix Studio とそのコンポーネントのスタンドアロンでの展開における PowerShell バージョン 2.0 への依存関係が削除されています。

> 注:
> PowerShell のバージョンは、そのコンポーネントの 1 つまたは複数をインストールするマシンには引き続き必要ですが、バージョン 2.0 については不要になりました。Delivery Controller サーバーと StoreFront サーバーでは、PowerShell 2.0 が引き続き必要です。詳しくは、[LD0184] を参照してください。

- VDA または Delivery Controller のインストールに失敗すると、MSI アナライザーはエラーのある MSI ログを解析し、正確なエラーコードを表示します。このアナライザーは、既知の問題であった場合は、CTX 記事を示します。アナライザーはまた、故障エラーコードに関する匿名化データも収集します。このデータは、CEIP によって収集された他のデータに含まれます。CEIP への登録を終了すると、収集された MSI アナライザーのデータは Citrix に送信されなくなります。

新しい展開環境

新しく CU4 を展開するには

CU4 Metainstaller を使用して、CU4 に基づく新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU4 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：展開環境のすべての LTSR コンポーネントを CU4 に更新することをお勧めします。例：Provisioning Services が LTSR 展開環境に含まれる場合、Provisioning Services コンポーネントを CU4 に更新します。Provisioning Services が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU4** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.4000	
VDA for Server OS	7.15.4000	
Citrix Studio	7.15.4000	
Citrix Director	7.15.4000	
Delivery Controller	7.15.4000	
フェデレーション認証サービス	7.15.4000	
グループポリシー管理のエクスペリエンス	3.1.4000	
Linux VDA	7.15.4000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.4000	
Provisioning Services	7.15.15	
Session Recording	7.15.4000	Platinum Edition のみ
StoreFront	3.12.4000	
ユニバーサルプリントサーバー	7.15.4000	

XenApp および **XenDesktop 7.15 LTSR CU4** の互換性のあるコンポーネント

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

7.15 LTSR CU4 の互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	1903
* ブラウザーコンテンツのリダイレクト	15.15
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13

7.15 LTSR CU4 の互換性のあるコンポーネントおよびプラットフォーム	バージョン
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.3000
ライセンスサーバー	11.15.0.0 ビルド 26000
セルフサービスパスワードリセット	1.1.10.0
Workspace Environment Management	1811

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

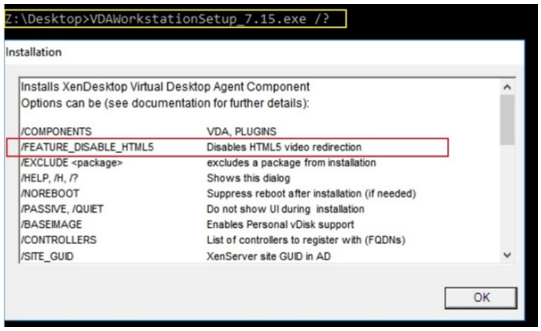
システム要件:

これらの要件は、XenApp および XenDesktop 7.15 LTSR CU4 の BCR.msi に特化したものです。XenApp、XenDesktop のその他のバージョン、Citrix Virtual Apps and Desktops で使用されているブラウザーコンテンツリダイレクトのシステム要件は含まれません。

- Delivery Controller および VDA の両方にバージョン 7.15 LTSR CU4。
- Windows 向け Citrix Workspace アプリ 1809 以降。
- BCR.msi - シトリックスのダウンロードページからダウンロードできます。
- Chrome（Web ブラウザーコンテンツのリダイレクト拡張機能を Chrome ウェブストアからインストール）または Internet Explorer 11（Browser Helper Object（BHO）の Citrix HDXJsInjector を有効化）。

インストール:

1. コマンドライン「/FEATURE_DISABLE_HTML5」オプションを使用して、VDA にバージョン 7.15 LTSR CU4 をインストールまたはアップグレードします。



このオプションは HTML5 ビデオリダイレクション機能を削除するため、BCR.msi の実行前に完了する必要があります。BCR.msi は、インストール中にこの機能を再度追加し、ブラウザーコンテンツリダイレクトサービスも追加します。この手順が完了したら、services.msc コンソールを開き、**Citrix HDX HTML5 Video Redirection Service** が表示されていないことを確認します。

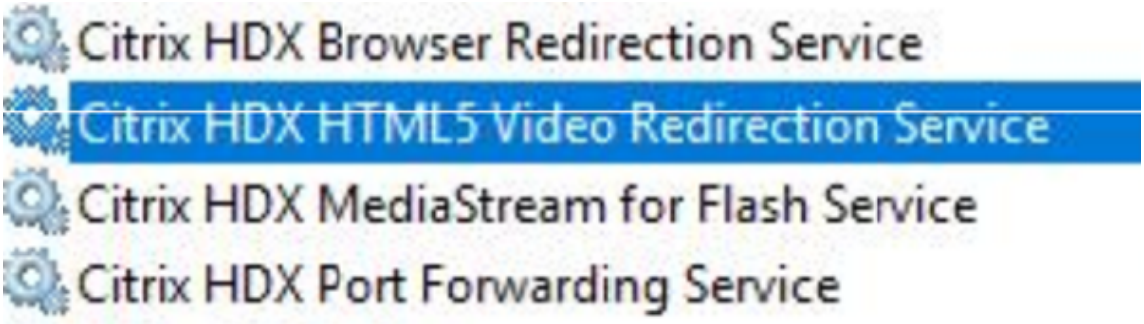
2. BCR.msi でブラウザーコンテンツリダイレクトサービスのインストールを開始します。システムに応じて、BCR.msi のファイルは次の場所にインストールされます:

   C:\Program Files\Citrix\ICAService

   または

   C:\Program Files(86)\Citrix\ICAService

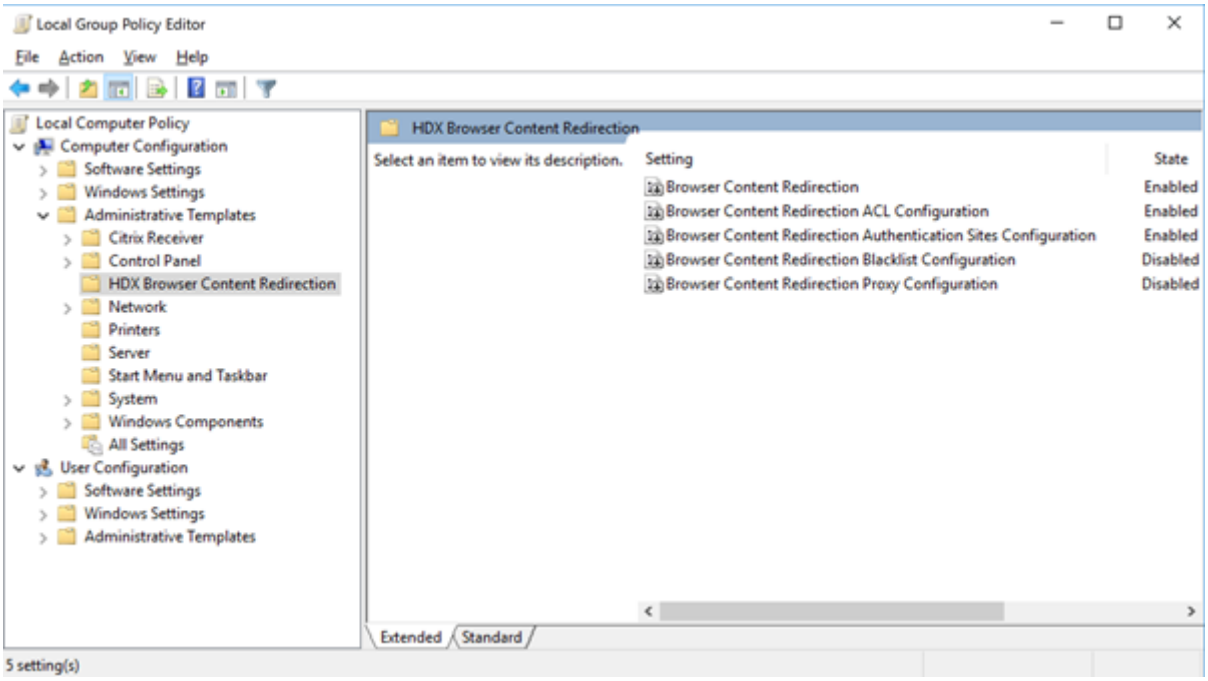
   インストールが高速であるため、ダイアログボックスがすぐに閉じることがあります。この場合、services.msc に戻ってサービスが追加されたことを確認します。



ポリシー:

VDA で HKEY_LOCAL_MACHINE レジストリを使用して、またはグループポリシー管理コンソールで Citrix 管理テンプレートの **HDX Browser Content Redirection** を使用してポリシーを制御できます。

Citrix Virtual Apps and Desktops（XenApp および XenDesktop）、XenApp 7.15 LTSR または XenDesktop 7.15 LTSR、コンポーネント の順に移動し、citrix.comダウンロードページからテンプレートをダウンロードできます。Citrix Studio にはこれらのポリシーは含まれません。



ポリシー情報について詳しくは、「Web ブラウザーコンテンツのリダイレクトのポリシー設定」を参照してください。トラブルシューティングについて詳しくは、Knowledge Center のCTX230052を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU4 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーションと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU4 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します：

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU4 インストーラーを実行します。これにより、新しいサイトで使用する新しい Virtual Delivery Agent for Server OS に自動アップグレードされます。
- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。
- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU4 サイトにインポートできます：一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU4 Controller 上で PowerShell インポートコマンドレットを実行して、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- Citrix Director で ［フィルター］ > ［セッション］に移動すると、セッションデータの代わりにチェックボックスが表示されます。[LC9871]
- Citrix Director が Delivery Controller バージョン 7.6 に接続されている場合、カスタム管理者が VDA バージョン 7.15 からセッションの詳細を取得できないことがあります。[LD0134]
- NetScaler Management and Analytics System（MAS） と Citrix Director との統合が失敗することがあります。この問題は、グループポリシーが組み込みの管理者アカウントを変更するか名前を変更した場合に発生します。Director はローカルの管理者アカウントを使用して **C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml** を暗号化、または暗号化解除するためです。この修正により、コードで変更が行われた時に問題も解決されます。変更後、**C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml** の暗号化、または暗号化解除には、Director がインストールされているマシンのマシンアカウントが使用されます。[LD0231]
- オペレーティングシステムで夏時間（Daylight Saving Time：DST）がオンになっています。前の月のエクスポートレポートを生成するために、CSV 形式を選択してデータをエクスポートしようとすると、2 つのラジオボタン ［グラフデータのエクスポート］と ［テーブルデータのエクスポート］が表示されないことがあります。[LD0569]
- ［傾向］ > ［リソース使用率］ > ［サーバー **OS** マシン］に移動し、スクロールバーを操作してマシンの完全な一覧を表示しようとすると、いくつかのテーブルレコードだけが表示されます。残りのレコードが表示されません。スクロールバーが正しく機能しないときに、この問題が発生します。[LD0789]
- Director で接続に関するカスタムレポートを作成するとき、セッションエラー時間（Session.FailureDate）やセッション変更時間（Session.ConnectionStateChangeDate）などのいくつかの DateTime フィールドが、UTC からローカル時間に変換されないことがあります。[LD1001]
- Citrix Director でユーザーを検索するときにそのユーザー名が長いと、名前が切り捨てられることがあります。[LD1106]

Citrix ポリシー

- グループポリシー管理コンソール（Group Policy Management Console：GPMC、gpmc.msc）を使用して Citrix ポリシー設定を含むグループポリシーオブジェクト（Group Policy Object：GPO）をコピーしようとすると、失敗することがあります。Microsoft 管理コンソール（MMC）は予期せず終了します。[LD0322]
- Citrix ユニバーサルプリンターオブジェクトは、ユニバーサルプリンタードライバーの環境設定を［**XPS**］または［ネイティブドライバー］に設定した場合でも、セッション内の EMF ユニバーサルプリンタードライバーで作成されます。この修正を有効にするには、Citrix Receiver for Windows 4.9.5000 LTSR 累積更新プログラム 5（CU5）以降をインストールしてください。[LD0360]
- Citrix Studio でポリシーを変更すると、このエラーメッセージが［構成ログ］に表示されることがあります。

  ポリシー変更の詳細を判別するときにエラーが発生しました。

  このエラーメッセージが表示されると、［構成ログ］でポリシー変更の詳細を確認できません。[LD0596]
- 多数のサイトポリシーが構成されていて、そのポリシーに IP ベースまたは OU ベースのフィルターが設定されている場合、ログオンプロセスに遅延が生じることがあります。[LD0221]

Citrix Studio

- このリリースでは、Citrix Studio とそのコンポーネントのスタンドアロンでの展開における PowerShell バージョン 2.0 への依存関係が削除されています。

> 注:
> PowerShell のバージョンは、そのコンポーネントの 1 つまたは複数をインストールするマシンには引き続き必要ですが、バージョン 2.0 については不要になりました。Delivery Controller サーバーと StoreFront サーバーでは、PowerShell 2.0 が引き続き必要です。Windows 7 または Windows Server 2008 R2 システムでは、Citrix Studio などの Controller コンポーネントをインストールするマシンに、PowerShell バージョン 3.0 以降が必要です。[LD0184]

- 1 つのサイトに複数の App-V パッケージ追加すると、Studio で次のエラーメッセージが表示されることがあり、管理者は新しいアプリケーションを公開できません：

  サーバーとの通信に問題がありました。
  Get-AppLibAppVPackage：受信メッセージの最大メッセージサイズクォータ（**41943040**）を超えました。[LD0232]
- 別のドメインサーバーに作成されたターゲットデバイス用のマシンカタログを作成すると、ターゲットデバイスが認識されないことがあります。[LD0319]
- Citrix ユニバーサルプリンターオブジェクトは、ユニバーサルプリンタードライバーの環境設定を［**XPS**］または［ネイティブドライバー］に設定した場合でも、セッション内の EMF ユニバーサルプリンタードライバーで作成されます。この修正を有効にするには、Citrix Receiver for Windows 4.9.5000 LTSR 累積更新プログラム 5（CU5）以降をインストールしてください。[LD0360]

- アプリケーションプロパティでアプリケーションの名前を変更し、Citrix Studio のアプリケーションからデリバリーグループを削除しようとすると、次のエラーメッセージが表示されます:

  オブジェクトは存在しません。

  この問題は、アプリケーション名を変更した後に、アプリケーションプロパティ **ApplicationNameWithFolder** で新しい名前に置き換えることなく、古い名前を使用する場合に発生します。[LD0594]

- [マシンの追加] ウィザードで、1 つまたは複数のマシンを既存のデリバリーグループまたは新しいデリバリーグループに追加すると、次のエラーが返されることがあります:

  マシンは既に割り当てられています。

  このメッセージは、[戻る] ボタンをクリックして、少なくとも 1 回最初のウィザード画面に戻った場合にのみ表示されます。[LD0924]

- デリバリーグループ内の他のカタログのマシンを表示できないことがあります。この問題は、[マシンの追加] ウィザードで新しいデリバリーグループまたは既存のデリバリーグループにマシンを追加すると発生します。[LD0988]

- この修正により、マシンカタログを作成する際に、一時データのキャッシュ、[キャッシュに割り当てられたメモリ (MB):]、および [ディスクキャッシュサイズ (GB):] がデフォルトで無効になります。[LD1120]

コントローラー

- デリバリーグループ用に構成されているマルチタイプのライセンスシナリオで、デリバリーグループ用に構成されていない不正なライセンスの種類がチェックアウトされることがあります。[LC9086]

- このリリースでは、Citrix Studio とそのコンポーネントのスタンドアロンでの展開における PowerShell バージョン 2.0 への依存関係が削除されています。

> 注:
> PowerShell のバージョンは、そのコンポーネントの 1 つまたは複数をインストールするマシンには引き続き必要ですが、バージョン 2.0 については不要になりました。Delivery Controller サーバーと StoreFront サーバーでは、PowerShell 2.0 が引き続き必要です。Windows 7 または Windows Server 2008 R2 システムでは、Citrix Studio などの Controller コンポーネントをインストールするマシンに、PowerShell バージョン 3.0 以降が必要です。[LD0184]

- デリバリーグループに少なくとも 1 つのドレインモードの VDA が含まれている場合、公開アプリケーションを起動する場合にそのデリバリーグループが選択されないことがあります。[LD0194]

- 1 つのサイトに複数の App-V パッケージ追加すると、Studio で次のエラーメッセージが表示されることがあり、管理者は新しいアプリケーションを公開できません:

  サーバーとの通信に問題がありました。
  Get-AppLibAppVPackage: 受信メッセージの最大メッセージサイズクォータ (**41943040**) を超えました。 [LD0232]

- PowerShell コマンド **get-brokericon -filename** を**-servername** パラメーターを指定して実行すると、エラーメッセージが返されます。[LD0324]
- Citrix Virtual Apps の公開アプリケーションが断続的に列挙されないことがあります。その結果、セッションが開始された後またはアプリケーションの起動に失敗した後に、空白の画面が表示されます。SQL サーバーで CPU 使用率が高くなったり、SQL モニターでブロックされたプロセスや高価なプロセスが表示されることがあります。[LD0336]
- Citrix ユニバーサルプリンターオブジェクトは、ユニバーサルプリンタードライバーの環境設定を［**XPS**］または［ネイティブドライバー］に設定した場合でも、セッション内の EMF ユニバーサルプリンタードライバーで作成されます。この修正を有効にするには、Citrix Receiver for Windows 4.9.5000 LTSR 累積更新プログラム 5（CU5）以降をインストールしてください。[LD0360]
- Citrix Director のリソース使用率データが正しい順序で並べ替えられない場合があります。この問題は、SQL 文が間違った順序で表示される場合に発生します。[LD0388]
- セッションを開始すると、以前に開始された VDA よりも新しく作成された VDA がブローカーによって選択されることがあります。この選択により、ログオン時間が長くなることがあります。VM がセッション要求を受信する前に、選択した VM が起動後の操作を完了しないとログオン時間が長くなります。[LD0511]
- アプリケーションプロパティでアプリケーションの名前を変更し、Citrix Studio のアプリケーションからデリバリーグループを削除しようとすると、次のエラーメッセージが表示されます:

  オブジェクトは存在しません。

  この問題は、アプリケーション名を変更した後に、アプリケーションプロパティ **ApplicationNameWithFolder** で新しい名前に置き換えることなく、古い名前を使用する場合に発生します。[LD0594]
- Citrix Studio でポリシーを変更すると、このエラーメッセージが［構成ログ］に表示されることがあります。

  ポリシー変更の詳細を判別するときにエラーが発生しました。
- このエラーメッセージが表示されると、［構成ログ］でポリシー変更の詳細を確認できません。[LD0596]
- **MonitorData.Session** テーブルでセッションの **FailureDate** 列が **Null** に設定されると、Citrix Director が誤ったユーザー接続エラーを表示することがあります。その結果、**MonitorData.ConnectionFailureLog** テーブルでエラーの種類が更新されません。監視データベースから取得された接続エラー値と、サイトデータベースから取得された **Get-BrokerConnectionLog** の出力値が一致しません。[LD0726]
- .vhd 拡張子が大文字の場合（.VHD）、VHD ピッカーがそのファイルを有効な VHD イメージとして検出しないことがあります。Azure 環境で Machine Creation Services カタログを作成すると、問題が発生します。[LD0746]
- ID ディスクが Amazon Web Services（AWS）の Machine Creation Services（MCS）から削除されることがあります。[LD1043]
- 該当する製品リリースを使用しており、VMware 環境で NSX-T ネットワークを有効にしている場合、管理者が Studio でホスト接続を作成できないことがあります。MCS で NSX-T の不透明ネットワークが列挙されて

いない場合に、この問題が発生します。[LD1102]

- HDX 接続のログオンデータが［ログオン期間］グラフに表示されないことがあります。[LD1113]
- `CreateNewInstanceOnReset`は使用停止になり、機能しなくなりました。VM は、電源の再投入時またはマシンカタログの更新時に常に保持されます。[LD1114]
- Amazon Web Services（AWS）の使用中にマシンを再起動すると、数分の遅れが発生することがあります。[LD1220]
- Citrix Monitor Service はかなりの量のメモリを消費することがあります。その結果、Delivery Controller が応答しなくなり、Director からの通話要求がタイムアウトします。[LD1370]

HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 7.15 LTSR CU4 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU4 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Personalization for App-V

Studio

- アプリケーション名が英語以外の言語の場合、App-V パッケージから不正なアプリケーションが起動することがあります。[LD0222]

VDA

- アプリケーション名が英語以外の言語の場合、App-V パッケージから不正なアプリケーションが起動することがあります。[LD0222]

Profile Management

- 2 度目の Citrix Virtual Apps サーバーへのログオンで、ユーザープロファイルが破損します。この問題は、プロファイルがシステムで使用されていることで、ログオフ時に Profile Management がプロファイルを削除できない場合に発生します。Profile Management サービスを再起動してプロファイルを削除します。[LD0560]

- **CopyFileWithRetries** 関数がディレクトリの 1 つのファイルをコピーできない場合、残ったファイルもコピーされないことがあります。この問題は、Citrix Profile Management サービスがデフォルトのテンプレートプロファイルディレクトリから現在のユーザーのプロファイルディレクトリにファイルをコピーしようとするときに発生します。コピー処理中に、権限の制限によって現在のディレクトリにある 1 つのファイルをコピーできない場合、対応する関数 **CopyDirectory** はコピー操作を終了します。その結果、他のファイルはコピーされません。[LD0648]
- VDA for Server OS は Microsoft Windows 10 バージョン 1709 以降で実行されています。Profile Management ポリシーの同期用に *.tmp ファイルを除外することを選択した場合、Word ファイルや PowerPoint ファイルなどの Microsoft Office ドキュメントに対する変更は、ログアウト中に保存されないことがあります。ログオンしてファイルを再度開くと、変更内容は保持されません。[LD0782]
- AppData（Roaming）フォルダーのリダイレクトが、Microsoft Windows 10 で実行されている Profile Management で機能しないことがあります。この問題は、AppData（Roaming）フォルダーがあらかじめファイル格納フォルダーに存在しない場合に発生します。[LD0797]

Provisioning Services

Provisioning Services 7.15 LTSR CU4は、このリリースの更新に関する特定の情報を提供します。

Session Recording

管理

- Session Recording を使用する場合、スケーラビリティとパフォーマンスの問題が発生する可能性があります。[LD0970]
- Session Recording をバージョン 7.15 からバージョン 7.15 累積更新プログラム 2（CU2）にアップグレードしようとすると、長時間かかることがあります。[LD1042]

エージェント

- フランス語およびスペイン語版の Microsoft Windows オペレーティングシステムに Session Recording Agent バージョン 7.15 CU3 をインストールしようとすると失敗することがあります。[LD1161]

プレーヤー

- 切断されたセッションに再接続すると、Session Recording Player にはセッションの実行可能ファイルへのアプリケーションの完全パスが表示されます。Session Recording Player では、セッションの公開アプリケーション名が表示される必要があります。[LD0426]
- Session Recording Player バージョン 7.15 CU2 では、Session Recording Player がアプリケーションとして起動されると、録画ファイルの再生に失敗し、応答を停止することがあります。[LD0578]

StoreFront

- アンダースコア（_）を含むベース URL を使用して StoreFront を構成し、それを Citrix Gateway で使用すると、エラーが発生することがあります。[LC9678]
- StoreFront にログオンして Citrix Receiver for Web ページを更新すると、タイムアウトのダイアログボックスが表示されないことがあります。[LD0214]
- StoreFront にログオンしようとすると、［要求を完了できません］エラーで失敗することがあります。この問題は、TCP 動的ポートを使い果たしている場合に発生します。[LD0573]
- StoreFront のバージョンを 3.5 から 3.12 にアップグレードした後、次のイベントログの詳細がイベントビューアに表示されることがあります:

  ユーザー名とパスワードの認証が **StoreFront** で有効になっていません。
  Citrix.DeliveryServicesClients.Authentication.Exceptions.ProtocolNotAvailableException, Citrix.DeliveryServicesClients.Authentication, Version=3.12.0.0, Culture=neutral, PublicKeyToken=null Invalid protocol exception. The requested protocol is: ExplicitForms Protocol: ExplicitForms at Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.CreateExpli
  [LD0608]
- 利用可能なアプリケーションやデスクトップが表示されていても、［現在、使用可能なアプリケーションやデスクトップはありません］というメッセージが表示されたままになります。[LD0857]
- Safari 12 以降のブラウザーを使用すると、Citrix Receiver for Web でクライアント検出が失敗することがあります。これは、Netscape Plugin Application Programming Interface（NPAPI）のサポートが廃止されたためです。詳しくは、Knowledge Center のCTX238286の記事を参照してください。[LD0863]
- ストアにある default.ica ファイルの各アプリケーションのセクションに **ConnectionBar=0** プロパティを追加すると、指定したデリバリーグループの **Desktop Viewer** ツールバーが無効になります。セッションを切断してから再接続すると、**Desktop Viewer** ツールバーが再び表示されます。[LD1051]
- StoreFront 管理コンソールで、［複数の **STA** サーバーを負荷分散する］オプションが選択されている場合にのみ、Secure Ticket Authorities（STA）の順序を変更できます。［複数の **STA** サーバーを負荷分散する］が選択されていない場合にのみ STA の順序を変更できるようにするには、この論理を逆にする必要があります。[LD1118]
- デフォルトの Web サイト設定が、オンプレミスの複数サーバーグループの他のノードに正しく表示されないことがあります。その結果、Web ブラウザーが正しい URL ではなく、そのノードの HTTP URL に転送されます。[LD1119]
- この修正により、セキュリティ上の脆弱性に関する問題が解決されます。詳しくは、Knowledge Center の記事CTX251988を参照してください。[LD1361]

ユニバーサルプリントサーバー

クライアント

- ドキュメントを印刷する前に、公開デスクトップセッションの印刷ダイアログボックスで使用可能なプリンターの一覧からプリンターを選択します。プリンターがドキュメントの印刷を開始するときに、遅延が発生することがあります。[LC9601]
- 印刷スプーラーサービスが異常終了することがあります。この問題は、**CRawStreamHeaderWriter::EndPage** と **CRawStreamHeaderWriter::StartPage** がヌルオブジェクトにアクセスしようとしたときに発生します。[LC7893]
- VDA のインストール後、プリンタープロパティのプリンターポートが、マップされたネットワークプリンターに表示されなくなることがあります。[LD0949]

サーバー

- アクセス違反のため、ユニバーサルプリントサーバー（UPServer.exe）が予期せず終了し、イベント ID 7031 を生成することがあります。[LC7821]
- **CPTStream::ThisStream** のアクセス違反により、印刷スプーラーサービスが応答しなくなることがあります。[LC8856]
- 多くの Active Directory グループのメンバーになっているユーザーは、ユニバーサルプリントサーバーから自分のプリンターに接続できないことがあります。[LC8714]
- Citrix ユニバーサルプリンタードライバーの、ホチキス留めや給紙方法などの詳細なプリンター機能のメニューが、空白で表示されることがあります。[LC9711]

VDA for Desktop OS

HDX RealTime Windows Media リダイレクト

- HDX Web カメラにアクセスしようとすると、Citrix HDX RealTime Media Engine が予期せず終了することがあります。[LD0062]
- **HDX MediaStream Windows Media** リダイレクト設定が無効な場合、Windows Media Player で特定のビデオファイル形式を開こうとすると、以下のメッセージが表示されることがあります：

  ファイルの再生中に **Windows Media Player** に問題が発生しました。

  ただし、一部のビデオファイル形式の場合は、ビデオの縦横比が正しくありません。[LD0279]

キーボード

- ユーザーセッションで中国語のキーボードレイアウトを使用すると、Input Method Editor（IME）が自動的に五筆字型入力方法（Wubi）に変更されます。この問題は、デフォルトの IME が **Wubi** に設定されていない

場合に発生します。[LD0429]

印刷

- XenApp および XenDesktop をバージョン 7.9 からバージョン 7.15 にアップグレードすると、ドキュメントを別のプリントレイに出力できない場合があります。印刷ダイアログから別のトレイを選択した場合でも、印刷ジョブはデフォルトのトレイにドキュメントを出力します。[LC9247]
- PDF を生データ形式で印刷キューに送信すると、PDF が印刷されないことがあります。[LC9755]
- ページを印刷しようとすると、印刷設定ウィンドウが正しく表示されないことがあります。この問題は、印刷設定ウィンドウに翻訳の問題がある場合に発生します。その結果、**Citrix** アイコンと ［ローカルプリンター設定］ボタン名は切り捨てられます。[LD0359]
- デフォルトのプリンターが Citrix のマップされたプリンターである場合、Microsoft Windows Server 2016 はレジストリキー **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device** の値を更新できません。この失敗が原因で、.NET 以外のアプリケーションではデフォルトプリンターが設定されていないことがあります。[LD1032]

セッション/接続

- 一部のサードパーティ製アプリケーションでは、Shift+F2 キーを使用してセッションをウィンドウモードに切り替えてからシームレスモードに戻すまで、シームレスセッションで応答しなくなることがあります。[LC9727]
- 公開アプリケーションを最大化すると、タスクバーのセクション上部に重なることがあります。[LD0025]
- デリバリーグループで ［**Secure ICA** を有効にする］設定を有効にした場合、レジストリキー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Security に **DHParaml** 値が存在しないと、アプリケーションの起動に失敗することがあります。このエラーメッセージが表示されます:

  アプリケーションを起動できません。ヘルプデスクに連絡して、次のエラー情報を提供してください:
  Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to “VOA Win 7 LTSR” failed with status (Unknown client error).[LD0117]
- ユーザーデバイスからクレジットカードのトランザクションを処理すると、アプリケーションとユーザーデバイスが応答しなくなったり、データのサブセットのみが受信されることがあります。[LD0152]
- ランダムにサーバーからアプリケーションを起動しようとすると失敗することがあります。このエラーメッセージが表示されます:

  アプリケーションを起動できません。**Citrix XenApp** サーバーに接続できません。選択した **Citrix SSL** サーバーは、接続を受け入れていません。

  サーバーが SSL を有効にした VDA で接続の受け入れを停止すると、この問題が発生します。[LD0239]

- この修正プログラムは、「クライアントドライブに自動接続する」ポリシーが無効になっている場合に起きるメモリリークの問題を解決します。[LD0370]
- TWI モジュール（twi3.dll）のスレッドを終了する関数によって、サーバーが応答しなくなる可能性があります。[LD0406]
- ローカルアプリアクセスが有効な場合、Microsoft Windows 10 バージョン 1803 の公開デスクトップでアプリケーションを開こうとすると、アプリケーションを最小化できません。[LD0411]
- 特定のサードパーティのアプリケーションを使用するときに、数分間ユーザーデバイスセッションが応答を停止することがあります。[LD0419]
- Internet Explorer、Chrome、または Firefox ブラウザーで Google アカウントメールを開き、新しいメールを作成しようとすると、［キーボードの自動表示］が機能しないことがあります。[LD0470]
- シームレスモードのアプリケーションが、アプリケーションのサイズを最大化からウィンドウ化、またはウィンドウ化から最大化に変更すると、応答しなくなることがあります。[LD0498]
- scardhook64.dll によって例外 X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL が発生すると、ターゲットデバイスが予期せず再起動することがあります。[LD0504]
- **AutoLogon** の値をゼロ（0）以外に設定して Citrix 診断ファシリティ（CDF）トレースを実行すると、セッションへの再接続に失敗することがあります。[LD0602]
- 公開アプリケーションのウィンドウの一部が更新されないことがあります。この問題は、バックグラウンドで実行されている Citrix 公開アプリケーションのいずれかがフォアグラウンドに表示された場合に発生する可能性があります。[LD0711]
- 公開デスクトップの特定のサードパーティ録音アプリケーションを再生すると、Internet Explorer が予期せず終了することがあります。[LD0830]
- この修正により、CtxUvi Hooking ドライバーが安全なプロセスに MfApHook.dll を読み込まなくなります。[LD0847]
- 場所 API からの応答を待っている間、公開アプリケーションがブロックされることがあります。

  タイムアウト値を構成して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：

  - *32* ビットシステムの場合

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    名前：LatlongWaitTime

    種類：REG_DWORD

    値：ミリ秒デフォルト値は 60000 ミリ秒です。この値は、場所情報の取得に使用できる待ち時間です。

  - *64* ビットシステムの場合

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

    名前：LatlongWaitTime

種類：REG_DWORD

値：ミリ秒デフォルト値は 60000 ミリ秒です。この値は、場所情報の取得に使用できる待ち時間です。[LD0905]

- この修正により、CtxUvi ドライバーが Citrix dll の読み込みから vmsp.exe プロセスを除外することがあります。詳しくは、Knowledge Center の記事CTX107825を参照してください。[LD1024]
- ユーザーセッションの他のユーザーが同じタイミングで同じアクションを ［許可しない］に設定している場合に、ローカルコンソールで Ctrl+Alt+Delete キーを繰り返し押すと、問題が発生することがあります。新しいローカルコンソール画面が 30 秒間表示されることがあります。その結果、コンソール上のコンテンツが、同じセッションの別の仮想画面のように見えます。[LD1077]

システムの例外

- ターゲットデバイスをバージョン 7.6 からバージョン 7.15 にアップグレードすると、Internet Explorer、Windows Media Player、テーマサービスが予期せず終了することがあります。[LC9872]
- VM Hosted App を起動すると、mmvdhost.exe プロセスが予期せず終了することがあります。[LC9976]
- VDA で wdica.sys の重大な例外が発生し、バグチェックコード 0x3b (SYSTEM_SERVICE_EXCEPTION) によるブルースクリーンが表示されることがあります。[LD0089]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x22 によるブルースクリーンが表示されることがあります。[LD0119]
- アクセス違反により、VDA で重大な例外が発生し、ブルースクリーンが表示されることがあります。[LD0281]
- VDA で vd3dk.sys の重大な例外が発生し、ブルースクリーンが表示されることがあります。[LD0368]
- 例外 **DivideByZeroException** によって、VDA で wfshell.exe プロセスが予期せず終了することがあります。このプロセスには、「**wfshellshell** が動作を停止しました。」というエラーメッセージが表示されます。[LD0373]
- VDA で wdica.sys の重大な例外が発生し、バグチェックコード 0x50 によるブルースクリーンが表示されることがあります。[LD0410]
- LIST_ENTRY の破損によって VDA で CtxUVI.sys の致命的な例外が発生し、ブルースクリーンエラーが発生することがあります。[LD0421]
- 公開された Internet Explorer のインスタンスで長い URL にアクセスしようとすると、wfshell.exe プロセスが予期せず終了することがあります。[LD0454]
- Null ポインターによって、VDA にログオンすると mmvdhost.exe プロセスが予期せず終了することがあります。[LD0474]
- Internet Explorer（iexplore.exe）プロセスが例外コード **0xc00001a5** で予期せず終了することがあります。この問題は、障害がある CtxSensVcLibDll.dll モジュールのアンロードで発生します。[LD0485]

- デスクトップ OS 用の VDA でビデオクリップをエクスポートしようとすると、サードパーティのアプリケーションが予期せず終了することがあります。[LD0506]

ユーザーエクスペリエンス

- Microsoft Windows バージョン 10 クライアントで、DPI スケーリングが 100 に設定されたクライアントの高解像度モニターのスケーリングが大きくなる場合があります。[LD0131]
- アイテムの上にマウスポインターを置くと、ツールチップのポップアップが消え、アプリケーションがフォーカスを失うことがあります。[LD0365]
- セッションに再接続すると、ユーザーデバイスのシステムトレイに無損失インジケーターアイコンが表示されなくなります。この問題に対応するには、以下のレジストリキーを設定する必要があります [LD0919]:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator\Interval
種類：DWORD
値：3（デフォルト：0）

ユーザーインターフェイス

- 切断されたセッションに再接続しようとしているときに、VM Hosted App を起動すると、最後にクリックされたアプリケーション以外の、そのセッションに存在するすべてのアプリケーションが表示されます。[LD0189]
- 修正 LD0419 を適用しました。カーソル名を変更せずにアプリケーションでカーソル形状を変更しようとしても、カーソル形状が変更されないことがあります。[LD0983]

VDA for Server OS

HDX MediaStream Windows Media リダイレクト

- VC-1 ライブストリームをリダイレクトするために、HDX MediaStream Windows Media リダイレクトと Windows Media Player を使用していますが、ライブストリームがフォールバックして、サーバー側でレンダリングすることがあります。[LD0251]
- HDX Web カメラにアクセスしようとすると、Citrix HDX RealTime Media Engine が予期せず終了することがあります。[LD0062]
- **HDX MediaStream Windows Media** リダイレクト設定が無効な場合、Windows Media Player で特定のビデオファイル形式を開こうとすると、以下のメッセージが表示されることがあります:

  ファイルの再生中に **Windows Media Player** に問題が発生しました。

  ただし、一部のビデオファイル形式の場合は、ビデオの縦横比が正しくありません。[LD0279]

キーボード

- ユーザーセッションで中国語のキーボードレイアウトを使用すると、Input Method Editor（IME）が自動的に五筆字型入力方法（Wubi）に変更されます。この問題は、デフォルトの IME が **Wubi** に設定されていない場合に発生します。[LD0429]

印刷

- XenApp および XenDesktop をバージョン 7.9 からバージョン 7.15 にアップグレードすると、ドキュメントを別のプリンタートレイに出力できない場合があります。印刷ダイアログから別のトレイを選択した場合でも、印刷ジョブはデフォルトのトレイにドキュメントを出力します。[LC9247]
- PDF を生データ形式で印刷キューに送信すると、PDF が印刷されないことがあります。[LC9755]
- デフォルトのプリンターが Citrix のマップされたプリンターである場合、Microsoft Windows Server 2016 はレジストリキー **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device** の値を更新できません。この失敗が原因で、.NET 以外のアプリケーションではデフォルトプリンターが設定されていないことがあります。[LD1032]

セッション/接続

- 一部のサードパーティ製アプリケーションでは、Shift+F2 キーを使用してセッションをウィンドウモードに切り替えてからシームレスモードに戻すまで、シームレスセッションで応答しなくなることがあります。[LC9727]
- 音質を［高］に設定してオーディオを聴くと、ポップ音やパチパチという音が聞こえることがあります。この問題は、オーディオを数秒間停止してから再開したときに発生します。[LC9975]
- 公開アプリケーションを最大化すると、タスクバーのセクション上部に重なることがあります。[LD0025]
- デリバリーグループで［**Secure ICA** を有効にする］設定を有効にした場合、レジストリキー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Security に **DHParaml** 値が存在しないと、アプリケーションの起動に失敗することがあります。このエラーメッセージが表示されます：

  アプリケーションを起動できません。ヘルプデスクに連絡して、次のエラー情報を提供してください：
  Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to “VOA Win 7 LTSR” failed with status (Unknown client error). [LD0117]
- ユーザーデバイスからクレジットカードのトランザクションを処理すると、アプリケーションとユーザーデバイスが応答しなくなったり、データのサブセットのみが受信されることがあります。[LD0152]
- ランダムにサーバーからアプリケーションを起動しようとすると失敗することがあります。このエラーメッセージが表示されます：

  アプリケーションを起動できません。**Citrix XenApp** サーバーに接続できません。選択した **Citrix SSL** サーバーは、接続を受け入れていません。

サーバーが SSL を有効にした VDA で接続の受け入れを停止すると、この問題が発生します。[LD0239]

- この修正プログラムは、「クライアントドライブに自動接続する」ポリシーが無効になっている場合に起きるメモリリークの問題を解決します。[LD0370]
- TWI モジュール（twi3.dll）のスレッドを終了する関数によって、サーバーが応答しなくなる可能性があります。[LD0406]
- ローカルアプリアクセスが有効な場合、Microsoft Windows 10 バージョン 1803 の公開デスクトップでアプリケーションを開こうとすると、アプリケーションを最小化できません。[LD0411]
- 障害通知が Delivery Controller に送信されると、サーバー OS の VDA が断続的に再登録されることがあります。[LD0466]
- Internet Explorer、Chrome、または Firefox ブラウザーで Google アカウントメールを開き、新しいメールを作成しようとすると、［キーボードの自動表示］が機能しないことがあります。[LD0470]
- シームレスモードのアプリケーションが、アプリケーションのサイズを最大化からウィンドウ化、またはウィンドウ化から最大化に変更すると、応答しなくなることがあります。[LD0498]
- scardhook64.dll によって例外 X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL が発生すると、ターゲットデバイスが予期せず再起動することがあります。[LD0504]
- エンドポイント上のオーディオデバイスの表示がタイムアウトすることがあります。その結果、セッションのオーディオが機能しなくなります。[LD0663]
- 公開アプリケーションのウィンドウの一部が更新されないことがあります。この問題は、バックグラウンドで実行されている Citrix 公開アプリケーションのいずれかがフォアグラウンドに表示された場合に発生する可能性があります。[LD0711]
- シームレスアプリケーションは固定サイズモードで起動します。この問題は、セッション画面の保持が無効になっている場合、ネットワークが中断されてから復旧したときに発生します。[LD0733]
- この修正により、CtxUvi Hooking ドライバーが Citrix dll の読み込みから安全なプロセスを除外することがあります。[LD0847]
- 場所 API からの応答を待っている間、公開アプリケーションがブロックされることがあります。

  タイムアウト値を構成して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：

  - *32* ビットシステムの場合

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    名前：LatlongWaitTime

    種類：REG_DWORD

    値：ミリ秒デフォルト値は 60000 ミリ秒です。この値は、場所情報の取得に使用できる待ち時間です。

  - *64* ビットシステムの場合

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

名前：LatlongWaitTime

種類：REG_DWORD

値：ミリ秒デフォルト値は 60000 ミリ秒です。この値は、場所情報の取得に使用できる待ち時間です。[LD0905]

- この修正により、CtxUvi ドライバーが Citrix dll の読み込みから vmsp.exe プロセスを除外することがあります。詳しくは、Knowledge Center の記事CTX107825を参照してください。[LD1024]
- VDA をバージョン 7.15 累積更新プログラム 3（CU3）にアップグレードすると、アプリケーションの起動が遅くなることがあります。この問題は、ユーザーグループが ［表示の制限］に設定されている場合に発生します。[LD1215]

システムの例外

- VM Hosted App を起動すると、mmvdhost.exe プロセスが予期せず終了することがあります。[LC9976]
- VDA で wdica.sys の重大な例外が発生し、バグチェックコード 0x3b (SYSTEM_SERVICE_EXCEPTION) によるブルースクリーンが表示されることがあります。[LD0089]
- VDA で picadm.sys の重大な例外が発生し、バグチェックコード 0x22 によるブルースクリーンが表示されることがあります。[LD0119]
- アクセス違反により、VDA で重大な例外が発生し、ブルースクリーンが表示されることがあります。[LD0281]
- 例外 **DivideByZeroException** によって、VDA で wfshell.exe プロセスが予期せず終了することがあります。このプロセスには、「**wfshellshell** が動作を停止しました。」というエラーメッセージが表示されます。[LD0373]
- VDA で wdica.sys の重大な例外が発生し、バグチェックコード 0x50 によるブルースクリーンが表示されることがあります。[LD0410]
- LIST_ENTRY の破損によって VDA で CtxUVI.sys の致命的な例外が発生し、ブルースクリーンエラーが発生することがあります。[LD0421]
- 公開された Internet Explorer のインスタンスで長い URL にアクセスしようとすると、wfshell.exe プロセスが予期せず終了することがあります。[LD0454]
- Internet Explorer（iexplore.exe）プロセスが例外コード **0xc00001a5** で予期せず終了することがあります。この問題は、障害がある CtxSensVcLibDll.dll モジュールのアンロードで発生します。[LD0485]

ユーザーエクスペリエンス

- アイテムの上にマウスポインターを置くと、ツールチップのポップアップが消え、アプリケーションがフォーカスを失うことがあります。[LD0365]

ユーザーインターフェイス

- 切断されたセッションに再接続しようとしているときに、VM Hosted App を起動すると、最後にクリックされたアプリケーション以外の、そのセッションに存在するすべてのアプリケーションが表示されます。[LD0189]
- デスクトップに表示されるグラフィックが壊れている可能性があります。[LD1115]

累積更新プログラム 3（CU3）

September 16, 2021

リリース日：2018 年 10 月 29 日

このリリースについて

XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 3（CU3）では、7.15 LTSR CU2 リリース以降に報告された 200 を超える問題が修正されています。

7.15 LTSR（一般情報）

XenApp および XenDesktop 7.15 LTSR CU2 以降の解決された問題

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU3 をダウンロード

この累積更新プログラムの新機能

ブラウザーコンテンツリダイレクトは、XenApp および XenDesktop 7.15 LTSR と互換性のある新しいコンポーネントで、個別にダウンロードできます。この累積更新プログラムのブラウザーコンテンツリダイレクト機能について詳しくは、「XenApp および XenDesktop 7.15 LTSR CU3 の互換性のあるコンポーネント」で「ブラウザーコンテンツリダイレクト」を参照してください。

新しい展開環境

新しく CU3 を展開するには

CU3 メタインストーラーを使用して、CU3 に基づく真新しい XenApp および XenDesktop 環境を設定できます。この設定を実行する前に、製品に慣れ親しんでおくことをお勧めします。

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

既存の展開環境

更新対象について

CU3 では、7.15 LTSR のベースラインコンポーネントの更新プログラムを提供します。注意：Citrix では展開環境のすべての LTSR コンポーネントを CU3 に更新することをお勧めします。例：Provisioning Services が LTSR 展開環境に含まれる場合、Provisioning Services コンポーネントを CU3 に更新します。Provisioning Services が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

XenApp および **XenDesktop 7.15 LTSR CU3** のベースラインコンポーネント

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.3000	
VDA for Server OS	7.15.3000	
Delivery Controller	7.15.3000	
Citrix Studio	7.15.3000	
Citrix Director	7.15.3000	
グループポリシー管理のエクスペリエンス	3.1.3000	
StoreFront	3.12.3000	
Provisioning Services	7.15.9	
ユニバーサルプリントサーバー	7.15.3000	
Session Recording	7.15.3000	Platinum Edition のみ
Linux VDA	7.15.3000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.3000	
フェデレーション認証サービス	7.15.3000	

XenApp および **XenDesktop 7.15 LTSR CU3** の互換性のあるコンポーネント

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

7.15 LTSR CU3 互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	4.15.0
* ブラウザーコンテンツのリダイレクト	15.15
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4.2000
ライセンスサーバー	11.15.0.0 Build 25000
セルフサービスパスワードリセット	1.1.10.0
Workspace Environment Management	4.7

***** ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバーなど）はリダイレクトしません。詳しくは、「Web ブラウザーコンテンツのリダイレクト」を参照してください。

システム要件:

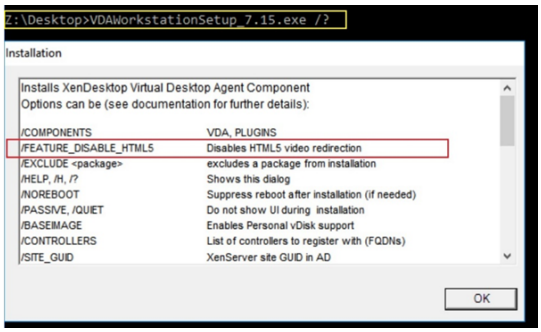
これらの要件は、XenApp および XenDesktop 7.15 LTSR CU3 の BCR.msi に特化したものです。XenApp、XenDesktop のその他のバージョン、Citrix Virtual Apps and Desktops で使用されているブラウザーコンテンツリダイレクトのシステム要件は含まれません。

- Delivery Controller および VDA の両方にバージョン 7.15 LTSR CU3。

- Windows 向け Citrix Workspace アプリ 1809 以降。
- BCR.msi - シトリックスのダウンロードページからダウンロードできます。
- Chrome（Web ブラウザーコンテンツのリダイレクト拡張機能を Chrome ウェブストアからインストール）または Internet Explorer 11（Browser Helper Object（BHO）の Citrix HDXJsInjector を有効化）。

インストール:

1. コマンドライン「/FEATURE_DISABLE_HTML5」オプションを使用して VDA にバージョン 7.15 LTSR CU3 をインストールまたはアップグレードします。



   このオプションは HTML5 ビデオリダイレクション機能を削除するため、BCR.msi の実行前に完了する必要があります。BCR.msi は、インストール中にこの機能を再度追加し、ブラウザーコンテンツリダイレクトサービスも追加します。この手順が完了したら、services.msc コンソールを開き、**Citrix HDX HTML5 Video Redirection Service** が表示されていないことを確認します。

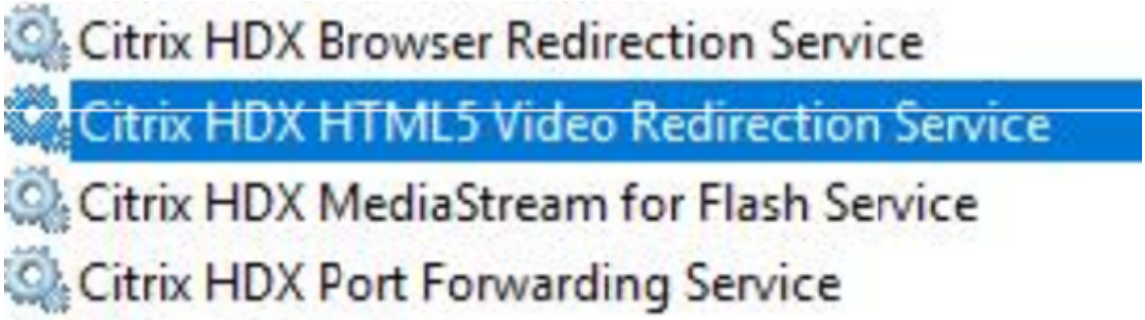
2. BCR.msi でブラウザーコンテンツリダイレクトサービスのインストールを開始します。システムに応じて、BCR.msi のファイルは次の場所にインストールされます:

   C:\Program Files\Citrix\ICAService

   または

   C:\Program Files(86)\Citrix\ICAService

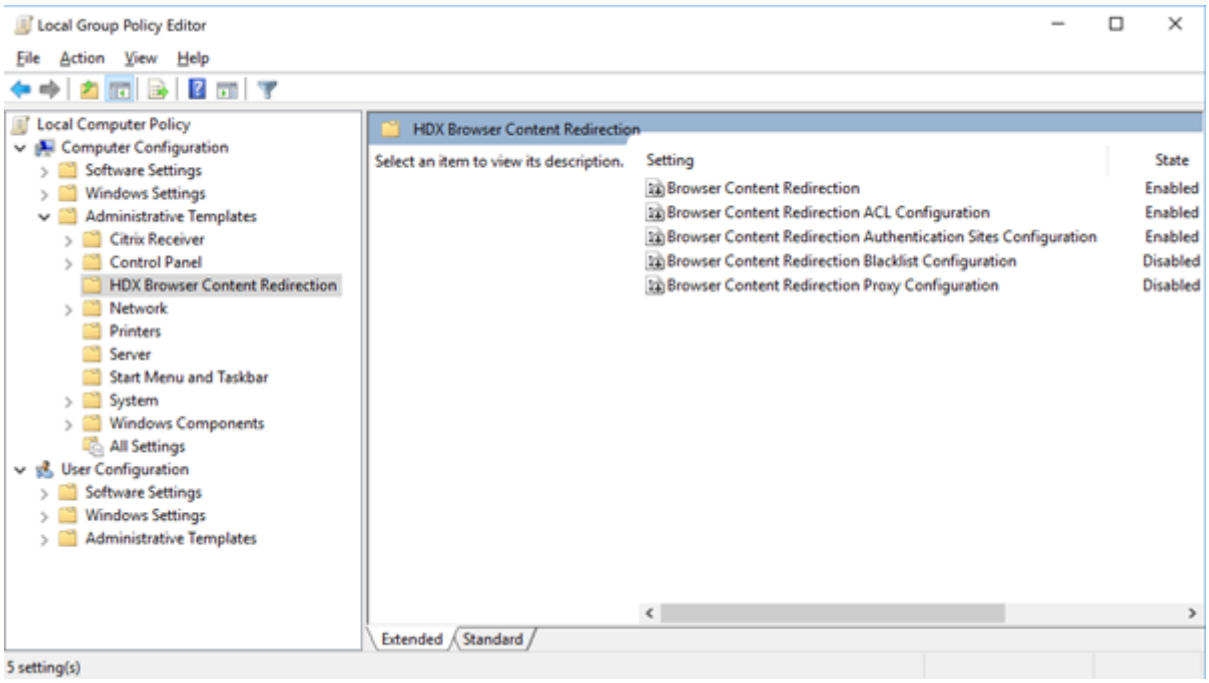
   インストールが高速であるため、ダイアログボックスがすぐに閉じることがあります。この場合、services.msc に戻ってサービスが追加されたことを確認します。



ポリシー:

VDA で HKEY_LOCAL_MACHINE レジストリを使用して、またはグループポリシー管理コンソールで Citrix 管理テンプレートの **HDX Browser Content Redirection** を使用してポリシーを制御できます。

Citrix Virtual Apps and Desktops（XenApp および XenDesktop）、XenApp 7.15 LTSR または XenDesktop 7.15 LTSR、コンポーネント の順に移動し、citrix.comダウンロードページからテンプレートをダウンロードできます。Citrix Studio にはこれらのポリシーは含まれません。



ポリシー情報について詳しくは、「Web ブラウザーコンテンツのリダイレクトのポリシー設定」を参照してください。トラブルシューティングについて詳しくは、Knowledge Center のCTX230052を参照してください。

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk

除外対象の機能
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

XenApp 6.5 からの移行

XenApp 6.5 の移行プロセスでは、XenApp 6.5 ファームを XenApp 7.15 LTSR CU3 のサイトにすばやく効率的に移行できます。この移行方法では、多数のアプリケーションと Citrix グループポリシーを含む環境で、アプリケーションと Citrix グループポリシーを手動で新しい XenApp サイトに移行する場合のエラーの発生リスクを軽減させることができます。

XenApp 7.15 LTSR CU3 のコアコンポーネントをインストールしてサイトを作成したら、次の手順で移行プロセスを実行します：

- 各 XenApp 6.5 ワーカー上で XenApp 7.15 CU3 インストーラーを実行します。これにより、Virtual Delivery Agent for Server OS にアップグレードされます。
- いずれかの XenApp 6.5 Controller 上で PowerShell エクスポートコマンドレットを実行して、アプリケーション設定と Citrix ポリシー設定を XML ファイルにエクスポートします。

- 必要に応じて XML ファイルを編集して、新しいサイトにインポートしないデータや設定を削除します。XML ファイルをカスタマイズすることにより、ポリシー設定とアプリケーション設定を段階的に XenApp 7.15 LTSR CU3 サイトにインポートできます：一部を先にインポートしてから残りを後でインポートするなど。
- 新しい XenApp 7.15 CU3 Controller 上で PowerShell インポートコマンドレットを実行して、XML ファイルから新しい XenApp サイトに設定をインポートします。

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- カスタムロールを持つ委任管理者が Citrix Studio、PowerShell、または Citrix Director を使用しているデスクトップからユーザー割り当てを削除しようとすると、失敗することがあります。この問題は、カスタム管理者が配信グループの操作を実行する権限を持っていても、コンピュータカタログに対するアクセス許可がない場合に発生します。[LC8174]
- ユーザーをマシンに割り当てる時にユーザーを検索しようとすると、失敗することがあります。選択したユーザーは null として表示されます。[LC8395]
- **UDP** ベースのデータ転送プロトコル（**UDT**）を使用している場合、Citrix Director がマルチストリーム ICA を非アクティブとして報告することがあります。この問題は、HDX WMI プロバイダが EDT または UDT セッションのアカウントに更新されていない場合に発生します。[LC8960]
- w3wp.exe プロセスの CPU 使用率が、Citrix Director で非常に高くなる可能性があります。[LC9222]
- ブラウザの言語を英語以外の特定の言語に設定して Citrix Director を起動すると、セッションが実行されていなくても、セッションの詳細ペインにアクティブなセッションが 1 つ表示されることがあります。[LC9392]
- Citrix Director を使用している場合、Microsoft Internet Explorer 11 の［フィルタ］>［マシン］>［すべてのマシン］ページの ［マシンの詳細］セクションに、機能しないスクロールバーが表示されることがあります。[LC9505]
- **Citrix Director** の ［傾向］ページで、Internet Explorer が自動的に Google Analytics（https://www.google-analytics.com）を信頼済みサイトとして追加することがあります。Internet Explorer によるこのアクションは停止できません。レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall で自動アップロードの値 **SendExperienceMetrics** を無効にしても、Citrix Director ダッシュボードとアプリケーションページで Google Analytics の呼び出しが確立されます。自動アップロードを無効にするには、「Citrix Insight Services」の手順を使用します。この修正を適用すると、Citrix Director のログオン時に Google Analytics に ping が送信されますが、データはアップロードされません。[LC9736]

- Citrix Director のログオンパフォーマンスを CSV 形式で生成したレポートで、ローカル時間ではなく UTC タイムゾーンが使用されることがあります。[LC9854]
- 管理者によっては、web.config ドメインリストに追加された一部のドメインにアクセスできない場合があります。その結果、ユーザーのセッションを検索すると例外が発生し、セッションの詳細は表示されません。[LC9865]
- 値 **ExportCsvDrilldownLimit** は、Citrix Director のカスタムレポートに適用されないことがあります。[LD0004]

Citrix ポリシー

- マージモードでループバックポリシーを VDA に適用し、StoreFront の URL を Citrix Studio の VDA のデリバリーグループに追加すると、公開アプリケーションのアイコンが重複して表示されることがあります。[LC8889]
- マシンカタログを作成しようとすると、サマリーを作成できないという例外が発生して失敗する場合があります。また、作成カタログウィザードを使用しているとき、例外が表示される前に、ドメインを一覧表示するはずのドロップダウンリストが空になります。[LC9636]
- VDA 7.15.2000 と共にインストールされているマシンのグループポリシー管理コンソールからグループポリシーの結果ツールを実行すると、次のエラーメッセージが表示されます：レポートの生成中にエラーが発生しました：見つかりません [LC9825]
- Citrix Print Manager Service（cpsvc.exe）が予期せず終了することがあります。この問題は、グループポリシーオブジェクト（GPO）に接続されている印刷レジストリキーにガベージエントリがある場合に発生します。[LC9921]
- グループポリシーエンジンが、**ApplicationStartDetails** レジストリキーへのすべての値の挿入に失敗することがあります。その結果、App-V アプリケーションを起動しようとしても失敗する場合があります。[LC9942]
- レジストリエントリがレジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix のセッションキーに手動で事前入力されている場合、セッション開始時にキーが更新されないことがあります。[LC9977]
- 組織単位（OU）フィルターを使用して Citrix ポリシーを Citrix Studio に適用しようとすると、次のエラーメッセージが表示されることがあります：不明なエラーが発生しました。

  次の例外が表示されます：
  コレクションが変更されました。列挙操作が実行されないことがあります。[LD0044]
- グループポリシーをバックアップし、グループポリシー管理コンソール（GPMC）バージョン 3.1.2 でグループポリシーをインポートしようとすると、GPMC が応答しなくなることがあります。しかし、このポリシーはインポートされます。[LD0173]

Citrix Studio

- カスタムロールを持つ委任管理者が Citrix Studio、PowerShell、または Citrix Director を使用しているデスクトップからユーザー割り当てを削除しようとすると、失敗することがあります。この問題は、カスタム管理者が配信グループの操作を実行する権限を持っていても、コンピュータカタログに対するアクセス許可がない場合に発生します。[LC8174]
- Delivery Controller のうち 1 つがオフラインになったり使用できなくなったりすると、Citrix Studio が数分後に開き、次のメッセージが表示されることがあります:

  このスナップインは応答していません。[LC8993]
- VDA から App-V パッケージを非公開および削除しようとすると失敗する可能性があります。[LC9161]
- [操作] ペインの [デリバリーグループの編集] を選択後、[マシン割り当て] ページを 2 回目に表示したとき、[マシン割り当て] ページが空白になり、マシン名やユーザーなどの詳細が表示されないことがあります。[LC9465]
- アプリケーショングループの公開アプリケーションを移動させた後、Citrix Studio のアプリケーションフォルダーを削除しようとすると、権限エラーで失敗する可能性があります。[LC9520]
- Citrix Studio をバージョン 7.15 の累積更新プログラム 2 にアップグレードすると、ポリシーがローカライズされないことがあります。詳しくは、Knowledge Center のCTX234711を参照してください。[LC9613]
- マシンカタログを作成しようとすると、サマリーを作成できないという例外が発生して失敗する場合があります。また、作成カタログウィザードを使用しているとき、例外が表示される前に、ドメインを一覧表示するはずのドロップダウンリストが空になります。[LC9636]
- デリバリーグループから App-V アプリケーションを削除しようとすると、アプリケーションが削除されることがあります。エラーメッセージが表示されます。[LC9985]
- 組織単位（OU）フィルターを使用して Citrix ポリシーを Citrix Studio に適用しようとすると、次のエラーメッセージが表示されることがあります：不明なエラーが発生しました。

  次の例外が表示されます:
  コレクションが変更されました。列挙操作が実行されないことがあります。[LD0044]
- 組織単位（OU）フィルターを使用して Citrix スタジオで Citrix ポリシーを適用しようとするか、カタログウィザードで OU を追加すると、例外が発生します。[LD0112]

コントローラー

- カスタムロールを持つ委任管理者が Citrix Studio、PowerShell、または Citrix Director を使用しているデスクトップからユーザー割り当てを削除しようとすると、失敗することがあります。この問題は、カスタム管理者が配信グループの操作を実行する権限を持っていても、コンピュータカタログに対するアクセス許可がない場合に発生します。[LC8174]

- Citrix Studio で VDA の電源状態が断続的に無効になることがあります。Studio は、VDA が動作しているときでも電源状態がオフであることを示します。[LC8898]
- Delivery Controller のうち 1 つがオフラインになったり使用できなくなったりすると、Citrix Studio が数分後に開き、次のメッセージが表示されることがあります:

  このスナップインは応答していません [LC8993]
- プリンシパルブローカーからローカルホストキャッシュ（LHC）データベースに変更をインポートし、Citrix Studio からはユーザーまたはマシンを削除せずに Active Directory からユーザーまたはマシンを削除します。その結果、エラーが発生し、LHC が更新されません。[LC9054]
- 接続時間のピーク時に、アプリケーションイベント **ID 2013** の XenApp でデッドロックが発生することがあります。このエラーメッセージが表示されます:

  Citrix Broker Service が **HTTP** 要求を処理している間に予期しない例外が発生しました。[LC9134]
- XenApp 7.6 を XenApp 7.15 にアップグレードすると、**C:\Windows\ServiceProfiles\NetworkService\Licensing** 配下の Delivery Controller 上にある Licensing フォルダーのアクセス許可が上書きされます。[LC9445]
- Citrix High Availability Service（HighAvailabilityService.exe）のメモリ使用量が 2GB を超える場合があります。[LC9446]
- Citrix Studio からターゲット VDA に再起動コマンドを送信すると、ターゲット VDA がシャットダウンすることがあります。[LC9479]
- アプリケーショングループの公開アプリケーションを移動させた後、Citrix Studio のアプリケーションフォルダーを削除しようとすると、権限エラーで失敗する可能性があります。[LC9520]
- ESXi ホスト上でホスティングされている仮想デスクトップインフラストラクチャ（VDI）は電源状態が不明になる可能性があり、自動的に電源が投入されることはありません。この問題は、ESXi ホストがメンテナンスモードから外れた後に仮想マシン（VM）が ESXi ホストに移動した後に発生します。[LC9619]
- マシンカタログを作成しようとすると、サマリーを作成できないという例外が発生して失敗する場合があります。また、作成カタログウィザードを使用しているとき、例外が表示される前に、ドメインを一覧表示するはずのドロップダウンリストが空になります。[LC9636]
- Citrix Studio に ［開始］オプションが表示されません。その結果、Remote PC の電源がオンになりません。[LC9702]
- このパフォーマンス向上機能を Monitor サービスに使用すると、Monitor データベースが大規模である場合に、SQL サーバーの CPU 使用率が低下します。[LC9726]
- セキュアブートが有効になっていると、Machine Creation Services（MCS）でプロビジョニングされた仮想マシン（VM）が作成されないことがあります。この問題は、Extensible Firmware Interface（EFI）を使用して、かつセキュアブートが有効な状態でマスターテンプレートが作成された場合でも起こることがあります。[LC9841]

- デフォルトでは、Machine Creation Services（MCS）でプロビジョニングされたマシンの Amazon Web Services（AWS）ID は非永続的です。これにより、仮想マシンの電源管理アクションが AWS で失敗する可能性があります。

  AWS ID の永続性を設定するには、次のオプションを使用できます：

  - AWS ID の永続化を有効にするには、ホスト接続の詳細プロパティの［接続］オプションを「**Create-NewInstanceOnReset=False**」に設定します。
  - AWS ID の永続性を無効にするには、ホスト接続の詳細プロパティの［接続］オプションを「**Create-NewInstanceOnReset=True**」に設定するか、オプションを削除します。

  変更したオプションが適用されるまで、10 秒ほどかかります。[LC9960]

- **New-BrokerApplication** コマンドと-AdminFolder パラメーターを使用してアプリケーションを作成しようとすると、特定のシナリオで指定されたフォルダーが作成されない場合があります。[LC9982]
- デリバリーグループから App-V アプリケーションを削除しようとすると、アプリケーションが削除されることがあります。エラーメッセージが表示されます。[LC9985]
- 多くのアプリケーショングループが使用されている大規模な環境では、Studio の［アプリケーション］タブをクリックすると、**Get-BrokerApplicationGroup** 出力のフェッチ中にセッションがタイムアウトします。その結果、次の例外が表示されます：

  データベースに接続できませんでした。

  例外をスローする前に、Studio は応答しなくなり、アプリケーショングループを列挙します。[LD0012]

- 組織単位（OU）フィルターを使用して Citrix ポリシーを Citrix Studio に適用しようとすると、次のエラーメッセージが表示されることがあります：不明なエラーが発生しました。

  次の例外が表示されます：
  コレクションが変更されました。列挙操作が実行されないことがあります。[LD0044]

- 特殊文字を含むデリバリーグループ名を使用してローカルホストキャッシュを再作成しようとすると、イベント **ID 505** で失敗することがあります。[LD0068]
- Citrix Studio ホスティング接続では、HTTPS 接続がサポートされていない場合でも、HTTPS を XenServer ホスティング接続用に使用するよう警告するメッセージが表示されることがあります。[LD0210]
- XenApp および XenDesktop をバージョン 7.15 にアップグレードすると、次にスケジュールされているイベントで開始するのではなく、最初の再起動スケジュールがすぐに開始される可能性があります。[LD0308]

HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 7.15 LTSR CU3 のドキュメントに は、このリリースの更新に関する特定の情報が記載されています。

ID アサーション

- ログオンするセッションで使用可能な認証証明書にアクセスしようとすると、失敗することがあります。[LC9728]
- フェデレーション認証サービスのセッション内証明書を使って TLS 1.1（またはそれ以前）の接続を認証しようとすると、接続に失敗する場合があります。ハッシュ ID がサポートされていないことを示す、イベント ID 305 がログに記録されます。フェデレーション認証サービスは、SHAMD5 ハッシュをサポートしません。[LD0018]

インストーラー

- 既に Adobe Acrobat Reader 2015 DC アプリケーションがインストールされている環境に VDA をインストールしようとすると、次のエラーメッセージが表示されることがあります:

  コンピューターから **mfc120u.dll** が見つからないため、プログラムを開始できません。問題を解決するにはプログラムを再インストールしてください。[LC9979]

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU3 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Profile Management

- Citrix Director で ［プロファイルのリセット］をクリックして Microsoft Active Directory ポリシーを使用してフォルダーリダイレクトを構成すると、リダイレクトされたフォルダもリセットされます。その結果、ドキュメント、ピクチャ、ミュージック、ビデオ、お気に入りなどの特定のフォルダーの名前が変更されます。しかし、スタートメニュー、連絡先、ダウンロード、リンク、検索、保存したゲームなどのフォルダーの名前は変更されません。[LC9237]
- Profile Management サービスが例外コード 0xc0000374 で予期せず終了することがあります。[LC9355]
- プロファイル管理は、Microsoft Windows 10、バージョン 1709 で実行されている VDA の特定の設定を同期させないことがあります。[LC9503]
- アクティブライトバックレジストリポリシーを有効にすると、Software\Microsoft\AppV\Client\Integration や Software\Microsoft\AppV\Client\Publishing といった、レジストリを除外するデフォルトのポリシーが機能しないことがあります。[LC9550]
- 既定のユーザープロファイルに対する完全なアクセス許可があります。最初のログオン時に、プロファイル管理によって、ポリシーによって構成された除外されたフォルダーが既定のユーザープロファイルから削除されることがあります。この問題は、ログオン除外チェックが除外されたファイルとフォルダを削除するように構成されている場合に発生します。[LC9575]

- 設定されたプロファイル管理アクティブなライトバックレジストリすべてのレジストリを処理し、レジストリが除外されているか含まれているかにかかわらず、すべての変更を一時ファイルに記録します。その結果、CPU 使用率が高くなります。[LC9624]
- 7.15 LTSR CU2 セッションが黒い画面として起動することがあります。この問題は、Profile Management が有効なときに、XenApp および XenDesktop 7.15 LTSR CU2 および 7.17 VDA で実行されているセッションで発生します。回避策などを含め、詳しくは Knowledge Center のCTX235100を参照してください。[LC9648]
- Profile Management の［ミラーリングするフォルダー］ポリシーが機能しないことがあります。[LC9691]
- Profile Management を有効にすると、公開デスクトップの［スタート］メニューに空のアイコンが表示されることがあります。この問題は、2 回目以降のログオン時に発生します。

  注：この修正は、新規インストールでのみ有効です。アップグレードシナリオでは、HDX グループポリシーエディターまたは Active Directory ポリシーエディターで手動で ［ミラーリングするフォルダー］ポリシーを設定する必要があります。[LC9692]
- Profile Management で AppData（Roaming）フォルダーのリダイレクトが失敗し、次のエラーメッセージが表示されることがあります：

  アクセスが拒否されました。

  この問題は、**AppData/Roaming** から共有フォルダーへ正しくリンクされず、誤って/Application Data/Roaming が付加された場合に発生します。[LC9830]

Provisioning Services

Provisioning Services 7.15 LTSR CU3は、このリリースの更新に関する特定の情報を提供します。

Remote Broker Provider

- デフォルトでは、Machine Creation Services（MCS）でプロビジョニングされたマシンの Amazon Web Services（AWS）ID は非永続的です。これにより、仮想マシンの電源管理アクションが AWS で失敗する可能性があります。

  AWS ID の永続性を設定するには、次のオプションを使用できます：

  - AWS ID の永続化を有効にするには、ホスト接続の詳細プロパティの［接続］オプションを「**CreateNewInstanceOnReset=False**」に設定します。
  - AWS ID の永続性を無効にするには、ホスト接続の詳細プロパティの［接続］オプションを「**CreateNewInstanceOnReset=True**」に設定するか、オプションを削除します。

  変更したオプションが適用されるまで、10 秒ほどかかります。[LC9960]

Session Recording

管理

- ドメイン **B** のユーザーがドメイン A の Session Recording サーバーにログオンして、Session Recording プロパティを更新しようとしても、マシンのグローバル一意識別子が生成されず、エラーが発生します。この問題は、ユーザーがドメイン **B** に存在する一方、Session Recording サーバーがドメイン **A** に存在することが原因です。[LC9562]

エージェント

- 発行された Microsoft Internet Explorer のインスタンスが、Session Recording Player リストで **explorer.exe** と表示されることがあります。正しいファイル名は **Iexplore.exe** です。[LC9622]

StoreFront

- ブラウザを 125%にズームすると、カスタムロゴが表示されなくなることがあります。[LC9018]
- **OverrideIcaClientname** が有効な場合、リモートデスクトップクライアントからのリモートセッションの確立に失敗することがあります。この問題は、ライセンスが更新されていない場合に発生します。次のエラーメッセージのいずれかが表示されることがあります:

  「ライセンスを更新できなかったため、リモートデスクトップクライアント WR_XxXXxXXX からリモートセッションを確立できませんでした。」

  または

  「一時ライセンスの有効期限が切れのため、リモートデスクトップクライアント WR_XxXXxXXX からリモートセッションを確立できませんでした。」[LC9246]
- Delivery Controller 証明書を TLS v1.2 に更新した後、アプリケーションを列挙しようとすると失敗することがあります。[LC9337]
- XenDesktop のセットアップ中、構成されたサイトを選択すると、StoreFront でデフォルトの認証サービスを使用するデフォルトのストアが作成されることがあります。このストアを削除すると、Citrix Receiver for Windows ユーザーはストアを追加できなくなり、次のエラーメッセージが表示されることがあります。

  「認証サービスとの通信中にプロトコルエラーが発生しました。」[LC9404]
- StoreFront にログオンしようとすると、［要求を完了できません］エラーで失敗することがあります。この問題は、公開アプリケーションに最小解像度のカスタムアイコンがある場合に発生します。[LC9521]
- StoreFront SDK を使用して特定の機能をカスタマイズし、ストアのアグリゲーションを構成すると、［要求を完了できません］エラーでログオンが失敗することがあります。[LC9561]
- ［キーワードによるリソースフィルター］を構成するとセッションの事前起動が機能しないことがあります。[LC9642]

- ICA ファイルは、NetScaler Gateway 接続を使用している場合でも、UDPICAPort エントリに VDA の完全修飾ドメイン名（FQDN）を表示することがあります。[LC9760]

ユニバーサルプリントサーバー

クライアント

- ユニバーサルプリントサーバーにより、印刷スプーラーサービスが応答しなくなることがあります。[LC9341]

User Profile Management VDA

- VDA をバージョン 7.13 からバージョン 7.15.2000 にアップグレードすると、Citrix Director がリダイレクトされたフォルダーを表示しないことがあります。この問題は、フォルダーのリダイレクトが引き続き機能している場合に発生します。[LC9968]
- brokeragent.exe プロセスの CPU 使用率が高い可能性があります。[LD0310]

VDA for Desktop OS

HDX

- Citrix HDX HTML5 ビデオリダイレクションサービス（WebSocketService.exe）が予期せず終了し、ビデオが HTML5 ページにリダイレクトされないことがあります。[LC8825]
- VDA で実行されている公開アプリケーションで、%ProgramFiles% や%ProgramFiles(x86)% などの汎用パスを使用している場合は、セッションを再接続している間に新しい複製アプリケーションウィンドウが開くことがあります。[LC9741]

印刷

- **CpSvc!CDispatcher::UpdateCounters** のアクセス違反により、Citrix Print Manager Service（cpsvc.exe）が予期せず終了することがあります。[LC8804]
- .NET 以外のアプリケーションでは、デフォルトプリンターが設定されていない場合があります。デフォルトのプリンターが Citrix のマップされたプリンターである場合、Microsoft Windows Server 2016 はレジストリキー **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device** の値を更新できません。[LC8984]
- デフォルトのプリンターがセッションで正しく設定されていない可能性があります。この問題は、デフォルトプリンターが他のランダムプリンターに切り替わるときに発生します。[LC8999]
- セッションに再接続する際、従来のプリンター名を使用していると、セッションにマップされたプリンターの読み込みが遅くなることがあります。[LC9079]

- 特定の Microsoft Excel ファイルで［**Excel**］ > ［印刷］に移動し、Citrix ユニバーサルプリンター EMF ドライバーを使用してクライアントプリンターを自動作成すると、印刷プレビューイメージの文字が小さく表示されることがあります。[LC9700]
- Citrix Print Manager Service（cpsvc.exe）が予期せず終了することがあります。この問題は、**CpWSGetPrinterConnectionsFromPolicy** が Null ポインターを比較文字列 **[MS] _wcsicmp** に渡すと発生します。[LC9796]

セッション/接続

- Web カメラがユーザーセッション内で応答しなくなることがあります。この問題は、以下のいずれかの操作を実行すると発生します。
  - 特定のサードパーティのアプリケーションを使用してユーザーセッションで Web カメラを選択すると、Web カメラのビデオフレームが応答しなくなります。
  - GraphEdit ツールを使用して仮想 Web カメラを起動し、メニューで［クロックを使用する］オプションを選択した場合。
  - Citrix Diagnostics Facility（CDF）トレースを分析すると、VDA と Citrix Receiver for Windows 間のデリバリーパイプラインが確立されたときに、ビデオサンプルが 1 つしか配信されません。[LC8382]
- レジストリキー **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook** の **ExcludedImageNames** に複数の実行可能ファイルが追加されている場合、Citrix Hook を無効にできないことがあります。[LC8614]
- **UDP** ベースのデータ転送プロトコル（**UDT**）を使用している場合、Citrix Director がマルチストリーム ICA を非アクティブとして報告することがあります。この問題は、HDX WMI プロバイダが EDT または UDT セッションのアカウントに更新されていない場合に発生します。[LC8960]
- H 構成を使用するマルチモニター環境では、マウスの動作が一貫しないことがあります。Microsoft Skype for Business セッションを開始し、他のユーザーと画面の共有を開始します。Citrix グラフィックドライバーは、オペレーティングシステムから誤ったマウスの位置情報を受け取ります。

  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\ICA

  名前：DisableAppendMouse

  種類：DWORD

  データ：00000001

  ただし、レジストリキーを設定した後で HDX セッションを使用すると、プログラムによってマウスポインターの位置を設定する特定の機能が意図したとおりに機能しない場合があります。以下は対象の機能です。

  - マウススナップ機能。
  - ユーザー間のマウスの位置を GotoMeeting の画面共有と同期させる機能。
  - ユーザー間のマウスの位置を Skype for Business の画面共有と同期させる機能。[LC8976]

- 特定のシナリオで、VDA がイベント ID 1048 で自動的に再登録されることがあります。たとえば、Lotus Notes と Lotus Notes Standard という似た名前の 2 つのアプリケーションを起動し、起動した 2 つ目のアプリケーションを閉じると、1 つ目のアプリケーションのエントリがレジストリから削除されます。この情報が通知を介して Delivery Controller に送信されると、その通知は拒否され、再登録が行われます。[LC9223]
- HDX RealTime Connector が予期せず終了することがあります。ビデオプレビューウィンドウが閉じるか、ビデオプレビューウィンドウにブラックボックスが短時間表示され、その後閉じます。この問題は、HDX RealTime Media Engine がエンドポイントにインストールされていない場合に発生します。[LC9282]
- Citrix Audio Service が予期せず終了し、再度再起動することがあります。2 番目のエンドポイント（シンクライアント）から同じセッションに再接続すると、新しいデバイスはセッションに正しくマッピングされません。[LC9381]
- VDA 上で実行されている公開アプリケーションでクリップボードのクリアまたは削除を選択すると、VDA クリップボードはクリアされますが、テキストはエンドポイントのクリップボードに残ります。[LC9434]
- 最初のエンドポイントからユーザーセッションを切断し、2 番目のエンドポイント（シンクライアント）から同じセッションを再接続すると、クライアント側のオーディオデバイスが VDA 内で誤った順序でリストされることがあります。

  この修正を有効にするには、以下のレジストリキーを設定します:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  名前：CleanMappingWhenDisconnect

  種類：DWORD

  値：1[LC9440]
- 公開アプリケーションセッションが切断され、ユーザーセッションが VDA から正しくログオフされないことがあります。問題が発生すると、再接続できなくなり、Citrix Studio から切断できなくなる可能性があります。この状況を解決するには、PowerShell コマンドを使用してセッションを非表示に設定するか、VDA を再起動します。[LC9444]
- VDA バージョン 7.15.1000 を使用している場合、twi3.dll から異常な数の CPU 命令が発生し、Winlogon.exe プロセスを通過することがあります。[LC9450]
- クライアントドライブのリダイレクトポリシーを無効にして、ユーザーデバイスからアプリケーションを 2 回目に起動すると、アプリケーションの起動に時間がかかることがあります。[LC9477]
- 別のエンドポイントからアクティブな既存のセッションに再接続しようとすると、次のエラーメッセージが表示されます:

  接続が中断されました。受信者は **5** 分間再接続を続けます。

  この問題は、VDA 7.15 がインストールされている Microsoft Windows 7 で発生します。[LC9485]
- Web ベースのアプリケーションは、Microsoft Internet Explorer または Mozilla Firefox ブラウザを使用して開かれます。アプリケーションで特定のタブを開くと、デスクトップ全体が応答しなくなることがあります。[LC9508]

- サーバー合計インスタンスのパフォーマンスカウンターが **ICA** セッションカウンターに存在しない可能性があります。[LC9537]
- ファイルが分散ファイルシステム（DFS）ドライブ上にある場合、ローカルアプリアクセスとのファイルタイプの関連付けは、有効になっていても機能しないことがあります。[LC9538]
- イベント ID 31「接続のリスンを開始します」がイベントビューアーに渡されないことがあります。[LC9556]
- **Unicode** キーボードレイアウトマッピングを有効にすると、公開アプリケーションをログオフできません。[LC9590]
- キーボードレイアウトを切り替えると、ポップアップウィンドウが表示されることがあります。次のレジストリキーを設定して、ポップアップウィンドウを非表示にします：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  名前：HideNotificationWindow

  種類：DWORD

  値：1[LC9592]
- 公開アプリケーションは、予期されない失敗のため、アプリケーションの起動直後に断続的に終了することがあります。この問題は、アクティブなプロセスに関する情報が取得されたときに発生します。[LC9661]
- XenApp および XenDesktop をバージョン 7.6 からバージョン 7.15 LTSR 累積更新プログラム 1 にアップグレードすると、特定のサービスが予期せず停止または終了したり、ログオン中に断続的に応答しなくなることがあります。[LC9679]
- XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 2 をインストールすると、VDA が応答しなくなることがあります。[LC9701]
- Microsoft レジストリ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN で特定の暗号を無効にすると、TLS が有効にならない場合があります。[LC9743]
- リモート PC アクセスを使用して Windows ワークステーションにアクセスし、リモート PC アクセスセッションから切断すると、ワークステーションがロックされないことがあります。したがって、当該のワークステーションには、そのワークステーションに物理的に到達できるすべての人がアクセスできます。[LC9812]
- VDA にログオンすると、日本語 IME（Input Method Editor）のかな言語入力キーが自動的に有効になることがあります。[LC9932]
- この修正により、ホワイトリストプロセスメカニズムが SCardHook に追加されました。ホワイトリストがレジストリで定義されている場合、ホワイトリストに含まれるプロセスのみがスマートカードのリダイレクトを使用できます。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  名前：HookProcessWhitelist

  種類：REG_SZ

値：<process name>[LC9961]

- 最初のエンドポイントからユーザーセッションを切断し、シンクライアントから同じセッションを再接続すると、クライアント側のオーディオデバイスが VDA 内で誤った順序でリストされることがあります。

  この修正を有効にするには、以下のレジストリキーを設定します：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  名前：CleanMappingWhenDisconnect

  種類：DWORD

  値：1[LD0458]

システムの例外

- サーバーで picadm.sys の致命的な例外が発生し、バグチェックコード 0x22（FILE_SYSTEM）によるブルースクリーンが表示されることがあります。[LC7726]
- Enlightened Data Transport（EDT）が有効な場合、サーバーで tdica.sys に関する重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** のブルースクリーンが表示されることがあります。[LC8794]
- サーバーで picadm.sys の致命的な例外が発生し、バグチェックコード 0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQ によるブルースクリーンが表示されることがあります。[LC8830]
- VDA で wdica.sys の致命的な例外が発生し、ブルースクリーンエラーが発生することがあります。[LC9695]
- 公開アプリケーションを開始しようとすると、wfshell.exe プロセスが予期せず終了することがあります。この問題は双方向コンテンツリダイレクトポリシーが有効な場合に発生し、URL は提供されません。[LC9705]
- Microsoft Windows Server 2008 R2 で重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** によるブルースクリーンが表示されることがあります。この問題は、XenApp および XenDesktop 7.15 LTSR CU2 が Microsoft Windows Server にインストールされている場合に発生します。[LC9849]
- picavc.sys でサーバーに重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** によるブルースクリーンが表示されることがあります。[LD0006]

ユーザーエクスペリエンス

- 公開アプリケーションのサイズを変更し、そのアプリケーションをあるモニターから別のモニターに移動しようとすると、アプリケーションの周りに白い罫線が表示されることがあります。[LC9570]
- **Unicode** キーボードレイアウトマッピングを使用するように VDA を設定して、ローカル IME を有効にした状態で Citrix Receiver から HDX セッションを確立します。公開アプリケーションで任意の文字を入力し、出力された文字の一部または全部を選択すると、選択した文字が新しい文字に置き換わるのではなく、選択した文字の前に新しい文字が挿入されます。[LC9591]

- 画面の解像度を変更して VDA for Desktop OS から公開アプリケーションに再接続すると、アプリケーションウィンドウが切り捨てられることがあります。[LC9947]
- マルチモニター環境において、特定のシナリオでは画面が正しくロックされません。[LD0186]

ユーザーインターフェイス

- シームレスなセッションのアプリケーションウィンドウが応答しなくなると、アプリケーションウィンドウのタスクバーアイコンが削除され、再度作成される可能性があります。[LC9807]

VDA for Server OS

HDX

- Citrix HDX HTML5 ビデオリダイレクションサービス（WebSocketService.exe）が予期せず終了し、ビデオが HTML5 ページにリダイレクトされないことがあります。[LC8825]
- VDA で実行されている公開アプリケーションで、%ProgramFiles% や%ProgramFiles(x86)% などの汎用パスを使用している場合は、セッションを再接続している間に新しい複製アプリケーションウィンドウが開くことがあります。[LC9741]

印刷

- **CpSvc!CDispatcher::UpdateCounters** のアクセス違反により、Citrix Print Manager Service（cpsvc.exe）が予期せず終了することがあります。[LC8804]
- .NET 以外のアプリケーションでは、デフォルトプリンターが設定されていない場合があります。デフォルトのプリンターが Citrix のマップされたプリンターである場合、Microsoft Windows Server 2016 はレジストリキー HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device の値を更新できません。[LC8984]
- デフォルトのプリンターがセッションで正しく設定されていない可能性があります。この問題は、デフォルトプリンターが他のランダムプリンターに切り替わるときに発生します。[LC8999]
- セッションに再接続する際、従来のプリンター名を使用していると、セッションにマップされたプリンターの読み込みが遅くなることがあります。[LC9079]
- 特定の Microsoft Excel ファイルで［Excel］>［印刷］に移動し、Citrix ユニバーサルプリンター EMF ドライバーを使用してクライアントプリンターを自動作成すると、印刷プレビューイメージの文字が小さく表示されることがあります。[LC9700]
- Citrix Print Manager Service（cpsvc.exe）が予期せず終了することがあります。この問題は、**CpWSGetPrinterConnectionsFromPolicy** が Null ポインターを比較文字列 **[MS]_wcsicmp** に渡すと発生します。[LC9796]

セッション/接続

- VDA をバージョン 7.12 からバージョン 7.13 にアップグレードすると、バッジリーダーが動作しなくなる可能性があります。[LC7667]
- Web カメラがユーザーセッション内で応答しなくなることがあります。この問題は、以下のいずれかの操作を実行すると発生します。
  - 特定のサードパーティのアプリケーションを使用してユーザーセッションで Web カメラを選択すると、Web カメラのビデオフレームが応答しなくなります。
  - GraphEdit ツールを使用して仮想 Web カメラを起動し、メニューで［クロックを使用する］オプションを選択した場合。
  - Citrix Diagnostics Facility（CDF）トレースを分析すると、VDA と Citrix Receiver for Windows 間のデリバリーパイプラインが確立されたときに、ビデオサンプルが 1 つしか配信されません。[LC8382]
- レジストリキー **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook** の **ExcludedImageNames** に複数の実行可能ファイルが追加されている場合、Citrix Hook を無効にできないことがあります。[LC8614]
- リモートデスクトップセッションが切断されて再接続すると、VDA for Server OS に偽の XenApp セッションが作成されることがあります。[LC8706]
- H 構成を使用するマルチモニター環境では、マウスの動作が一貫しないことがあります。Microsoft Skype for Business セッションを開始し、他のユーザーと画面の共有を開始します。Citrix グラフィックドライバーは、オペレーティングシステムから誤ったマウスの位置情報を受け取ります。

  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\ICA

  名前：DisableAppendMouse

  種類：DWORD

  値：00000001

  ただし、レジストリキーを設定した後で HDX セッションを使用すると、プログラムによってマウスポインターの位置を設定する特定の機能が意図したとおりに機能しない場合があります。以下は対象の機能です。
  - マウススナップ機能。
  - ユーザー間のマウスの位置を GotoMeeting の画面共有と同期させる機能。
  - ユーザー間のマウスの位置を Skype for Business の画面共有と同期させる機能。[LC8976]
- 特定のシナリオで、VDA がイベント ID 1048 で自動的に再登録されることがあります。たとえば、Lotus Notes と Lotus Notes Standard という似た名前の 2 つのアプリケーションを起動し、起動した 2 つ目のアプリケーションを閉じると、1 つ目のアプリケーションのエントリがレジストリから削除されます。この情報が通知を介して Delivery Controller に送信されると、その通知は拒否され、再登録が行われます。[LC9223]
- HDX RealTime Connector が予期せず終了することがあります。ビデオプレビューウィンドウが閉じるか、ビデオプレビューウィンドウにブラックボックスが短時間表示され、その後閉じます。この問題は、HDX RealTime Media Engine がエンドポイントにインストールされていない場合に発生します。[LC9282]

- 公開デスクトップで Microsoft Excel 2007 を起動し、マクロを有効にした.xslm ファイルを開き、Desktop Viewer のウィンドウモードでファイルのサイズを変更します。セッションが応答しなくなることがあります。キーボードショートカットの **Alt+Enter** キーを使用しているときに、この問題が発生します。[LC9379]
- Citrix Audio Service が予期せず終了し、再度再起動することがあります。2 番目のエンドポイント（シンクライアント）から同じセッションに再接続すると、新しいデバイスはセッションに正しくマッピングされません。[LC9381]
- VDA 上で実行されている公開アプリケーションでクリップボードのクリアまたは削除を選択すると、VDA クリップボードはクリアされますが、テキストはエンドポイントのクリップボードに残ります。[LC9434]
- 公開アプリケーションセッションが切断され、ユーザーセッションが VDA から正しくログオフされないことがあります。問題が発生すると、再接続できなくなり、Citrix Studio から切断できなくなる可能性があります。この状況を解決するには、PowerShell コマンドを使用してセッションを非表示に設定するか、VDA を再起動します。[LC9444]
- VDA バージョン 7.15.1000 を使用している場合、twi3.dll から異常な数の CPU 命令が発生し、Winlogon.exe プロセスを通過することがあります。[LC9450]
- クライアントドライブのリダイレクトポリシーを無効にして、ユーザーデバイスからアプリケーションを 2 回目に起動すると、アプリケーションの起動に時間がかかることがあります。[LC9477]
- Web ベースのアプリケーションは、Microsoft Internet Explorer または Mozilla Firefox ブラウザを使用して開かれます。アプリケーションで特定のタブを開くと、デスクトップ全体が応答しなくなることがあります。[LC9508]
- サーバー合計インスタンスのパフォーマンスカウンターが **ICA** セッションカウンターに存在しない可能性があります。[LC9537]
- ファイルが分散ファイルシステム（DFS）ドライブ上にある場合、ローカルアプリアクセスとのファイルタイプの関連付けは、有効になっていても機能しないことがあります。[LC9538]
- **Unicode** キーボードレイアウトマッピングを有効にすると、公開アプリケーションをログオフできません。[LC9590]
- キーボードレイアウトを切り替えると、ポップアップウィンドウが表示されることがあります。次のレジストリキーを設定して、ポップアップウィンドウを非表示にします：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  名前：HideNotificationWindow

  種類：DWORD

  値：1[LC9592]
- 公開アプリケーションは、予期されない失敗のため、アプリケーションの起動直後に断続的に終了することがあります。この問題は、アクティブなプロセスに関する情報が取得されたときに発生します。[LC9661]

- 複数ドメインまたは複数フォレスト環境では、ローカルグループの可視性が制限されている場合、2 番目のアプリケーションを起動できないことがあります。[LC9665]
- XenApp および XenDesktop をバージョン 7.6 からバージョン 7.15 LTSR 累積更新プログラム 1 にアップグレードすると、特定のサービスが予期せず停止または終了したり、ログオン中に断続的に応答しなくなることがあります。[LC9679]
- XenApp および XenDesktop 7.15 LTSR 累積更新プログラム 2 をインストールすると、VDA が応答しなくなることがあります。[LC9701]
- Microsoft レジストリ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN で特定の暗号を無効にすると、TLS が有効にならない場合があります。[LC9743]
- セッションログオン中に USB ストレージデバイスを接続すると、一般モードでリダイレクトされます。USB デバイスを取り外した後もドライブが存在する可能性があります。[LC9783]
- VDA にログオンすると、日本語 IME（Input Method Editor）のかな言語入力キーが自動的に有効になることがあります。[LC9932]
- この修正により、ホワイトリストプロセスメカニズムが SCardHook に追加されました。ホワイトリストがレジストリで定義されている場合、ホワイトリストに含まれるプロセスのみがスマートカードのリダイレクトを使用できます。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  名前：HideNotificationWindow

  種類：REG_SZ

  値：<process name> [LC9961]
- wfshell.exe プロセスが、予期せずに終了する場合があります。この結果、その公開アプリケーションの起動に失敗します。[LD0102]
- VDA をバージョン 7.15 の累積更新プログラム 2 にアップグレードするか、バージョン 7.15 の累積更新プログラム 1 から累積更新プログラム 2 にアップグレードすると、レジストリキー HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix 配下の構成された値 **AnonymousUserIdleTime** と **MaxAnonymousUsers** が削除される可能性があります。[LD0378]

スマートカード

- レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent のレジストリ値 DisableLogonUISuppression を 0 に設定します。公開アプリケーションを起動すると、VDA ではスマートカード PIN の入力が必要になる場合があります。**DisableLogonUISuppression** 値 0 により LogonUI PIN プロンプトが表示されないため、Citrix Receiver for Windows に「ローカルセッションマネージャーをお待ちください**...**」というメッセージが表示され、最終的にタイムアウトします。結果として、PIN プロンプトが表示されなくなります。

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\Citrix Virtual Desktop Agent

名前：DisableLogonUISuppressionForSmartCardPublishedApps

種類：DWORD

値：1[LC9059]

システムの例外

- サーバーで picadm.sys の致命的な例外が発生し、バグチェックコード 0x22（FILE_SYSTEM）によるブルースクリーンが表示されることがあります。[LC7726]
- Enlightened Data Transport（EDT）が有効な場合、サーバーで tdica.sys に関する重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** のブルースクリーンが表示されることがあります。[LC8794]
- サーバーで picadm.sys の致命的な例外が発生し、バグチェックコード 0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQ によるブルースクリーンが表示されることがあります。[LC8830]
- VDA で wdica.sys の致命的な例外が発生し、ブルースクリーンエラーが発生することがあります。[LC9695]
- 公開アプリケーションを開始しようとすると、wfshell.exe プロセスが予期せず終了することがあります。この問題は双方向コンテンツリダイレクトポリシーが有効な場合に発生し、URL は提供されません。[LC9705]
- アプリケーションを起動すると、wfshell.exe プロセスが予期せず終了することがあります。この問題は、icaendpoint.dll モジュールに障害がある場合に発生します。[LC9737]
- Microsoft Windows Server 2008 R2 で重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** によるブルースクリーンが表示されることがあります。この問題は、XenApp および XenDesktop 7.15 LTSR CU2 が Microsoft Windows Server にインストールされている場合に発生します。[LC9849]
- picavc.sys でサーバーに重大な例外が発生し、バグチェックコード **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** によるブルースクリーンが表示されることがあります。[LD0006]

ユーザーエクスペリエンス

- VDA for Server OS で実行されている特定のサードパーティアプリケーション（Aurion など）からハイパーリンクを開こうとすると、URL の先頭に余分な文字列「%1」が追加されることがあります。[LC8952]
- 公開アプリケーションのサイズを変更し、そのアプリケーションをあるモニターから別のモニターに移動しようとすると、アプリケーションの周りに白い罫線が表示されることがあります。[LC9570]
- **Unicode** キーボードレイアウトマッピングを使用するように VDA を設定して、ローカル IME を有効にした状態で Citrix Receiver から HDX セッションを確立します。公開アプリケーションで任意の文字を入力し、

出力された文字の一部または全部を選択すると、選択した文字が新しい文字に置き換わるのではなく、選択した文字の前に新しい文字が挿入されます。[LC9591]

ユーザーインターフェイス

- 法的通知はユーザーセッションのログオン画面の開始時に表示されます。ローカルアプリアクセスを有効にした状態で、ログオン画面で［**OK**］をクリックして続行すると、ログオンを続行する前に画面に法的通知が数秒間表示されることがあります。[LC9408]
- シームレスなセッションのアプリケーションウィンドウが応答しなくなると、アプリケーションウィンドウのタスクバーアイコンが削除され、再度作成される可能性があります。[LC9807]
- 公開アプリケーションを起動しようとすると、Citrix Receiver for Windows の画面が右下に表示されることがあります。[LC9817]

仮想デスクトップコンポーネント **-** その他

- VDA から App-V パッケージを非公開および削除しようとすると失敗する可能性があります。[LC9161]
- Machine Creation Services のストレージ最適化（MCSIO）でキャッシュオーバーフローが発生すると、XenServer 仮想マシンのパフォーマンスが低下する可能性があります。[LC9351]
- VDA で実行されている WMI クエリは、無期限に応答しなくなる可能性があります。[LC9510]
- 同じセッションで同じ App-V アプリケーションの複数のインスタンスを実行しようとすると、失敗する可能性があります。この問題は、実行中のプロセスがマニフェストファイルで定義されているプロセスと異なる場合に発生します。[LC9652]
- Microsoft Edge ブラウザが VDA で実行されている場合、ユーザーを検索する際に、Citrix Director のアクティビティマネージャーで、複数のアプリケーションエントリが表示されることがあります。[LC9673]

累積更新プログラム **2**（**CU2**）

September 16, 2021

リリース日：2018 年 4 月 17 日

このリリースについて

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

7.15 LTSR（一般情報）

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

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

ダウンロード

7.15 LTSR CU2 をダウンロード

新しい展開環境

新しく CU2 を展開するには

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

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

既存の展開環境

更新対象について

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

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

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.2000	
VDA for Server OS	7.15.2000	
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
グループポリシー管理のエクスペリエンス	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
ユニバーサルプリントサーバー	7.15.2000	
Session Recording	7.15.2000	Platinum Edition のみ
Linux VDA	7.15.2000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.2000	
フェデレーション認証サービス	7.15.2000	

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

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

7.15 LTSR CU2 互換性のあるコンポーネントおよびプラットフォーム	バージョン
App Layering	4.10.0
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.4
ライセンスサーバー	11.14.0.1 ビルド 23101
セルフサービスパスワードリセット	1.1.10.0
Workspace Environment Management	4.6

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

詳しくは、「インストールとアップグレード分析」を参照してください。

XenApp 6.5 からの移行

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

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

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

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

August 24, 2021

Citrix Director

- DNS 名でマシンをフィルター処理すると、Citrix Director がマシンを表示しなかったり、重複したエントリが表示されたりすることがあります。この問題は、最初にマシンが Monitor データベースに追加されたものの、2 つの異なる Delivery Controller から同時に追加された場合に発生します。その結果、2 つのマシンエントリが作成されます。[LC4905]
- カスタム管理者として、マシンカタログからリモート PC 設定を取得できない場合、例外が発生することがあります。この問題は、マシンカタログを管理する権限があるにもかかわらず、スコープに特定のカタログが含まれていない場合に発生します。[LC8170]

- Citrix Director で［フィルター］>［セッション］の順に移動して Web ブラウザーのサイズを変更しようとするときに、テーブル全体が正しく配置されないことがあります。[LC8624]
- Citrix Director からデータをエクスポートすると、CSV ファイルが使用できなくなります。英語以外のバージョンの Microsoft Windows を Director の表示言語として設定すると、カンマが値の区切り文字と小数点記号の両方として使用される可能性があるため、この問題が発生することがあります。[LC8625]
- Citrix Director を起動すると、［インフラストラクチャ］タブに次のエラーメッセージが表示されます:

  「データを取得できません。Web サーバーとのネットワーク接続が無効になりました。ネットワーク接続を確認して再試行してください。」[LC8752]
- 複数の Citrix Director サイトを構成するとサイト名の一部が削除されることがありました。[LC9258]

Citrix ポリシー

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

  「Managed Code スナップインでの未処理の例外。」[LC7600]
- グループポリシー管理コンソール（GPMC）を使用して Citrix ポリシーを適用すると、GPMC ポリシー設定でポリシーが表示されないことがあります。ただし、グループポリシーオブジェクト（GPO）の編集で、ポリシーと設定が有効であることが表示されます。[LC8282]
- Citrix グループポリシー管理 3.1 を使用して Active Directory の ［ユーザーポリシー］に ［プリンター割り当て］設定を追加すると、ウィンドウのサイズが変更されるという問題が発生することがあります。ウィンドウを開いた後、ウィンドウのサイズが、画面の角に達するまで自動的に横方向に拡大されることがあります。その結果、すべての列にはアクセスできないため、ポリシーの編集が難しくなる場合があります。[LC8684]
- ローカルポリシーキャッシュフォルダー（%ProgramData%/CitrixCseCache）のファイルが「読み取り専用」に設定されていると、ポリシー設定が正常に適用されないことがあります。[LC8750]
- VDA からシングルユーザー管理モードで App-V アプリケーションを起動しようとすると、失敗することがあります。この問題は、**ApplicationStartDetails** レジストリキーの値が空の場合、またはアプリケーションの詳細がレジストリキーに存在しない場合に発生します。[LC8798]
- ユーザーの関連付けに NETBIOS 名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題は NETBIOS 名が間違った URL を使った場合に発生します。[LC9393]

Citrix Studio

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

  「Value cannot be null while publishing the application.」

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

- アプリケーションが Citrix Studio の **Application** ノードのサブフォルダーにある場合、デリバリーグループからアプリケーションを削除しようとすると失敗することがあります。[LC8705]
- ユーザーの関連付けに NETBIOS 名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題は NETBIOS 名が間違った URL を使った場合に発生します。[LC9393]

コントローラー

- 日本語 OS 上にインストールされた Citrix サービスの「サービス表示名」と「サービスの説明」の末尾に、不必要な文字が表示される場合があります。[LC5208]
- Citrix Director からセッションのデータを取得しようとすると、null エントリが監視データベースに表示されます。その結果、特定のデータが Citrix Director に表示されず、次のエラーメッセージが表示されます。

  「データを取得できませんでした」[LC6273]
- Linux VDA からアプリケーションを手動で追加しようとすると、次のエラーメッセージが表示されることがあります。

  「Value cannot be null while publishing the application.」

  ただし、表示されたエラーメッセージで［OK］をクリックすると、アプリケーションは正常に追加されます。[LC7910]
- Delivery Controller をバージョン 7.15 LTSR にアップグレードすると、マシンカタログの更新後に作成された古い基本ディスクがハイパーバイザーのイメージから削除されません。[LC8637]
- Citrix Broker Service（Brokerservice.exe）が突然終了することがあります。この問題は、LicPolEng.dll モジュールに障害がある場合に発生します。[LC8638]
- Machine Creation Services を使用して最小限必要な VMware 権限で仮想マシン（VM）をプロビジョニングすると、VM の削除が失敗することがあります。このエラーは、最小限許可されている VMware 権限でも発生する可能性があります。[LC8868]
- Premium Storage を使用するマシンカタログを作成しようとすると、E シリーズまたは L シリーズタイプの仮想マシンサイズを選択するオプションが使用できない場合があります。[LC9052]
- ゾーン基本設定が割り当てられている Active Directory ユーザーが削除されると、セカンダリブローカーへのブローカー構成のインポートが失敗することがあります。XenDesktop を最新のバージョンにアップグレード後、インポート操作が失敗することがあります。[LC9269]
- ユーザーの関連付けに NETBIOS 名を使って、デリバリーグループにマシンを追加しようとすると、失敗する場合があります。代わりに、ドメイン名が表示されることがあります。この問題は NETBIOS 名が間違った URL を使った場合に発生します。[LC9393]

HDX MediaStream Flash リダイレクト

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

インストーラー

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

Linux VDA

Profile Management

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

Provisioning Services

StoreFront

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

- **Set-STFWebReceiverSiteStyle** コマンドを使用して StoreFront ロゴを変更しようとすると、失敗することがあります。[LC8994]
- Citrix Receiver for Web サイトのカスタムファイルディレクトリ内に読み取り専用ファイルが存在する場合、StoreFront をアップグレードしようとすると失敗することがあります。[LC9252]

VDA for Desktop OS

HDX 3D Pro

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

HDX MediaStream Flash リダイレクト

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

HDX MediaStream Windows Media リダイレクト

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

HDX RealTime

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

キーボード

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

印刷

- Microsoft Word を使用してプリンター設定で用紙の両面に印刷しようとすると、失敗することがあります。[LC7501]

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

セッション/接続

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

  この修正を有効にするには、以下のレジストリ値を「0」に設定します。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名前：CacheTimeout
  種類：REG_DWORD
  値：デフォルト値は 60 秒です。CacheTimeOut が「0」に設定されている場合、ファイルの長さは直ちに再ロードされます。「0」に設定されていない場合は、定義されたタイムアウトが経過した後にロードされます。[LC6314]
- 従来のグラフィックモードを使用している場合、VDA for Desktop OS で実行されているセッションが応答しなくなることがあります。問題が発生すると、Desktop Viewer で更新操作ができなくなる場合がありますが、Desktop Viewer は応答します。また、30～60 分後には応答していなかったセッションも回復します。[LC7777]
- 残留セッション機能を有効にしてアプリケーションを起動すると、アプリケーションが表示された後にセッションがログオフすることがあります。[LC8245]
- VDA for Desktop OS を起動しようとすると、デスクトップが起動されてから数秒後に消えることがあります。[LC8373]
- 以下のいずれかの場合、Windows エクスプローラーは予期せずに閉じてしまうことがあります。
  - 名前に 260 文字を越える文字が含まれているファイルを大量に選択して、［送る］>［FAX 受信者］オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDF を使用して、ファイルを結合しようとした場合。[LC8423]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在の VDA for Desktop OS セッションには適用されても、それ以降のセッションには保持されないことがあります。この変更を永続的にするには、以下のレジス

トリキーを設定します。

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

- セッションを切断すると、次のローカルログオン時に monitor1 がプライマリモニターとして誤って表示されることがあります。この現象は、マルチモニター環境でリモート PC アクセス VDA にローカルでログオンし、monitor2 をプライマリモニターとして構成してからユーザーデバイス経由で接続し、Desktop Viewer を使用してセッションを切断する時に発生することがあります。[LC8675]

  この修正を有効にするには、VDA for Desktop OS で以下のレジストリキーを設定します：

  パス：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  名前：UseSDCForLocalModes

  種類：REG_DWORD

  データ：1

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

  この修正を有効にするには、以下のレジストリキーを設定します：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  名前：EnableSCardHookVcResponseTimeout
  種類：DWORD
  値：1 [LC8969]

- VM Hosted Apps を開こうとして失敗することがあります。[LC9001]
- セッションに再接続できないことがあります。[LC9040]
- セッションで WFAPI SDK **WFQuerySessionInformation** コマンドを使用して、インストールされている VDA のバージョン情報を取得するときに、コマンドが機能しないことがあります。[LC9041]
- XenApp および XenDesktop をバージョン 7.14 から 7.15 にアップグレードした後、公開アプリケーションのタブを切り替えると、アプリケーションが応答しなくなる可能性があります。また、シームレスウィンドウのサイズを小さなサイズに変更してからウィンドウを広げると、ウィンドウ内のすべての要素を描画するのに時間がかかります。[LC9078]
- 公開アプリケーションは、アプリケーションの起動直後に断続的に終了することがあります。[LC9167]
- 初期接続とは異なる画面解像度で Millennium スイート内のシームレスなアプリケーションに再接続すると、アプリケーションが誤ったサイズに変更されることがあります。その結果、ウィンドウが切り捨てられることがあります。[LC9214]
- ユーザーデバイス経由で Windows 10 バージョン 1709 の公開デスクトップに接続しようとすると、灰色の画面が表示されることがあります。ハイパーバイザーのコンソールから公開デスクトップに接続しようとすると、黒い画面に回転ホイールが表示されます。ただし、RDP 経由で公開デスクトップに接続すると正常に機能します。[LC9215]
- Citrix Receiver for Mac からアプリケーションを起動できないことがあります。この問題は、クライアントライセンス（LicenseRequestClientLicense）を取得できない場合に発生します。[LC9286]
- HDX 3D Pro が有効な場合、XenDesktop を起動しようとすると断続的に失敗することがあります。この問題は、GPU に障害が発生した場合に発生します。[LC9343]
- スムースローミングで、ユーザーセッションから管理対象外リモートデスクトップセッションにセッションが正しく表示されない可能性があります。[LC9471]

スマートカード

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

システムの例外

- サーバーにおいて、バグチェックコード 0x22 の重大な例外が picadm.sys で発生し、ブルースクリーンが表示されることがあります。[LC6177]
- サーバーの致命的な例外が発生し、picadm.sys のバグチェックコード 0x00000050(PAGE_FAULT_IN_NONPAGED_ARE によるブルースクリーンが表示されことがあります。[LC6985]
- サーバーにおいて、バグチェックコード 0x22 の重大な例外が picadm.sys で発生し、ブルースクリーンが表示されることがあります。[LC7574]

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

ユーザーエクスペリエンス

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

ユーザーインターフェイス

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

その他

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

VDA for Server OS

HDX MediaStream Windows Media リダイレクト

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

HDX RealTime

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

キーボード

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

印刷

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

サーバー/サイトの管理

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

セッション/接続

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

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

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

  この修正を有効にするには、以下のレジストリ値を「0」に設定します。

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

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

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

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

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

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

  「イベント ID 1009、picadm: クライアントからの応答メッセージを待機中のタイムアウト」[LC8339]

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

  - 名前に 260 文字を越える文字が含まれているファイルを大量に選択して、［送る］>［FAX 受信者］オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDF を使用して、ファイルを結合しようとした場合。[LC8423]

- Citrix Director で、複数の接続障害が報告されることがあります。この問題は、アプリケーションの表示制限を制御するために割り当てられたグループの拡張が、ユーザーごとに使用されている場合に発生します。この拡張プロセスは完了までに時間がかかり、複数のドメインにまたがる多数のグループがある大規模なネットワークで発生することがあります。[LC8652]
- COM ポートは、バージョン 7.15 の VDA にマップできないことがあります。[LC8656]
- Microsoft Windows Server 2012 または 2016 で実行されている公開アプリケーションを開始しようとすると、ロックアウトされる可能性があります。[LC8681]
- マルチモニター環境でアプリケーションを起動すると、両方のモニターにわたってログオンバナーが表示されることがあります。1 台のモニターを使用する場合、ログオンバナーウィンドウは全画面で表示されます。[LC8741]
- ローカルアプリアクセスが有効な場合、Microsoft Windows 10 で実行されている公開デスクトップでアプリケーションを開こうとすると、アプリケーションを最小化できません。[LC8813]
- ユーザーデバイスを VDA に接続すると、デスクトップが表示されないことがあります。代わりに、灰色の画面がデスクトップに表示されます。[LC8821]
- DLP ソフトウェアが UNC リンクでファイルをスキャンできないことがあります。[LC8893]
- 公開アプリケーションを起動すると、NumLock キーが機能しません。この問題は、NumLock キーの LED がユーザーデバイス上で表示されているにもかかわらず、ユーザーセッション内で数字が機能していない場合に発生します。新しく作成されたリモートデスクトップが LED 状態を初期化するよりも早くクライアントが LED の更新を要求した場合に発生します。この場合、WinStation は LED 状態を更新せず、LED 状態がエンドポイントと VDA 間で同期していない可能性があります。[LC8921]
- アプリケーションやデスクトップを起動しようとしても失敗することがあります。VDA for Server OS が応答しなくなると、この問題が発生することがあります。

  この修正を有効にするには、以下のレジストリキーを設定します:

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

- 初期接続とは異なる画面解像度で Millennium スイート内のシームレスなアプリケーションに再接続すると、アプリケーションが誤ったサイズに変更されることがあります。その結果、ウィンドウが切り捨てられることがあります。[LC9214]
- Citrix Receiver for Mac からアプリケーションを起動できないことがあります。この問題は、クライアントライセンス（LicenseRequestClientLicense）を取得できない場合に発生します。[LC9286]

スマートカード

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

システムの例外

- サーバーにおいて、バグチェックコード 0x22 の重大な例外が picadm.sys で発生し、ブルースクリーンが表示されることがあります。[LC6177]
- サーバーの致命的な例外が発生し、picadm.sys のバグチェックコード 0x00000050(PAGE_FAULT_IN_NONPAGED_ARE によるブルースクリーンが表示されことがあります。[LC6985]
- サーバーにおいて、バグチェックコード 0x22 の重大な例外が picadm.sys で発生し、ブルースクリーンが表示されることがあります。[LC7574]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、icaendpoint.dll モジュールに障害がある場合に発生します。[LC7694]
- サーバーで vdtw30.dll の致命的な例外が発生し、停止コード SYSTEM_SERVICE_EXCEPTION（3b）によるブルースクリーンが表示されることがあります。[LC8087]
- サーバーにおいて、バグチェックコード 0x3B の重大な例外が pdcrypt2.sys で発生し、ブルースクリーンが表示されることがあります。この問題は、VDA を起動するときに発生します。[LC8328]
- HDX 3D Pro および GPU ハードウェアエンコーディングが有効になっている場合に、NVIDIA GPU を使用すると、Citrix ソフトウェアグラフィックスプロセス（Ctxgfx.exe）が予期せず終了することがあります。この問題は、高解像度の画面を使用する場合に発生します。[LC8435]
- サーバーで重大な例外が発生し、icardd.dll のバグチェックコード 0x0000003B によるブルースクリーンが表示されることがあります。[LC8492]
- VDA for Server OS の picadm.sys でブルースクリーンエラーが発生することがあります。[LC8708]
- サーバーで重大な例外が発生し、icardd.dll のバグチェックコード 0x0000003B によるブルースクリーンが表示されることがあります。[LC8732]
- VDA で picadm.sys の致命的な例外が発生し、バグチェックコード 0x22 によるブルースクリーンが表示されることがあります。[LC8749]

- VDA を再起動して初めてログオンすると、予期しないアクセス違反の例外が発生することがあります。Citrix ソフトウェアグラフィックプロセス（Ctxgfx.exe）が予期せず終了します。その結果、VDA に表示される画像やテキストの品質が低下する可能性があります。[LC9005]
- 以下のいずれかの場合、Windows エクスプローラーは予期せずに閉じてしまうことがあります。
  - 260 文字を超える名前のファイルを大量に選択して、［送る］>［**FAX** 受信者］オプションを選択した場合。
  - サードパーティのアプリケーションを開こうとした場合。
  - Nitro PDF を使用して、ファイルを結合しようとした場合。[LC9076]

ユーザーエクスペリエンス

- クライアント上で実行されているアプリケーションからコンテンツをコピーして、ユーザーセッションでアプリケーションに貼り付けるときに、そのコンテンツが貼り付けられないことがあります。また、［貼り付け］が無効になっていることがあります。[LC8516]
- VDA for Server OS では、マウスカーソルがセッションから消えることがあります。この問題は、カーソルがテキスト選択カーソルに変更され、背景色がテキスト選択カーソルの色と同じである場合に発生します。Microsoft Windows の編集可能領域のデフォルトの背景色は白で、デフォルトのテキスト選択カーソルの色も常に白です。その結果、カーソルが表示されなくなる可能性があります。[LC8807]
- Microsoft Windows で、正しい資格情報を送信した後でも、セッションログオン中にパスワードフィールドが編集可能のままになることがあります。[LC9407]

ユーザーインターフェイス

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

その他

- Linux VDA のセッション表示を確認するために使用される一部のサードパーティアプリケーションでは、すべてのピクセルが表示されないことがあります。[LC8419]
- RunOnce レジストリキーが正しく実装されていない可能性があります。[LC9260]
- この修正では、Enlightened Data Transport（EDT）のパフォーマンスおよび品質のマイナーな強化に対応しています。[LC9278]

仮想デスクトップコンポーネント **-** その他

- VDA バージョン 7.15 LTSR を使用している場合に、Active Directory の LastPasswordset 属性が正しく更新されないことがあります。[LC8387]

- Delivery Controller をバージョン 7.15 にアップグレードすると、匿名ユーザー用のアクティブなセッションで、ログオンが継続中であると表示されます。この状況により、VDA の読み込みインデックスが不正になります。[LC8771]
- 起動されたアプリケーションが、ダブルホップシナリオで Citrix Director のアクティビティマネージャーに表示されないことがあります。[LC8985]
- Delivery Controller と VDA 間の登録ステータスが一致せず、VDA の起動時に再登録が必要になることがあります。[LC9216]

その他

Citrix Telemetry Service が無効になっているか停止している場合、メタインストーラーを使用して XenApp および XenDesktop 7.15 LTSR を累積更新プログラム 1（CU1）にアップグレードすると、次の警告メッセージが表示されることがあります:

「Call Home に登録するための Citrix サービスを開始できません。ガイダンスについては、CTX218094 を参照してください。」[LCM-3642]

累積更新プログラム **1**（**CU1**）

September 16, 2021

リリース日：2017 年 12 月 4 日

このリリースについて

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

7.15 LTSR（一般情報）

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

このリリースの既知の問題について

廃止と削除

Citrix Product Subscription Advantage の有効期限

7.6 LTSR CU5 からアップグレードする前に

7.6 LTSR CU5 から 7.15 LTSR CU1 へのアップグレードする主な利点は、基本の 7.15 LTSR には、基本の 7.6 LTSR よりも多くの機能が含まれていることです。ただし、アップグレードを検討している場合、7.6 LTSR CU5 に含まれ

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

新しい展開環境

新しく CU1 を展開するには

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

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

既存の展開環境

更新対象について

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

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

7.15 LTSR CU1 ベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15.1000	
VDA for Server OS	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	
グループポリシー管理のエクスペリエンス	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	

7.15 LTSR CU1 ベースラインコンポーネント	バージョン	メモ
ユニバーサルプリントサーバー	7.15.1000	
Session Recording	7.15.1000	Platinum Edition のみ
Linux VDA	7.15.1000	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15.1000	
フェデレーション認証サービス	7.15.1000	

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

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

7.15 LTSR 互換性のあるコンポーネントおよびプラットフォーム	バージョン
AppDNA	7.16
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.13
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.14
HDX RealTime Optimization Pack	2.2.100
ライセンスサーバー	11.14.0.1 ビルド 22103
Workspace Environment Management	4.4
App Layering	4.6
セルフサービスパスワードリセット	1.1

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、XenApp および XenDesktop 7.15 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

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

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

インストールとアップグレード分析

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

詳しくは、「インストールとアップグレード分析」を参照してください。

XenApp 6.5 からの移行

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

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

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

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

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

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

- LC6311
- LC6985
- LC7430
- LC7450
- LC7574
- LC7600
- LC7777
- LC7911
- LC8046
- LC8080
- LC8130

- LC8170
- LC8281
- LC8339
- LC8492
- LC8732
- LC8750
- LC8774

解決された問題

August 24, 2021

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

Citrix Director

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

Citrix ポリシー

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

Citrix Studio

- ユーザーが割り当てたマシンをデリバリーグループに追加しようとすると、未割り当てのマシンが［マシン割り当て］ページに表示されることがあります。[LC6755]

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

  「エラー ID：XDDS:ABB14FD9」[LC7961]

- 英語以外の Windows オペレーティングシステムで実行されている場合、[接続およびリソースの追加] ページで［Use storage local to the hypervisor］オプションのテキストが省略されることがあります。[LC8041]
- Citrix Studio をバージョン 7.14.1 にアップグレードした後、既存の App-V パッケージの［使用者］列（アプリケーションが使用されるデリバリーグループを指す）が空白になることがあります。[LC8075]
- Citrix Studio でデリバリーグループリンクをクリックすると、選択したデリバリーグループノードに移動しないことがあります。[LC8095]
- 「プリンター割り当て」ポリシーを管理しようとすると、以下の問題が発生することがあります。
  - プリンター割り当てポリシーを追加または編集しようとすると、例外「InvalidCastException」が発生します。
  - 新しいセッションプリンターを追加しようとすると、例外「InvalidOperationException」が発生します。
  - プリンター割り当てポリシーからセッションプリンターを削除しようとすると失敗します。この問題は、［Remove］オプションを無効にすると発生します。
  - 「プリンター割り当て」ポリシーの検索ボックスで入力をやめると、検索処理が開始されません。
  - セッションプリンターの上書き設定チェックボックス（PrintQuality、PaperSize、Scale、TrueTypeOption）は、前回無効にした場合でも、常に有効になっています。[LC8146]
- Delivery Controller をバージョン 7.15 にアップグレードすると、Delivery Controller での Citrix Studio の起動に失敗することがあり、次のエラーメッセージが表示されます。

  “MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand” [LC8396]

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

コントローラー

- デリバリーグループに保守モードのもう 1 つの VDA が含まれる場合、公開アプリケーションを起動するデリバリーグループを選択できないことがあります。[LC6943]
- Machine Creation Services（MCS）を使用して作成されたマシンカタログを更新すると、vSAN 6 以降のバージョンでホストされている仮想マシンが起動に失敗することがあります。VMware コンソールに次のエラーメッセージが表示されます。

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

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

  「エラー ID: XDDS:ABB14FD9」[LC7961]

- Citrix Director は 1 時間ごとに間違った切断セッション数を表示することがあります。[LC8006]
- サーバー OS でセッションの「AllowRestart」ポリシーによって、ユーザーが切断されたセッションからログオフできません。切断されたセッションを再起動すると、新しいセッションが開始されず、前回のセッションに再接続されます。[LC8090]
- 「プリンター割り当て」ポリシーを管理しようとすると、以下の問題が発生することがあります。
  - プリンター割り当てポリシーを追加または編集しようとすると、例外「InvalidCastException」が発生します。
  - 新しいセッションプリンターを追加しようとすると、例外「InvalidOperationException」が発生します。
  - プリンター割り当てポリシーからセッションプリンターを削除しようとすると失敗します。この問題は、［Remove］オプションを無効にすると発生します。
  - 「プリンター割り当て」ポリシーの検索ボックスで入力をやめると、検索処理が開始されません。
  - セッションプリンターの上書き設定チェックボックス（PrintQuality、PaperSize、Scale、TrueTypeOption）は、前回無効にした場合でも、常に有効になっています。[LC8146]
- Monitoring Service が、監視データベースへの新しいセッションデータの挿入に失敗することがあります。[LC8191]
- ［**Director**］>［傾向］>［ログオンパフォーマンス］の下の［ユーザーセッションごとのログオン期間］パネルに、一部のログオンレコードしか表示されないことがあります。[LC8265]
- Delivery Controller をバージョン 7.15 にアップグレードすると、Delivery Controller での Citrix Studio の起動に失敗することがあり、次のエラーメッセージが表示されます。

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

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

HDX MediaStream Flash リダイレクト

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

Linux VDA

Profile Management

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

Provisioning Services

StoreFront

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

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

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

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

VDA for Desktop OS

HDX MediaStream Flash リダイレクト

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

HDX Plug-n-Play

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

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

印刷

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

サーバー/サイトの管理

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

セッション/接続

- ローカルアプリアクセスが有効な場合、インタラクティブなログオン時の免責事項ポリシーを使用すると、黒または灰色の画面が 45 秒間表示されることがあります。[LC6518]
- アプリケーションに再接続しようとすると、失敗することがあります。この問題は、セッションが最初に切断されたときに切断されたアプリケーションのいずれかが応答しなくなった場合に発生します。[LC6550]
- HDX 3D Pro を使用してデュアルモニターセッションをロックすると、プライマリモニターだけがロックされます。[LC7767]

- Skype for Business のビデオ通話を確立すると、サードパーティアプリケーションのウィンドウと交差した後、青色のウィンドウ枠が表示されることがあります。[LC7773]
- ローカルアプリアクセスが有効な場合、インタラクティブなログオン時の免責事項ポリシーを使用すると、黒または灰色の画面が表示されることがあります。[LC7798]
- 一部の公開アプリケーションが、最大化されたときに画面全体が表示されないことがあります。[LC7854]
- VDA バージョン 7.9 上で実行される、2 つの Microsoft Excel 2010 ワークシート間で挿入処理を実行する場合、Excel のウィンドウが応答しなくなることがあります。[LC7912]
- 特定のシナリオでは、シームレスモードでシームレスアプリケーションが表示されない、または一部の機能が動作しないことがあります。[LC8030]
- VDA で HDX 3D Pro を有効にし、ログオン画面が表示されたときの「ログオンしようとしているユーザー向けのメッセージテキスト」のポリシーを有効にすると、公開されたデスクトップの起動に失敗し、灰色の画面が表示されることがあります。

  この修正を有効にするには、以下のレジストリキーを設定します:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig
  名前：HKLM_DisableMontereyFBCOnInit
  値：DWORD 種類:
  有効にする場合は 1[LC8082]
- ローカルアプリアクセスを有効にした状態で、対話型のログオン免責事項ポリシーを使用すると、VDA に接続したときに Desktop Viewer に灰色の画面が表示されることがあります。[LC8136]
- Skype for Business や VLC メディアプレーヤーなど、リダイレクトされた Web カメラを使用するアプリケーションを使用していると、初期セッションの開始時に Web カメラがリダイレクトされて検出される場合があります。ただし、ユーザーセッションに再接続すると、Web カメラは検出されなくなります。代わりに、ビデオプレビューではなく灰色の画面が表示されます。[LC8588]

スマートカード

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

システムの例外

- wfshell.exe プロセスが予期せず終了し、タスクバーのグループ化モジュールを指すことがあります。[LC6968]
- USB リダイレクトポリシーを有効にすると、VDA に致命的な例外が発生し、バグチェックコード SYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）のブルースクリーンが表示されることがあります。[LC7999]

- バグチェックコード 0x7E による重大な例外エラーが発生し、VDA でブルースクリーンが表示されることがあります。この問題は、しばらくの間 VDA セッションをアイドル状態のままにした場合に発生します。[LC8045]
- サーバーに致命的な例外が発生し、picavc.sys のバグチェックコード SYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）によるブルースクリーンが表示されることがあります。[LC8063]

ユーザーエクスペリエンス

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

ユーザーインターフェイス

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

VDA for Server OS

HDX MediaStream Flash リダイレクト

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

HDX Plug-n-Play

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

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

印刷

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

サーバー/サイトの管理

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

セッション/接続

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

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

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名前：MaxPolicyAge
    種類：DWORD
    値：最後のポリシー評価とエンドポイントでのライセンス認証の間で許容される最長時間（秒単位）。デフォルトは 30 秒です。
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名前：PolicyTimeout
    種類：DWORD
    値：ポリシーが最新ではないと判断した後、システムがポリシーを待機する最長時間（ミリ秒単位）。デフォルトは 4,000 ミリ秒です。タイムアウトが発生すると、システムはポリシーを読み取り、初期化を

続行します。この値を（0）に設定すると、Active Directory ポリシーチェックは行われず、ポリシーがすぐに処理されます。[LC7495]

- Skype for Business のビデオ通話を確立すると、サードパーティアプリケーションのウィンドウと交差した後、青色のウィンドウ枠が表示されることがあります。[LC7773]
- 一部の公開アプリケーションが、最大化されたときに画面全体が表示されないことがあります。[LC7854]
- vGPU を使用しているときに VDA のバージョン 7.13、7.14、または 7.15 にアップグレードすると、Microsoft Windows Server オペレーティングシステムで実行されている公開アプリケーションまたはデスクトップに黒い領域が表示されることがあります。[LC7875]
- VDA バージョン 7.9 上で実行される、2 つの Microsoft Excel 2010 ワークシート間で挿入処理を実行する場合、Excel のウィンドウが応答しなくなることがあります。[LC7912]
- 特定のシナリオでは、シームレスモードでシームレスアプリケーションが表示されない、または一部の機能が動作しないことがあります。[LC8030]
- ローカルアプリアクセスを有効にした状態で、対話型のログオン免責事項ポリシーを使用すると、VDA に接続したときに Desktop Viewer に灰色の画面が表示されることがあります。[LC8136]
- 障害通知が Delivery Controller に送信されると、サーバー OS の VDA が断続的に再登録されることがあります。[LC8228]
- Skype for Business や VLC メディアプレーヤーなど、リダイレクトされた Web カメラを使用するアプリケーションを使用していると、初期セッションの開始時に Web カメラがリダイレクトされて検出される場合があります。ただし、ユーザーセッションに再接続すると、Web カメラは検出されなくなります。代わりに、ビデオプレビューではなく灰色の画面が表示されます。[LC8588]

スマートカード

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

システムの例外

- wfshell.exe プロセスが予期せず終了し、タスクバーのグループ化モジュールを指すことがあります。[LC6968]
- タスクバーのボリュームコントロールをクリックすると、Windows シェルエクスペリエンスホストが突然終了することがあります。[LC7000]
- サービスホスト（svchost.exe）プロセスで、アクセス違反が発生して、予期せずに終了する場合があります。この問題は、icaendpoint.dll モジュールに障害がある場合に発生します。[LC7900]

- USB リダイレクトポリシーを有効にすると、VDA に致命的な例外が発生し、バグチェックコード SYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）のブルースクリーンが表示されることがあります。[LC7999]
- サーバーに致命的な例外が発生し、picavc.sys のバグチェックコード SYSTEM_THREAD_EXCEPTION_NOT_HANDLED（7e）によるブルースクリーンが表示されることがあります。[LC8063]

ユーザーエクスペリエンス

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

ユーザーインターフェイス

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

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

  この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。[LC6075]
- Excel 2010 で、複数のブックでスプレッドシートを開いた場合、タスクバーに最新のブックしか表示されません。[LC7557]
- Microsoft Windows Server 2008 R2 デスクトップセッションからログオフしようとすると、ログオフ画面が表示されないことがあります。セッションからログオフできたとしても、セッションが予期せずに切断されたように見えます。[LC8016]

仮想デスクトップコンポーネント - その他

- Citrix Director は 1 時間ごとに間違った切断セッション数を表示することがあります。[LC8006]
- Monitoring Service が、監視データベースへの新しいセッションデータの挿入に失敗することがあります。[LC8191]

- [**Director**] > [傾向] > [ログオンパフォーマンス] の下の [ユーザーセッションごとのログオン期間] パネルに、一部のログオンレコードしか表示されないことがあります。[LC8265]
- VDA をインストールした Microsoft Windows 10 を Build 1511 から Build 1703 にアップグレードした後、System Center Configuration Manager（SCCM）クライアントが突然終了することがあります。[LC8632]
- Machine Creation Services (MCS) を使用している場合、Microsoft Office 2016 のリセットが Microsoft Windows 10 で失敗する場合があります。[LC8680]
- 大規模な XenApp および XenDesktop 環境では、Monitor データベースのサイズが大きい場合、Monitor データベースのグルーミングのストアドプロシージャが正しく動作しません。[LC8770]

7.15 LTSR（初期リリース）

September 16, 2021

リリース日：2017 年 4 月 4 日

このリリースについて

XenApp および XenDesktop の 7.15 長期サービスリリース（LTSR）には、Windows VDA の新規バージョンと、複数の XenApp および XenDesktop コアコンポーネントの新規バージョンが含まれています。
次の操作を実行できます：

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

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

- 既存のサイトで **VDA** をインストールまたはアップグレードする

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

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

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

StoreFront

AppDNA

XenApp および XenDesktop 用 Citrix SCOM Management Pack

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

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

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

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

XenApp 6.5 ワーカーから新しい **VDA** へのアップグレード

XenApp 6.5 ファームに移行した後、XenApp 6.5 ワーカーを新しい VDA にアップグレードできます。以前は、ワーカーサーバーで XenApp および XenDesktop インストーラーを実行すれば、自動的に XenApp 6.5 ソフトウェアが削除され、新しい VDA がインストールされました。今回のリリースでは、最初にサーバーから HRP7 と XenApp 6.5 ソフトウェアを別プロセスで削除してください。その後に、新しい VDA をインストールしてください。詳しくは、「XenApp 6.5 ワーカーから新しい VDA へのアップグレード」を参照してください。

MCS の第 **2** 世代 **VM** のサポート

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

ローカルホストキャッシュ

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

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

Director

アプリケーション障害の監視。Director は ［アプリケーション障害］タブで、公開アプリケーションに関連した障害履歴を表示するために、［傾向］ビューが拡張されています。選択されたアプリケーションまたはプロセスが、選択さ

れた期間中、起動時または実行中に発生した障害とエラーを確認することができます。この情報によって、アプリケーション特有の問題を理解して、トラブルシューティングすることができます。詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーション障害履歴の監視」を参照してください。

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

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

Virtual Delivery Agent（VDA）7.15

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

Session Recording 7.15

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

新しい展開環境

新しく 7.15 LTSR を展開するには

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

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

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

既存の展開環境

更新対象について

XenApp および XenDesktop 7.15 LTSR では、7.6 LTSR のすべてのベースラインコンポーネントが更新されています。注意：展開環境のすべての LTSR コンポーネントを 7.15 LTSR に更新することをお勧めします。たとえば、

Provisioning Services が LTSR 展開環境に含まれる場合、Provisioning Services コンポーネントを更新します。Provisioning Services が展開環境に含まれない場合は、インストールや更新を行う必要はありません。

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

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

7.15 LTSR のベースラインコンポーネント	バージョン	メモ
VDA for Desktop OS	7.15	
VDA for Server OS	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
グループポリシー管理のエクスペリエンス	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
ユニバーサルプリントサーバー	7.15	
Session Recording	7.15	Platinum Edition のみ
Linux VDA	7.15	サポートされるプラットフォームについては、Linux VDA のドキュメントを参照してください。
Profile Management	7.15	
フェデレーション認証サービス	7.15	

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

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

7.15 LTSR 互換性のあるコンポーネントおよびプラットフォーム	バージョン
AppDNA	7.15
ライセンスサーバー用 Citrix SCOM Management Pack	1.2
Provisioning Services 用 Citrix SCOM Management Pack	1.19
StoreFront 用 Citrix SCOM Management Pack	1.12
XenApp および XenDesktop 用 Citrix SCOM Management Pack	3.13
HDX RealTime Optimization Pack	2.3
ライセンスサーバー	11.14.0 ビルド 21103
Workspace Environment Management	4.4
App Layering	4.3
セルフサービスパスワードリセット	1.1

Citrix Workspace アプリの互換バージョン

現在サポートされているすべてのバージョンの Citrix Workspace アプリは、Citrix Virtual Apps and Desktops 1912 LTSR と互換性があります。Citrix Workspace アプリのライフサイクルについては、「Citrix Workspace アプリと Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Workspace アプリの新バージョンが利用可能になったときに通知を受けることができるように、Citrix Workspace アプリの RSS フィードに登録することをお勧めします。

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

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

除外対象の機能
Framehawk
StoreFront Citrix Online の統合

除外対象のコンポーネント
Personal vDisk：Windows 10 マシンでは除外されます。
AppDisk

除外対象の **Windows** プラットフォーム *
Windows 2008 32 ビット（ユニバーサルプリントサーバー用）

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

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

XenApp 6.5 からの移行

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

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

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

新しいサイトを必要に応じて再構成してテストします。

詳しくは、「XenApp 6.x からの移行」を参照してください。

解決された問題

October 22, 2021

バージョン 7.14.1 では、次の問題が解決されています。

7.14.1 と比較して解決された問題

7.6 LTSR CU4 と比較して解決された問題

7.14.1 と比較して解決された問題

AppDNA

Citrix Director

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

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

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

  「データを取得できません。」[LC8207]

Citrix ポリシー

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

Citrix Studio

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

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

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

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

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

コントローラー

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

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

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

HDX RealTime Optimization Pack

Profile Management

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

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

StoreFront

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

  「変更の保存時にエラーが発生しました。」[LC7781]

ユニバーサルプリントサーバー

クライアント

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

サーバー

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

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

VDA for Desktop OS

インストール、アンインストール、アップグレード

- VDA をバージョン 5.6.400 からバージョン 7.9 にアップグレードした後、VDA を再起動させると以前のバージョンでインストールされたミラードライバーが残される場合があります。[LC6295]
- Microsoft Windows オペレーティングシステムの英語以外のバージョン上で VDA のバージョン 7.12 または 7.13 をインストールした後に、特定の WMI クラスの名前が変更されることがあります。[LC7555]
- Microsoft Windows オペレーティングシステムの英語以外のバージョン上で VDA のバージョン 7.12 または 7.13 をインストールした後に、特定の WMI クラスの名前が変更されることがあります。[LC7587]

印刷

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

セッション/接続

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

スマートカード

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

システムの例外

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

ユーザーエクスペリエンス

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

  注:

  - この修正は Windows Server 2008 R2 が実行されているセッションには影響しません。
  - この修正を有効にするには、Citrix Receiver 4.4 for Windows Long Term Service Release（LTSR）CU5 以降のバージョン、および XenApp および XenDesktop 7.6 LTSR CU4 以降の VDA バージョンを使う必要があります。[LC5842]
- VDA バージョン 7.9 上で実行される、2 つの Microsoft Excel 2010 ワークシート間で挿入処理を実行する場合、Excel のウィンドウが応答しなくなることがあります。[LC7481]
- マルチモニター環境では、外部モニターを Windows の「メインディスプレイ」として定義し、コントロールパネルのディスプレイ設定でこれをノートブックまたはタブレットのセカンダリモニターの右に配置します。外部モニターに表示される公開アプリケーションを起動し、このアプリケーションを外部モニターに接続されたタブレットモニターまたはノートブックモニターに移動すると、タブレットやノートブックの開閉時に公開アプリケーション画面が黒く表示されることがあります。

  これを修正するには、VDA で次のレジストリキー値を設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire、名前：EnableDrvTw2NotifyMonitorOrigin、種類：REG_DWORD、値：1（有効化）および 0（無効化。デフォルト値）。デフォルトでは、レジストリ値は設定されていません。[LC7760]

ユーザーインターフェイス

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

VDA for Server OS

インストール、アンインストール、アップグレード

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

印刷

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

サーバー/サイトの管理

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

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

セッション/接続

- VDA for Desktop OS 上に同じモデルの複数の Web カメラがインストールされている環境で、最新の Web カメラだけがセッションから認識されマップされることがあります。[LC5008]
- セッションに再接続しようとすると断続的に失敗し、VDA for Server OS が「初期化中」状態に移行します。この問題は VDA が Delivery Controller に再度登録されると発生します。[LC6647]
- Delivery Controller の接続が切断されると、XenApp サーバーでアクティブなセッションが切断されることがあります。この問題は、VDA が「事前起動」から「アクティブ」へ正しく移行するセッションの状態を追跡できない時に発生します。そのため、Delivery Controller が再起動されると、VDA のリソースをクリアし

ようとし、アプリケーションがアクティブにもかかわらず、事前起動状態のセッションが切断されるかログオフされます。[LC6819]

- Microsoft Windows Server 2016 で公開アプリケーションを起動すると、アプリケーションが表示されるまでしばらく黒い画面が表示されることがあります。[LC7947]

システムの例外

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

ユーザーエクスペリエンス

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

  注:

  - この修正は Windows Server 2008 R2 が実行されているセッションには影響しません。
  - この修正を有効にするには、Citrix Receiver 4.4 for Windows Long Term Service Release（LTSR）CU5 以降のバージョン、および XenApp および XenDesktop 7.6 LTSR CU4 以降の VDA バージョンを使う必要があります。[LC5842]

- VDA バージョン 7.9 上で実行される、2 つの Microsoft Excel 2010 ワークシート間で挿入処理を実行する場合、Excel のウィンドウが応答しなくなることがあります。[LC7481]
- マルチモニター環境では、外部モニターを Windows の「メインディスプレイ」として定義し、コントロールパネルのディスプレイ設定でこれをノートブックまたはタブレットのセカンダリモニターの右に配置します。外部モニターに表示される公開アプリケーションを起動し、このアプリケーションを外部モニターに接続されたタブレットモニターまたはノートブックモニターに移動すると、タブレットやノートブックの開閉時に公開アプリケーション画面が黒く表示されることがあります。

  これを修正するには、VDA で次のレジストリキー値を設定します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire、名前：EnableDrvTw2NotifyMonitorOrigin、種類：REG_DWORD、値：1（有効化）および 0（無効化。デフォルト値）。デフォルトでは、レジストリ値は設定されていません。[LC7760]

ユーザーインターフェイス

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

仮想デスクトップコンポーネント **-** その他

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

7.6 LTSR CU4 と比較して解決された問題

Citrix Director

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

Citrix ポリシー

- Citrix ポリシー処理が応答しなくなることがあります。これにより、ユーザーセッションも応答しなくなります。この問題が発生すると、Citrix Receiver およびリモートデスクトップ（RDP）への接続要求が失敗します。[LA4969]
- システムに修正 LC1987（GPCSExt170W2K8R2X64006 またはそれに代わるもの）がインストールされると、Citrix と Microsoft の両方の設定を含む Active Directory（AD）ポリシーが適用されないことがあります。

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

- この機能強化により、Citrix Group Policy Engine は、Citrix ポリシーの処理時に追加のイベントログメッセージを生成します。[LC3664]
- 7.6 からバージョン 7.8 または 7.9 にアップグレードすると、Citrix Studio の一部の配色で、テキストが適切に表示されないほど表示が暗くなることがあります。[LC5690]
- Citrix フェデレーション認証サービスをインストールした後、StoreFront サーバー上の ［ユーザー規則］の下に ［**Security** アクセス制御一覧］を構成しようとすると、構成ウィンドウが応答しなくなる場合があります。[LC5788]
- マクロを含む、XLSM ファイル拡張子のファイルを開く間に、Microsoft Excel の CPU とメモリの消費が急増することがあります。結果として、ファイルを開こうとすると失敗します。[LC6142]
- Citrix と Microsoft の両方の設定を含むグループポリシーオブジェクトが適用されない場合があります。この問題は、一覧内の拡張ユニットが 2 つ以上のグローバル一意識別子を含む場合に発生します。[LC7533]

Citrix Studio

- 複数のユーザーが複数の Studio セッションでポリシーを作成すると、Citrix Studio が更新された時に、一番新しく作成されたポリシーによって、それ以前のポリシーが上書きされます。[LA5533]
- Citrix Studio によって XenDesktop App Edition ライセンスが認識されず、次のエラーメッセージが表示されることがありました。

  「有効なライセンスが見つかりません
  使用できる適切なライセンスがありません。ライセンスサーバーのアドレス、製品エディション、およびモデルを確認してください。」[LC0822]
- クロスドメインユーザーを Delivery Group に追加しようとすると、Citrix Studio によってこれらのユーザーの実際のドメインがローカルドメインアカウントとして解決されるという問題がありました。[LC1886
- 引用符（”）を含むコマンドライン引数を使用して Citrix Studio 7.7 でアプリケーションを公開しようとすると、エラーメッセージが表示されることがあります。[LC4525]
- カタログの更新が実行されていない場合、Citrix Studio がカタログロールバックオプションを提供することがあります。ロールバックを選択すると、例外が発生します。[LC4791]
- Citrix Studio からマシンを Machine Catalog に追加しようとすると、次のエラーメッセージが表示されることがあります。この問題は、XenDesktop セットアップウィザードを使用した場合は発生しません。[LC5030]
- 2 つのアプリケーションが同じ ApplicationID を持つ場合、App-V アプリケーションを更新すると、Citrix Studio による App-V パッケージ名の設定が不正確になることがあります。[LC5261]
- Delivery Controller がオフラインまたは使用不可になると、Citrix Studio の動作が遅くなることがありました。[LC5335]

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

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

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

  たとえば、ドメイン名が xyz.ad.airxyz.aa で、NetBIOS 名が xyz-Ad である場合、GUI モードを使用すると、NetBIOS 名は xyz-Ad の代わりに xyz として受け入れられます。結果として、マシンアカウントは既存および新規のコンピューターアカウントのどちらにも追加できません。[LC6679]
- Citrix Delivery Controller をバージョン 7.12 にアップグレードした後、マルチドメイン環境でマシンを Citrix Provisioning Services（PVS）からカタログに追加しようとすると、失敗する場合があります。この問題は PVS がデバイス名と一緒にドメイン名を返さなかった場合に発生します。Citrix Studio がローカルドメインでアカウント名を検索する場合は、アカウントが見つかりません。[LC6818]
- XenApp サイトをアップグレードした時に、予期せずライセンスモデルが XenApp から XenDesktop に変更される場合があります。[LC6981]

- PowerShell 5 での実行時に、「Get-XDSite」およびその他の XenDesktop の高レベル管理 PowerShell コマンドに対する「Start-Transcript」コマンドが失敗する場合があります。[LC7006]
- 管理者が App-V アプリケーションを分離グループからデリバリーグループに追加しようとするか、分離グループを作成しようとすると、Citrix Studio で以下のエラーメッセージが表示されることがあります。

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

コントローラー

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

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

「内部エラーが発生しました：エラーコード 0x2 により、インベントリの更新に失敗しました。」[LC5051]

- 日本語 OS 上にインストールされた Citrix サービスの「サービス表示名」と「サービスの説明」の末尾に、不必要な文字が表示される場合があります。[LC5208]
- 2 つのアプリケーションが同じ ApplicationID を持つ場合、App-V アプリケーションを更新すると、Citrix Studio による App-V パッケージ名の設定が不正確になることがあります。[LC5261]
- XenApp または XenDesktop を 7.6 から 7.7 にアップグレードした後に、アップグレードを求めるメッセージが Citrix Studio に表示されることがありました。[LC5478]
- アプリケーションのタイトルにアンパサンド（&）が含まれていると、StoreFront XML が破損し、アプリケーションまたはアイコンが表示されなくなることがあります。[LC5505]
- 多くのパッケージを含む App-V サーバーとともに構成されているバージョン 7.9 の Citrix Studio インスタンスを閉じて、再度開こうとした時に、Studio が開いたままになり、開けなくなります。[LC5643]
- XenDesktop 7.9 にアップグレードした後に、NetScaler ブローカーが正しく資格情報を送信しないために、ログオンが失敗することがあります。[LC5753]
- Citrix Studio を使うと、サイトに App-V サーバーを 1 台しか追加できません。更に App-V サーバーをサイトに追加するには、PowerShell を使う必要があります。[LC5767]
- Citrix フェデレーション認証サービスをインストールした後、StoreFront サーバー上の ［ユーザー規則］の下に ［**Security** アクセス制御一覧］を構成しようとすると、構成ウィンドウが応答しなくなる場合があります。[LC5788]
- 分析、ブローカー、ログなどの Flexcast Management Architecture サービスの SDK ポートを変更すると、Citrix Studio が正しく接続されない原因になります。[LC6005]
- Citrix Studio を介して新しい XenDesktop サイトを作成し、SQL AlwaysOn Listener を参照すると、次のエラーが表示されることがあります。

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

- Citrix Monitoring Service または Citrix Delivery Controller の再起動後、イベント ID 1013 が表示される場合があります。

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

  この問題は、Citrix Monitor Service が停止している時に発生します。[LC6438]

- Citrix Delivery Controller 上で特定のサードパーティ製アプリケーション（RayStation など）を使用しようとすると、失敗して次のエラーメッセージが表示されます。

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

- Citrix Studio から追加の Controller を追加するオプションと PowerShell コマンドの「Add-XDController」を使用して、ミラーリングされたデータベースの設定に Delivery Controller を追加しようとすると失敗する場合があります。[LC6563]

- VMware VSAN の MCS カタログを削除しようとすると失敗する場合があります。[LC6691]

- Monitoring Service のメモリ消費が急増する場合があり、これによりサーバーの反応が遅くなります。[LC6705]

- Citrix Studio を以前のバージョンからアップグレードしたり、Citrix Studio バージョン 7.12 を新規インストールしたりした後で、Delivery Controller が原因で Citrix Studio が必須のアップグレードループに陥る場合があります。[LC6737]

- Machine Creation Service のバージョン 7.12 を使用して仮想マシンを作成すると、XenTools のインストールが失敗し、仮想マシンを通常の方法でシャットダウンできません。[LC6769]

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

- App-V パッケージの公開許可を、完全なアクセス権を持たない管理者に設定しようとすると、次の例外が発生して拒否される場合があります。

  「Citrix.Console.Models.Exceptions.PermissionDeniedException：この操作を実行する権限がありません。」[LC6897]

- HighAvailabilityService.exe プロセスによってメモリの消費量が多くなることがあります。[LC6918]

- XenApp サイトをアップグレードした時に、予期せずライセンスモデルが XenApp から XenDesktop に変更される場合があります。[LC6981]

- PowerShell 5 での実行時に、「Get-XDSite」およびその他の XenDesktop の高レベル管理 PowerShell コマンドに対する「Start-Transcript」コマンドが失敗する場合があります。[LC7006]

- この修正により Citrix Host Service のメモリの問題が解決されます。[LC7516]

- カスタムの管理権限を持つ管理者が分離グループを作成しようとすると失敗して、次のエラーメッセージが表示されることがあります。

  「この要求を完了するために必要な権限がありません。詳しくは、XenDesktop サイト管理者に問い合わせてください。」[LC7563]

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

  「不明なエラーが発生しました。」[LC7594]

- Microsoft リモートデスクトップセッションホストの役割サービスが既にインストールされている時に、Microsoft Windows サーバー上に VDA をインストールしようとすると、失敗することがあります。[LC7680]

- Citrix Delivery Controller 上で TLSv1.0 を無効にしようとすると、VMware vCenter ハイパーバイザーとの通信の損失が発生する場合があります。[LC7686]

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

ライセンス

- 「X-Frame-Options」ヘッダータイプが設定されていないため、ライセンスサーバーによる、クリックジャッキングに対する Payment Card Industry（PCI）コンプライアンススキャンが失敗します。[LC1983]

- 名前が 32 文字より多いドメイングループを追加しようとすると、失敗することがあります。[LC1986]

- NetBios ドメイン名にアンパサンド（&）が含まれている場合、Studio で［ライセンス］タブを開こうとすると失敗して次のエラーメッセージが表示されます。

  「Citrix ライセンスサーバーを使用できません」[LC2728]

Profile Management

- ログオンまたはログオフ時に、一部のサードパーティ製アプリケーションによるファイル名の変更やファイルの移動に失敗することがありました。たとえば、ローカルプロファイル内に file0、file1、および file2 という名前のファイルがあった場合に、ログオフ時に file2 から file3、file1 から file2、および file0 から file1 への変更に失敗します。この問題は、待機領域またはユーザーストア内に file2 が既に存在する場合に発生します。[LC0465]

- ユーザーのログオフ時に、Profile Management サービス（UserProfileManager.exe）が異常停止することがありました。[LC0625]

- パフォーマンスモニター（Perfmon）の［ログオン期間］パネルに、Profile Management によって管理されていないユーザーログオンのデータが記録される場合がありました。[LC0779]

- Profile Management によるファイルとユーザーストアの同期が一定期間行われない場合がありました。[LC1338]
- 次のログオプションを有効にすると、デバッグ情報が次のログファイルに記録されませんでした。
  - ポリシー：Active Directory 操作
  - ポリシー：ログオンおよびログオフ時のポリシー値
  - ポリシー：ログオフ時のレジストリ差分 [LC2003]
- ユーザーがhttps://support.microsoft.com/ja-jp/kb/2890783で説明されているようにプロファイルのバージョンを有効にすると、Profile management は次の理由で移行を行わない場合がありました。
  - Microsoft 移動プロファイルが「V4」という拡張子で作成されている。
  - UPM プロファイルが「デフォルトユーザー」テンプレートから移行および作成されなかった。[LC2427]
- ユーザープロファイルを Desktop Director でリセットすると、ユーザーが初めてログオンする場合にフォルダーへのリダイレクトが動作しなくなっていました。フォルダーへのリダイレクトは、ユーザーが後でログオンする時には動作します。[LC2602]
- Profile Management（UserProfileManager.exe）サービスが予期せずに閉じる場合がありました。[LC2979]
- LC0625 の修正を適用すると、Profile Management（UserProfileManager.exe）サービスが予期せずに閉じる場合がありました。[LC3058]
- Windows 8.1 では、拡張保護モードが有効の場合、Internet Explorer 11 を使用してファイルをダウンロードしようとしても失敗します。[LC3464]
- Profile Management でのログオフプロセスで、次のエラーメッセージとともにファイルのロックが発生する可能性があります：

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

  ロックが解除されるまで、Profile Management によってロックされたファイルを削除しようとしても失敗することがあります。[LC3532]
- ユーザーデバイスがシャットダウンのプロセス中に、Profile Management が予期せずに終了することがありました。[LC3626]
- 再起動されるまで、ファームの XenApp サーバーが応答しなくなることがあります。[LC4318]
- RDP を使用して XenApp 7.7 サーバーにログオンしようとすると、サーバーがようこそ画面のまま応答しなくなることがあります。[LC5169]
- VDA をバージョン 7.6.1000 以前からバージョン 7.7 以降にアップグレードした後で Profile Management や VDA を削除、修復、または再インストールしようとすると、失敗することがあります。[LC5207]
- ログオフ時に、Profile Management でサーバー上のファイル/フォルダーがロックされ、そのためにアプリケーションが起動に失敗することがあります。ローカルにキャッシュされたプロファイルも削除されません。[LC5266]

- Profile Management で、ユーザープロファイル内のファイルがロックされることがあります。その場合、それらのプロファイルのロックが解除されるまで、ユーザーは再接続試行時に一時プロファイルを受け取ります。[LC5278]
- ユーザーのログオフ時に、ローカルでキャッシュしたプロファイルが削除されません。[LC5470]
- ライセンスサーバーがオフラインの時、サーバーでユーザーリダイレクトフォルダーを使用するファイルが失われます。[LC5595]
- 更新しないままライセンスの試用期間が終了すると、ユーザーのファイルが失われます。[LC5775]
- Profile Management により、ネットワークが失われたことを示す「NetworkDetection」フラグが誤って発生することがあります。この修正には、ネットワークが一時的に使用できないかどうかに代わって、ネットワークが利用できないかを確認する追加のチェックが導入されています。[LC5943]
- Windows Server 2012 R2 で、ユーザーログオン画面が応答しなくなることがあります。[LC6149]
- 移動プロファイルを Profile Management に移行しようとすると、失敗することがあります。この問題は、不正確なバージョン番号がプロファイルに追加された時に発生します。[LC6150]
- WAN 接続で Profile Management のユーザープロファイルストアからアプリケーションのアイコンをコピーしようとすると、アイコンが灰色表示されることがあります。[LC6152]
- ファイルの種類の関連付けが Microsoft Windows 10 および Windows Server 2016 上で実行中の Profile Management が有効なセッションでローミングできないことがあります。[LC6736]
- Microsoft Windows 10 または Windows Server 2016 でログオフ時にローカルキャッシュを削除するポリシーを有効にしていると、ログオフ時に NTUSER.DAT ファイルが削除されないことがあり、次回のログオン時に別のローカルプロファイルが作成されます。[LC6765]
- Microsoft Windows Server 2016 上で Profile Management を使用し、usrclass.dat が含まれていると、［スタート］メニューが動作しないことがあります。[LC6914]
- プロファイルストリーミングを有効にしてプロファイルでファイルを開こうとすると、ログオン後にファイルが空として表示されることがあります。[LC6996]
- Microsoft Windows 10 のセッションの起動時に、Profile Management により黒い画面が表示されることがあります。この修正では、「同期するディレクトリ」ポリシーを構成し、フォルダー「*AppData\Local\Microsoft\Windows\Caches*」を追加する必要があります。[LC7596]

Provisioning Services

コンソールの問題

- この修正により、［次の vDisk 更新をこの日に実行する］オプションおよび［vDisk 更新を検出したらすぐに適用する］オプションは Provisioning Services で利用できなくなります。[LA4166]
- XenDesktop セットアップウィザードを介して仮想マシンを作成しようとすると、英語版以外の Microsoft System Center Virtual Machine Manager（SCVMM）環境で失敗することがあります。[LC5451]

- New-BootDeviceManager PowerShell スクリプトで ISO を作成しようとすると失敗し、次のエラーメッセージが表示されることがあります。「ISOFileName は、作成する新しい ISO ファイルの名前にする必要があります」[LC5559]
- クラスターストレージボリュームを使用する場合は、ストリーム配信仮想マシンセットアップウィザードでボリュームを選択できませんが、ランダムボリュームにターゲットデバイスを作成できます。[LC5890]
- XenDesktop セットアップウィザードまたはストリーム配信仮想マシンセットアップウィザードの実行後に Provisioning Services コンソールを閉じようとすると、例外が発生することがあります。[LC6048]
- PVS 7.11 をバージョン 7.6 からアップグレードすると、他のドメインのユーザーがコンソールにログオンできないことがあります。[LC6216]
- サーバー通信のタイムアウト。ログイン処理時間が大幅に長くなる（2 分を超えるなど）こともあり、これによって、PVS コンソールと SOAP サーバーの間でサーバータイムアウトが発生することがあります。デフォルトでは、こうした接続のタイムアウトは 2 分で発生します。タイムアウト時間を延長するには、次のレジストリ値を変更します。HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=。ログイン時間が約 4 分より長くなると、PVS コンソールを含む Microsoft 管理コンソール（MMC）からタイムアウトします（このタイムアウトは破棄することもできます）。秒単位のタイムアウト >

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

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

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

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

```
{


"Domains":

[

```



```
8   "sub.xs.local",
9
10  "sb.xs.local"
11
12  ]
13
14   }
15
16  <!--NeedCopy-->
```

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

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

サーバーの問題

- VMware ESX 環境で、XenDesktop のセットアップウィザードで例外が発生し、テンプレートおよびマシンを正しくセットアップできなくなることがありました。[LA2499]
- 2 つの PVS サーバーで、相手サーバーの vDisk の複製状態は表示できませんが、自身の vDisk の状態は適切に表示できることがあります。[LC4317]
- Citrix PXE サービスが、BOOTPTAB ファイルのエントリを無視することがあります。[#LC4600]
- BDM パーティションを使用している場合、VMware 上のターゲットデバイスは、リストの最上位に表示されているサーバーにアクセスできないと、リスト上のどのサーバーにもログオンを試みません。[LC4736]
- XenDesktop セットアップウィザードを介して仮想マシンを作成しようとすると、英語版以外の Microsoft System Center Virtual Machine Manager（SCVMM）環境で失敗することがあります。[LC5451]
- ハードドライブのすべてのパーティションが複製されているのでなければ、最後のパーティションの複製が失敗する場合があります。[LC5452]
- PVS コンソールで 2 つの PVS サーバーの複製状態を実行すると、どちらのサーバーの状態も不完全として表示されます。[LC5700]
- クラスターストレージボリュームを使用する場合は、ストリーム配信仮想マシンセットアップウィザードでボリュームを選択できませんが、ランダムボリュームにターゲットデバイスを作成できます。[LC5890]
- PVS 7.11 をバージョン 7.6 からアップグレードすると、他のドメインのユーザーがコンソールにログオンできないことがあります。[LC6216]
- サーバー通信のタイムアウト。ログイン処理時間が大幅に長くなる（2 分を超えるなど）こともあり、これによって、PVS コンソールと SOAP サーバーの間でサーバータイムアウトが発生することがあります。

デフォルトでは、こうした接続のタイムアウトは 2 分で発生します。タイムアウト時間を延長するには、次のレジストリ値を変更します。HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=。ログイン時間が約 4 分より長くなると、PVS コンソールを含む Microsoft 管理コンソール（MMC）からタイムアウトします（このタイムアウトは破棄することもできます）。秒単位のタイムアウト >

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

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

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

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

```
{

"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

 }

<!--NeedCopy-->
```

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

ターゲットの問題

- Provisioning Services ターゲットデバイスの自動更新機能を使用している時に、更新が利用できない場合、ターゲットのイベントビューアーで次のアプリケーションエラーメッセージ（イベント ID：0）が生成されるという問題がありました。
  「No update server found. Stopping client service.（更新サーバーが見つかりません。クライアントサービスを停止しています。）」[LC0450]
- ターゲットデバイスのソフトウェアが AppDisk ドライブを認識せず、AppDisk ドライブを書き込みキャッシュ用に使用して、競合が引き起こされることがあります。[LC5409]
- 「RAM の書き込みキャッシュ」を使用して vDisk を構成し、RAM キャッシュサイズを 4,096MB または 4,097MB に設定した場合に、Hyper-V 第 2 世代仮想マシンから起動するとターゲットデバイスに重大な例外が発生しブルースクリーンが表示されることがあります。[LC6707]

StoreFront

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

  注: この問題は解決されましたが、新しい値を読み込むには最大 1 時間を要することがあります。[DNA-41380]
- StoreFront 3.5 をインストールすると、カテゴリビューのフォルダーの色に、StoreFront 管理コンソールで定義されたカスタム色が使用されなくなる可能性があります。フォルダーの色はデフォルト色に戻ります。[LC5001]
- Citrix Receiver for Web サイトを管理している時に、StoreFront が予期せず終了することがあります。この問題は、style.css が Citrix Receiver for Web 用にカスタマイズされると発生します。[LC5589]
- StoreFront でフェデレーション認証サービスを有効にすると、ログオンエラーが発生することがあります。[LC5708]
- Citrix StoreFront で Citrix Receiver for HTML5 を有効にしている場合でも、StoreFront コンソールには HTML バージョンが表示されず「未使用」と表示されることがあります。[LC6626]
- XenDesktop のセットアップ中、構成されたサイトを選択すると、StoreFront でデフォルトの認証サービスを使用するデフォルトのストアが作成されることがあります。このストアを削除すると、Citrix Receiver for Windows ユーザーはストアを追加できなくなり、次のエラーメッセージが表示されることがあります。

  「認証サービスとの通信中にプロトコルエラーが発生しました。」[LC6664]
- StoreFront コンソールを使用して特定のストアでセルフサービスパスワードリセット（SSPR）を構成すると、この構成は選択された特定のストアだけではなくすべてのストアに適用されます。[LC6987]
- マルチサイト集約環境で切断されたセッションに再接続しようとすると、失敗することがあります。これによって、同じリソースの 2 つ目のインスタンスを受信することがあります。[LC7453]

- 集約されたアプリケーションのソースのいずれかが無効になっている場合は、アプリケーションが予期せずエンドユーザーから非表示になることがあります。[LC7675]
- StoreFront で［アカウントセルフサービス］オプションを無効にしようとすると、無効と表示されていても無効にならないことがあります。[LC7744]
- StoreFront でストアから共有認証を削除しようとすると、変更の保存中、次のエラーメッセージが表示されることがあります。

  「変更の保存時にエラーが発生しました。」[LC7781]

ユニバーサルプリントサーバー

クライアント

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

サーバー

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

  「内部エラーが発生しました。Internet Explorer はこのドキュメントを印刷できません。」[LC4735]
- ドキュメントを印刷しようとすると失敗する場合があり、次のエラーメッセージが表示されます。

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

VDA for Desktop OS

コンテンツリダイレクト

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

HDX Broadcast

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

インストール、アンインストール、アップグレード

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

キーボード

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

印刷

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

サーバー/サイトの管理

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

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect

種類：DWORD
値：1 [LC8049]

セッション/接続

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

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect
  種類：DWORD
  値：0 [LC6163]

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

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

システムの例外

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

スマートカード

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

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

ユーザーエクスペリエンス

- Excel 2010 のスプレッドシートで複数のブックを開いた場合、タスクバーに最新のブックしか表示されません。[LC5370]

- XenDesktop 7.11 Windows 7 VDA で従来のグラフィックモードを使用すると画面の左上しか表示されません。[LC6532]
- VDA バージョン 7.9 上で実行される、2 つの Microsoft Excel 2010 ワークシート間で挿入処理を実行する場合、Excel のウィンドウが応答しなくなることがあります。[LC7481]

ユーザーインターフェイス

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

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

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

VDA for Server OS

コンテンツリダイレクト

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

インストール、アンインストール、アップグレード

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

  「wfapi.dll がありません」[LC6874]
- Microsoft Windows オペレーティングシステムの英語以外のバージョン上で VDA のバージョン 7.12 または 7.13 をインストールした後に、特定の WMI クラスの名前が変更されることがあります。[LC7555]
- Microsoft Windows オペレーティングシステムの英語以外のバージョン上で VDA のバージョン 7.12 または 7.13 をインストールした後に、特定の WMI クラスの名前が変更されることがあります。[LC7587]

印刷

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

サーバー/サイトの管理

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

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

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

セッション/接続

- （Hotfix Rollup Pack 6 に含まれる）修正 LC2702 が適用されているシステムで、クライアントがマップされたドライブへのアプリケーションの保存が失敗し、代わりに破損したファイルが生成されるという問題がありました。[LC3976]
- Streaming Profiler または Offline Plug-in がインストールされている場合、WinDbg.exe でのプロセスの起動に失敗することがありました。この問題は、RadeAPHook によって

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\< プロセス名 > および HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\< プロセス名 > の設定がフックされることによって発生します。

この修正を有効にするには、以下のレジストリキーを作成します。

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

  *[LC4750]

- 新しいセッションを開始すると、Citrix Audio Redirection Service が無効な情報を含む仮想チャネルセッションに接続しようとして失敗することがあります。[LC5024]
- Framehawk を有効にすると、XenDesktop 7.8 の VDA セッションで、マウスのスクロールボタンによる操作が実行されないことがあります。XenDesktop 7.9 で、対応する VDA 側の修復を利用できます。[LC5302]
- VDA を Version 7.6.300 から 7.8 にアップグレードした後、クリップボード同期が機能しなくなることがあります。[LC5699]
- Framehawk を有効にすると、XenDesktop 7.9 の VDA セッションで、マウスのスクロールボタンによる操作が実行されないことがあります。[LC5779]
- フェデレーション認証サービス用に構成された VDA が接続の受け入れを停止し、再起動するまで「ようこそ」画面で応答しなくなることがあります。[LC5978]
- ［視覚効果］の下の［システムの詳細設定］の変更が、現在の VDA セッションには適用されても、それ以降のセッションには保持されないことがあります。そのような変更を永続的にするには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名前：EnableVisualEffect
  種類：DWORD
  値：0[LC6163]

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

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

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

スマートカード

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

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

システムの例外

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

ユーザーエクスペリエンス

- Excel 2010 のスプレッドシートで複数のブックを開いた場合、タスクバーに最新のブックしか表示されません。[LC5370]

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

ユーザーインターフェイス

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

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

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

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

仮想デスクトップコンポーネント **-** その他

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

  「<applicationname> を開始できません」[LC5483]

- ネットワークを介して App-V アプリケーションをロードしようとすると、次のエラーメッセージが表示されることがあります:

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

- XenApp を Version 7.7 から Version 7.8 にアップグレードした後で、App-V アプリケーションの起動に失敗することがあります。この問題は、「TargetIn」ブール値の値が「1」でなく「0」と設定されている時に発生します。また、値を手動で設定しても、何も変わらないことがあります。アプリケーションを更新すると、値が元に戻ることがあります。[LC5861]
- Citrix Studio に複数のアプリケーションを含む App-V パッケージを追加して、パッケージ内のすべてのアプリケーションを公開すると、ユーザーセッションで最初のアプリケーションだけが起動することがあります。[LC5863]

- App-V アプリケーションを起動できるのは単一ユーザーのみです。同じサーバー上で同じアプリケーションを別のユーザーが起動しようとすると失敗する場合があります。[LC6414]
- シーケンスされた App-V アプリケーションが、パッケージ（InTarget=False）によって参照されている場合でも、実際の App-V パッケージに含まれない場合があります。その結果、アプリケーションを正常に機能させるために必要な、依存関係にある接続グループでアプリケーションを起動できません。[LC6534]
- XenApp/XenDesktop 7.11 から 7.12 にアップグレードすると、既存のデリバリーグループ再起動スケジュールが適用されません。[LC6766]
- マップされたドライブから App-V アプリケーションを起動しようとすると失敗する場合があります。[LC6961]
- App-V アプリケーションを公開しようとすると、失敗する場合があります。

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

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

その他の解決された問題

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

既知の問題

October 22, 2021

このページの 7.15ベースラインおよびCU1、CU2、CU3、CU4、CU5、CU6セクションで説明されている既知の問題は、「解決された問題」の一覧に記載されていない限り CU7 でも引き続き存在します。

累積更新プログラム **8** の既知の問題

- セキュア XML キーがレジストリに作成されていない場合、ローカルホストキャッシュデータベースが見つからないか破損している可能性があります。ローカルホストキャッシュデータベースを再作成する方法については、CTX228758 を参照してください。[LCM-9660]
- StoreFront が Delivery Controller と同じサーバーにインストールされている場合、Delivery Controller のアップグレード後に StoreFront をアップグレードしようとすると失敗します。ただし、Delivery Controller をアップグレードする前に StoreFront をアップグレードすると、StoreFront のアップグレードは成功します。

  回避策として、Delivery Controller のアップグレード後に StoreFront をアップグレードする必要がある場合は、StoreFront のアップグレードを実行する前に Citrix Telemetry Service を停止してください。[LCM-9706]

累積更新プログラム **7** の既知の問題

- `Set-LicCEIPOption`コマンドレットを使用して Licensing CEIP オプションを更新しようとすると、`CommunicationError`で操作が失敗します。この問題は、Citrix Licensing Manager 経由で CEIP オプションを有効にすることで回避できます。詳しくは、Knowledge Center の記事CTX220679を参照してください。

累積更新プログラム **6** の既知の問題

- Citrix Workspace アプリ 1912 以降では、XenApp および XenDesktop 7.15 LTSR CU6 リリースの一部である HDX-Flash リダイレクトはサポートされていません。HDX-Flash リダイレクトは、Citrix Workspace アプリ 1911 以前でのみ使用できます。Citrix Receiver 4.9 LTSR を 7.15 LTSR CU6 とともに使用することもできます。[LCM-8140]
- CU6 リリースには、新しいバージョンのセルフサービスパスワードリセットサービスが含まれています。この新しいバージョンのサービスでは、中央ストアのセキュリティ構成を検出する新機能が導入されています。Windows Server 2008 R2 で中央ストアまたはサービスを作成すると、警告ダイアログボックスが表示されます。この問題は、Windows Server 2008 R2 が SMB 暗号化をサポートしていないためにセキュリティ検出が失敗し、発生します。この問題は、さらに操作を行うことを禁止しません。回避策として、SMB 暗号化をサポートする Windows Server 2012 以降で、中央ストアとサービスを作成します。[LCM-8179]
- 7.15 LTSR CU6 VDA に関連付けられたセッションの詳細を表示すると、Citrix Director がポリシー情報の列挙に失敗する場合があります。この問題は、Citrix Director が VDA バージョン 7.15 LTSR CU6 より前のバージョンである場合に発生します。この問題を回避するには、Citrix Director バージョン 7.15 LTSR CU6 を使用してください。または、VDA で次のレジストリを変更してから再起動します。
  - レジストリパス：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

    名前：SaveRsopToFile

種類：REG_DWORD

値：1

- レジストリパス：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

  名前：SaveRsopToMemory

  種類：REG_DWORD

  値：0

- レジストリパス：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

  名前：SaveRsopToRegistry

  種類：REG_DWORD

  値：0

[LCM-8201]

累積更新プログラム **5** の既知の問題

- Windows 7 VDA を 7.6 LTSR CU8 からこのリリースにアップグレードしようとすると、重大な例外が発生し、ブルースクリーンが表示されることがあります。利用できる回避策はありません。

  Windows 7 VDA を 7.6 LTSR CU8 からこのリリースにアップグレードする場合、次の回避策のいずれかを実行します：

  - 7.6 LTSR CU8 をアンインストールしてから、7.15 LTSR CU5 をインストールします。
  - Windows 7 マシンで Citrix WDDM ドライバーを手動で無効にしてから、このリリースにアップグレードします。Citrix WDDM ドライバーを無効にするには、次の手順を実行します：
    * `Device Manager`を開きます。
    * `Display adapters`をクリックして選択肢を展開します。
    * `Citrix Display Driver (Citrix Systems - WDDM)`を右クリックして`Disable`を選択します。[LCM-6798]

- Windows 7 または Windows Server 2008 R2 を実行している VDA では、App-V アプリケーションの起動時に VC++ エラーが発生することがあります。この問題は、App-V クライアントが動作するために特定のバージョンの VC++ 2013 に依存していることが原因で発生します。

  回避策として、Microsoft Hotfix（https://support.microsoft.com/en-in/help/4014009/march-2017-servicing-release-for-microsoft-desktop-optimization-pack）を適用します。または、App-V クライアントを最初にインストールしてから、VDA の累積更新プログラム 5 バージョンをインストールします。[LCM-6809]

- Citrix Scout は、Windows 2008 R2 を実行している Delivery Controller のヘルスチェックの実行に失敗することがあります。その結果、次のメッセージが表示されます：チェックに失敗しました。この問題

は、Delivery Controller にインターネット接続がない場合に発生します。これを回避するには、チェックスクリプトをダウンロードしてから、スクリプトを手動で実行します。詳しくは、Knowledge Center の記事CTX263240を参照してください。[LCM-6837]

累積更新プログラム **4** の既知の問題

- PowerShell 2.0 をターゲットとする Citrix XenDesktop Admin モジュールのカスタム管理スクリプトが失敗することがあります。この問題は、モジュールが PowerShell 2.0 をサポートしなくなったことが原因で発生します。
- スペイン語版の Microsoft Windows オペレーティングシステムで、コンポーネントの初期化に失敗することがあります。この問題は、Delivery Controller をバージョン 7.6 の累積更新プログラムからバージョン 7.15 の累積更新プログラム 4（CU4）にアップグレードするとき、事前のサイトテストを実行すると発生します。
- Citrix Director で［傾向］表のレコードのすべての行が表示されない場合があります。一部のレコードと余分な空きスペースが表示されますが、下にスクロールすると残りのレコードを見つけることができます。[LCM-5841]

累積更新プログラム **3** の既知の問題

- Windows 10 October 2018 Update（バージョン 1809）に関する Citrix の既知の問題の一覧については、Knowledge Center のCTX234973を参照してください。
- AWS 環境では、XenApp および XenDesktop 7.15 LTSR CU2 イメージまたはスナップショットに対するサーバー VDA のロールバックが失敗する可能性があります。回避策として、次の PowerShell コマンドレットを使用して、ロールバックタイムアウトのタイムアウト値を 30 分に延長します:

  Set-ProvServiceConfigurationData -Name ImageManagemntPrep_preparationTimeout -Value 30 [LCM-4364]
- XenApp および XenDesktop 7.15 LTSR CU3 へのアップグレード後、サイトのライセンスサーバーが CU3 の対応バージョンに更新されなかった場合、サイトがアップグレードできないことがあります。アップグレード時、製品インストーラーからこのことが通知されることはありません。[LCM-5467]
- XenDesktop ウィザードを完了した後、Studio のマシンカタログが空になり、管理 IP アドレスではなくストリーム配信 IP アドレスが表示されますが、これは正しくありません。管理 IP アドレスを使用するには、以下のレジストリキーを設定します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices
名前：UseManagementIpInCatalog
種類：DWORD
値：1

[LD0125]

累積更新プログラム **2** の既知の問題

- Windows 2016 VDA では、スマートカードを使用してログインするユーザーは、ログオン時に使用可能なすべてのユーザーを表示できないことがあります。この問題は、ログオンウィンドウのデフォルトのサイズ（600x520）によって発生します。回避策などを含め、詳しくは Knowledge Center のCTX204070を参照してください。[LCM-3951]
- Windows 10 Redstone 4（Insider Preview ビルド）の既知の問題の一覧については、Knowledge Center のCTX231942を参照してください。
- Citrix Studio をバージョン 7.15 の累積更新プログラム 2 にアップグレードすると、ポリシーがローカライズされないことがあります。詳しくは、Knowledge Center のCTX234711を参照してください。[LC9613]
- 7.15 LTSR CU2 セッションが黒い画面として起動することがあります。この問題は、Profile Management が有効なときに、XenApp および XenDesktop 7.15 LTSR CU2 および 7.17 VDA で実行されているセッションで発生します。回避策などを含め、詳しくは Knowledge Center のCTX235100を参照してください。[LC9648]

累積更新プログラム **1** の既知の問題

- HKEY_LOCAL_MACHINE 下の picadm や MultiStreamIca などのユーザーが構成可能なレジストリキーが、累積更新プログラムのインストール中に削除される、またはデフォルト値によって上書きされる可能性があります。[CVADHELP-16481]
- StoreFront 3.12（XenApp および XenDesktop 7.15 LTSR）から StoreFront 3.12.1000（XenApp および XenDesktop 7.15 LTSR CU1）へのアップグレード後、または StoreFront 3.12.1000 のインストール後に StoreFront 管理コンソールが開きません。StoreFront 管理コンソールに「MMC がスナップインを作成できませんスナップインが正しくインストールされていない可能性があります。」というエラーが表示されます。この問題を解決するには、CTX233206の手順に従います。[LC8935]
- Windows 7 または Windows Server 2008 R2 マシンに SHA-256 証明書で署名されたドライバーをインストールすると、Microsoft WHQL（Windows Hardware Quality Labs）のメッセージが表示されることがあります。この問題を解決するには、マシンに以下のマイクロソフトの修正プログラムをインストールします。
  - Windows 7（1 つの修正プログラム）: Microsoft の修正プログラム
  - Windows Server 2008 R2 (2 つの修正プログラム): 修正プログラム 1、修正プログラム 2 [LCM-2836]
- Citrix Telemetry Service が無効になっているか停止している場合、メタインストーラーを使用してXenApp および XenDesktop 7.15 LTSRを累積更新プログラム 1（CU1）にアップグレードすると、次の警告メッセージが表示されることがあります:
  「Call Home に登録するための Citrix サービスを開始できません。ガイダンスについては、CTX218094 を参照してください。」[LCM-3642]
- Microsoft Windows 10 のセッションの起動時に、Profile Management により黒い画面が表示されることがあります。この修正では、「同期するディレクトリ」ポリシーを構成し、フォルダー「*App-

Data\Local\Microsoft\Windows\Caches*」を追加する必要があります。回避策などを含め、詳しくは Knowledge Center のCTX234144を参照してください。[LC9030]

7.15 LTSR（初期リリース）の既知の問題

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

VDA

- SAS 通知⋆が有効になっている場合、コンソールで既存のセッションに接続している複数のモニターを持つユーザーは、モニターのレイアウトが正しく復元されていないことを発見することがあります。たとえば、右側のモニターが 1 で、メインモニターとして選択され、左側のモニターが 2 の場合、ユーザーは再接続時に位置が入れ替わっていることに気付く可能性があります。この問題は、物理デスクトップを使用しているリモート PC ユーザーにのみ影響します。これは、2 つの機能間で互換性がないことによるものです。[CVADHELP-14249]

  ⋆ SAS 通知は、別のユーザーが接続を試みていることをリモート PC のコンソールユーザーに通知する機能です。

App-V

- Studio の［アプリケーション］ノードから、または選択したデリバリーグループから、1 つまたは複数の App-V アプリケーションを削除した場合、「不明なエラーが発生しました」というメッセージが表示されます。このメッセージは無視しても問題ありません。アプリケーションは削除されます。[DNA-29702]
- App-V アプリケーションの子プロセスが起動していると、デリバリーグループからそのアプリケーションを削除できないが、アプリケーションを終了させても子プロセスが終了できません。アプリケーションが使用中であるというエラーが表示されます。プロセス名を確認するために、Get-AppVVirtualProcess を実行します。タスクマネージャーまたは Stop-AppVClientPackage で、そのプロセスを終了させます。[DNA-23624]
- App-V パッケージをアプリケーションライブラリから削除しても、Studio の表示はなくなるが VDA から削除されません。この問題を回避するには、管理者権限を引き上げて以下のコマンドレットを実行します。

  Import-Module AppvClient
  Get-AppVClientPackage -all
  # 削除するパッケージの PackageId および VersionId を特定します
  Remove-AppVClientPackage -PackageId <*packageid*> -VersionId <*versionid*> [DNA-47379]

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

Citrix Director

- マルチセッション環境で［フィルター］>［セッション］>［すべて］に移動してセッションからログオフすると、セッションはログオフします。同じユーザー名の別のセッションを二度目に選択してログオフしようとすると、このエラーメッセージが開きます：

  データソースが応答しないか、エラーが報告されました。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。[LC8826]

インストールとアップグレード

- VDA 7.14 を VDA 7.15 にアップグレードすると、管理用テンプレートを使用して適用される Citrix ポリシー設定用のレジストリキー HKEY_LOCAL_MACHINE\Software\Policies\Citrix で作成されたキーが、VDA から削除される可能性があります。[LCM-3876]
- インストールメディア上の AutoSelect アプリケーションを使用してコンポーネントをインストールする時に、autorun.log ファイルに、不十分な権限に関するエラーと例外が含まれる場合があります。インストールが成功していれば、これらのエラーは無視できます。ただし、これを避けるには、［管理者として実行］を使って AutoSelect を起動してください。[DNA-45937]
- XenDesktop 5.6 環境を XenDesktop 7.15 LTSR にアップグレードした場合、グループポリシーが不明になります。この問題を回避するには、最初に XenDesktop 5.6 を XenDesktop 7.13 にアップグレードしてください。次に、7.13 から 7.15 LTSR にアップグレードしてください。[DNA-44818]
- Controller をインストールして、インストールウィザードの［**Smart Tools**］ページに表示される［**Smart Tools** と **Call Home** に接続します］を選択すると、Call Home が有効にならない場合があります。この問題を回避するには、Citrix Scoutのスケジュール機能を使用するか、PowerShell で Call Homeを有効にしてください。[CAM-9907]
- Windows Server 2012 R2 または Windows Server 2016 に Delivery Controller をインストールする場合、Smart Tools への接続を選択し、お使いの Citrix Cloud アカウントに 1 つまたは複数の組織をリンクさせると、Citrix Cloud の資格情報でログオンする時にログオン処理が完了しないことがあります。この問題を回避するには、次のいずれかを実行してください。
  - Windows Server と Internet Explorer が最新のバージョンに更新されていることを確認します。
  - Internet Explore ブラウザーの設定で次のオプションをオフにします：［インターネットオプション］>［セキュリティ］>［ローカルイントラネット］>［サイト］>［プロキシサーバーを使用しないサイトをすべて含める］[CAM-9816]
- StoreFront がインストールメディアから実行可能ファイルを使用してインストールされている場合、以降のバージョンの全製品インストーラーを使用した時に、StoreFront はアップグレードの対象とされません。この問題を回避するには、インストールメディアから実行可能ファイルを使用して StoreFront をアップグレードしてください。[#DNA-47816]
- Delivery Controller を 7.13 より前のバージョンから 7.13 以降のバージョンにアップグレードすると、「クライアントの自動再接続のタイムアウト」設定がいずれかのポリシーで設定されている場合に、エラー（例外）

が発生することがあります。このエラーは、「クライアントの自動再接続のタイムアウト」の設定値が、バージョン 7.13 で初めて導入された許容範囲 0〜300 を超えている場合に発生します。このエラーを回避するには、Citrix Group Policy PowerShell Provider を使用して設定を構成解除するか、指定された範囲内の値に設定します。例については、CTX22947を参照してください。[DNA-52476]

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

一般

- MCS が AWS で永続的ではないマシンを作成する場合、`DeleteOnTermination`フラグは *True* に設定されます。ただし電源を入れ直すと、MCS は新しい EBS ボリュームを再作成し、古いボリュームから切り替えられるため、`DeleteOnTermination`フラグは *False* に変更されます。[PMCS-4953]
- フェデレーション認証サービスのセッション内証明書を使って TLS 1.1（またはそれ以前）の接続を認証しようとすると、接続に失敗する場合があります。ハッシュ ID がサポートされていないことを示す、イベント ID 305 がログに記録されます。フェデレーション認証サービスは、SHAMD5 ハッシュをサポートしません。この問題を回避するには、TLS 1.2 接続を使用します。この問題は、XenApp および XenDesktop 7.9 から本バージョンまで影響があります。[DNA-47628]
- プリンタードライバーマッピングと互換性ポリシーには、ポリシー設定が保存されません。この問題を回避するには、Citrix Group Policy PowerShell プロバイダーを使用して、この設定を編集してください。回避策について詳しくは、CTX226589を参照してください。[DNA-47423]
- Windows イベントログエラー：「Windows は MfApHook64.dll ファイルのイメージの整合性を検証できません」。詳しくは、CTX226397を参照してください。[HDX-9063]
- StoreFront からアプリケーションを起動した時、アプリケーションがフォアグラウンドで起動されないか、フォアグラウンドではあるがフォーカスを持たないことがあります。この問題を回避するには、タスクバーのアイコンをクリックしてアプリケーションを前面に移動させるか、アプリケーション画面でフォーカスに移動させます。[HDX-10126]
- 公開コンテンツは、Citrix Receiver から開始されると開始に失敗します。StoreFront Web クライアント（または Web Interface）で開始されたコンテンツは問題なく開始できます。[LC6316、RFWIN-4957]
- Azure Resource Manager マシンカタログを削除したときに、関連するマシンとリソースグループを保持するように指定しても、Azure から削除されます。[DNA-37964]
- Citrix Receiver for Windows バージョン 4.6 以降を使用すると、マルチキャストがビデオを表示しない場合があります。オーディオは再生されます。この問題を回避するには、エンドポイントに次のレジストリキーを追加します。

HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream
名前：DisableVMRSupport

種類：DWORD
値：4 [HDX-10055]

印刷

- Citrix Print Manager サービスを停止または再起動した時に、CpSvc.exe プロセスが応答しなくなることがあります。この問題を回避するには、サービススナップインのサービスを停止または再起動する前に、CpsSvc.exe プロセスを終了させるか、VDA を再起動させます。[HDX-10071]
- 仮想デスクトップで選択されたユニバーサルプリントサーバープリンターが Windows コントロールパネルの ［デバイスとプリンター］に表示されない場合があります。この問題が発生しても、アプリケーションからこのプリンターを使って正しく印刷できます。この問題は、Windows Server 2012、Windows 10、および Windows 8 プラットフォームでのみ発生します。詳しくは、Knowledge Center の CTX213540を参照してください。[335153]

Session Recording

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

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

サードパーティの問題

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

  警告：Azure Active Directory（AAD）を使用している場合、CTX225819 に記載されたようにレジストリに変更は加えないでください。このように変更すると、AAD ユーザーがセッションを起動できない可能性があります。[HDX-5000]
- 負荷テスト環境で 20,000 回のログオンを行ったときに、Microsoft Windows の WinLogon.exe は 0.001% 未満の頻度で断続的にクラッシュすることがあります。[HDX-9938]

サードパーティ製品についての通知

August 24, 2021

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 および **XenDesktop** サードパーティ通知（**PDF** のダウンロード）（英語）

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

FLEXnet Publisher Documentation Supplement：**FlexNet Publisher 11.14.0** で使用されるオープンソースソフトウェア（**PDF** のダウンロード）

Session Recording サードパーティ製品についての通知（**PDF** のダウンロード）

廃止と削除

August 24, 2021

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

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

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

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Microsoft Edge Legacy に対する StoreFront ブラウザーのサポート	7.15 LTSR CU7	-	Microsoft Edge（Chromium がベース）にアップグレードします。
Web ブラウザーコンテンツのリダイレクト	7.15 LTSR CU7	-	1912 LTSR にアップグレードします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Citrix ライセンス管理コンソール（最後に Windows ライセンスサーバー 11.16.3 ビルド 30000 に含まれ、Windows ライセンスサーバー v11.16.6 ビルド 31000 で削除されました）。	7.15 LTSR CU6	7.15 LTSR CU6	Citrix Licensing Manager を使用します。
Citrix Virtual Apps and Desktops インストールメディアからの Citrix Smart Tools Agent の削除。	1903 および 7.15 LTSR CU4	7.15 LTSR CU4	—
Citrix Receiver for Web クラシックエクスペリエンス（「緑色の泡」ユーザーインターフェイス）	7.15 LTSR（および StoreFront 3.12）	—	Citrix Receiver for Web 統合エクスペリエンス。
Windows 10 バージョン 1511（Threshold 2）および Windows8.x と Windows7 を含む、以前の Windows デスクトップ OS リリース用 VDA	7.15 LTSR（および 7.12）	7.16	Windows 10 バージョン 1607（Redstone 1）以降の半期チャネル用デスクトップ OS VDA をインストールします。1607 LTSB を使用している場合、7.15 VDA をお勧めします。
Windows Server 2008 R2 および Windows Server 2012 上の VDA（Service Pack を含む）。	7.15 LTSR（および 7.12）	7.16	Windows Server 2012 R2 または Windows Server 2016 など、サポートされているバージョンにサーバー OS VDA をインストールします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows Server 2012 および 2008 R2 上の Delivery Controller (Service Pack を含む)。	7.15 LTSR	—	オペレーティングシステムをサポートする代替の Delivery Controller をインストールします。
Windows 7 上の Studio (Service Pack を含む)。	7.15 LTSR	7.18	オペレーティングシステムをサポートする代替の Studio をインストールします。
Flash リダイレクト。	7.15 LTSR	—	Citrix Workspace アプリ 1912 以降では、XenApp および XenDesktop 7.15 LTSR CU6 リリースの一部である HDX-Flash リダイレクトはサポートされていません。HDX-Flash リダイレクトは、Citrix Workspace アプリ 1911 以前でのみ使用できます。Citrix Receiver 4.9 LTSR を 7.15 LTSR CU6 とともに使用することもできます。
DirectX コマンドリモート処理（DCR)。	7.15 LTSR	7.16	Thinwireを使用します。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
StoreFront を含む Citrix Online Integration（Goto 製品）	7.14（および StoreFront 3.11）	StoreFront 3.12	StoreFront 3.12 からは、StoreFront 管理コンソールでこの機能を構成することはできません。StoreFront 3.12 へのアップグレードの場合、引き続きこの機能を使用できます。構成を変更するには、PowerShell コマンドレットの Update-DSGenericApplications を使用します。詳しくは、「Citrix Online アプリケーションをストアに統合する」を参照してください。
StoreFront 2.0、2.1、2.5、および 2.5.2 からのインプレースアップグレード。	7.13	7.16	これらのバージョンは、以降のサポート対象バージョンにアップグレードしてから、XenApp および XenDesktop 7.13 にアップグレードします。
XenDesktop 5.6 または 5.6 FP1 からのインプレースアップグレード。	7.12	7.16	XenDesktop 5.6 または 5.6 FP1 展開を、最新の XenDesktop バージョンに移行します。
Windows 8.1 およびそれ以前の Windows デスクトップリリース上の VDA。	7.12	—	Windows Server 2012 R2 または Windows Server 2016 など、サポートされているバージョンにサーバー OS VDA をインストールします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows XP 上で使用される XenDesktop 5.6。Windows XP 上の VDA インストールはサポートされません。	7.12	—	サポートされている Windows バージョンに VDA をインストールします。
CloudPlatform 接続。	7.12	—	サポートされている各種ハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（別名 Azure Service Management）接続。	7.12	—	Azure Resource Manager を使用します。
32 ビットマシン上へのコアコンポーネント（Studio 以外）のインストール：Delivery Controller、Director、StoreFront、および License Server。	7.12	7.16	64 ビットマシンを使用します。
接続リース。	7.12	7.16	ローカルホストキャッシュを使用します。
従来の Thinwire モード	7.12	7.16	Thinwireを使用します。
HDX デスクトップコンポジションリダイレクト（DCR）	7.12	—	—
AppDisk の機能（およびそれをサポートする Studio への AppDNA の統合）*	7.13	2003	Citrix App Layering を使用します。
Personal vDisk の機能 *	7.13	2006	Citrix App Layering ユーザーレイヤーテクノロジ、またはユーザー個人設定レイヤーテクノロジを使用します。

* 長期サービスリリース（LTSR）サービスオプションでは機能がカバーされていません。

Section 508 Voluntary Product Accessibility Template（VPAT）

March 25, 2020

第 **508** 条のコンプライアンスおよび **WCAG 2.0** のコミットメント

シトリックスは、誰もがアクセスできるテクノロジを開発することにコミットしています。現在優先度の高い取り組みは、障がいの有無にかかわらずすべてのお客様により優れたユーザビリティとアクセシビリティを提供する製品を設計し、開発することです。このため、第 508 条のコンプライアンスおよび WCAG 2.0 のような、代表的なアクセシビリティ標準のサポートに取り組んでいます。

第 **508** 条のコンプライアンスと **WCAG 2.0** との調和

World Wide Web Consortium (W3C) は、*Web Content Accessibility Guidelines*（WCAG）を開発しました。これは、世界的に認められた ISO/IEC 40500 標準であり、Web コンテンツのアクセシビリティを高めるための広範囲におよぶ推奨事項が網羅されています。米国内にも、同様の要件があります。第 508 条は、1973 年に制定されたリハビリテーション法の Federal Acquisition Regulation（FAR）の一部です。WCAG のように、その主な目的は、障がいを持つ個人が連邦機関の電子および情報技術（ICT）に平等にアクセスし、使用できるようにすることです。2017 年 1 月、米国アクセス委員会は、第 508 条および WCAG 2.0 を調和させるための規則を発表しました。その結果を受けて、シトリックスは WCAG の最新のアップデートを取り入れ、お客様によりアクセシビリティの高い製品を提供することに注力しています。

Voluntary Product Accessibility Template（**VPAT**）ドキュメント

さまざまなシトリックス製品およびコンポーネントの VPAT に関するドキュメントは、https://www.citrix.com/about/legal/security-compliance/section-508.htmlからダウンロードできます。

システム要件

October 22, 2021

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、Citrix

Workspace アプリとプラグイン、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。

> 注：
>
> *Windows オペレーティングシステムのサポート：Citrix XenApp および XenDesktop、およびそれに関連するコンポーネントは、製造元がサポートするバージョンのオペレーティングシステムでのみサポートされます。お客様は、オペレーティングシステムの製造元から延長サポートを購入する必要がある場合があります。

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、Citrix 製品のインストールメディアにも収録されています。

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

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

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

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

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

詳細については、CX224843を参照してください。

ハードウェア要件

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

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

次の表は、コアコンポーネントでの最小要件を示しています。

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

デスクトップやアプリケーションを配信する仮想マシンのサイジング

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

Microsoft Visual C++ Runtime のバージョン

Microsoft Visual C++ 2015 Runtime がインストールされているマシンに Microsoft Visual C++ 2017 Runtime をインストールすると、自動的に Visual C++ 2015 Runtime が削除されることがあります。これは仕様です。

Visual C++ 2015 Runtime を自動的にインストールする Citrix コンポーネントをインストール済みの場合、これらのコンポーネントは Visual C++ 2017 バージョンでも正常に機能します。

詳しくは、Microsoft 社の記事「https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html」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、Standard、および Datacenter エディション。
- Windows Server 2012 R2、Standard、および Datacenter エディション。

- Windows Server 2012、Standard、および Datacenter エディション。
- Windows Server 2008 R2 SP1、Standard、Enterprise、および Datacenter エディション *

要件:

- Microsoft .NET Framework 3.5.1（Windows Server 2008 R2 のみ）
- Microsoft .NET Framework 4.5.2（4.6～4.8 もサポートされます）
- CU3 以前：Windows PowerShell 2.0
- CU4 以降：Windows PowerShell 2.0 と Windows PowerShell 3.0 以降の両方
- Microsoft Visual C++ 2015 Runtime（32 および 64 ビット）

データベース

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

- SQL Server 2019 の Express、Standard、および Enterprise Edition。
- SQL Server 2017 の Express、Standard、および Enterprise Edition。
- SQL Server 2016 SP1 および SP2 の Express エディション、Standard エディション、および Enterprise エディション。
- SQL Server 2014 SP1～SP3 の Express、Standard、および Enterprise Edition。デフォルトでは、Controller のインストール時に適切なバージョンの SQL Server が検出されない場合、SQL Server 2014 SP2 Express がインストールされます。
- SQL Server 2012 の SP4 までの Express、Standard、Enterprise Edition。
- SQL Server 2008 R2 SP2 および SP3 の Express、Standard、Enterprise、および Datacenter Edition。

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

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

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

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

詳しくは、次の記事を参照してください:

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

Citrix Studio

以下のオペレーティングシステムがサポートされています:

- Windows 10（[はじめに］セクションのエディションサポート参照）
- Windows 8.1、Professional、および Enterprise エディション *
- Windows 7 Professional、Enterprise、および Ultimate エディション *
- Windows Server 2016、Standard、および Datacenter エディション。
- Windows Server 2012 R2、Standard、および Datacenter エディション。
- Windows Server 2012、Standard、および Datacenter エディション。
- Windows Server 2008 R2 SP1、Standard、Enterprise、および Datacenter エディション *

要件:

- Microsoft .NET Framework 4.5.2（4.6～4.8 もサポートされます）
- 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（CU3 以前）
- Windows PowerShell 3.0 以降（CU4 以降）

Citrix Director

以下のオペレーティングシステムがサポートされています:

- Windows Server 2016、Standard、および Datacenter エディション。
- Windows Server 2012 R2、Standard、および Datacenter エディション。
- Windows Server 2012、Standard、および Datacenter エディション。
- Windows Server 2008 R2 SP1、Standard、Enterprise、および Datacenter エディション *

要件:

- Microsoft .NET Framework 4.5.2（4.6～4.8 もサポートされます）。
- Microsoft .NET Framework 3.5 SP1（Windows Server 2008 R2 の場合のみ）。
- Microsoft インターネットインフォメーションサービス（IIS）7.0 および ASP.NET 2.0。IIS と一緒に［静的コンテンツ］の役割サービスがインストールされていることを確認してください。これらがインストールされていない場合は、Windows Server のインストールメディアを指定するためのメッセージが表示され、自動的にインストールされます。

> 注:
>
> Citrix Director がインストールされているマシンのイベントログを表示するには、Microsoft .NET Framework 2.0 をインストールする必要があります。

Citrix User Profile Manager:

- Citrix User Profile Manager と Citrix User Profile Manager WMI プラグインが VDA にインストールされていて（インストールウィザードの［追加コンポーネント］セクション）、Citrix Profile Management サービスが実行され Director でユーザープロファイルの詳細を表示できることを確認します。

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

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

Director を表示するための以下の Web ブラウザー。

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

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

Virtual Delivery Agent（VDA）for Desktop OS

以下のオペレーティングシステムがサポートされています：

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

要件：

- Microsoft .NET Framework 4.5.2（4.6～4.8 もサポートされます）
- Microsoft .NET Framework 3.5.1（Windows 7 のみ）
- Microsoft Visual C++ 2013 および 2015 Runtime（32 および 64 ビット）
- PowerShell 3.0 以降

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

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

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

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

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

Virtual Delivery Agent（VDA）for Server OS

以下のオペレーティングシステムがサポートされています:

- Windows Server 2016、Standard、および Datacenter エディション。
- Windows Server 2012 R2、Standard、および Datacenter エディション。
- Windows Server 2012、Standard、および Datacenter エディション。
- Windows Server 2008 R2 SP1、Standard、Enterprise、および Datacenter エディション *

インストーラーにより、以下が自動的に展開されます。これらのソフトウェアは、シトリックスが提供するインストールメディアの Support フォルダーに収録されています:

- Microsoft .NET Framework 4.5.2（4.6～4.8 もサポートされます）
- Microsoft .NET Framework 3.5.1（Windows Server 2008 R2 のみ）
- Microsoft Visual C++ 2013 および 2015 Runtime（32 および 64 ビット）
- PowerShell 3.0 以降

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

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

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

- Flash リダイレクト
- Windows Media リダイレクト
- HTML5 ビデオリダイレクト
- HDX Realtime Web カメラリダイレクト

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

ホスト/仮想化リソース

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

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

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

XenServer

最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

VMware vSphere（vCenter + ESXi）

vSphere vCenter のリンクモードはサポートされません。

最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

詳しくは、「VMware 仮想化環境」を参照してください。

System Center Virtual Machine Manager

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

最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

詳しくは、「Microsoft System Center Virtual Machine Manager 仮想化環境」を参照してください。

Nutanix Acropolis

最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

詳しくは、「Nutanix 仮想化環境」を参照してください。

Amazon Web Services（AWS）

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

CloudPlatform

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

Microsoft Azure

Microsoft Azure Resource Manager

Active Directory の機能レベル

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

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

HDX

Windows 向け Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリでは、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。

Windows 向け Citrix Workspace アプリでは、エコーキャンセルがサポートされています。

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

HDX - デスクトップコンポジションリダイレクト

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

- DirectX 9
- Pixel Shader 2.0（ハードウェアでのサポート）
- 32 ビット/ピクセル
- 1.5GHz、32 ビットまたは 64 ビットプロセッサ
- 1GB の RAM

- IGP（Integrated Graphics Processor）またはグラフィックカード上の 128MB のビデオメモリ。

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

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

HDX - Windows Media 配信

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

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、https://developer.nvidia.com/cuda/cuda-gpusを参照してください。

HDX Flash リダイレクト

> 注：
>
> Citrix Workspace アプリ 1912 以降では、XenApp および XenDesktop 7.15 LTSR CU6 リリースの一部である HDX-Flash リダイレクトはサポートされていません。HDX-Flash リダイレクトは、Citrix Workspace アプリ 1911 以前でのみ使用できます。

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

- Citrix Workspace アプリ for Windows（第 2 世代の Flash リダイレクト機能用）- 第 2 世代 Flash リダイレクト機能には、Adobe Flash Player for Other Browser（「NPAPI（Netscape Plugin Application Programming Interface）Flash Player」と呼ばれることもあります）が必要です。
- Citrix Workspace アプリ 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時に、HDX 3D Pro バージョンのインストールを選択できます。

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

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

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

GPU（Graphical Processing Unit）:

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

ユーザーデバイス:

- HDX 3D Pro では、ホストコンピューター上の GPU でサポートされるすべてのモニターの解像度がサポートされます。ただし、推奨されている最低限のユーザーデバイスおよび GPU 仕様でのパフォーマンスを最適

化するには、最大モニター解像度を 1920×1200 ピクセル（LAN 接続の場合）または 1280×1024 ピクセル（WAN 接続の場合）にすることをお勧めします。

- ユーザーデバイスでは、1GB 以上の RAM と 1.6GHz 以上の CPU を推奨します。低帯域幅接続で必要とされるデフォルトの深圧縮コーデックを使用する場合は、より強力な CPU が必要です（ハードウェアでデコードしない場合）。パフォーマンスを最適化するには、ユーザーデバイスに 2GB 以上の RAM および 3GHz 以上のデュアルコア CPU を推奨します。
- マルチモニター環境の場合は、クアッドコア CPU を推奨します。
- HDX 3D Pro で配信されたデスクトップやアプリケーションにアクセスする場合、ユーザーのデバイスに GPU は必要ありません。
- Citrix Workspace アプリ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：Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Linux 向け Citrix Workspace アプリ。

サポートされるビデオ会議アプリケーションは以下のとおりです：

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

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

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

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

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

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

値の名前：skype.exe、種類：REG_DWORD、値のデータ：0

そのほかのユーザーデバイス要件：

- サウンド再生のためのハードウェア

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

Session Recording

Session Recording Administration コンポーネント

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

Session Recording データベース

以下のオペレーティングシステムがサポートされています：

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

サポートされている Microsoft SQL Server のバージョン：

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

要件：.NET Framework 4.7、4.6.2、4.5.2

Session Recording サーバー

以下のオペレーティングシステムがサポートされています：

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

そのほかの要件：

- インターネットインフォメーションサービス（IIS）10、8.5、8.0 または 7.5
- .NET Framework Version 4.7、4.6.2、4.5.2
- Session Recording サーバーで、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)。
- 管理者ログの場合：Chrome、Firefox、または Internet Explorer 11 の最新バージョン

Session Recording ポリシーコンソール

以下のオペレーティングシステムがサポートされています：

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

要件：.NET Framework 4.7、4.6.2、4.5.2

Session Recording Agent

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

以下のオペレーティングシステムがサポートされています：

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*
- Windows 10
- Windows 8.1*
- Windows 7 SP1*

要件：

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

Session Recording Player

以下のオペレーティングシステムがサポートされています：

- Windows 10

- Windows 8.1*
- Windows 7 SP1*

要件：.NET Framework 4.7、4.6.2、4.5.2

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

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

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

ユニバーサルプリントサーバー

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

UpsServer は以下でサポートされています。

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

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

Windows Server OS 対応 VDA で、印刷操作間にユーザー認証を実行するには、ユニバーサルプリントサーバーは、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」を参照してください。

その他

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

> 注：
>
> サイレントインストールを使用して StoreFront 3.12.5000 をインストールしようとすると、インストーラーが予期せず終了する場合があります。この問題は、PowerShell バージョン 3.0 以降がサーバーにインストールされていない場合に発生します。

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

XenApp および XenDesktop 7.15 LTSR CU6 でサポートされる最小ライセンスサーバーバージョンは 11.15.0.0 ビルド 24100 です。以前の CU バージョンについて詳しくは、「ライセンス」を参照してください。

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

Windows 7 または Windows 2008 R2 マシンで Citrix Scout を使用する予定がある場合は、これらのマシンに PowerShell 3.0 をインストールする必要があります。完全な要件については、「Citrix Scout」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 をインストールした場合、デフォルトで Windows 向け Citrix Workspace アプリはインストールされません。

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

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

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

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

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

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

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

製品の技術概要

August 24, 2021

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

XenApp および XenDesktop では、以下の機能が提供されます。

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

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

主要な **XenApp** および **XenDesktop** コンポーネント

このトピックは、XenApp や XenDesktop の初心者に非常に役立ちます。6.x 以前の XenApp ファームまたは XenDesktop 5.6 以前のサイトを使用している場合は、「7.x での変更点」も参照してください。

次の図は、サイトと呼ばれる典型的な展開での主要なコンポーネントを示しています。

Delivery Controller:

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

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

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

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

Controller は、仮想デスクトップの状態を管理してユーザーからの要求や管理構成に基づいてそれらを起動および停止します。一部のエディションでは、Profile Management をインストールして、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できます。

データベース:

XenApp または XenDesktop の各サイトでは、構成情報やセッション情報を格納するための Microsoft SQL Server データベースが少なくとも 1 つ必要です。このデータベースには、Controller を構成する各サービスによって収集および管理されたデータが格納されます。データセンター内にデータベースをインストールして、Controller

と永続的に接続されるようにしてください。サイトは、構成ログデータベースおよび監視データベースも使用します。これらはデフォルトではサイトデータベースと同じ場所にインストールされますが、その場所は変更できます。

Virtual Delivery Agent（VDA）:

サイトでユーザーが利用可能な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。これらのマシンでは、アプリケーションやデスクトップが配信されます。VDA により、これらのマシンが Controller に登録され、ユーザーがこれらのマシンおよびマシン上でホストされるリソースを使用できるようになります。VDA は、マシンとユーザーデバイス間の接続を確立して、そのユーザーやセッションに必要な Citrix ライセンスを検証して、適切なポリシーを適用します。

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

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

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

Citrix StoreFront:

StoreFront は、リソースをホストするサイトにアクセスするユーザーを認証して、ユーザーのデスクトップやアプリケーションのストアを管理します。StoreFront により、デスクトップやアプリケーションへのセルフサービスアクセスをユーザーに提供する「エンタープライズアプリケーションストア」がホストされます。また、ユーザーのアプリケーションの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を追跡します。これにより、ユーザーが複数のデバイス間で一貫性のある操作を行えるようになります。

Citrix Receiver:

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

Citrix Studio:

Studio は、XenApp および XenDesktop の展開の設定および管理を可能にする管理コンソールです。このコンソールにより、アプリケーションやデスクトップの配信を管理するための個別の管理コンソールが不要になります。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、および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を案内するさまざまなウィザードが提供されます。Studio では、サイトの Citrix ライセンスの割り当てや追跡も可能です。

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

詳細については、こちらの画像をクリックしてください:

Citrix Director:

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

Director には次のものが表示されます:

Controller の Broker Service のリアルタイムセッションデータ。Broker Service が VDA のブローカーエージェントから取得するデータが含まれます。

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

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

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

Citrix ライセンスサーバー:

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

ハイパーバイザーまたはクラウドサービス:

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

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

XenApp および XenDesktop の多くの展開ではハイパーバイザーが必要ですが、リモート PC アクセスを提供する場合はハイパーバイザーは必要ありません。Provisioning Services（PVS）を使用して VM をプロビジョニングする場合も、ハイパーバイザーは必要ありません。

詳細情報の参照先:

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

追加のコンポーネント

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

Provisioning Services（PVS）:

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

NetScaler Gateway:

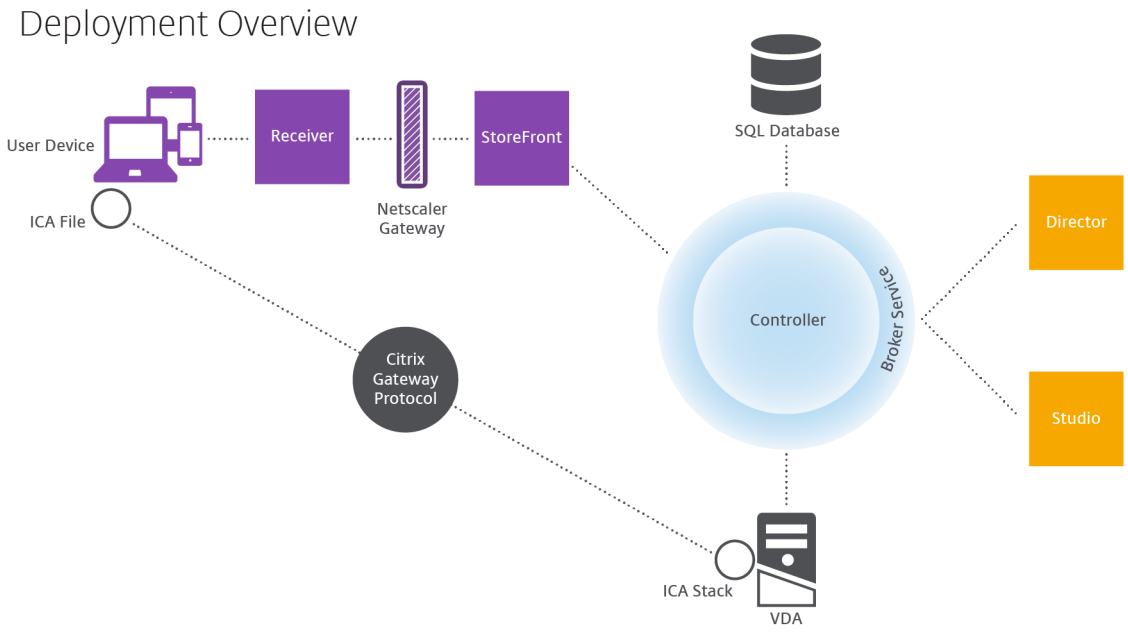
ユーザーが組織のファイアウォールの外側から接続する場合、XenApp および XenDesktop で Citrix NetScaler Gateway（旧称「Access Gateway」）技術を使用して接続を TLS で保護できます。NetScaler Gateway や NetScaler VPX 仮想アプライアンスは非武装地帯（DMZ）に配置する SSL VPN アプライアンスで、企業ファイアウォールを介した安全な単一アクセスポイントを提供します。

NetScaler SD-WAN:

ブランチオフィスなどの遠隔拠点のユーザーが WAN を介して仮想デスクトップに接続する環境では、Citrix NetScaler SD-WAN 技術により WAN 接続のパフォーマンスを最適化できます（このテクノロジは、以前は Citrix CloudBridge、Branch Repeater、または WANScaler でした）。リピーターによって、広域ネットワーク間でのパフォーマンスが向上します。ネットワーク内のリピーターによって、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支店のユーザーに提供されます。NetScaler SD-WAN では、さまざまなユーザー操作に優先順位を付けることができます。たとえば、ネットワーク上で大きなファイルや印刷ジョブを送信する操作に高い優先度を割り当てて、遠隔地のユーザーがストレスなく作業できるようにします。HDX WAN の最適化によりトークン化された圧縮およびデータ重複排除が提供され、帯域幅消費が減少してパフォーマンスが向上します。

典型的な展開方法

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、計画的にセキュアなソリューションを提供します。サイトは、VDA がインストールされている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。



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。各サイトには 1 つまたは複数の Delivery Controller があります。セッションは遅延、帯域幅、ネットワークの信頼性の影響を受けるため、すべての Controller が同じ LAN 上にあることが理想的です。

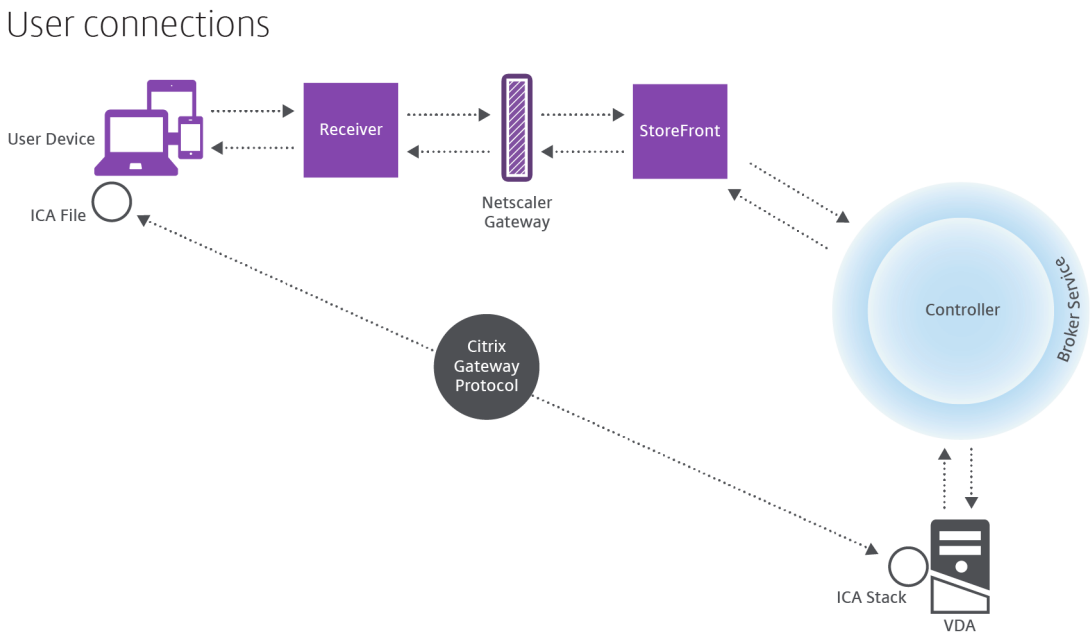
ユーザーが Controller に直接アクセスすることはありません。ユーザーと Controller 間の通信の中継点として VDA が機能します。ユーザーが StoreFront を使用してサイトにログオンすると、その資格情報は Controller 上の Broker Service にパススルーされます。Broker Service は、設定されているポリシーに基づいてプロファイルと利用可能なリソースを取得します。

ユーザー接続を処理するしくみ

ユーザーが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ている Citrix Receiver、または StoreFront Citrix Receiver for Web サイトを使用して接続します。

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

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



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。ユーザーがこのリスト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 に送信されます。Controller は、特定のアプリケーションまたはデスクトップをホストするための適切な VDA を決定します。

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

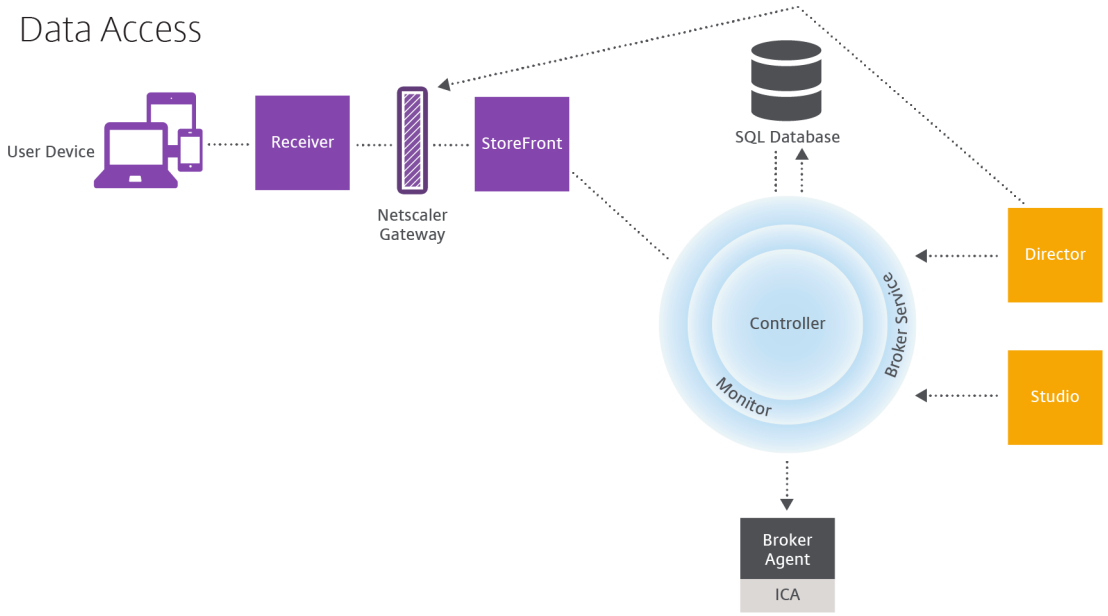
ICA ファイルがユーザーデバイスにコピーされ、VDA 上で実行される ICA スタックとの直接接続が確立されます。この接続により、管理インフラストラクチャ（Citrix Receiver、StoreFront、および Controller）がバイパスされます。

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

クライアントが VDA に接続すると、VDA はユーザーがログオンしていることを Controller に通知します。Controller はその情報をサイトデータベースに送信し、監視データベースにデータを記録し始めます。

データアクセスのしくみ

IT 担当者は、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 を使用すると、管理者は 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管理できます。Director は、同じ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ている履歴データにアクセスします。また、ヘルプデスクによるサポートとトラブルシューティングのために NetScaler Gateway からの HDX データにアクセスします。



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

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

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

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

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

マシンカタログ：

マシンカタログとは、単一のエンティティとして管理される物理マシンまたは仮想マシンのグループを指します。これらのマシンおよびそのアプリケーションや仮想デスクトップは、ユーザーに提供する「リソース」です。カタログ

内のすべてのマシンには、同じオペレーティングシステムおよび VDA がインストールされている必要があります。また、同じアプリケーションまたは仮想デスクトップがある必要があります。

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

有効なマシンの種類は以下のとおりです。

- サーバー **OS** マシン：サーバーオペレーティングシステムをベースとした仮想マシンまたは物理マシン。XenApp 公開アプリケーション（「サーバーベースでホストされるアプリケーション」と呼ばれます）および 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」と呼ばれます）の配信に使用されます。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をベースとした仮想マシンまたは物理マシン。VDI デスクトップ（オプションでパーソナライズ可）、VM でホストされるアプリケーション（デスクトップ OS のアプリケーション）、およびホストされる物理デスクトップの配信に使用されます。これらの各デスクトップに一度にアクセスできるのは 1 人のユーザーのみです。
- リモート **PC** アクセス：リモートユーザーが Citrix Receiver が動作するあらゆるデバイスからオフィスの物理 PC にアクセスできるようにします。オフィスの PC は XenDesktop 環境を介して管理します。ユーザーデバイスはホワイトリストに指定する必要があります。

詳しくは、「マシンカタログの作成」を参照してください。

デリバリーグループ：

デリバリーグループは、どのマシンのどのアプリケーションやデスクトップをどのユーザーが使用できるかを指定します。デリバリーグループには、マシンカタログに記載されているマシンと、サイトへのアクセス権を持つ Active Directory ユーザーが含まれています。Active Directory グループとデリバリーグループは同様の要件に基づいてユーザーをグループ化する方法であるため、Active Directory グループを使用してデリバリーグループにユーザーを割り当てることができます。

1 つのデリバリーグループに複数のカタログからのマシンを含めることができ、1 つのカタログからのマシンを複数のデリバリーグループで使用できます。ただし、1 つのマシンが複数のデリバリーグループに属することはできません。

管理者は、デリバリーグループ内のユーザーがどのリソースにアクセスできるのかを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信する場合、1 つのマシンカタログのマスターイメージにそれらのすべてのアプリケーションをインストールしておき、複数のデリバリーグループに分配するための十分な数のマシンをそのカタログに作成します。次に、マシンにインストールされているアプリケーションの異なるサブセットが配信されるように各デリバリーグループを構成します。

詳しくは、「デリバリーグループの作成」を参照してください。

アプリケーショングループ：

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

詳しくは、「アプリケーショングループの作成」を参照してください。

Active Directory

August 24, 2021

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

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

以下の環境がサポートされています。

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

必要に応じて、Virtual Delivery Agent（VDA）で登録可能な Controller を検出するときに、Active Directory の情報を使用することもできます。この機能は主に後方互換性を保持するためのもので、VDA と Controller が同

じ Active Directory フォレストに属している場合のみ使用できます。この検出方法について詳しくは、「Active Directory OU ベースの検出」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

このトピックの内容は、XenDesktop 7.1 以降および XenApp 7.5 以降に適用されます。これらの製品の以前のバージョンの XenDesktop または XenApp 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、シトリックス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. <ProgramFiles>\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	Direction	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

August 24, 2021

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

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

各 Delivery Controller は、サイトデータベースと通信します。Controller とデータベース間の接続には Windows 認証が必要です。任意の Controller をシャットダウンしても、そのサイトのほかの Controller には影響しません。しかしながら、これはサイトデータベースが単一障害点になりうることを意味します。このデータベースサーバーで

障害が発生しても、既存の接続は、ユーザーがログオフまたは切断するまでは機能し続けます。サイトデータベースが利用不可能な場合の接続動作について詳しくは、「ローカルホストキャッシュ」を参照してください。

Delivery Controller をサイトに追加する際には、そのマシンのログオン資格情報を、高可用性のために使用するレプリカ SQL Server に追加してください。

データベースのバックアップを定期的に作成して、データベースサーバーに障害が発生してもバックアップから復元できるようにすることを Citrix ではお勧めします。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、サイトベースは引き続きプライマリゾーンに格納します。すべてのゾーンのコントローラーは、このデータベースと通信します。

高可用性

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

- **AlwaysOn** 可用性グループ機能（基本的な可用性グループを含む）： 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、「https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?redirectedfrom=MSDN&view=sql-server-ver15」を参照してください。
- **SQL Server** データベースのミラーリング：データベースをミラーリングすると、アクティブなデータベースサーバーが停止しても自動フェールオーバー処理が実行され、ユーザーは通常、停止の影響を受けません。各データベースサーバー上に完全な SQL Server ライセンスが必要になるため、ほかのソリューションよりも費用が高くつきます。SQL Server Express エディションを使用してデータベースをミラーリングすることはできません。
- **SQL** クラスタリング： Microsoft の SQL クラスタリングテクノロジを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQL ミラーリングなどほかのソリューションよりも自動フェールオーバー処理には一般的に時間がかかります。
- ハイパーバイザーの高可用性機能の使用：この方法では、仮想マシンとしてデータベースを展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションでは既存のハイパーバイザーソフトウェアを使用でき、また SQL Server Express エディションも使用できるため、ミラーリングよりも費用が安いというメリットがあります。ただし、データベースの新しい仮想マシンの起動に時間がかかるため、自動フェールオーバー処理が遅くなり、ユーザーへのサービスが中断する可能性があります。

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

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

> 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。

データベースソフトウェアのインストール

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

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

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

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

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

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

サイトの作成ウィザードを使ったデータベースのセットアップ

［サイトの作成］ウィザードの ［データベース］ページで、データベースの名前とアドレス（場所）を指定します。「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。

構成ログや監視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。

サイトの作成後にミラーリング設定を検証するには、PowerShell コマンドレット`get-configdbconnection`を実行して、ミラーに対する接続文字列でフェールオーバーパートナーが設定されていることを確認します。

ミラー化されたデータベース環境で Delivery Controller を後から追加、移動、または削除する場合は、「Delivery Controller」の記事を参照してください。

自動セットアップ

必要なデータベース権限を持っている場合は、サイトの作成ウィザードの［データベース］ページにある「Studio でデータベースを作成および設定する」オプションを選択し、プリンシパルデータベースの名前とアドレスを指定します。

指定したアドレスにデータベースが存在する場合、そのデータベースは空でなければなりません。指定されたアドレスにデータベースが存在しない場合、データベースが見つからないというメッセージが表示され、データベースを作成するかどうかの確認を求められます。作成に同意すると、Studio により自動的にデータベースが作成され、プリンシパルデータベースとレプリカデータベースに初期化スクリプトが適用されます。

スクリプトを使ったセットアップ

必要なデータベース権限がない場合は、データベース管理者など、権限を持っている人に支援を依頼する必要があります。その手順は以下のとおりです。

1. サイトの作成ウィザードで［スクリプトを生成］オプションを選択します。この操作により、合計 6 つのスクリプトが作成されます。3 つのデータベースそれぞれに対して 2 つずつ（1 つはプリンシパルデータベース、もう 1 つは各レプリカデータベース）が使用されます。スクリプトの格納先を指定します。
2. これらのスクリプトをデータベース管理者に渡します。この時点で、サイトの作成ウィザードは自動的に停止します。あとでサイトの作成を続行しに戻ってきたときに、プロンプトが表示されます。

その後、データベース管理者がデータベースを作成します。個々のデータベースには、次の特性が必要です:

- 「_CI_AS_KS」で終わる照合順序を使用します。Citrix は、「_100_CI_AS_KS」で終わる照合順序の使用を推奨しています。
- 最適なパフォーマンスを実現するには、SQL Server Read-Committed Snapshot を有効化します。詳しくは、CTX137161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、［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

操作	目的	サーバーロール	データベースロール
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*	
Controller の削除	サイトから Controller を削除します	**	db_owner
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。

**Controller を直接か Desktop Studio で、または Desktop Studio か SDK で生成されたスクリプトを使用してサイトから削除すると、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、XenDesktop サービス以外で使用される同じマシン上の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 サーバーロールのメンバーシップが必要です。

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

構成ログや監視データベースの場所は、サイトの作成後に変更できます。（サイト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。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。それが失敗すると、データベースユーザーの資格情報の入力を求められます。アクセスに成功すると、Studio によりデータベーススキーマがデータベースにアップロードされます（資格情報はデータベース作成時のみ保持されます）。
6. Studio にデータベースを作成させない場合、または必要な権限がない場合は、［スクリプトを作成］をクリックします。作成されるスクリプトには、データベースおよびミラーデータベース（構成する場合）を手動で作成するためのコマンドが記述されます。スキーマをアップロードする前に、データベースが空であること、および 1 人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

詳細情報

- データベースのサイズ評価ツール
- 「サイト構成データベースのサイズ変更」および「接続文字列の構成」（SQL Server の高可用性のためのソリューションを使用する場合）

配信方法

August 24, 2021

単一の仮想化環境ですべてのユーザーのニーズを満たすことは容易ではありません。XenApp および XenDesktop の管理者は、さまざまな方法（「FlexCast」と呼ばれます）を使用してユーザーエクスペリエンスをカスタマイズできます。

これらの配信方法にはそれぞれ一長一短があり、ユーザーの使用方法に応じて最適なユーザーエクスペリエンスを提供できます。

Windows アプリケーションをモバイルデバイス用に最適化する：

今日、スマートフォンやタブレットなどのタッチスクリーンデバイスが移動環境として一般的に使用されています。これらのデバイス上で、大きな画面と従来のポインティングデバイスでの使用が前提となっている Windows ベースのアプリケーションを操作する場合、問題が生じることがあります。

XenApp と Citrix Receiver によるソリューションでは、Windows ベースのアプリケーションを修正することなく、すべての機能を安全にモバイルユーザーに提供できます。

XenApp の公開アプリケーションによる配信方法では、HDX Mobile テクノロジにより Windows アプリケーションがモバイル環境に最適化されます。この方法では、Windows アプリケーションがタッチスクリーン上で操作できるようになり、マルチタッチジェスチャ、ネイティブのメニューコントロール、カメラ、および GPS 機能がサポートされます。XenApp および XenDesktop では、アプリケーションのソースコードを変更しなくても、多くのタッチ機能がそのまま使用可能になります。

以下のタッチ操作が含まれます。

- 編集フィールド操作時にキーボードが自動的に表示されます。
- Windows コンボボックスコントロールの代わりにタッチ操作に適したピッカーコントロールが表示されます。
- ピンチやズームなどのマルチタッチジェスチャを使用できます。
- 慣性スクロールが適用されます。
- タッチパッドまたはカーソル操作でナビゲーションできます。

PC の更新コストを削減する:

多くの業種で 3 年から 5 年ごとに必要になる物理マシンの更新は面倒な作業であり、最新のオペレーティングシステムやアプリケーションが必要な部署では特に大掛かりになりがちです。また、組織の成長による新しいマシンの導入に伴う諸経費も無視できません。

VDI Personal vDisk を使用した配信方法では、ユーザーによる完全なパーソナル設定が可能なデスクトップオペレーティングシステムをサーバーリソースからシンクライアントを含むさまざまなマシンに提供できます。管理者は、プロセッサ、メモリ、およびストレージなどのリソースをネットワーク上のデータセンターで提供する仮想マシンを作成できます。

これにより、古いマシンの使用を延長しながら最新のソフトウェアを維持して、アップグレード時のダウンタイムを最小限に抑えることができます。

契約社員やパートナーが仮想アプリケーション/デスクトップに安全にアクセスできるようにする:

ネットワークセキュリティの問題はますます重要になっており、契約社員やパートナーなどの社外作業者に社内のアプリケーションやデータへのアクセスを許可する場合は特に慎重に行う必要があります。作業者にラップトップなどのデバイスを貸与する場合も、セキュリティに対する配慮が必要です。

XenDesktop および XenApp では、データ、アプリケーション、およびデスクトップがファイアウォールで保護された安全なネットワーク内に格納されます。エンドユーザーが転送する情報は、画面の更新、マウスのクリック、キーボード入力のみです。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、単一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。

物理デスクトップをホストして配信する方法を使用すると、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、デスクトップをホストする方法があります。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

August 24, 2021

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。

ユースケース:

- 安価なサーバーベースのアプリケーション配信により、最小限のコストでアプリケーションを多くのユーザーに配信し、しかも高度なセキュリティと良好なユーザーエクスペリエンスを提供する。
- 明確に定義されたタスクだけを実行し、個人用設定やオフラインアクセスが不要なユーザー。たとえば、コールセンターのオペレーター、販売員、ワークステーションを共有する作業者など。
- アプリケーションの種類:任意のアプリケーション。

特長と注意事項:

- データセンター内で簡単に管理できるスケーラブルなソリューション。
- 最もコスト効率に優れたアプリケーション配信ソリューション。
- ホスト上のアプリケーションを一元管理でき、ユーザーはアプリケーションを変更できません。また、安全で信頼性が高く一貫したユーザーエクスペリエンスが提供されます。
- アプリケーションにアクセスするユーザーは常にオンライン状態である必要があります。

ユーザーエクスペリエンス:

- ユーザーは、StoreFront、[スタート] メニュー、または特定の URL からアプリケーションにアクセスします。
- アプリケーションはユーザーデバイス上に仮想的に配信され、シームレスかつ高品位に表示されます。
- プロファイル設定によっては、ユーザーによる変更内容がアプリケーションセッションの終了時に保存されます。それ以外の場合、変更は削除されます。

プロセス、ホスト、および配信:

- アプリケーションのプロセスはユーザーデバイスではなくホストマシン上で実行されます。物理マシンまたは仮想マシンでアプリケーションをホストできます。
- アプリケーションおよびデスクトップはサーバー OS マシン上にインストールされます。
- マシンは、マシンカタログを作成することで使用可能になります。
- 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、単一の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」を参照してください。

VM Hosted Apps

August 24, 2021

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。

ユースケース:

- セキュアなクライアントベースのアプリケーション配信により、シームレスかつ高品位に表示されるアプリケーションをユーザーに配信し、管理を一元化して単一ホストサーバー（またはハイパーバイザー）で多くのユーザーをサポートする。
- ユーザーは、内部または外部契約社員、サードパーティの協力者、臨時社員などである。ホスト上のアプリケーションへのオフラインアクセスは不要。
- アプリケーション種類：ほかのアプリケーションと共存できないアプリケーションや、オペレーティングシステムと一緒に動作する Microsoft .NET Framework などのアプリケーション。これらのアプリケーションは、仮想マシン上でのホストに適しています。

特長と注意事項:

- マスターイメージ上のアプリケーションおよびデスクトップは、データセンター内のマシン上でセキュアに管理、ホスト、および実行されます。また、最もコスト効率に優れたアプリケーション配信ソリューションでもあります。

- ユーザーがログオンすると、同じアプリケーションをホストするデリバリーグループ内のマシンにランダムに割り当てられます。管理者は、ユーザーがログオンするたびに同じマシンが割り当てられるように構成することもできます。このようにマシンをユーザーに静的に割り当てると、ユーザーが仮想マシンにアプリケーションをインストールしたり独自に管理したりできるようになります。
- デスクトップ OS マシンでは、複数のセッションを実行できません。このため、ユーザーがログオンするとデリバリーグループ内の 1 つのマシンが消費され、オフライン状態ではアプリケーションにアクセスできなくなります。
- この方法では、アプリケーションの処理のためのサーバーリソースと、ユーザーの Personal vDisk 用のストレージ容量が多くなります。

ユーザーエクスペリエンス:

サーバー OS マシン上でホストされる共有アプリケーションと同様のシームレスなユーザーエクスペリエンスが提供されます。

プロセス、ホスト、および配信:

仮想デスクトップ OS マシンが使用されることを除き、サーバー OS マシンの場合と同様です。

セッション管理と割り当て:

- 1 つのデスクトップ OS マシンで実行できるデスクトップセッションは 1 つのみです。アプリケーションにのみアクセスする場合は、各アプリケーションが個別のセッションと見なされるため、1 人のユーザーが複数のアプリケーションを使用できます。
- デリバリーグループ内では、ログオンしたユーザーは、静的に割り当てられたマシン（毎回、必ず同じマシンにログオンする）、またはセッションの可用性に基づいてランダムに割り当てられたマシンにアクセスします。

VM Hosted App を配信するには、次の手順に従います。

1. サポートされる Windows デスクトップ OS のマスターイメージ上に、配信するアプリケーションをインストールします。
2. このマスターイメージのマシンカタログを作成するか、既存のマシンカタログをこのマスターイメージで更新します。
3. カタログのデスクトップエクスペリエンスを定義するときに、ユーザーがログオンするたびに新しい仮想マシンに接続するのか同じ仮想マシンに接続するのかを指定します。
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」を参照してください。

ネットワークポート

August 24, 2021

次の表は、XenApp および XenDesktop Delivery Controllers、Windows VDA、Director、Citrix ライセンスサーバーで使用されるデフォルトのネットワークポート一覧です。Citrix コンポーネントをインストールすると、これらのデフォルトのネットワークポートと一致するように、オペレーティングシステムのファイアウォールもデフォルトで更新されます。

他の Citrix テクノロジおよびコンポーネントで使用される通信ポートの概要については、「Citrix テクノロジで使用される通信ポート」を参照してください。

以下のように、このポートの情報が必要な場合があります:

- 法的なコンプライアンスが必要である。
- これらのコンポーネントと他の Citrix 製品またはコンポーネントとの間にネットワークファイアウォールがある場合、ファイアウォールを適切に構成できる。
- オペレーティングシステムのホストファイアウォールではなく、アンチマルウェアパッケージなどが付属したサードパーティ製のホストファイアウォールを使用する。
- これらのコンポーネントでホストファイアウォールの構成を変更する（通常 Windows ファイアウォールサービス）。
- これらのコンポーネントの機能を再構成して、別のポートやポート範囲を使用し、構成で使用されていないポートを無効にする、またはブロックする必要がある。詳しくは、コンポーネントのドキュメントを参照してください。

StoreFront および Provisioning Services のような他のコンポーネントのポート情報について詳しくは、コンポーネントの現在の「システム要件」記事を参照してください。

表は、受信ポートのみの一覧です。送信ポートは、通常オペレーティングシステムによって決定され、無関係な番号を使用します。送信ポートの情報は通常、上記に記載された目的には必要ありません。

これらのポートの一部は、Internet Assigned Numbers Authority（IANA）に登録されています。こうした割り当てについて詳しくは、https://www.iana.org/assignments/port-numbersを参照してください。IANA の説明は、最新の使用状況に対応していない場合もあることに注意してください。

また、VDA および Delivery Controller のオペレーティングシステムには、専用の受信ポートが必要です。詳しくは、Microsoft Windows のドキュメントを参照してください。

VDA、Delivery Controller、Director

コンポーネント	用途	プロトコル	デフォルトの受信ポート	メモ
VDA	ICA/HDX	TCP、UDP	1494	EDT プロトコルでは、UDP 用に 1494 が開放されている必要があります。「ICA のポリシー設定」を参照してください。
VDA	ICA/HDX（セッション画面の保持機能）	TCP、UDP	2598	EDT プロトコルでは、UDP 用に 2598 が開放されている必要があります。マルチストリームとマルチポートが有効な場合、管理者は 3 つの追加ストリームに対するポート番号を定義します。「ICA のポリシー設定」を参照してください。
VDA	ICA/HDX（TLS/DTLS 経由）	TCP、UDP	443	すべての Citrix Receiver
VDA	ICA/HDX（WebSocket 経由）	TCP	8008	Citrix Receiver for HTML5、Citrix Receiver for Chrome 1.6 以前のみ
VDA	ICA/HDX（UDP でのオーディオリアルタイムトランスポート）	UDP	16500 から 16509	

コンポーネント	用途	プロトコル	デフォルトの受信ポート	メモ
VDA	ICA/ユニバーサルプリントサーバー	TCP	7229	ユニバーサルプリントサーバー印刷データストリーム CGP（Common Gateway Protocol）リスナーが使用。
VDA	ICA/ユニバーサルプリントサーバー	TCP	8080	HTTP/SOAP 要求の受信のためにユニバーサルプリントサーバーのリスナーが使用。
VDA	Wake On LAN	UDP	9	リモート PC アクセスの電源管理
VDA	ウェイクアッププロキシ	TCP	135	リモート PC アクセスの電源管理
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA、StoreFront、Director、Studio	TCP	80	
Delivery Controller	StoreFront、Director、Studio (TLS 経由)	TCP	443	
Delivery Controller	Delivery Controller、VDA	TCP	89	ローカルホストキャッシュ（ポート 89 の使用は将来のリリースで変更される可能性があります）
Delivery Controller	オーケストレーション	TCP	9095	オーケストレーション
Director	Delivery Controller	TCP	80、443	

Citrix ライセンスサーバー

以下のポートが Citrix ライセンスサーバーに使用されます。

コンポーネント	用途	プロトコル	デフォルトの受信ポート
ライセンスサーバー	ライセンスサーバー	TCP	27000
ライセンスサーバー	Citrix のライセンスサーバー（ベンダーデーモン）	TCP	7279
ライセンスサーバー	ライセンス管理コンソール	TCP	8082
ライセンスサーバー	Web Services for Licensing	TCP	8083

HDX

August 24, 2021

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

Citrix HDX には、高品位なユーザーエクスペリエンスを提供する、幅広い機能セットが含まれています。

デバイスで:

ユーザーデバイスのコンピューティング能力を利用して、ユーザーエクスペリエンスを拡張および最適化します。HDX テクノロジにより、スムーズでシームレスなマルチメディアコンテンツが仮想デスクトップやアプリケーションに提供されます。ワークスペースコントロール機能により、仮想デスクトップやアプリケーションのセッションを一時停止して、ほかのデバイスでそのセッションでの作業を再開できます。

ネットワーク上で:

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。

HDX 機能は環境のさまざまな条件に応じて最適化されます。パフォーマンスと消費帯域幅を調和させる機能。社内ネットワークからデスクトップやアプリケーションにローカルにアクセスする場合やファイアウォールの外側からリモートにアクセスする場合など、各ユーザーシナリオに応じて最適な機能が適用されます。

データセンターで:

HDX では、サーバー側の処理能力およびスケーラビリティを利用して、クライアントデバイス側の能力に制限されずに高度なグラフィックパフォーマンスを提供できます。

Citrix Director では、ユーザーデバイスに接続している HDX チャネルの状態を監視できます。

HDX Insight

HDX Insight により、NetScaler Network Inspector および Performance Manager が Director に統合されます。ICA トラフィックに関するデータを収集して、リアルタイムおよび履歴の詳細をダッシュボードに表示します。このデータには、クライアント側およびサーバー側の ICA セッション遅延、ICA チャネルの帯域幅使用量、および各セッションの ICA 往復時間値が含まれます。

仮想デスクトップからの **HDX** 機能の体験

- 3 つの HDX マルチメディアリダイレクトテクノロジの 1 つである Flash リダイレクトにより Adobe Flash マルチメディアコンテンツの配信がどのように高速化されるかを体験するには、次の手順に従います。
  1. Adobe Flash Player（https://get.adobe.com/flashplayer/）をダウンロードして仮想デスクトップおよびユーザーデバイスにインストールします。
  2. Desktop Viewer のツールバーで［基本設定］をクリックします。Desktop Viewer の［基本設定］ダイアログボックスで［**Flash**］タブを選択し、［最適化する］を選択します。
  3. Flash リダイレクトによる Flash マルチメディアコンテンツの配信パフォーマンスを体験するには、仮想デスクトップで YouTube などの Web サイトにアクセスして、Flash ビデオを再生します。Flash リダイレクトはシームレスであるため、ユーザー側にはいつ動作しているかはわかりません。ただし、Flash リダイレクトが使用されているかどうかは確認できます。Flash Player が起動する前に画面上に一瞬だけカラーブロックが現れます。また、ビデオを右クリックすると、メニューに［Flash リダイレクト］が表示されます。
- HDX により高品位オーディオがどのように配信されるかを体験するには、次の手順に従います。
  1. Citrix Receiver で、最高の音質を選択します。詳しくは、Citrix Receiver のドキュメントを参照してください。
  2. デスクトップ上のデジタルオーディオプレーヤー（iTunes など）で音楽ファイルを再生します。

HDX では、特別な構成を行わなくてもデフォルトで、一般的なユーザーに適したグラフィックおよびビデオ配信が提供されます。Citrix ポリシー設定は、一般的な使用環境で最適なユーザーエクスペリエンスが提供されるようにデフォルトで有効になっています。

- HDX は、クライアントプラットフォーム、アプリケーション、およびネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、状況の変化に応じて自動調整します。
- HDX は、2D および 3D のグラフィックおよびビデオのパフォーマンスを最適化します。
- HDX は、インターネットやイントラネット上のマルチメディアコンテンツなどをホストサーバーを介さず直接ユーザーデバイス上にストリーム配信します。このクライアント側でのコンテンツ取得に必要な条件が満た

されない場合、メディア配信はサーバー側でのコンテンツ取得とマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能に関するポリシーを変更する必要はありません。

- マルチメディアリダイレクトが利用できない場合、HDX は仮想デスクトップにサーバー側でレンダリングしたビデオコンテンツを提供します。https://www.microsoft.com/silverlight/iis-smooth-streaming/demo/などのサイトにアクセスして、高品位ビデオを含む Web サイト上のビデオをご覧ください。

ヒント:

- HDX 機能に関するサポートおよび要件については、「システム要件」を参照してください。特に注記のあるものを除き、Windows サーバー OS マシン、Windows デスクトップ OS マシン、およびリモート PC アクセスのデスクトップで HDX 機能を使用できます。
- このセクションのトピックでは、ユーザーエクスペリエンスをさらに最適化したり、サーバーのスケーラビリティを改善したり、消費帯域幅を抑えたりする方法について説明します。Citrix ポリシーおよびそのポリシー設定について詳しくは、このリリースの「Citrix ポリシー」を参照してください。
- レジストリを編集する場合は細心の注意が必要です: レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

制限事項

セッション内でリモート音声およびビデオ拡張機能（RAVE）を有効にして Windows Media Player を使用しているときに、ビデオコンテンツを右クリックして ［プレイビューを常に手前に表示］ を選択すると、画面表示が黒くなることがあります。

クライアントの自動再接続とセッション画面の保持

ホストされるアプリケーションまたはデスクトップにアクセスすると、ネットワークが中断される場合があります。再接続をスムーズに行うために、クライアントの自動再接続とセッション画面の保持が利用できます。デフォルト構成では、セッション画面の保持が起動した後、クライアントの自動再接続が起動します。

クライアントの自動再接続:

クライアントの自動再接続によってクライアントのエンジンが再起動され、切断されたセッションに再接続します。クライアントの自動再接続によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。クライアントの自動再接続の実行中に、システムからユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます。

- デスクトップ。セッションウィンドウが灰色表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。

- アプリケーション。セッションウィンドウがクローズし、ダイアログが開いて再接続が試行されるまでの時間を示すカウントダウンタイマーが表示されます。

クライアントの自動再接続中に、セッションはネットワーク接続を見越して再起動されます。クライアントの自動再接続の実行中は、セッションを操作できません。

再接続では、切断されたセッションは、保存された接続情報を使って再接続されます。ユーザーは、正常にアプリケーションおよびデスクトップを操作できます。

クライアントの自動再接続のデフォルト設定:

- クライアントの自動再接続のタイムアウト: 120 秒
- クライアントの自動再接続: 有効
- クライアントの自動再接続時の認証: 無効
- クライアントの自動再接続のログ: 無効

詳しくは、「クライアントの自動再接続のポリシー設定」を参照してください。

セッション画面の保持:

セッション画面の保持によって ICA セッションは、ネットワークの中断を挟んでもシームレスに再接続されます。セッション画面の保持によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。セッション画面の保持がタイムアウトした後で、クライアントの自動再接続設定が有効になり、切断されたセッションへの再接続が行われます。セッション画面の保持の実行中に、ユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます。

- デスクトップ。セッションウィンドウが半透明表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。
- アプリケーション。ウィンドウが半透明表示になると同時に、通知領域に中断された接続のポップアップが表示されます。

セッション画面の保持がアクティブの間は、ユーザーは ICA セッションを操作できません。ただし、キー入力のようなユーザー操作は、ネットワーク中断直後の数秒間バッファーされ、ネットワークが再接続されたら再送信されます。

再接続されると、クライアントとサーバーは、プロトコルを交換したポイントからセッションを再開します。セッションウィンドウの半透明表示が解除され、アプリケーションに対する適切なポップアップが通知領域に表示されます。

セッション画面の保持のデフォルト設定

- セッション画面の保持のタイムアウト 180 秒
- 再接続 UI の透過レベル: 80%
- セッション画面の保持の接続: 有効
- セッション画面の保持のポート番号: 2598

詳しくは、「セッション画面の保持のポリシー設定」を参照してください。

NetScaler とクライアントの自動再接続およびセッション画面の保持:

マルチストリームポリシーとマルチポートポリシーがサーバー上で有効化され、次の条件のいずれかまたはすべてに合致する場合、クライアントの自動再接続は機能しません。

- セッション画面の保持機能が NetScaler Gateway で無効化されている。
- NetScaler アプライアンスでフェールオーバーが発生している。
- NetScaler Gateway で NetScaler SD-WAN を使用している。

タッチスクリーンデバイス用タブレットモード

Windows 10 VDA に接続またはローミングされたタッチ対応デバイスは、デフォルトでタブレットモードで起動されます。

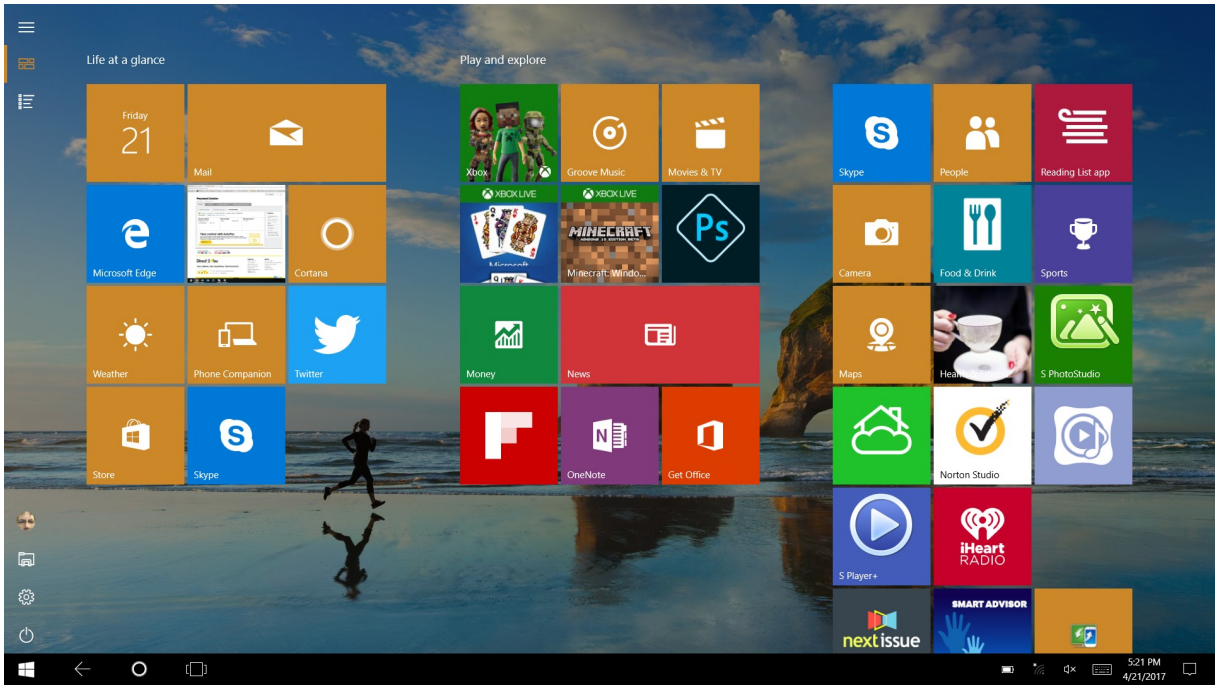
タブレットモードの使用には、XenServer バージョン 7.2 以上が必要です。XenServer 7.2 は XenDesktop VDA と統合されており、2-in-1 デバイスの仮想ファームウェア設定が有効になるようにハイパーバイザーが変更されています。Windows 10 は、この更新された BIOS を基にターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるのに使用されます。詳しくは、「https:/docs.citrix.com/en-us/xenserver/current-release/downloads/release-notes.pdf」を参照してください。

タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます:

- やや大きめのボタン
- スタート画面や開始したアプリケーションを全画面で開く
- タスクバーに［戻る］ボタンを表示
- タスクバーからアイコンを削除

File Explorer にアクセスできます。

Web Receiver ではテーブルモードはサポートされません。



ラップトップとタブレットの切り替えを許可する XenServer CLI コマンドを実行します。


```
xe vm-param-set uuid=\<VM\\_UUID\> platform:acpi\\_laptop\\_slate=1
```

タブレットモードを無効または有効にするには、XenApp および XenDesktop のこのレジストリ設定を構成します。

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

名前：CitrixEnhancedUserExperience
種類：REG_DWORD

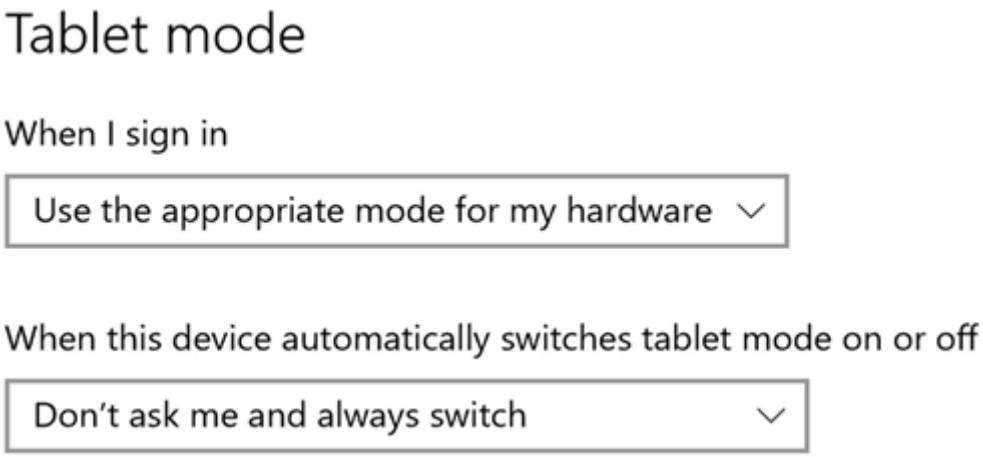
値：
0（無効）
1（有効）

セッション開始前：

セッション開始前に VD で ［設定］**>**［システム］**>**［タブレットモード］に移動して、ドロップダウンメニューから以下のオプションを設定することをお勧めします：

- ハードウェアに適切なモードを使用する
- 確認なしで常に切り替える

セッション開始前にこれらのオプションを設定しない場合には、セッション開始後に設定し、VDA を再起動してください。



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。メディアのデフォルト設定による実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレーム数仮想デスクトップからユーザーデバイスに送信されるイメージの 1 秒あたりの最大フレーム数（fps）を指定します。デフォルトは 30fps です。CPU が低速なデバイスでは、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。サポートされている 1 秒あたりの最大フレームレートは 60 です。

- 表示メモリの制限。セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。デフォルトは 65536KB 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。

ビデオ会議パフォーマンスの改善

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介する XenApp および XenDesktop からの配信に最適化されています（「HDX RealTime Optimization Pack」などを参照）。最適化されていないアプリケーションでは、HDX Web カメラビデオ圧縮を使用すると、セッションでのビデオ会議で Web カメラの帯域幅使用効率および遅延に対する耐性が向上します。この機能では、Web カメラのトラフィックが専用のマルチメディア仮想チャネルでストリーム配信されます。この機能では、HDX Plug-n-Play USB リダイレクトサポートのアイソクロナス転送に比べて帯域幅消費が少なく、WAN 接続に適しています。

このデフォルト設定は、Citrix Receiver ユーザーが Desktop Viewer の［マイクと Web カメラ］設定で ［マイクおよび **Web** カメラを使用しない］を選択することで無効になります。ユーザーが［HDX Web カメラビデオ圧縮］から切り替えられないようにするには、［ICA ポリシーの設定］>［USB デバイスのポリシー］のポリシー設定を使用して、USB デバイスのリダイレクトを無効にします。

HDX Web カメラビデオ圧縮を使用するには、以下のポリシー設定を有効にする必要があります（これらの設定項目はデフォルトで有効になっています）。

- クライアントオーディオリダイレクト
- クライアントマイクリダイレクト
- マルチメディア会議
- Windows Media リダイレクト

Web カメラで H.264 ハードウェアエンコード機能がサポートされる場合、HDX Web カメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェアエンコードが使用されるようにするには、レジストリキー HKEY_CURRENT_USER\Software\Citrix\HdxRealTime に DWORD 値 DeepCompress_ForceSWEncode=1 を設定します。

ネットワークトラフィックの優先度

QoS（Quality of Service）機能をサポートするルーターを使ってセッションに複数の接続を使用する場合、ネットワークトラフィックの優先度を割り当てることができます。ユーザーデバイスとサーバー間の ICA トラフィックでは、4 つの TCP ストリーム（リアルタイム、インタラクティブ、バックグラウンド、およびバルク）と 2 つのユーザーデータグラムプロトコル（UDP）ストリーム（ボイスおよび Framehawk ディスプレイリモート）を使用できます。各仮想チャネルには特定の優先度が割り当てられており、対応する接続を使って転送が行われます。これらの仮想チャネルには、使用される TCP ポート番号に基づいて個別に優先度を設定できます。

Windows 10、Windows 8 および Windows 7 マシンにインストールした Virtual Delivery Agent（VDA）では、複数チャネルのストリーム接続がサポートされます。ネットワーク管理者に問い合わせて、［マルチポートポリシー］

設定で指定した CGP（Common Gateway Protocol）ポートが、ネットワークルーター上で正しく割り当てられていることを確認してください。

QoS（Quality of Service）は、セッション画面の保持機能のポートまたは CGP ポートが複数設定されている環境でのみサポートされます。

> 注意：
>
> この機能を使用する場合は、トランスポートセキュリティを使用してください。IPsec（Internet Protocol Security）または TLS（Transport Layer Security）を使用することをお勧めします。TLS 接続がサポートされるのは、マルチストリーム ICA をサポートする NetScaler Gateway を通過するトラフィックのみです。企業内ネットワークでは、TLS を使用したマルチストリーム接続はサポートされません。

マルチストリーム接続のサービス品質を設定するには、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されるポートおよびそのネットワーク優先度を指定します。
  - ［CGP デフォルトポートの優先度］ボックスの一覧で、優先度を選択します。デフォルトでは、プライマリポート（2598）に優先度［高］が設定されています。
  - ［CGP ポート 1］、［CGP ポート 2］、および［CGP ポート 3］ボックスに追加の CGP ポートを入力して、それぞれ優先度を選択します。各ポートには異なる優先度を設定する必要があります。

  VDA 側のファイアウォールで、追加した TCP トラフィックを明示的に許可する必要があります。
- マルチストリームコンピューター設定 - この設定は、デフォルトでは無効になっています。Citrix NetScaler SD-WAN でマルチストリーム機能をサポートする場合は、この設定項目を使用する必要はありません。このポリシー設定は、サードパーティ製のルーターや従来の Branch Repeater を使用する環境で QoS（Quality of Service）優先度を指定するときに使用できます。
- マルチストリームユーザー設定 — この設定は、デフォルトでは無効になっています。

ポリシーの設定を反映させるには、ユーザーがネットワークに再ログオンする必要があります。

Unicode キーボードマッピング

Windows 以外の Citrix Receiver は、ローカルのキーボードレイアウト（Unicode）を使用します。ユーザーがローカルのキーボードレイアウトとサーバーのキーボードレイアウト（スキャンコード）を変更すると、それらが同期しない可能性があり、出力が不正になります。たとえば、User1 が、ローカルのキーボードレイアウトを英語からドイツ語に変更しました。その後、User1 は、サーバー側のキーボードをドイツ語に変更しました。両方のキーボードレイアウトがドイツ語であっても、これらが同期しない可能性があり、不正な文字出力の原因となります。

Unicode キーボードレイアウトマッピングの有効化または無効化：

デフォルトでは、この機能は VDA 側で無効になっています。この機能を有効にするには、VDA のレジストリエディター regedit を使用してこの機能を切り替えます。

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix の下に CtxKlMap キーを作成します。
EnableKlMap の DWORD 値を 1 に設定します。

この機能を無効にするには、EnableKlMap の DWORD 値を 0 に設定するか、CtxKlMap キーを削除します。

Unicode キーボードレイアウトマッピング互換モードの有効化:

デフォルトでは、Unicode キーボードレイアウトマッピングは、サーバー側のキーボードレイアウトを変更すると、新しい Unicode キーボードレイアウトマップをリロードするためになんらかの Windows API に自動的にフックします。いくつかのアプリケーションはフックされないことがあります。互換性を維持するために、機能を互換モードに変更して、これらのフックされないアプリケーションをサポートすることができます。

1. HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap キーの下で、DisableWindowHook の DWORD 値を 1 に設定します。
2. 通常の Unicode キーボードレイアウトマッピングを使用するには、DisableWindowHook の DWORD 値を 0 に設定します。

関連情報

- グラフィック
- マルチメディア
- 一般コンテンツリダイレクト
- アダプティブトランスポート

アダプティブトランスポート

August 24, 2021

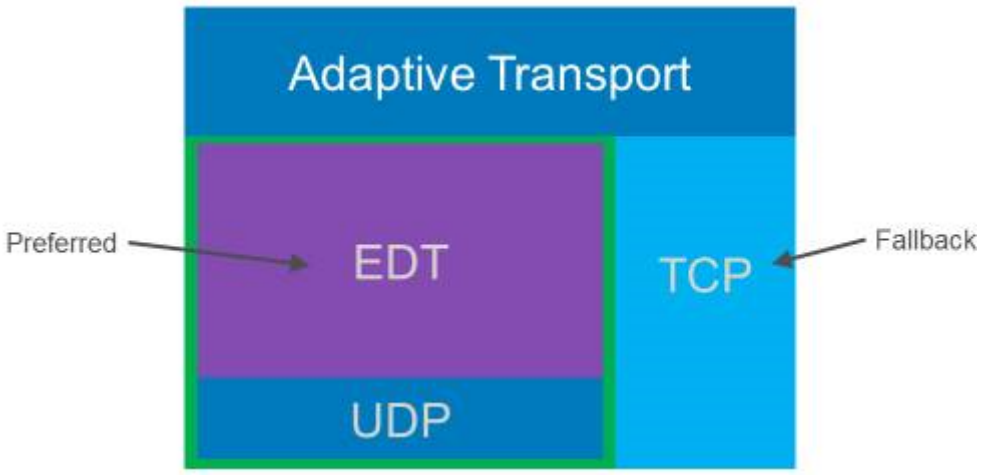
はじめに

アダプティブトランスポートは、XenApp と XenDesktop の新しいデータ転送メカニズムです。高速で拡張性が高く、アプリケーションの対話機能が向上し、厳しい長距離の WAN とインターネット接続でのインタラクティブ性を高めます。アダプティブトランスポートでは、サーバーの高スケーラビリティと帯域幅の使用効率が維持されます。アダプティブトランスポートを使用すると、ICA 仮想チャネルはネットワーク状況の変化に自動的に対応します。Enlightened Data Transport（EDT）と呼ばれる新しい Citrix プロトコルと TCP との間で、基になるプロトコルをインテリジェントに切り替えて、最適なパフォーマンスが実現されます。これにより、Thinwire ディスプレイリモート、ファイル転送（クライアントドライブマッピング）、印刷、マルチメディアリダイレクトなど、すべての ICA 仮想チャネルのデータスループットが向上します。同じ設定を LAN と WAN の両方の条件に適用できます。

［優先］に設定すると、EDT 経由のデータ転送がプライマリとして使用され、TCP にフォールバックします。

デフォルトでは、アダプティブトランスポートは無効（［オフ］）になっており、常に TCP が使用されます。

テスト目的で、［診断モード］に設定できます。このモードでは、EDT のみが使用され、TCP へのフォールバックは無効になります。



Citrix SD-WAN WAN 最適化との互換性

Citrix SD-WAN WAN 最適化（WANOP）は、URL ベースのビデオキャッシュを含むセッションを越えたトークン化圧縮（データ重複排除）を提供します。オフィスで 2 人以上のユーザーが同じクライアントが取得したビデオを見たり、同じファイルまたはドキュメントの大部分を転送または印刷したりする場合、WANOP によって大幅に帯域幅を削減できます。さらに、ブランチオフィスアプライアンス上で ICA データ削減および印刷ジョブ圧縮プロセスを実行することにより、VDA サーバーの CPU 負荷を軽減し、XenApp および XenDesktop サーバーでより高いスケーラビリティを実現します。

> 重要：
>
> TCP がデータ転送プロトコルとして使用される場合、Citrix WANOP は前の段落で説明した最適化をサポートします。ネットワーク接続で Citrix WANOP を使用する場合は、TCP を選択します。WANOP は、TCP フロー制御と輻輳制御を使用することにより、低速で中程度のパケット損失がある状況で EDT と同等の対話機能を提供できます。

要件および考慮事項

- XenApp および XenDesktop：バージョン 7.13 以降
- デスクトップ OS 用 VDA：バージョン 7.13 以降
- サーバー OS 用 VDA：バージョン 7.13 以降
- StoreFront：バージョン 3.9 以降
- Citrix Receiver for Windows：バージョン 4.7 以降
- Citrix Receiver for Mac：バージョン 12.5 以降
- Citrix Receiver for iOS：バージョン 7.2 以降
- Citrix Receiver for Linux：直接 VDA 接続のみの場合はバージョン 13.6、NetScaler Gateway を使用する DTLS サポート（または直接 VDA 接続用の DTLS）の場合は 13.7。

- Citrix Receiver for Android：直接 VDA 接続のみの場合はバージョン 3.12.3、NetScaler Gateway を使用する DTLS サポート（または直接 VDA 接続用の DTLS）の場合は 3.13。
- IPv4 VDA のみ。IPv6 および IPv6 と IPv4 の混在構成はサポートされません。
- NetScaler：バージョン 11.1-51.21 以降。NetScaler 構成について詳しくは、「Configuring NetScaler Gateway to support Advanced Transport」を参照してください。

構成

1. XenApp および XenDesktop をインストールします。
2. StoreFront をインストールします。
3. VDA（for Desktop OS または Server OS）をインストールします。
4. Citrix Receiver for Windows（Citrix Receiver for Mac または Citrix Receiver for iOS）をインストールします。
5. Studio で、ポリシー設定「HDX Adaptive Transport」を有効化します（デフォルトでは無効）。また、この機能を、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。
   - ポリシー設定を有効にするには、値を［優先］に設定し、［OK］をクリックします。
     - 優先。可能な場合、Adaptive transport over EDT が使用され、TCP にフォールバックします。
     - 診断モード。EDT が強制的にオンになり、TCP へのフォールバックは無効になります。この設定はトラブルシューティングでのみお勧めします。
     - オフ。TCP が強制的にオンになり、EDT が無効になります。
6. ［次へ］をクリックし、ウィザードの手順を完了します。
7. ユーザーが ICA セッションに再接続するときに新しいポリシーが有効になります。任意で **gpupdate /force** を実行してポリシー設定をサーバーにプルできますが、ユーザーはやはり ICA セッションを再接続する必要があります。
8. サポートされている Citrix Receiver からセッションを起動し、アダプティブトランスポートを使用して接続を確立します。
9. 外部アクセスをセキュリティで保護するために、NetScaler Unified Gateway 上で DTLS 暗号化を構成します。詳しくは、「Configuring NetScaler Gateway to support Advanced Transport」を参照してください。

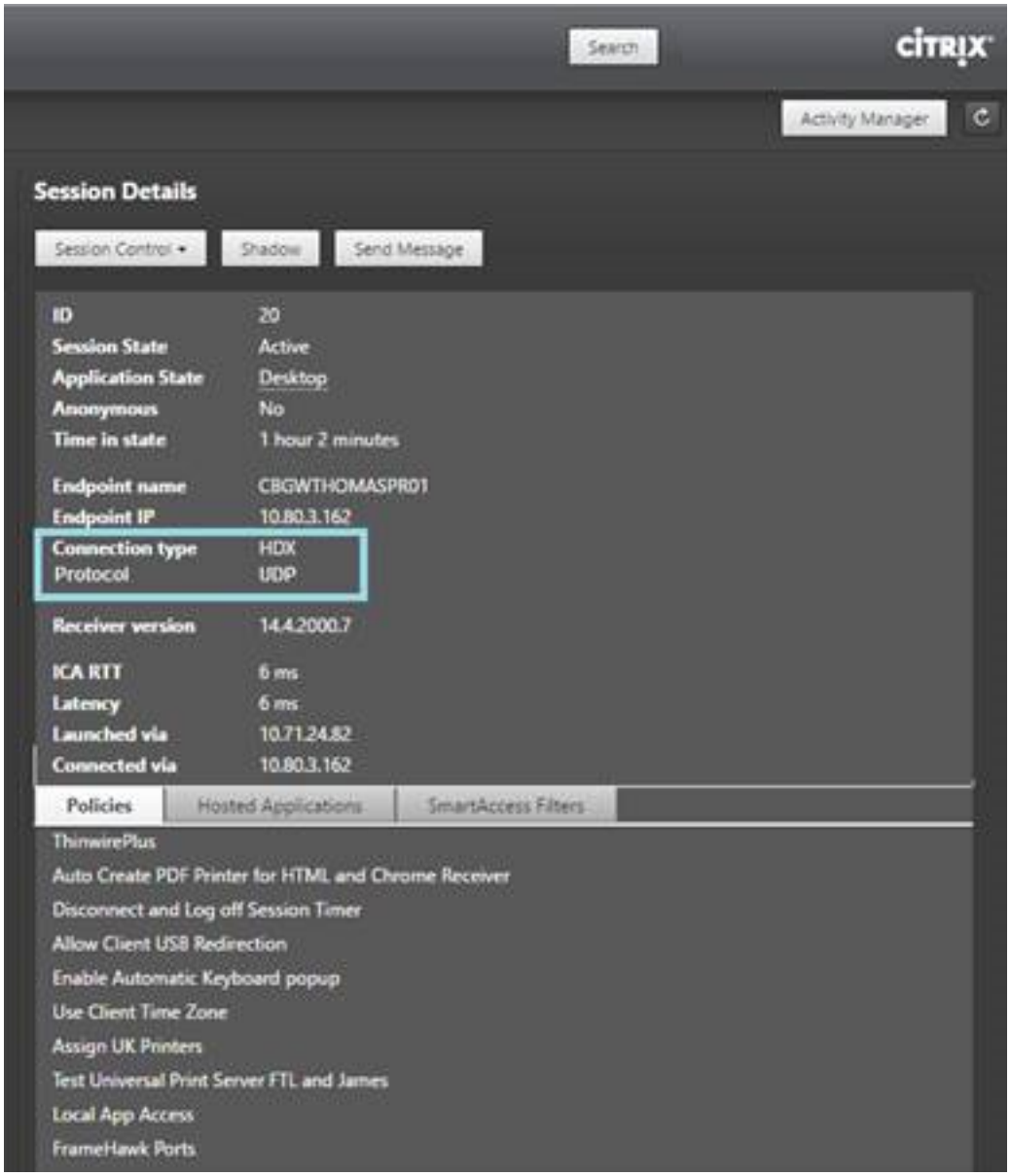
ポリシー設定の有効化を確認するには：

- netstat -a**を使用して、ICA ユーザーデータグラムプロトコル（UDP）サービスが VDA 上で有効であることを確認します。
- **Director**、または VDA で利用できる **CtxSession.exe** コマンドラインユーティリティを使用して、仮想チャネルが EDT 経由で実行されていることを確認します。

Director の使用例：

Director の ［セッション詳細］**>**［接続の種類］に、ポリシー設定が表示されます。［接続の種類］で ［**HDX**］を探します。［プロトコル］が ［**UDP**］の場合、EDT はこのセッションでアクティブです。［プロトコル］が ［**TCP**］の場合、セッションはフォールバックしているか、デフォルトのモードです。［接続の種類］が ［**RDP**］の場合、ICA は使

用されておらず、［プロトコル］は ［なし］です。詳しくは、「セッションの監視」を参照してください。



CtxSession.exe の例:

この例は、UDP 経由の EDT がアクティブなセッションを示しています。コマンドラインで「CtxSession.exe」と入力します。

C:\Program Files (x86)\Citrix\System32>CtxSession

セッション 2 のトランスポートプロトコル: UDP > CGP > ICA

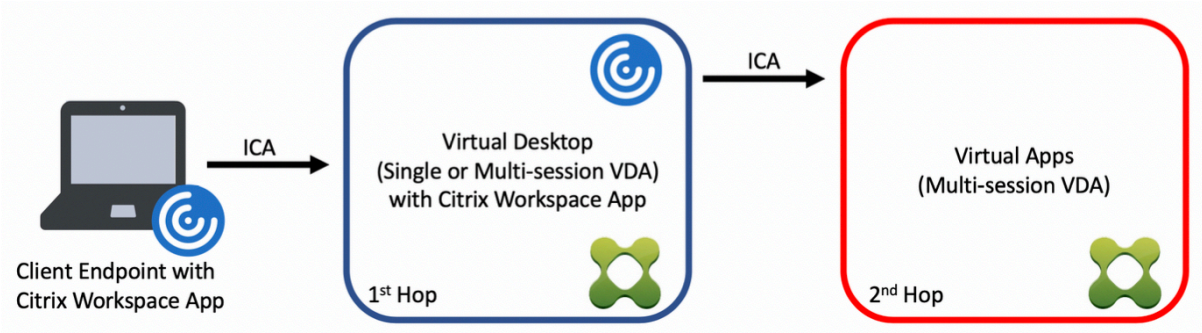
詳細な統計情報を参照するには、-v スイッチを使用します。

```
CtxSession -v
```


Citrix Virtual Apps and Desktops でのダブルホップ

August 24, 2021

Citrix クライアントセッションでは、「ダブルホップ」という用語は、Citrix Virtual Desktops セッション内で実行されている Citrix Virtual Apps セッションを指します。次の図は、ダブルホップを示しています。



ダブルホップのシナリオでは、シングルセッション OS VDA（VDI）またはマルチセッション OS VDA（公開デスクトップ）で実行されている Citrix Virtual Desktops にユーザーが接続すると、それが最初のホップと見なされます。仮想デスクトップに接続すると、ユーザーは Citrix Virtual Apps セッションを起動できます。これは 2 番目のホップと見なされます。

ダブルホップ展開モデルを使用して、さまざまなユースケースをサポートできます。Citrix Virtual Desktops 環境と Citrix Virtual Apps 環境が異なるエンティティによって管理されるケースはよくある一例です。この方法は、アプリケーションの互換性の問題を解決するのにも有効です。

システム要件

Citrix Cloud サービスを含むすべての Citrix Virtual Apps and Desktops エディションは、ダブルホップをサポートしています。

最初のホップでは、サポートされているバージョンのシングルセッションまたはマルチセッション OS VDA と Citrix Workspace アプリを使用する必要があります。2 番目のホップでは、サポートされているバージョンのマルチセッション OS VDA を使用する必要があります。サポートされているバージョンについては、製品マトリクスのページを参照してください。

最高のパフォーマンスと互換性を実現するために、使用中の VDA バージョンと同じバージョンまたは新しいバージョンの Citrix クライアントを使用することをお勧めします。

最初のホップに、Citrix Virtual Apps セッションと組み合わされたサードパーティ製（Citrix 以外）の仮想デスクトップソリューションが含まれる環境では、サポートは Citrix Virtual Apps 環境に制限されます。Citrix Workspace アプリの互換性、ハードウェアデバイスのリダイレクト、セッションのパフォーマンスなど、サードパーティ製の仮想デスクトップに関連する問題が発生した場合、シトリックスは限られた容量でテクニカルサポートを提供できます。トラブルシューティングの一環として、最初のホップの Citrix Virtual Desktops が必要になる場合があります。

ダブルホップでの **HDX** の展開に関する考慮事項

一般に、ダブルホップの各セッションは一意であり、クライアントサーバー機能は特定のホップに分離されます。このセクションには、Citrix 管理者による特別な配慮が必要な領域が含まれています。必要な HDX 機能を徹底的にテストし、特定の環境構成のユーザーエクスペリエンスとパフォーマンスが適切であることを確認することをお勧めします。

グラフィック

最初のホップと 2 番目のホップでは、デフォルトのグラフィック設定（選択的エンコーディング）を使用します。HDX 3D Proの場合、グラフィックアクセラレーションを必要とするすべてのアプリケーションは、VDA で利用可能な適切な GPU リソースを使用して、最初のホップでローカルで実行することを強くお勧めします。

遅延

エンドツーエンドの遅延は、全体的なユーザーエクスペリエンスに影響を与える可能性があります。最初のホップと 2 番目のホップの間に付加される遅延を考慮します。これは、ハードウェアデバイスのリダイレクトで特に重要です。

マルチメディア

オーディオおよびビデオコンテンツのサーバー側（セッション内）レンダリングは、最初のホップで最も効果を発揮します。2 番目のホップでのビデオ再生には、最初のホップでのデコードと再エンコードが必要なため、結果として帯域幅とハードウェアリソースの使用率が高まります。オーディオおよびビデオのコンテンツは、可能な限り最初のホップに限定する必要があります。

USB デバイスリダイレクト

HDX には、汎用リダイレクトモードと最適化されたリダイレクトモードがあり、さまざまな種類の USB デバイスをサポートしています。各ホップで使用するモードには特に注意し、次の表を参考にして最良の結果が得られるようにしてください。汎用リダイレクトモードと最適化されたリダイレクトモードについて詳しくは、「一般的 USB デバイス」を参照してください。

最初のホップ（VDI または公開されたデスクトップ）	2 番目のホップ（Virtual Apps）	サポートノート
最適化	最適化	推奨（デバイスサポートに基づく）。たとえば、USB 大容量記憶装置、TWAIN スキャナー、Web カメラ、オーディオなどです。
汎用	汎用	最適化されたオプションが使用できないデバイスの場合。

最初のホップ（VDI または公開されたデスクトップ）	2 番目のホップ（Virtual Apps）	サポートノート
汎用	最適化	技術的には可能ですが、デバイスサポートが使用可能な場合には、両方のホップで最適化されたモードを使用することをお勧めします。
最適化	汎用	未サポート

> 注:
>
> USB プロトコル固有のチャット性のために、ホップ全体でパフォーマンスが低下することがあります。機能と結果は、特定のデバイスおよびアプリケーションの要件によって異なります。検証テストは、デバイスリダイレクトのすべてのケースで強く推奨され、ダブルホップのシナリオでは特に重要です。

サポートの例外

ダブルホップセッションでは、以下を除くほとんどの HDX 機能をサポートしています:

- Web ブラウザーコンテンツのリダイレクト
- ローカルアプリアクセス
- RealTime Optimization Pack for Skype for Business
- Microsoft Teams の最適化

インストールと構成

August 24, 2021

個々の展開手順を開始する前に、参考記事を確認して、展開中に何が起こるか、何を指定する必要があるのかを前もって確認してください。

次の手順に従って、XenApp または XenDesktop を展開します。

準備

「インストールの準備」を確認し、必要なタスクをすべて完了します。

- コンセプト、機能、これまでのリリースとの差異、システム要件、およびデータベースに関する情報の参照先。
- コアコンポーネントのインストール先を決定する際の考慮事項。
- Active Directory の権限と要件。

- 利用できるインストーラー、ツール、およびインターフェイスに関する情報。

コアコンポーネントのインストール

Delivery Controller、Citrix Studio、Citrix Director、Citrix ライセンスサーバー、Citrix StoreFront をインストールします。詳しくは、「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

サイトの作成

コアコンポーネントのインストール後、Studio を起動すると、操作は自動的にサイトの作成へ誘導されます。

1 つまたは複数の **Virtual Delivery Agent**（**VDA**）のインストール

Windows オペレーティングシステムが実行されているマシンに VDA をインストールします。このとき、マスターイメージにインストールすることも、各マシン上に直接インストールすることもできます。「VDA のインストール」または「コマンドラインを使ったインストール」を参照してください。Active Directory 経由で VDA をインストールする場合のスクリプト例が用意されています。

Linux オペレーティングシステムを使用しているマシンでは、「Linux Virtual Delivery Agent」のガイダンスに従ってください。

リモート PC アクセス機能を使用する場合は、オフィスにある各ユーザーのコンピューター上に VDA for Desktop OS をインストールします。コア VDA サービスのみが必要な場合は、スタンドアロンの VDAWorkstationCoreSetup.exe インストーラーと、既存の電子ソフトウェア配信（ESD）の方法を使用します。（利用できる VDA のインストーラーに関する完全な情報については、「インストールの準備」を参照してください。）

その他のオプションコンポーネントのインストール

Citrix Universal Print Server の使用を計画している場合は、そのサーバーコンポーネントをプリントサーバーにインストールします。「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

StoreFront での認証オプション（SAML アサーションなど）の使用を許可するには、Citrix Federated 認証サービスをインストールします。

エンドユーザーが自身のユーザーアカウントをより詳細に制御できるようにするには、セルフサービスパスワードリセットをインストールします。詳しくは、「セルフサービスパスワードリセット」ドキュメントを参照してください。

必要に応じて、XenApp/XenDesktop 展開に Citrix コンポーネントをさらに統合します。

- Provisioning Services は XenApp および XenDesktop のオプションコンポーネントで、マスターイメージをターゲットデバイスにストリーム配信してマシンをプロビジョニングします。

- Citrix NetScaler Gateway はアプリケーションアクセスのセキュリティを保護するソリューションで、詳細なアプリケーションレベルのポリシーと操作の制御機能を管理者に提供し、アプリケーションとデータへのアクセスのセキュリティを保護します。
- Citrix NetScaler SD-WAN は、WAN 接続のパフォーマンスを最適化するための一連のアプライアンスです。

インストールのガイダンスについては、これらのコンポーネント、機能、およびテクノロジに関するドキュメントを参照してください。

マシンカタログの作成

Studio でサイトの作成が完了すると、マシンカタログの作成へ誘導されます。

カタログには、物理マシンまたは仮想マシン（VM）のどちらでも使用できます。仮想マシンはマスターイメージから作成できます。VM の提供に、ハイパーバイザーまたはクラウドサービスを使用している場合は、まず、そのホストにマスターイメージを作成します。その後、カタログ作成時に、このイメージを指定します。これは VM を作成するときに使用されます。

デリバリーグループの作成

Studio で 1 つ目のマシンカタログの作成が完了すると、デリバリーグループの作成へ誘導されます。

デリバリーグループは、選択されたカタログにあるマシンにアクセスできるユーザーと、そのユーザーが利用可能なアプリケーションを指定します。

アプリケーショングループの作成（オプション）

デリバリーグループの作成後、オプションでアプリケーショングループを作成できます。さまざまなデリバリーグループで共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットで使用されるアプリケーションについて、アプリケーショングループを作成できます。

インストールの準備

October 22, 2021

XenApp および XenDesktop の展開は、次のコンポーネントのインストールから始まります。このプロセスでは、アプリケーションとデスクトップをファイアウォール内のユーザーに配信する準備をします。

- 1 つまたは複数の Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront

- Citrix ライセンスサーバー
- 1 つまたは複数の Citrix Virtual Delivery Agent（VDA）
- オプションのコンポーネントやテクノロジ（たとえば、Universal Print Server、フェデレーション認証サービス、およびセルフサービスパスワードリセット）

ファイアウォール外のユーザーについては、NetScaler などの追加コンポーネントをインストールして構成します。StoreFront で NetScaler を使用する方法については、「XenApp および XenDesktop の NetScaler Gateway との統合」を参照してください。

コンポーネントをインストールできるようにするには

XenApp および XenDesktop ISO に含まれる全製品インストーラーを使用すると、多くのコンポーネントとテクノロジを展開できます。VDA は、スタンドアロン VDA インストーラーを使用してインストールできます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。「インストーラー」を参照してください。

製品 ISO には、Active Directory のマシンの VDA をインストール、アップグレード、または削除するサンプルスクリプトも収録されています。また、これらのスクリプトを使って Machine Creation Services（MCS）および Provisioning Services（PVS）のマスターイメージを管理することもできます。詳しくは、「スクリプトを使用した VDA のインストール」を参照してください。

Citrix Smart Tools ではこれらのインストーラーを使用せずに、ブループリントを使用して XenApp および XenDesktop の展開環境を自動で作成します。詳しくは、Smart Tools の製品マニュアルを参照してください。

インストール前に確認する情報

- 「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。
- 7.x での変更点：XenApp 6.x または XenDesktop 5.6 展開環境から最新のバージョンに移行する場合。
- セキュリティ：展開環境について計画する場合。
- 既知の問題：このバージョンで起きる可能性がある問題。
- データベース：システムデータベースおよびこれらの設定方法について理解を深めてください。Controller のインストール時に、サイトデータベース用に SQL Server Express をインストールできます。コアコンポーネントをインストールした後のサイト作成時に、データベース情報のほとんどを設定します。
- リモート PC アクセス：ユーザーがオフィスの物理マシンにリモートでアクセスできる環境を展開している場合。
- 接続とリソース：ハイパーバイザーまたはクラウドサービスを使用してアプリケーションやデスクトップの VM マシンをホストまたはプロビジョニングしている場合。（コアコンポーネントをインストールした後の）サイト作成時に、最初の接続を構成することができます。仮想化環境はそれより前に、いつでも設定できます。
- Microsoft System Center Configuration Manager：ConfigMgr を使用してアプリケーションおよびデスクトップへのアクセスを管理しているか、リモート PC アクセスとともに Wake on LAN 機能を使用している場合。

コンポーネントのインストール先

サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。記載されているものを除いて、コンポーネントの必須条件は自動的にインストールされます。サポートされるプラットフォームと前提条件については、Citrix StoreFront および Citrix ライセンスサーバーのドキュメントを参照してください。

コアコンポーネントは、同じサーバー上にインストールしたり別のサーバー上にインストールしたりできます。

- 1 つのサーバー上にすべてのコアコンポーネントをインストールすれば、評価展開、テスト展開、または小規模実稼働展開に使用できます。
- 将来の拡張に対応するには、異なるサーバーにコンポーネントをインストールすることを検討してください。たとえば、Controller をインストールしたサーバーとは別のマシンに Studio をインストールすると、サイトをリモートで管理できます。
- 大部分の実稼働展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

Delivery Controller と VDA for Server OS を同一サーバー上にインストールできます。インストーラーを起動して目的の Delivery Controller（およびマシンにインストールするその他のコンポーネント）を選択します。次に、もう一度インストーラーを起動して Virtual Delivery Agent for Server OS を選択します。

各オペレーティングシステムを最新の状態にアップデートしておく必要があります。たとえば、Windows 更新プログラム KB2919355 がインストールされていない場合、Windows Server 2012 R2 への Controller のインストールおよび Windows 8.1 または Windows Server 2012 R2 への VDA のインストールは失敗します。

すべてのマシンのシステムクロックを同期しておく必要があります。この同期は、Kerberos でマシン間の通信を保護するために必要です。

Windows 10 マシンでの最適化ガイダンスは、CTX216252にあります。

コンポーネントのインストールが不適切な場所:

- Active Directory ドメインコントローラーには一切コンポーネントをインストールしないでください。
- SQL Server クラスター化インストール、SQL Server ミラー化インストール、または Hyper-V を実行しているサーバーにおけるノード上への Controller のインストールはサポートされていません。
- XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2 またはそれ以前のバージョンの XenApp が動作するサーバーには Studio をインストールしないでください。

Active Directory の権限と要件

コンポーネントをインストールするマシンのドメインユーザーおよびローカル管理者である必要があります。

スタンドアロン VDA インストーラーを使用するには、管理者権限を持っているか、［管理者として実行］を使用する必要があります。

インストールを開始する前に、Active Directory ドメインを設定してください。

- サポートされる Active Directory の機能レベルの一覧は「システム要件」に記載されています。詳細は「Active Directory」に記載されています。

- 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に XenApp または XenDesktop コンポーネントをインストールしないでください。
- Studio で組織単位名を指定するときは、スラッシュ（/）を使用しないでください。

Citrix ライセンスサーバーのインストールに使用した Windows ユーザーアカウントが、そのライセンスサーバーのすべての管理タスクの実行権限を持つ委任管理者として自動的に設定されます。

さらに、以下の情報を参照してください：

- セキュリティに関する推奨事項
- 委任管理
- Active Directory の構成手順に関する Microsoft 社のドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

任意のコンポーネントのインストール時

通常、コンポーネントの前提条件が存在していない場合は、インストーラーによってインストールされます。前提条件によっては、マシンの再起動が必要なものがあります。

インストールの前、最中、および後に作成するオブジェクトには、重複しない名前を指定してください。こうしたオブジェクトには、ネットワーク、グループ、カタログ、リソースなどがあります。

正しくインストールできないコンポーネントがあった場合は、インストールが停止してエラーメッセージが表示されます。この時点でインストール済みのコンポーネントは保持されるため、再インストールする必要はありません。

コンポーネントをインストール（またはアップグレード）すると、分析情報が自動的に収集されます。デフォルトでは、インストールの完了時に、そのデータが Citrix へ自動的にアップロードされます。また、コンポーネントをインストールすると、自動的に Citrix カスタマーエクスペリエンス向上プログラム（CEIP）に登録され、匿名データがアップロードされます。インストール中に、メンテナンスやトラブルシューティングのために診断情報を収集するほかの Citrix プログラム（Smart Tools など）に参加することもできます。これらのプログラムについて詳しくは、「Citrix Insight Services」を参照してください。

VDA インストール時

Citrix Receiver for Windows は、VDAWorkstationCoreSetup.exe インストーラーを使用する場合を除き、VDA をインストールするときにデフォルトで含まれます。Citrix Receiver はインストールから除外できます。Citrix Receiver および他の Citrix Receiver は、管理者またはユーザーが Citrix Web サイトからダウンロードできます。また、StoreFront サーバーでこれらの Citrix Receiver を公開することもできます。「Citrix Receiver インストールファイルをサーバーから入手できるようにする」、または使用している StoreFront バージョンの該当するコンテンツを参照してください。

サポートされる Windows サーバーでは、印刷スプーラーサービスがデフォルトで有効になります。このサービスを無効にすると、Windows サーバー OS に対して VDA を正常にインストールできなくなるため、このサービスが有効であることを確認してから VDA をインストールしてください。

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

VDA をインストールすると、Direct Access Users（直接アクセスユーザー）という名前の新しいローカルユーザーグループが自動的に作成されます。VDA for Desktop OS では、このグループは RDP 接続のみに適用されます。VDA for Server OS では、このグループは ICA 接続と RDP 接続に適用されます。

VDA には、通信を行う Controller の有効なアドレスが保持されている必要があります。保持されていない場合は、セッションを確立することができません。Controller のアドレスは、VDA のインストール時に指定することも、後で指定することもできます。ただし、必ず指定しなければならないことを覚えておいてください。

VDA インストール時およびその後の再起動

VDA のインストールプロセスの最後にマシンを再起動する必要があります。デフォルトでは、再起動は自動で行われます。

VDA インストール中の再起動の回数を最小限に抑えるには:

- VDA のインストールが開始される前に.NET Framework バージョンがインストールされていることを確認してください。
- Windows サーバー OS マシンでは、RDS の役割サービスをインストールして有効にしてから VDA をインストールしてください。

VDA インストール前にこれらの前提条件をインストールしない場合:

- グラフィカルインターフェイスを使用した場合、またはコマンドラインインターフェイスを/noreboot オプションなしで使用した場合、前提条件のインストール後にマシンが自動で再起動します。
- コマンドラインインターフェイスで/noreboot オプションを使用した場合、手動で再起動を開始する必要があります。

再起動するたびに、もう一度インストーラーまたはコマンドを実行して VDA インストールを続行します。

インストーラー

全製品インストーラー

XenApp および XenDesktop ISO で提供される全製品インストーラーを使用して、以下のことができます。

- XenApp および XenDesktop コアコンポーネント（Delivery Controller、Studio、Director、StoreFront、License Server）のインストール、アップグレード、または削除
- サーバーまたはデスクトップオペレーティングシステム用の Windows VDA のインストールまたはアップグレード

- プリントサーバーへのユニバーサルプリントサーバー Ups Server コンポーネントのインストール
- フェデレーション認証サービスのインストール
- セルフサービスパスワードリセットサービスのインストール

(Web サイト開発などで) 1 人のユーザー用に Server OS からデスクトップを配信するには、全製品インストーラーのコマンドラインインターフェイスを使用します。詳しくは、「サーバー VDI」を参照してください。

スタンドアロン **VDA** インストーラー

スタンドアロン VDA インストーラーは Citrix のダウンロードページから入手できます。スタンドアロン VDA インストーラーは、全製品 ISO よりはるかにサイズが小さいです。これらのインストーラーを使用すると、以下のような展開環境に簡単に対応することができます:

- ステージングするかまたはローカルにコピーした電子ソフトウェア配信 (ESD) パッケージを使用する環境
- 物理マシンのある環境
- リモートオフィスのある環境

デフォルトでは、自己抽出型のスタンドアロン VDA 内のファイルは Temp フォルダーに抽出されます。Temp フォルダーに抽出される場合は、全製品インストーラーを使用する場合よりも、マシンに多くのディスクスペースが必要です。ただし、インストールの完了後、Temp フォルダーに抽出されたファイルは自動的に削除されます。もしくは、絶対パスと/extract コマンドを使用できます。

3 つのスタンドアロン VDA インストーラーを、ダウンロードで入手できます。

VDAServerSetup.exe

VDA for Server OS をインストールします。全製品インストーラーで利用できる VDA for Server OS オプションをすべてサポートしています。

VDAWorkstationSetup.exe

VDA for Desktop OS をインストールします。全製品インストーラーで利用できる VDA for Desktop OS オプションをすべてサポートしています。

VDAWorkstationCoreSetup.exe

リモート PC アクセス展開またはコア VDI インストールに最適化された VDA for Desktop OS をインストールします。リモート PC アクセスマシンでは物理マシンを使用します。コア VDI インストールとは、マスターイメージには使用されない VM のことを指します。コア VDI インストールでは、こうした展開環境への VDA 接続に必要なコアサービスのみがインストールされます。このため、全製品インストーラーまたは VDAWorkstationSetup インストーラーで有効であるオプションのサブセットだけがサポートされます。

このインストーラーは、次のものに使用されるコンポーネントをインストールしないか、含みません:

- App-V。
- Profile Management。インストールから Citrix Profile Management を除外すると、Citrix Director の表示に影響があります。詳しくは、「VDA のインストール」を参照してください。
- Machine Identity Service
- Personal vDisk または AppDisk。

VDAWorkstationCoreSetup.exe インストーラーは、Citrix Receiver for Windows をインストールしないか、含みません。

VDAWorkstationCoreSetup.exe を使用することは、全製品または **VDAWorkstationSetup.exe** インストーラーを使用して Desktop OS VDA をインストールすることと同等であり、次のどちらかでインストールします。

- グラフィカルインターフェイス：［環境］ページで［リモート PC アクセス］オプションを選択し、［コンポーネント］ページで［Citrix Receiver］チェックボックスをオフにする。
- コマンドラインインターフェイス：/remotepc オプションおよび/components vda オプションを指定する。
- コマンドラインインターフェイス：/components vda および/exclude “Citrix Personalization for App-V - VDA” “Personal vDisk” “Machine Identity Service” “Citrix User Profile Manager” “Citrix User Profile Manager WMI Plugin” を指定する。

全製品インストーラーを実行すれば、省略したコンポーネントおよび機能を後からインストールできます。この操作では、不足しているコンポーネントがすべてインストールされます。

Microsoft Azure Resource Manager 仮想化環境

August 24, 2021

XenApp または XenDesktop 環境で Microsoft Azure Resource Manager を使用して仮想マシンをプロビジョニングする場合は、このガイダンスに従ってください。

XenApp または XenDesktop を構成して、XenApp または XenDesktop サイトを作成したとき（接続の作成も含みます）または（サイトを作成してから）後でホスト接続を作成したときにリソースが Azure Resource Manager でプロビジョニングされるようにすることができます。

これを行うには、以下に関する知識が必要です。

- Azure Active Directory：https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- 同意フレームワーク：https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- サービスプリンシパル：https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

Machine Creation Services を使用している場合、Azure Disk Encryption はサポートされません。

このバージョンの XenApp および XenDesktop は、Azure アンマネージドディスクストレージシステムのみをサポートしています。デフォルトでは、Azure はマネージドディスクストレージシステムを使用します。管理対象および非管理対象の Azure ストレージソリューションについて詳しくは、「Azure Managed Disks」を参照してください。

Azure Resource Manager への接続の作成

サイトまたは接続を作成するウィザードのすべてのページについて詳しくは、「サイトの作成」と「接続とリソース」を参照してください。以下の情報は、Azure Resource Manager の接続に固有の詳細のみを扱っています。

Azure Resource Manager へのホスト接続を確立するには、次の 2 通りの方法があります:

- Azure Resource Manager を認証してサービスプリンシパルを作成する。
- 以前作成されたサービスプリンシパルからの詳細を使って Azure Resource Manager に接続する。

Azure Resource Manager を認証してサービスプリンシパルを作成する

始める前に、以下の項目について確認してください。

- サブスクリプションの Azure Active Directory テナントにユーザーアカウントがあること。
- Azure AD のユーザーアカウントが、リソースのプロビジョニングに使用する Azure サブスクリプションの共同管理者でもあること。

サイトのセットアップまたは接続およびリソースの追加ウィザードで以下を行います。

1. [接続] ページで、接続の種類として [**Microsoft Azure**] を選択し、Azure 環境を選択します。
2. [接続の詳細] ページで、Azure サブスクリプション ID と接続の名前を入力します。接続名は 1〜64 文字にし、空白スペースのみにしたり記号（\/;:#.*?=<>|[]{}"'()'）を含めたりすることはできません。サブスクリプション ID および接続名を入力すると、[新規作成] ボタンが有効になります。
3. Azure Active Directory アカウントのユーザー名とパスワードを入力します。
4. [サインイン] をクリックします。
5. [承認] をクリックして一覧表示されている権限を XenApp または XenDesktop に付与します。XenApp または XenDesktop によって、指定されたユーザーの代わりに Azure Resource Manager リソースを管理することを許可するサービスプリンシパルが作成されます。
6. [承認] をクリックすると、Studio の [接続] ページに戻ります。Azure の認証が完了すると、[新規作成] および [既存を使用] ボタンが [接続済み] に置き換わり、Azure サブスクリプションへの正常な接続を示す緑色のチェックマークが表示されます。
7. 仮想マシンの作成にどのツールを使用するかを指定し、[次へ] をクリックします。(Azure の認証が完了し、必要な権限の付与を承認しない限り、ウィザードのこのページより先に進むことはできません)。

リソースには領域とネットワークが含まれます。

- [リージョン] ページで領域を選択します。
- [ネットワーク] ページで以下の設定を行います。

- 1～64 文字のリソース名を入力して、Studio で領域とネットワークの組み合わせを特定できるようにします。リソース名を空白スペースのみにすることはできず、記号（\/;:#.*?=<>|[]{}”’()’）を含めることもできません。
- 仮想ネットワークとリソースグループのペアを選択します（複数の仮想ネットワークを同じ名前にすることが可能なため、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります）。前のページで仮想ネットワークのない領域を選択した場合は、前のページに戻って仮想ネットワークのある領域を選択する必要があります。

ウィザードを完了します。

以前作成されたサービスプリンシパルからの詳細を使って **Azure Resource Manager** に接続する

手動でサービスプリンシパルを作成するには、Azure Resource Manager サブスクリプションに接続して、後述の PowerShell コマンドレットを使用します。

前提条件：

- $SubscriptionId：VDA をプロビジョニングするサブスクリプションの Azure Resource Manager SubscriptionID。
- $AADUser：サブスクリプションの AD テナントに対する Azure AD ユーザーアカウント。
- $AADUser をサブスクリプションの共同管理者にしてください。
- $ApplicationName：Azure AD 内で作成されるアプリケーションの名前。
- $ApplicationPassword：アプリケーションのパスワード。このパスワードは、ホスト接続を作成するときのアプリケーションシークレットとして使用します。

サービスプリンシパルを作成するには、次の手順に従ってください。

手順 **1**：Azure Resource Manager サブスクリプションに接続します。

```
1 Login-AzureRmAccount.
```

手順 **2**：サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

```
1 Select-AzureRmSubscription -SubscriptionID $SubscriptionId;
```

手順 **3**：AD テナントでアプリケーションを作成します。

```
1 $AzureADApplication = New-AzureRmADApplication -DisplayName
    $ApplicationName -HomePage "https://localhost/$ApplicationName" -
    IdentifierUris https://$ApplicationName -Password
    $ApplicationPassword
```

手順 **4**：サービスプリンシパルを作成します。

```
1 New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
    ApplicationId
```


手順 **5**：サービスプリンシパルに役割を割り当てます。

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $AzureADApplication.ApplicationId  - scope /
    subscriptions/$SubscriptionId
```

手順 **6**：PowerShell コンソールの出力ウィンドウから、ApplicationId をメモします。この ID は、ホスト接続を作成するときに使用します。

サイトのセットアップまたは接続およびリソースの追加ウィザードで以下を行います。

1. ［接続］ページで、接続の種類として ［**Microsoft Azure**］を選択し、Azure 環境を選択します。
2. ［接続の詳細］ページで、Azure サブスクリプション ID と接続の名前を入力します。接続名は 1～64 文字にし、空白スペースのみにしたり記号（\/;:#.*?=<>|[]{}”’()’）を含めたりすることはできません。
3. ［既存を使用］をクリックします。サブスクリプション ID、サブスクリプション名、認証 URL、管理 URL、ストレージのサフィックス、Active Directory ID またはテナント ID、アプリケーション ID、および既存のサービスプリンシパルのアプリケーションシークレット。詳細を入力すると、［**OK**］ボタンが有効になります。［**OK**］をクリックします。
4. 仮想マシンの作成にどのツールを使用するかを指定し、［次へ］をクリックします。入力したサービスプリンシパルの詳細は、Azure サブスクリプションへの接続に使用されます（［既存を使用］オプションで有効な詳細を入力しない限り、ウィザードの次のページに進めません）。

リソースには領域とネットワークが含まれます。

- ［リージョン］ページで領域を選択します。
- ［ネットワーク］ページで以下の設定を行います：
  - 1～64 文字のリソース名を入力して、Studio で領域とネットワークの組み合わせを特定できるようにします。リソース名を空白スペースのみにすることはできず、記号（\/;:#.*?=<>|[]{}”’()’）を含めることもできません。
  - 仮想ネットワークとリソースグループのペアを選択します（複数の仮想ネットワークを同じ名前にすることが可能なため、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります）。前のページで仮想ネットワークのない領域を選択した場合は、前のページに戻って仮想ネットワークのある領域を選択する必要があります。

ウィザードを完了します。

Azure Resource Manager マスターイメージを使用して、マシンカタログを作成する

以下の情報は、「マシンカタログの作成」のガイダンスを補完するものであり、

マスターイメージは、マシンカタログの仮想マシンの作成に使用されることになるテンプレートです。マシンカタログを作成する前に、Azure Resource Manager でマスターイメージを作成します。マスターイメージの一般的な情報については、「マシンカタログの作成」を参照してください。

Studio でのマシンカタログを作成する場合は、以下を確認してください。

- ［オペレーティングシステム］ページと［マシン管理］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
- ［マスターイメージ］ページで、リソースグループを選択してからコンテナ内を移動（ドリルダウン）して、マスターイメージとして使用する Azure VHD に移動します。VHD には Citrix VDA がインストールされている必要があります。仮想マシンに VHD が接続されている場合、仮想マシンを停止する必要があります。
- ［ストレージとライセンスの種類］ページは、Azure Resource Manager マスターイメージを使用しているときのみ表示されます。

  ストレージの種類（Standard または Premium）を選択します。ストレージの種類によって、ウィザードの［仮想マシン］ページで提供されるマシンのサイズが変わります。これらのストレージの種類はどちらも、単一のデータセンター内でデータの複数の同期コピーを作成します。Azure のストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください：

  https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction

  https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types#premium-ssd

  https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

  既存のオンプレミスの Windows Server ライセンスを使用するかを選択します。既存のオンプレミスの Windows Server イメージを使用する場合にそのように選択すると、Azure Hybrid Use Benefits（HUB）が利用されます。詳しくは、https://azure.microsoft.com/pricing/hybrid-use-benefit/を参照してください。

  HUB を使用すると、Azure ギャラリーから Windows Server ライセンスを追加する価格が不要になるため、Azure での仮想マシン実行のコストを基本計算料金のみに抑えられます。HUB を使用するためのオンプレミスの Windows Servers イメージを Azure に用意する必要があります。Azure ギャラリーのイメージはサポートされません。オンプレミスの Windows Client ライセンスは、現在サポートされていません。「https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/」を参照してください。

  プロビジョニングされた仮想マシンが HUB を正常に利用しているかどうか確認するには、PowerShell コマンド

  ```
  Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
  ```

  を実行し、ライセンスの種類が`Windows_Server`であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.jsonを参照してください。
- ［仮想マシン］ページで、作成する仮想マシンの数を指定します。少なくとも 1 つは指定してください。マシンのサイズを選択します。マシンカタログを作成した後で、マシンのサイズを変更することはできません。後で他のサイズに変更したくなった場合は、カタログを削除してから、同じマスターイメージを使用したカタログを作成し、希望のマシンサイズを指定します。

仮想マシンの名前に、ASCII 以外の文字や特殊文字を含めることはできません。

- ［ネットワークカード］ページ、［コンピューターアカウント］ページ、および［概要］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

Microsoft System Center Virtual Machine Manager 仮想化環境

August 24, 2021

Hyper-V と Microsoft System Center Virtual Machine Manager（VMM）を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

このリリースは、「システム要件」に記載された VMM バージョンをサポートします。

Provisioning Services および Machine Creation Services を使用して、次のものをプロビジョニングできます:

- 第 1 世代デスクトップまたはサーバー OS の VM
- 第 2 世代 Windows Server 2012 R2、Windows Server 2016、Windows 10 VM（Secure Boot あり、またはなし）

VMM 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、https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610649(v=sc.12)?redirectedfrom=MSDNを参照してください。VMM コンソールの要件については、https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610640(v=sc.12)?redirectedfrom=MSDN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

> 重要：
>
> 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。

1. ハイパーバイザーをインストールして構成します。
   a) サーバー上に Microsoft Hyper-V Server および VMM をインストールします。
   b) 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。コンソールのバージョンは管理サーバーと同じバージョンにする必要があります。古いコンソールを管理サーバーに接続することはできますが、バージョンが異なる場合、VDA のプロビジョニングは失敗します。
   c) 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 VM を作成します。
   a) 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。
   b) 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。
   a) ホストの種類として［Microsoft 仮想化］を選択します。
   b) 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。
   c) 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。

d) ［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, $vhdastext)
  $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 = $ims.CreateVirtualHardDisk($vhdastext);
$result
```

- **ID** ディスクのアップロード - HCL では、ID ディスクを SMB ストレージに直接アップロードすることはできません。そのため、Hyper-V マシンが ID ディスクをストレージにアップロードしてコピーする必要があります。Hyper-V マシンは 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 - アップロードの場合と同様に、ID ディスクが Hyper-V マシンから HCL に渡されます。次の処理により、Hyper-V サーバー上に VMM ユーザー権限のみを持つフォルダーが作成されます（存在しない場合）。

  1. PowerShell V3 リモートセッションで実行される PowerShell スクリプトにより、Hyper-V マシンが SMB ストレージからローカルの Hyper-V ストレージに ID ディスクをコピーします。
  2. HCL が Hyper-V マシンの管理者共有から ID ディスクをメモリ内に読み取ります。
  3. HCL が管理者共有からファイルを削除します。

- **Personal vDisk** の作成 - 管理者が Personal vDisk マシンカタログで仮想マシンを作成する場合、空のディスク（Personal vDisk）を作成する必要があります。

  空のディスクを作成する呼び出しでは、ストレージへの直接アクセスが不要です。メインまたはオペレーティングシステムディスクとは異なるストレージ上に Personal vDisk がある場合は、リモート PowerShell を使って作成元の仮想マシンと同じ名前のディレクトリに Personal vDisk を作成します。CSV または LocalStorage に対しては、リモート PowerShell を使用しないでください。空のディスクを作成する前にディレクトリを作成しておくと、VMM コマンドエラーを避けることができます。

  Hyper-V マシンから、ストレージ上で mkdir を実行します。

Microsoft System Center Configuration Manager 環境

August 24, 2021

Microsoft System Center Configuration Manager（Configuration Manager）で物理デバイス上のアプリケーションやデスクトップへのアクセスを管理しているサイトでは、Configuration Manager の管理機能を XenApp や XenDesktop 環境まで拡張できます。以下の統合オプションを使用できます。

- **Citrix Connector 7.5 for Configuration Manager 2012** - Citrix Connector により、Configuration Manager と XenApp/XenDesktop が連係して動作するようになります。Connector を使用すると、Configuration Manager による物理環境と XenApp/XenDesktop による仮想環境の両方の保守・管理操作を統一させることができます。Connector について詳しくは、「Citrix Connector 7.5 for System Center Configuration Manager 2012」を参照してください。
- **Configuration Manager** のウェイクアッププロキシ機能 - リモート PC アクセスの Wake on LAN 機能を使用するには Configuration Manager が必要です。詳しくは、後述の説明を参照してください。
- **XenApp** および **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 では仮想デスクトップを管理するためのプロパティを利用できます。

Configuration Manager に表示されるプロパティのブール値は、true と false ではなく 1 と 0 で表示されることがあります。

これらのプロパティは、Root\Citrix\DesktopInformation 名前空間の Citrix_virtualDesktopInfo クラスで使用できます。これらのプロパティの名前は、Windows Management Instrumentation（WMI）プロバイダーでのものです。

プロパティ	説明
AssignmentType	IsAssigned の値を設定します。有効な値：ClientIP、ClientName、None、User（*IsAssigned* を True に設定）
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。

プロパティ	説明
HostIdentifier	サイト名です。BrokerSiteName と同じ値を返します。
IsAssigned	デスクトップを各ユーザーに割り当てる場合は True、ランダムデスクトップの場合は False を設定します。
IsMasterImage	マスターイメージかどうかを指定します。たとえば、すべてのマシンがクリーンな状態で起動するように、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。有効な値：マスターイメージとして使用される仮想マシンでは **True** になります（この値は、選択オプションに基づいてインストール時に設定されます）。マスターイメージからプロビジョニングされる仮想マシンでは **Cleared** になります。
IsVirtualMachine	仮想マシンでは true、物理マシンでは false になります。
OSChangesPersist	再起動時にデスクトップのオペレーティングシステムイメージをクリーンな状態にリセットする場合は false、リセットしない場合は true になります。
PersistentDataLocation	Configuration Manager が永続データを格納する場所です。ユーザーはアクセスできません。
PersonalvDiskDriveLetter	デスクトップで Personal vDisk を使用する場合に、その Personal vDisk に割り当てるドライブ文字です。
BrokerSiteName、DesktopCatalogName、DesktopGroupName、HostIdentifier	デスクトップのコントローラーへの登録時に設定されるため、未登録のデスクトップでは Null になります。

これらのプロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager のリソースエクスプローラーを使用します。これらのインスタンスでは、名前にスペースが含まれたり、プロパティ名とわずかに違ったものになったりすることがあります。たとえば **BrokerSiteName** は、Broker Site Name と表示されることがあります。

- Configuration Manager を構成して Citrix VDA から Citrix WMI プロパティを収集する。
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する。
- Citrix WMI プロパティに基づいてグローバル条件を作成する。
- グローバル条件を使用してアプリケーションの展開の種類の要件を定義する。

また、Microsoft クラスの CCM_DesktopMachine の Microsoft プロパティを Root\ccm_vdi 名前空間で使用す

ることもできます。詳しくは、Microsoft 社のドキュメントを参照してください。

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。

- 組織内で ConfigMgr 2012、2012 R2、または 2016 を構成します。リモート PC アクセス用のすべてのマシンに ConfigMgr クライアントを展開し、スケジュールされている SCCM インベントリサイクルが実行されるのを待ちます（必要に応じて、手動で強制的に実行することもできます）。Studio で ConfigMgr 接続を構成するときのアクセス資格情報には、セキュリティスコープにコレクションが含まれており、リモートツールオペレーターロールが付与されている必要があります。
- Intel 社の Active Management Technology（AMT）を使用する場合。
  - PC で AMT 3.2.1 以降がサポートされている必要があります。
  - 適切な資格情報およびプロビジョニングプロセスを使用して、PC で AMT が使用されるようにプロビジョニングします。
  - ConfigMgr 2012 と 2012 R2 のみを使用できます。ConfigMgr 2016 は使用できません。
- ConfigMgr のウェイクアッププロキシやマジックパケットを使用する場合:
  - 各 PC の BIOS 設定で、Wake on LAN 機能を有効にします。
  - ウェイクアッププロキシの場合は、ConfigMgr でウェイクアッププロキシを有効にします。リモート PC アクセスの Wake on LAN 機能を使用する PC が属する各サブネットで、センチネルマシンとして動作可能なものが 3 台以上あることを確認します。
  - マジックパケットの場合は、サブネット宛てのブロードキャストまたはユニキャストを使用して、ネットワーク経路およびファイアウォールでパケットの転送がブロックされないようにします。

社内 PC 上に VDA をインストールしたら、Studio でリモート PC アクセス展開を作成するときに電源管理機能を有効または無効にします。

- 電源管理機能を有効にする場合は、接続の詳細として ConfigMgr のアドレス、アクセス資格情報、および名前を指定します。
- 電源管理機能を無効にした場合でも、電源管理（Configuration Manager）接続を後から追加して、リモート PC アクセスのマシンカタログを編集してこの接続を指定し、電源管理機能を有効にできます。

電源管理接続を編集すると、ConfigMgr のウェイクアッププロキシやマジックパケットの使用、およびパケットの転送方法を構成できます。

詳しくは、「リモート PC アクセス」を参照してください。

VMware 仮想化環境

August 24, 2021

VMware を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

vCenter Server および必要な管理ツールをインストールします（vSphere vCenter のリンクモードはサポートされません）。

MCS を使用する場合は、vCenter Server のデータストアブラウザー機能は無効にしないでください（https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567を参照）。この機能を無効にすると、MCS が正しく動作しなくなります。

必要な権限

以下の権限の組み合わせまたはそのすべてを使用して、VMware ユーザーアカウントおよび 1 つまたは複数の VMware の役割を作成します。さまざまな XenApp または XenDesktop 処理をいつでも要求できるようにするためのユーザーの権限に必要な特定の粒度レベルでの役割作成をベースにしています。いつでもユーザー固有の権限を付与できるようにするために、DataCenter 以上のレベルで、ユーザーを各役割に関連付けます。

以下のテーブルは、XenApp および XenDesktop 処理と、最低限必要な VMWare 権限の間のマッピングを示しています。

接続およびリソースの追加

SDK	ユーザーインターフェイス
System.Anonymous、System.Read、および System.View	自動的に追加されます。組み込みの読み取り専用の役割を使用できます。

マシンのプロビジョニング（**Machine Creation Services**）

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[データストア] > [領域の割り当て]
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
Network.Assign	[ネットワーク] > [ネットワークの割り当て]
Resource.AssignVMToPool	[リソース] > [仮想マシンのリソースプールへの割り当て]
VirtualMachine.Config.AddExistingDisk	[仮想マシン] > [構成] > [既存ディスクの追加]
VirtualMachine.Config.AddNewDisk	[仮想マシン] > [構成] > [新規ディスクの追加]

SDK	ユーザーインターフェイス
VirtualMachine.Config.AdvancedConfig	［仮想マシン］>［構成］>［詳細］
VirtualMachine.Config.RemoveDisk	［仮想マシン］>［構成］>［ディスクの削除］
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Inventory.CreateFromExisting	［仮想マシン］>［インベントリ］>［既存のものから作成］
VirtualMachine.Inventory.Create	［仮想マシン］>［インベントリ］>［新規作成］
VirtualMachine.Inventory.Delete	［仮想マシン］>［インベントリ］>［削除］
VirtualMachine.Provisioning.Clone	［仮想マシン］>［プロビジョニング］>［仮想マシンのクローン作製］
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 および vSphere 5.1, Update 1:［仮想マシン］>［状態］>［スナップショットの作成］vSphere 5.5:［仮想マシン］>［スナップショット管理］>［スナップショットの作成］

作成する仮想マシンにタグを設定する場合は、ユーザーアカウントに次の権限も必要です。

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。

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］

マシンのプロビジョニング（**Provisioning Services**）

「マシンのプロビジョニング（**Machine Creation Services**）」のすべての権限と、以下が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	［仮想マシン］>［構成］>［デバイスの追加または削除］
VirtualMachine.Config.CPUCount	［仮想マシン］>［構成］>［CPU カウントの変更］
VirtualMachine.Config.Memory	［仮想マシン］>［構成］>［メモリ］

SDK	ユーザーインターフェイス
VirtualMachine.Config.Settings	［仮想マシン］>［構成］>［設定］
VirtualMachine.Provisioning.CloneTemplate	［仮想マシン］>［プロビジョニング］>［テンプレートのクローン作成］
VirtualMachine.Provisioning.DeployTemplate	［仮想マシン］>［プロビジョニング］>［テンプレートの展開］

電源の管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Interact.Suspend	[Virtual machine] > [Interaction] > [Suspend]

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	［データストア］>［領域の割り当て］
Datastore.Browse	［データストア］>［データストアの参照］
Datastore.FileManagement	［データストア］>［低レベルのファイル操作］
Network.Assign	［ネットワーク］>［ネットワークの割り当て］
Resource.AssignVMToPool	［リソース］>［仮想マシンのリソースプールへの割り当て］
VirtualMachine.Config.AddExistingDisk	［仮想マシン］>［構成］>［既存ディスクの追加］
VirtualMachine.Config.AddNewDisk	［仮想マシン］>［構成］>［新規ディスクの追加］
VirtualMachine.Config.AdvancedConfig	［仮想マシン］>［構成］>［詳細］
VirtualMachine.Config.RemoveDisk	［仮想マシン］>［構成］>［ディスクの削除］
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]

SDK	ユーザーインターフェイス
VirtualMachine.Inventory.CreateFromExisting	[仮想マシン] > [インベントリ] > [既存のものから作成]
VirtualMachine.Inventory.Create	[仮想マシン] > [インベントリ] > [新規作成]
VirtualMachine.Inventory.Delete	[仮想マシン] > [インベントリ] > [削除]
VirtualMachine.Provisioning.Clone	[仮想マシン] > [プロビジョニング] > [仮想マシンのクローン作製]

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Inventory.Delete	[仮想マシン] > [インベントリ] > [削除]

AppDisk の作成

VMware vSphere バージョン 5.5 以降と XenApp および XenDesktop バージョン 7.8 以降で有効。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[データストア] > [領域の割り当て]
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.AddExistingDisk	[仮想マシン] > [構成] > [既存ディスクの追加]
VirtualMachine.Config.AddNewDisk	[仮想マシン] > [構成] > [新規ディスクの追加]
VirtualMachine.Config.AdvancedConfig	[仮想マシン] > [構成] > [詳細]
VirtualMachine.Config.EditDevice	[仮想マシン] > [構成] > [デバイス設定の変更]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]

AppDisk の削除

VMware vSphere バージョン 5.5 以降と XenApp および XenDesktop バージョン 7.8 以降で有効。

SDK	ユーザーインターフェイス
Datastore.Browse	[データストア] > [データストアの参照]
Datastore.FileManagement	[データストア] > [低レベルのファイル操作]
VirtualMachine.Config.RemoveDisk	[仮想マシン] > [構成] > [ディスクの削除]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]

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。

手順 **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。

手順 **2**：以下の 3 つの内いずれかの方法で、vCenter の証明書を入手します。

vCenter サーバーからコピーする。

1. vCenter サーバー上の rui.crt ファイルを、Delivery Controller からアクセス可能な場所にコピーします。
2. Controller で、エクスポートした証明書の保存先に移動し、rui.crt ファイルを開きます。

Web ブラウザーで証明書をダウンロードする： Internet Explorer で証明書をダウンロードまたはインストールするには、Internet Explorer を右クリックして ［管理者として実行］を選択しなければならない場合があります。

1. Web ブラウザーを開き、vCenter サーバー（`https://server1.domain1.com`など）への保護された接続を確立します。
2. セキュリティに関する警告を受け入れます。

3. 証明書のエラーが表示されるアドレスバーをクリックします。
4. 証明書を表示して、［詳細］タブをクリックします。
5. ［ファイルへコピー］を選択して、任意のファイル名を指定して CER 形式でエクスポートします。
6. エクスポートした証明書を保存します。
7. エクスポートした証明書の CER ファイルを開きます。

管理者として実行する **Internet Explorer** で直接インポートする。

1. Web ブラウザーを開き、vCenter サーバー（`https://server1.domain1.com`など）への保護された接続を確立します。
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。

手順 **3**：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。

Windows Server 2008 R2 で、［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。［信頼されたユーザー］を開きます。［ローカルコンピューター］を選択します。［次へ］、［完了］の順にクリックします。

以降のサポート対象バージョン：［信頼されたユーザー］を選択して ［**OK**］をクリックします。［次へ］、［完了］の順にクリックします。

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。

構成に関する考慮事項

マスター仮想マシンの作成：

管理者は、マシンカタログのユーザー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。

接続の作成：

接続の作成ウィザードで、以下を実行します。

- 接続の種類として［VMware］を選択します。
- vCenter SDK のアクセスポイントのアドレスを指定します。
- 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指定します。ユーザー名を「<domain/username>」形式で指定します。

VMware SSL の拇印機能

VMware SSL の拇印機能は、VMware vSphere ハイパーバイザーへのホスト接続を確立するときに頻繁に報告されるエラーに対処するためのものです。これまでは、接続を確立する前に、管理者がサイトの Delivery Controller とハイパーバイザーの証明書の信頼関係を手動で作成する必要がありました。VMware SSL の拇印機能により、この手作業が不要になりました。信頼性されていない証明書の拇印がサイトのデータベースに保管されるようになったため、ハイパーバイザーは、Controller から信頼されているとみなされない場合も、XenApp や XenDesktop からは常に信頼できるとみなされます。

Studio で vSphere のホスト接続を確立する場合、接続しようとしているマシンの証明書をダイアログボックスで見ることができます。その証明書を見て、信頼するかどうかを選択できます。

Nutanix 仮想化環境

August 24, 2021

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 Acropolix MCS Plugin Installation Guide』を参照してください。

Nutanix および Provisioning Services に関するサポート情報については、Knowledge Center の記事CTX131239を参照してください。

Nutanix プラグインのインストールと登録

XenApp または XenDesktop コンポーネントをインストールした後、次の手順に従って、Delivery Controller に Nutanix プラグインをインストールして登録します。これにより、Studio を使用して Nutanix ハイパーバイザーとの接続を作成し、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成できるようになります。

1. Nutanix プラグインを Nutanix から入手して、Delivery Controller にインストールします。
2. C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0 に Nutanix Acropolis フォルダーが作成されたことを確認します。

3. **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"** を実行します。
4. Citrix Host Service、Citrix Broker Service、および Citrix Machine Creation Service を再起動します。
5. 次の PowerShell コマンドレットを実行して、Nutanix Acropolis プラグインが登録されたことを確認します:

   Add-PSSnapin Citrix*

   Get-HypHypervisorPlugin

Nutanix との接続の作成

接続を作成するウィザードのすべてのページについて詳しくは、「サイトの作成」と「接続とリソース」を参照してください。

接続とリソースの追加ウィザードの ［接続］ページで、接続の種類として ［**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

以下の情報は、「マシンカタログの作成」のガイダンスを補完するものであり、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］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を選択します。

［マスターイメージ］ページで、イメージのスナップショットを選択します。XenApp および XenDesktop で使用するには、Acropolis のスナップショット名の先頭は「XD_」にしてください。必要に応じて、Acropolis コンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新された一覧を表示します。

［仮想マシン］ページで、仮想 CPU の数と仮想 CPU あたり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、［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。

Microsoft Azure 仮想化環境

October 22, 2021

接続の構成

Studio を使用して、Microsoft Azure 接続を作成する場合、Microsoft Azure 発行設定ファイルの情報が必要です。各サブスクリプションで使用されるこの XML ファイルには、以下の例にあるような情報が入っています（実際の管理証明書はこれよりも長くなります）:

```
<Subscription
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
   sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
<!--NeedCopy-->
```

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. ブラウザーで、https://manage.windowsazure.com/publishsettings/indexに移動します。
2. 検索ボックスの横にある Cloud Shell アイコンをクリックし、手順に従って公開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 の仮想マシンとクラウドサービスのサイズ：https://docs.microsoft.com/en-us/previous-versions/azure/dn197896(v=azure.100)?redirectedfrom=MSDN
- 仮想マシンの価格設定：https://azure.microsoft.com/en-us/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。

標準層：標準層 VM は、4 つの系列：A、D、DS、G で表示されます。

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、https://azure.microsoft.com/en-us/pricing/details/virtual-machines/を参照してください。

クラウド環境では、実際のコンピューティング要件を理解することが重要です。概念実証などのテスト作業では、高性能な種類の VM インスタンスを使いたくなるかもしれません。また、コスト節減のため、性能の低い VM を使いたくなることもあるでしょう。タスクに見合った VM を使用するようにしましょう。最高のパフォーマンスで始めても、必要な結果を得られないことがありますし、時間の経過に伴って、場合によっては 1 週間以内に、コストが非常に高額になります。パフォーマンスが低く、コストも安い種類の VM インスタンスでは、パフォーマンスとユーザーの操作性がタスクに適さない可能性があります。

デスクトップ OS（VDI）またはサーバー OS（RDSH）ワークロードの場合、中程度のワークロードに対して LoginVSI を使用したテスト結果から、インスタンスの種類に中（A2）と大（A3）を選択すると、価格性能比が最高になることがわかりました。

中（A2）と大（A3 または A5）は、ワークロードの評価において、最高の価格性能比を発揮します。これ以下の設定はお勧めしません。より高い性能を持つ 7VM シリーズはアプリケーションやユーザーが要求するパフォーマンスや操作性をもたらすかもしれませんが、性能の高い種類の VM インスタンスに本当の価値があるかどうかを判断するには、これら 3 種類のインスタンスの 1 つを基準にするのが一番です。

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、以下で最新情報を確認してください：https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/。

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。

コアコンポーネントのインストール

August 24, 2021

コアコンポーネントとは、Delivery Controller、Studio、Director、およびライセンスサーバーです。

（7.15 LTSR CU6 より前のバージョンでは、StoreFront もコアコンポーネントに含まれていました。引き続き、[拡張展開] セクションの［**Citrix StoreFront**］を選択するか、インストールメディアでコマンドを実行して StoreFront をインストールすることができます）

重要：インストールを始める前に、「インストールの準備」を確認してください。また、インストールを開始する前にこの記事を確認してください。

この記事では、コアコンポーネントをインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順 **1**：製品ソフトウェアをダウンロードしてウィザードを起動する

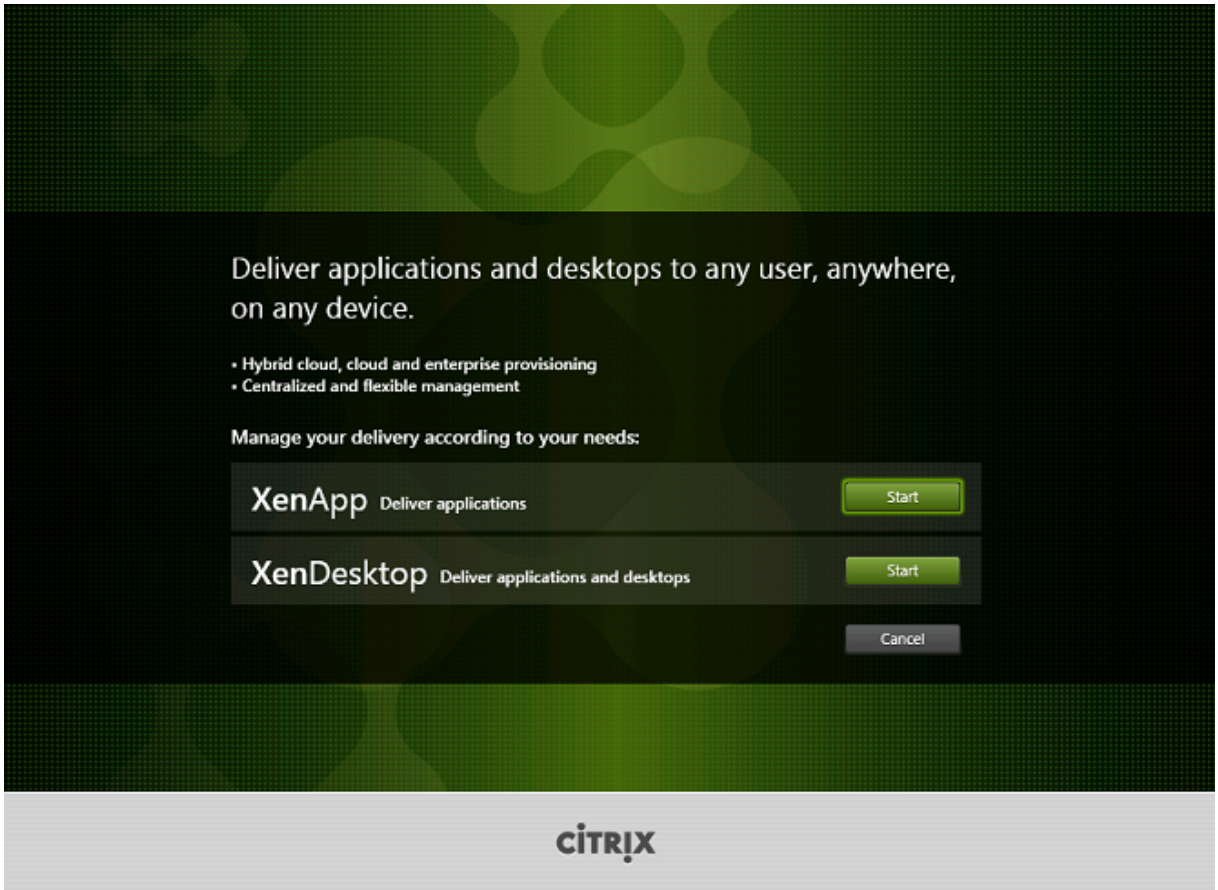
Citrix アカウント資格情報を使用して、XenApp および XenDesktop のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。

ローカルの管理者アカウントを使って、コアコンポーネントのインストール先マシンにログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

手順 **2**：インストールする製品を選択する

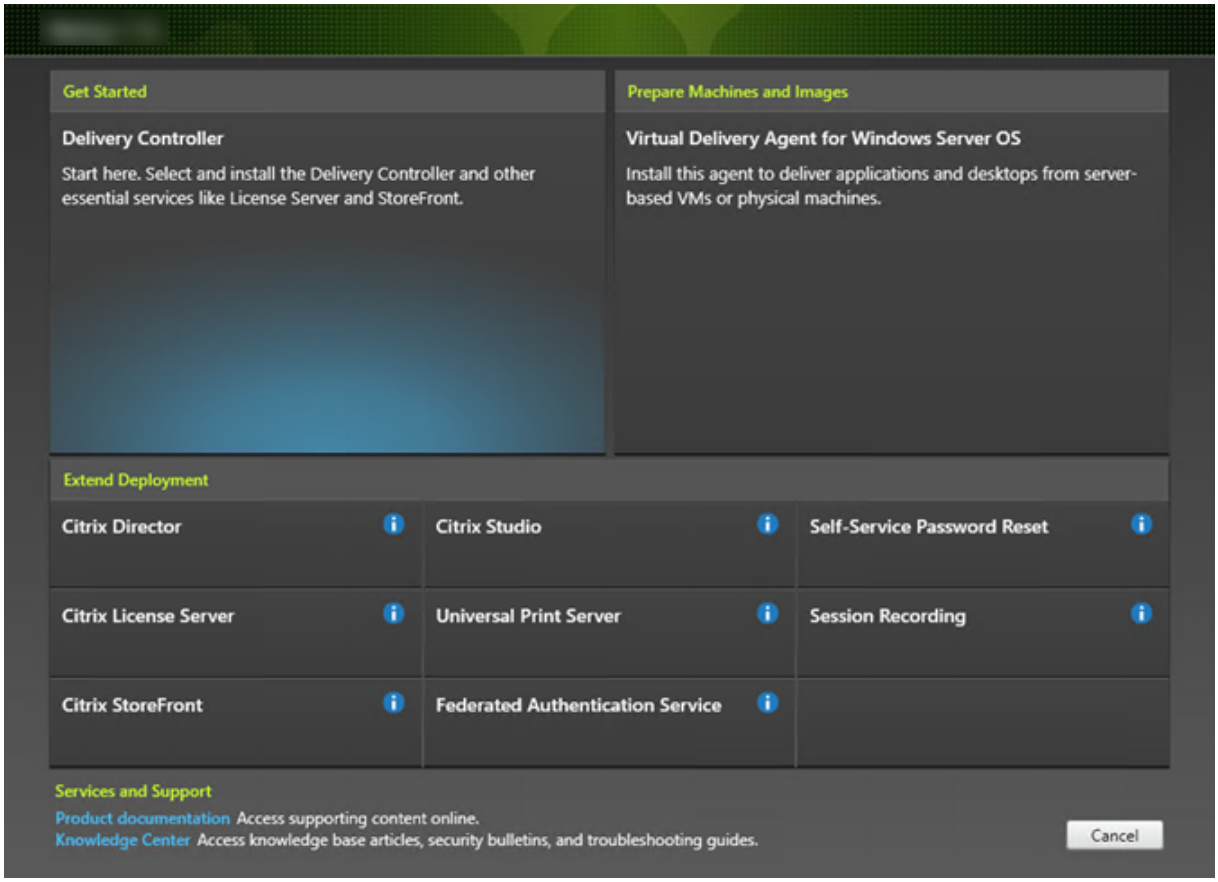


XenApp または XenDesktop の横にある ［開始］をクリックして、必要な製品をインストールします。

（マシンに XenApp または XenDesktop コンポーネントが既にインストールされている場合、このページは表示されません）。

コマンドラインオプション：XenApp をインストールする場合は/xenapp。オプションを省略すると XenDesktop がインストールされます

手順 **3**：インストールするものを選択する

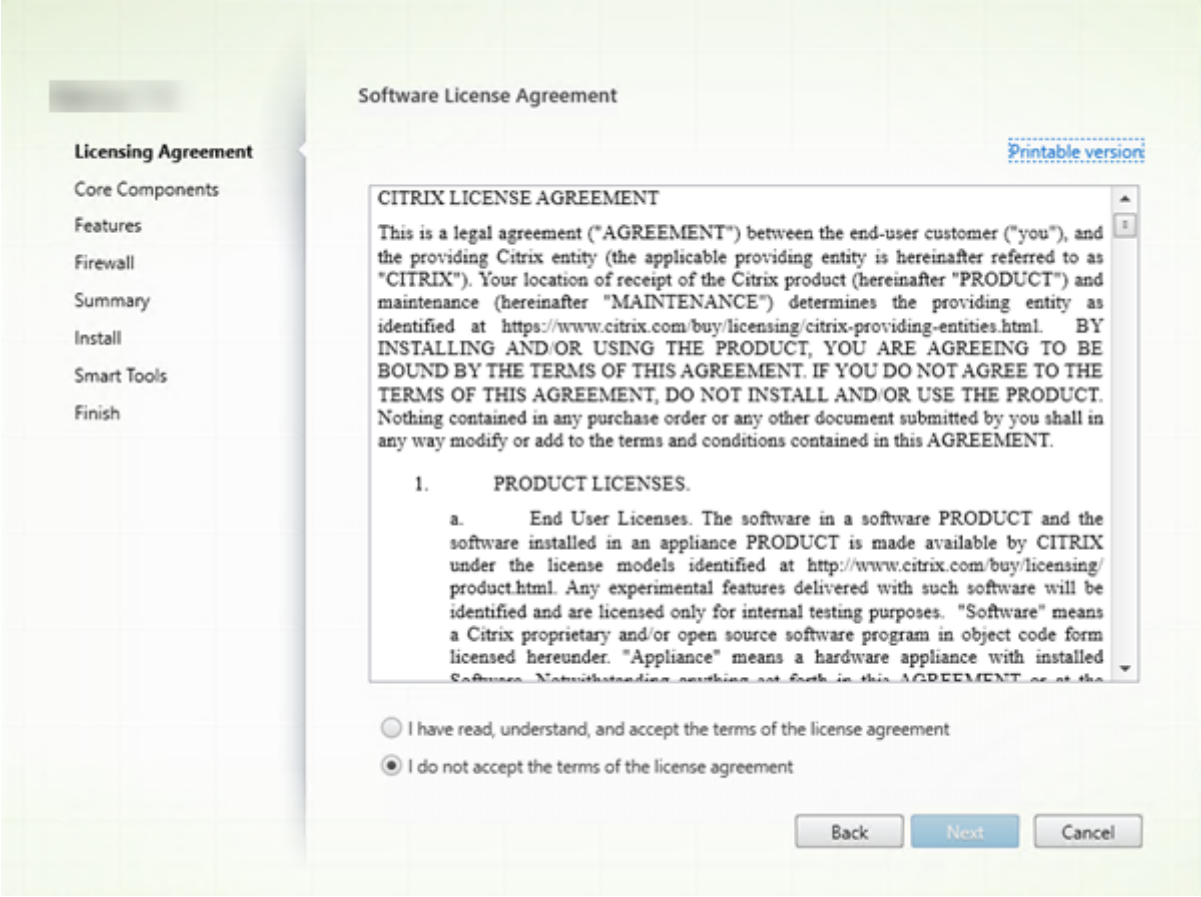


製品を初めてインストールする場合は、[**Delivery Controller**] をクリックします（後のページで、このマシンにインストールする特定のコンポーネントを選択します）。

Controller が（このマシンまたは別のマシンに）既にインストールされていて、別のコンポーネントをインストールする場合は、[拡張展開] セクションからコンポーネントを選択します。

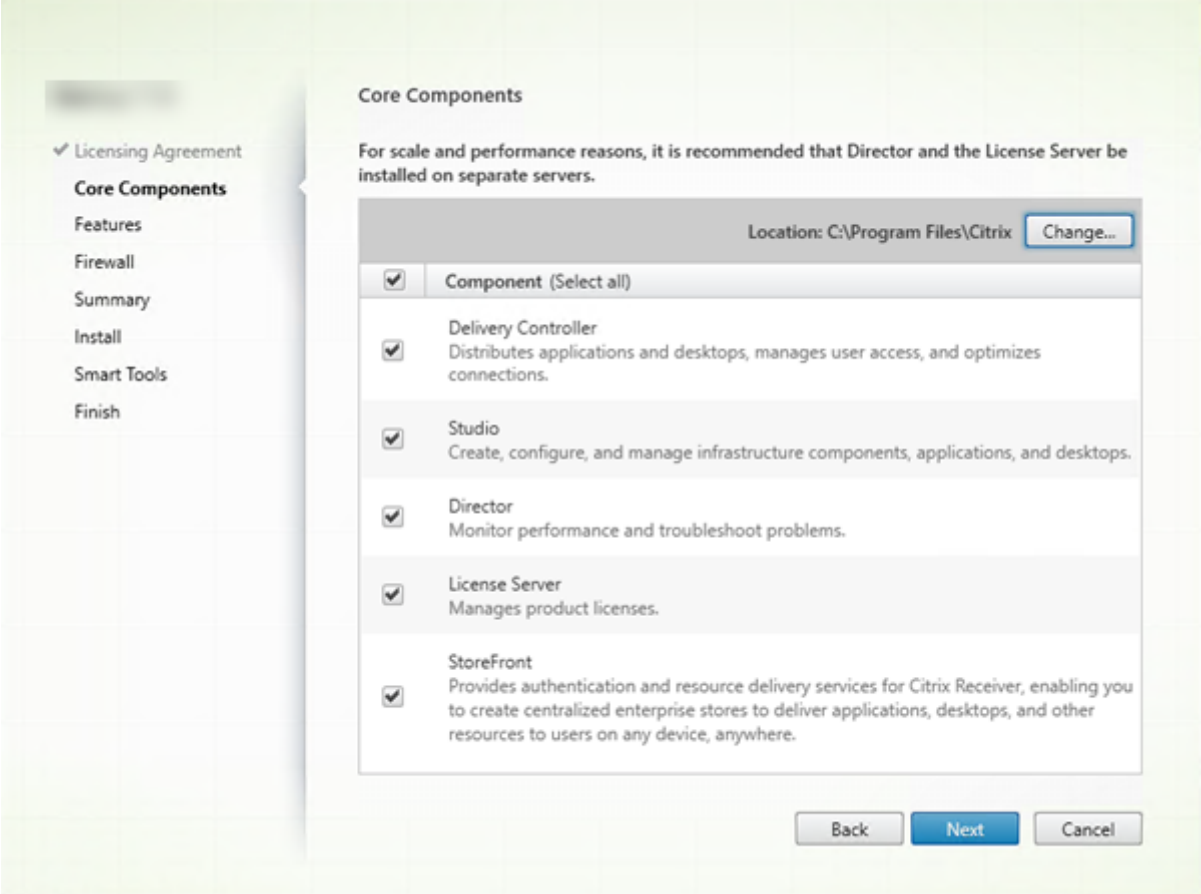
コマンドラインオプション：/controllers

手順 **4**：ライセンス契約書を読み、同意する



［ライセンス契約］ページで、ライセンス契約を読み、読んで同意したことを明示します。［次へ］をクリックします。

手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、C:\Program Files\Citrix に各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Service アカウントでの実行権限が必要です。
- コンポーネント：デフォルトでは、すべてのコアコンポーネントのチェックボックスがオンになっています。1 つのサーバー上にすべてのコアコンポーネントをインストールすることは、概念実証展開、テスト展開、または小規模実稼働展開には十分です。より大きな稼働環境では、Director、StoreFront、および License Server を別々のサーバーにインストールすることをお勧めします。

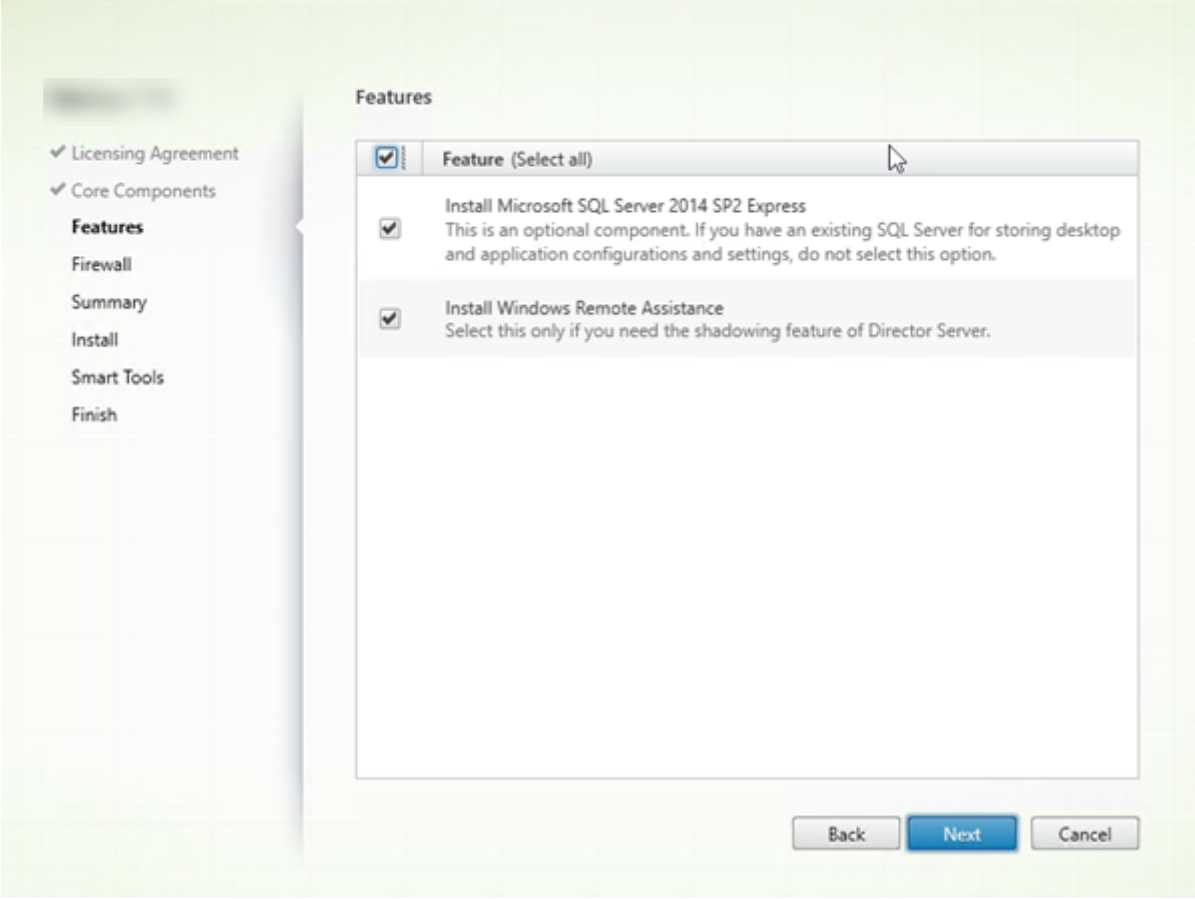
このマシンにインストールするコンポーネントのみを選択します。このマシンにコンポーネントをインストールした後、他のマシン上で再びインストーラーを実行して他のコンポーネントをインストールできます。

このマシン上で必要なコアコンポーネントをインストールしないように選択すると、アイコンの警告が表示されます。この警告では、このマシンでは不要であるにも関わらず、このコンポーネントをインストールするように通知されます。

［次へ］をクリックします。

コマンドラインオプション：/installdir、/components、/exclude

手順 **6**：機能を有効または無効にする



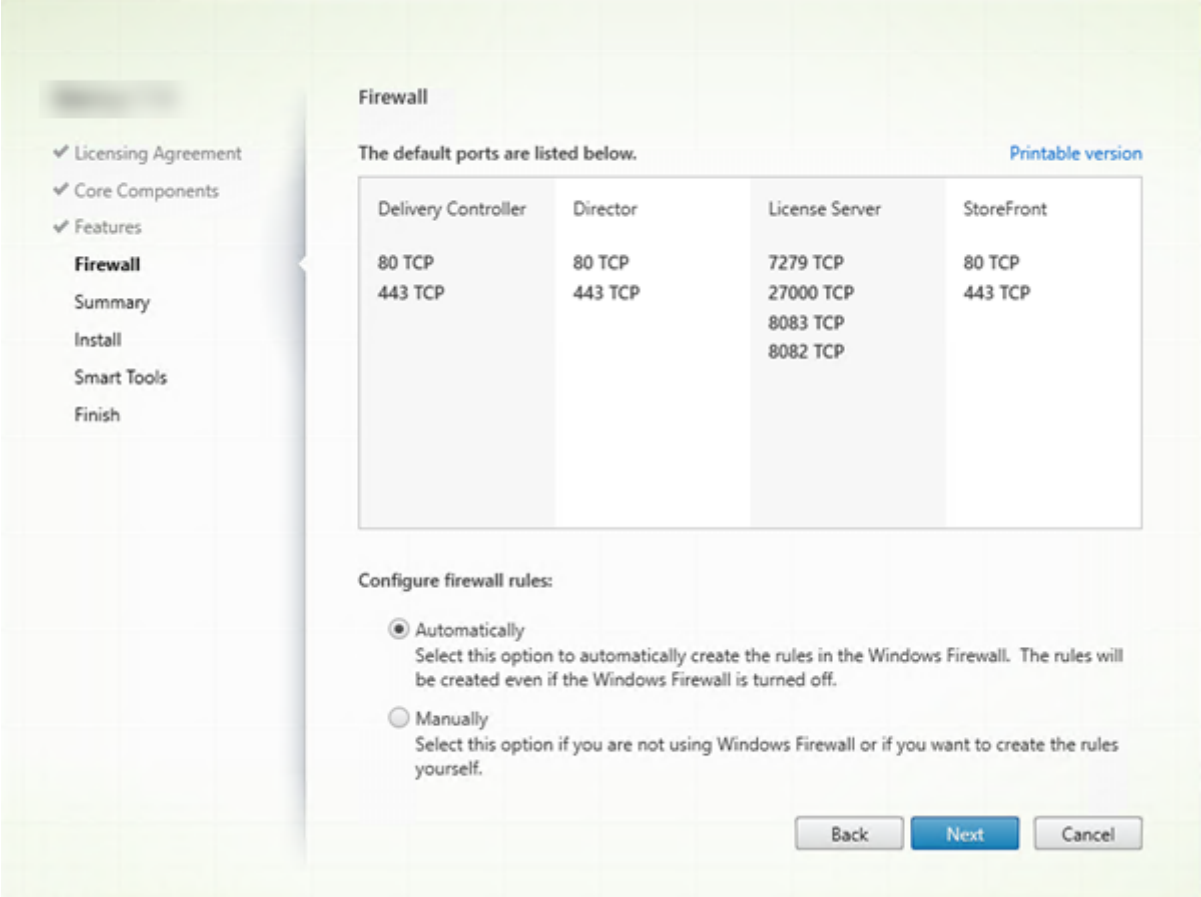
［機能］ページで次の作業を行います：

- Microsoft SQL Server Express をサイトデータベースとして使用するためにインストールするかどうかを選択します。デフォルトでは、これはオンになっています。「データベース」を参照し、XenApp および XenDesktop データベースについての理解を深めてください。
- Director をインストールすると、Windows リモートアシスタンスも自動的にインストールされます。Director ユーザーのシャドウで使用するために Windows リモートアシスタンスのシャドウ機能を有効にするかどうかを選択します。シャドウ機能を有効にすると、TCP ポート 3389 が開きます。この機能は、デフォルトで有効になります。ほとんどの展開ではデフォルト設定で十分です。この機能は Director のインストール時のみ表示されます。

［次へ］をクリックします。

コマンドラインオプション：/nosql（インストールを阻止するため）、/no_remote_assistance（有効化を阻止するため）

手順 **7**：**Windows** ファイアウォールポートを自動的に開放する



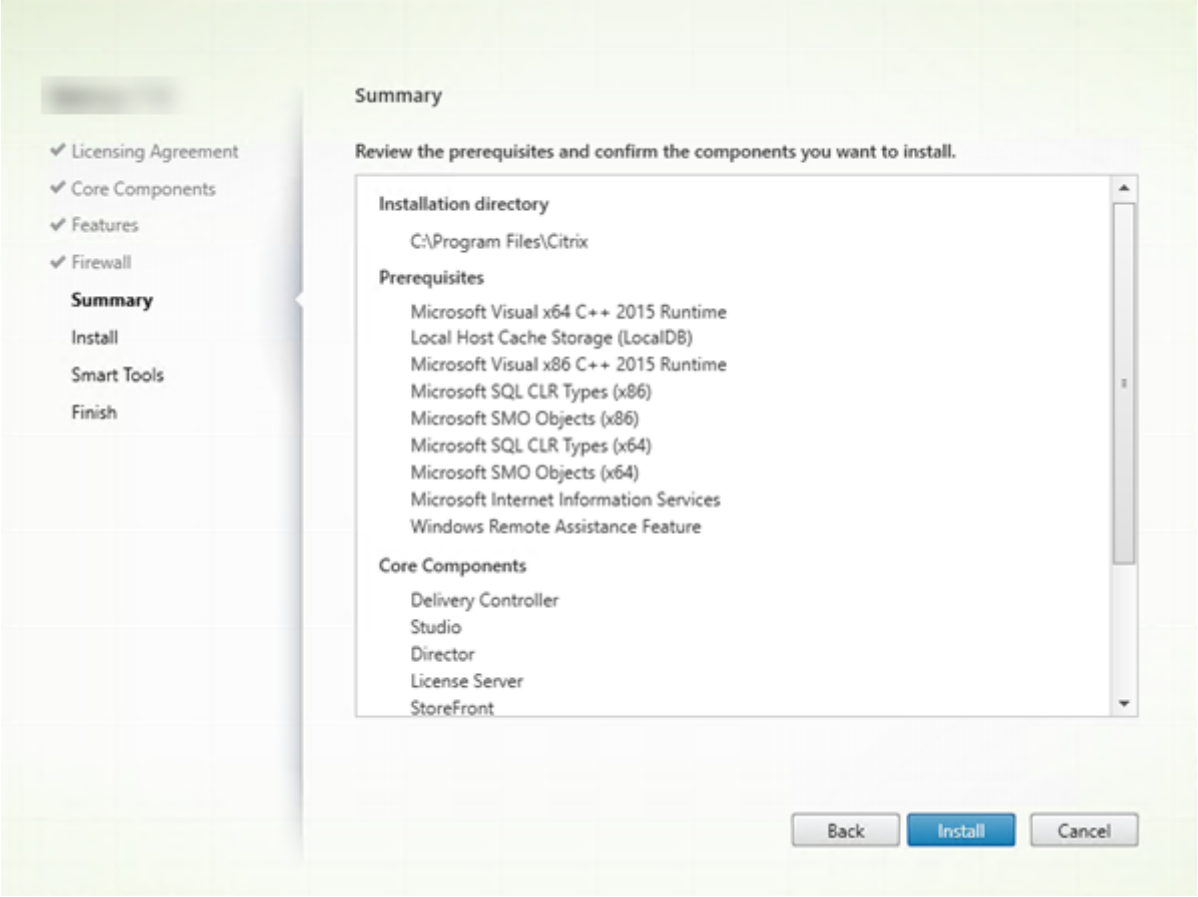
Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、デフォルトで ［ファイアウォール］ページに示されているポートが自動的に開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートの詳細については、「ネットワークポート」を参照してください。

［次へ］をクリックします。

（この図は、すべてのコアコンポーネントをこのマシンにインストールした場合のポート一覧を示します。このようなタイプのインストールは通常、テスト展開でのみ行われます）。

コマンドラインオプション：/configure_firewall

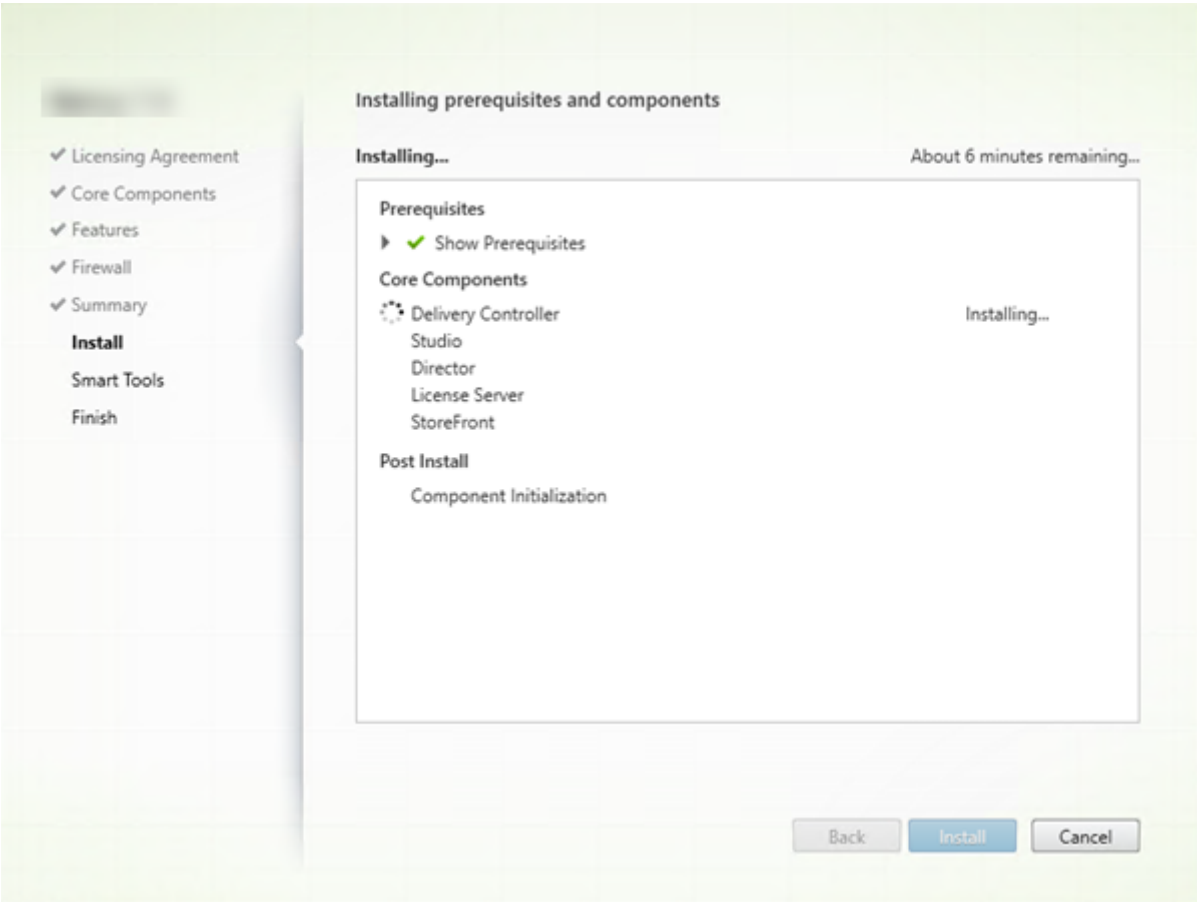
手順 **8.** インストール前に前提条件を確認する



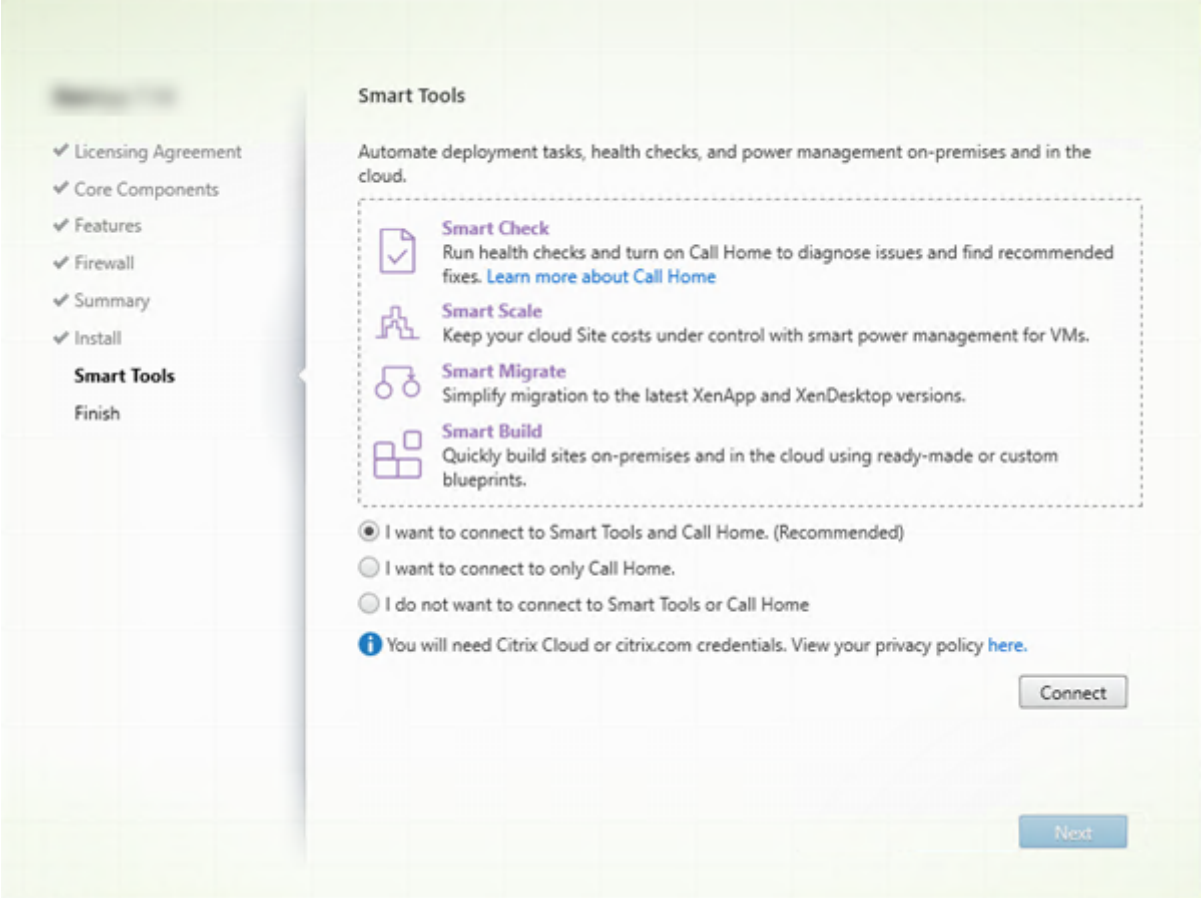
［概要］ページに、インストールされるものが表示されます。必要に応じて、［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

準備ができたら、［インストール］をクリックします。

画面にインストールの進捗が表示されます:



手順 **9. Smart Tools** と **Call Home** に接続する



Delivery Controller をインストールまたはアップグレードすると、［Smart Agent］ページに複数のオプションが表示されます:

- Smart Tools と Call Home への接続を有効にします。このオプションを選択することをお勧めします。
- Call Home への接続を有効にします。Call Home が既に有効な場合、またはインストーラーで Citrix Telemetry Service に関連するエラーが発生した場合には、アップグレード時にこのオプションは表示されません。
- Smart Tools または Call Home への接続を有効にしないでください。

StoreFront（Controller ではない）をインストールすると、**Smart Tools** ページがウィザードに表示されます。その他のコアコンポーネントはインストールされている（が Controller または StoreFront はインストールされていない）場合、ウィザードには ［**Smart Tools**］ページも ［**Call Home**］ページも表示されません。

Smart Tools と Call Home への接続を有効にするオプションを選択した場合は、以下を行います。

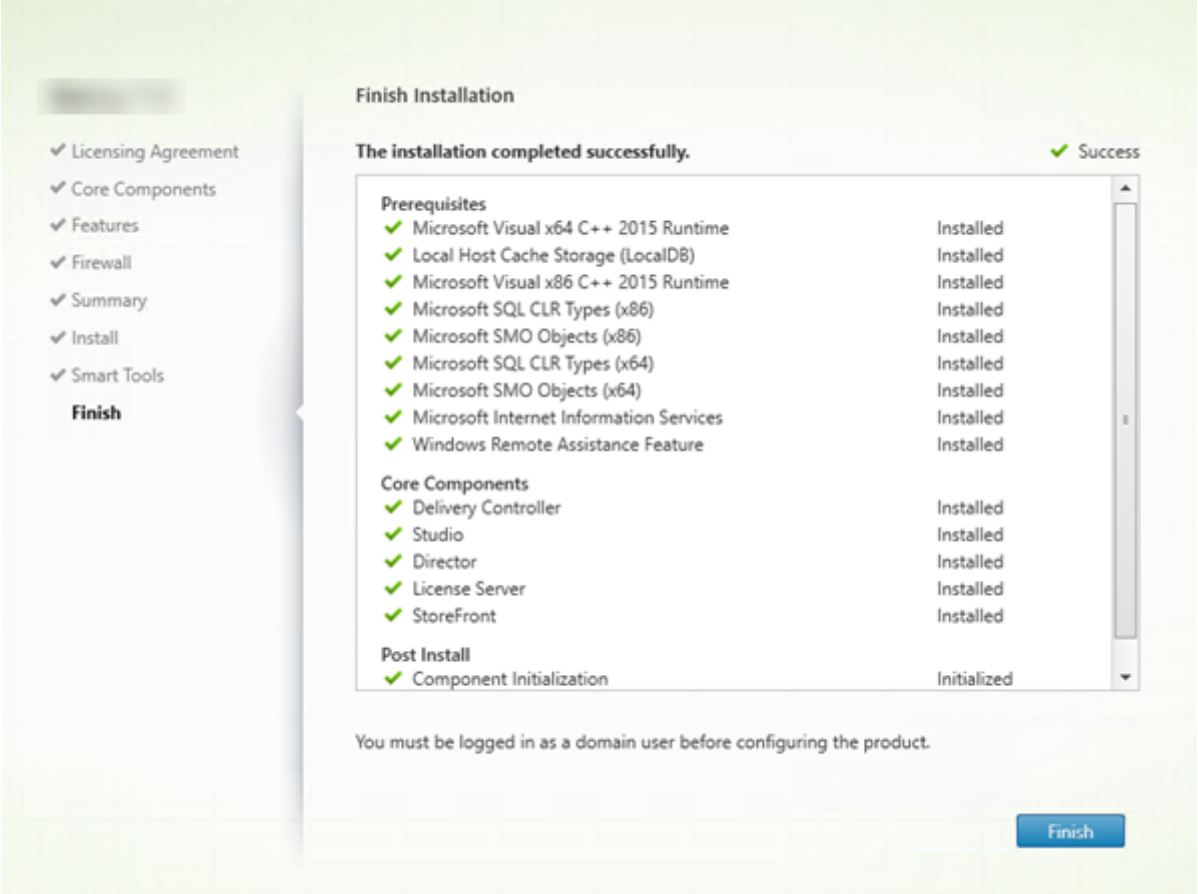
1. ［接続］をクリックします。
2. Citrix または Citrix Cloud の資格情報を入力します。
3. 資格情報が検証された後、Smart Agent 証明書がダウンロードされます。これが正常に終了したら、［接続］ボタンの横に緑のチェックマークが表示されます。この処理中にエラーが発生した場合、参加に関する選択を変更してください（参加しないに変更）。後で登録することもできます。

4.［次へ］をクリックしてインストールウィザードを続行します。

参加しないことを選択した場合、［次へ］をクリックします。

コマンドラインオプション：/exclude “Smart Tools Agent”（インストールしない）

手順 **10.** インストールを完了する



［完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックします。

手順 **11**：残りのコアコンポーネントを他のマシンにインストールする

1 台のマシンにすべてのコアコンポーネントをインストールした場合、次の手順に進みます。それ以外の場合は、その他のマシンでインストーラーを実行し、残りのコアコンポーネントをインストールします。追加の Controller を他のサーバーにインストールすることもできます。

次の手順

必要なコアコンポーネントをすべてインストールしたら、Studio を使用してサイトを作成します。

サイトを作成したら、VDA をインストールします。

いつでも全製品インストーラーを使用して展開を拡張し、次のコンポーネントを含めることができます。

- ユニバーサルプリントサーバーコンポーネント：プリントサーバー上でインストーラーを起動します。［拡張展開］セクションで ［ユニバーサルプリントサーバー］を選択します。ライセンス契約を承諾し、ウィザードを完了します。ほかに指定または選択するものはありません。コマンドラインからこのコンポーネントをインストールするには、「コマンドラインを使ったインストール」を参照してください。
- フェデレーション認証サービス：「フェデレーション認証サービス」を参照してください。
- セルフサービスパスワードリセットサービス：セルフサービスパスワードリセットサービスのドキュメントを参照してください。

VDA のインストール

August 24, 2021

Windows マシン用には 2 種類の VDA があります：VDA for Server OS と VDA for Desktop OS です（Linux マシン用の VDA については、「Linux Virtual Delivery Agent」を参照してください）。

> 重要：
>
> インストールを始める前に、「インストールの準備」を確認してください。たとえば、マシンに最新の Windows 更新プログラムが必要です。必要な更新プログラム（KB2919355 など）がない場合は、インストールに失敗します。

VDA をインストールする前に、コアコンポーネントをインストールしておく必要があります。VDA をインストールする前にサイトを作成することもできます。

この記事では、VDA をインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

VDA または Delivery Controller のインストールに失敗すると、MSI アナライザーはエラーのある MSI ログを解析し、正確なエラーコードを表示します。このアナライザーは、既知の問題であった場合は、CTX 記事を示します。アナライザーはまた、故障エラーコードに関する匿名化データも収集します。このデータは、CEIP によって収集された他のデータに含まれます。CEIP への登録を終了すると、収集された MSI アナライザーのデータは Citrix に送信されなくなります。

手順 **1**：製品ソフトウェアをダウンロードしてウィザードを起動する

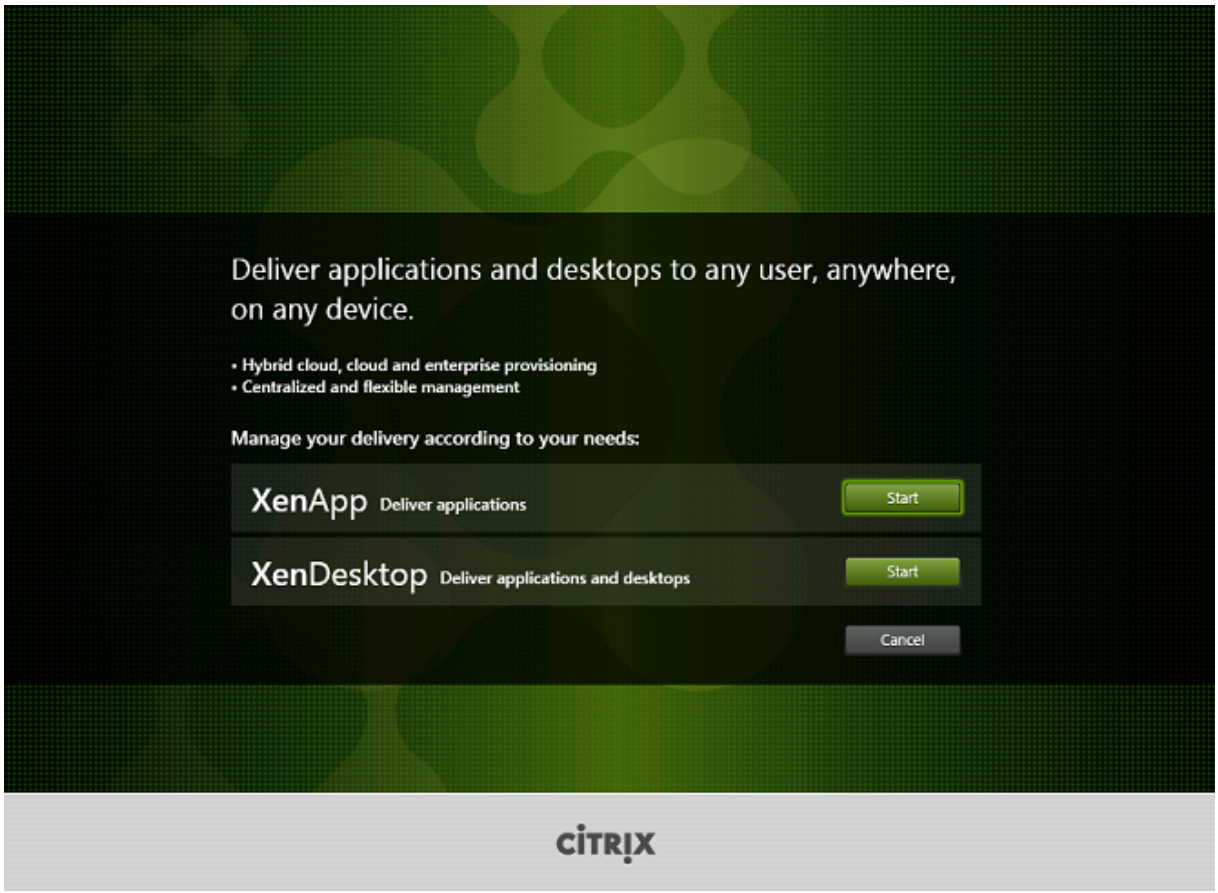
全製品インストーラーを使用する場合：

- XenApp および XenDesktop の ISO をまだダウンロードしていない場合:
  - Citrix アカウント資格情報を使用して、XenApp および XenDesktop のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。
  - ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。
- VDA をインストールするイメージまたはマシン上で、ローカル管理者アカウントを使用します。DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。
- インストールウィザードが起動します。

スタンドアロンパッケージを使用する場合:

- Citrix アカウント資格情報を使用して、XenApp および XenDesktop のダウンロードページにアクセスします。適切なパッケージをダウンロードします:
  - VDAServerSetup.exe: サーバー OS VDA バージョン >
  - VDAWorkstationSetup.exe: デスクトップ OS VDA バージョン >
  - VDAWorkstationCoreSetup.exe: デスクトップ OS 用 Core Services VDA バージョン >
- このパッケージを右クリックして、[管理者として実行] を選択します。
- インストールウィザードが起動します。

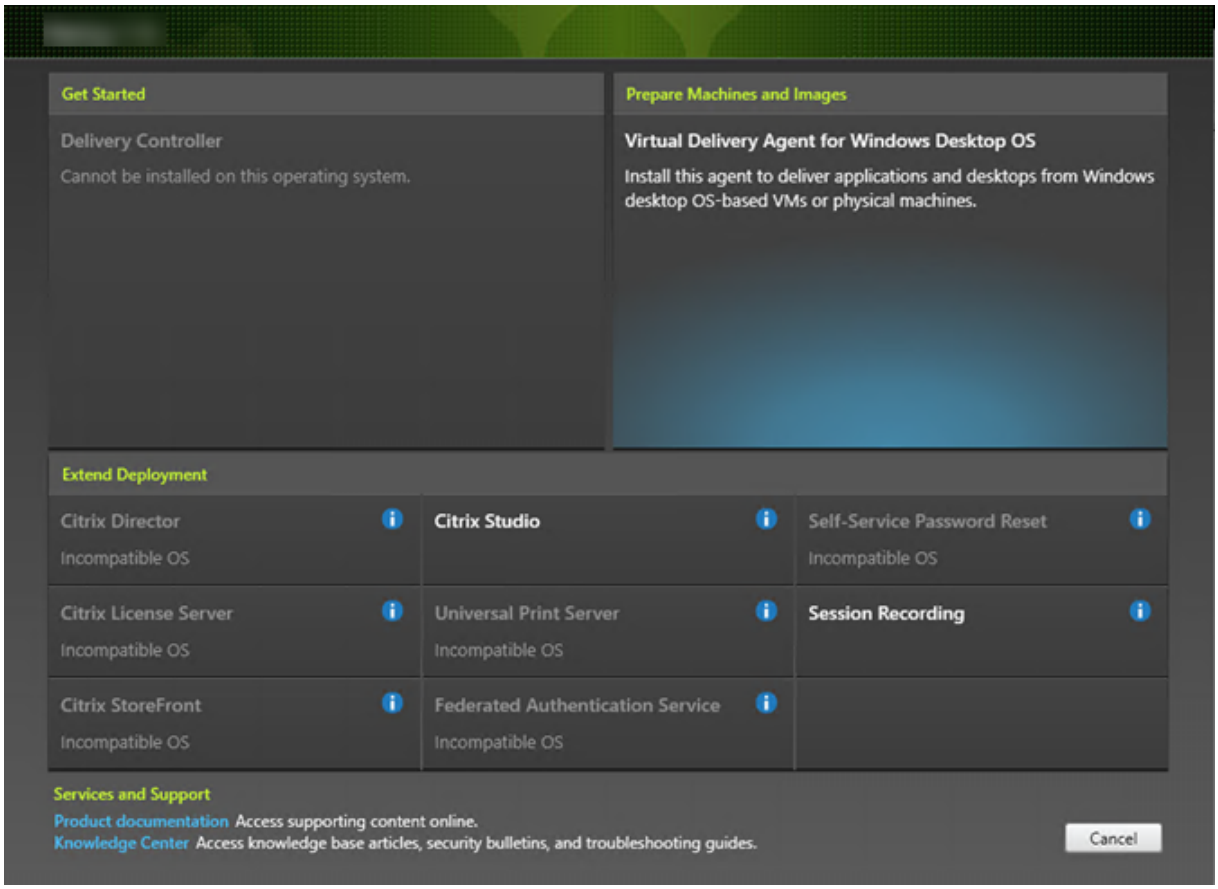
手順 **2**：インストールする製品を選択する



XenApp または XenDesktop の横にある ［開始］をクリックして、必要な製品をインストールします。（マシンに XenApp または XenDesktop コンポーネントが既にインストールされている場合、このページは表示されません）。

コマンドラインオプション：XenApp をインストールする場合は/xenapp。オプションを省略すると XenDesktop がインストールされます

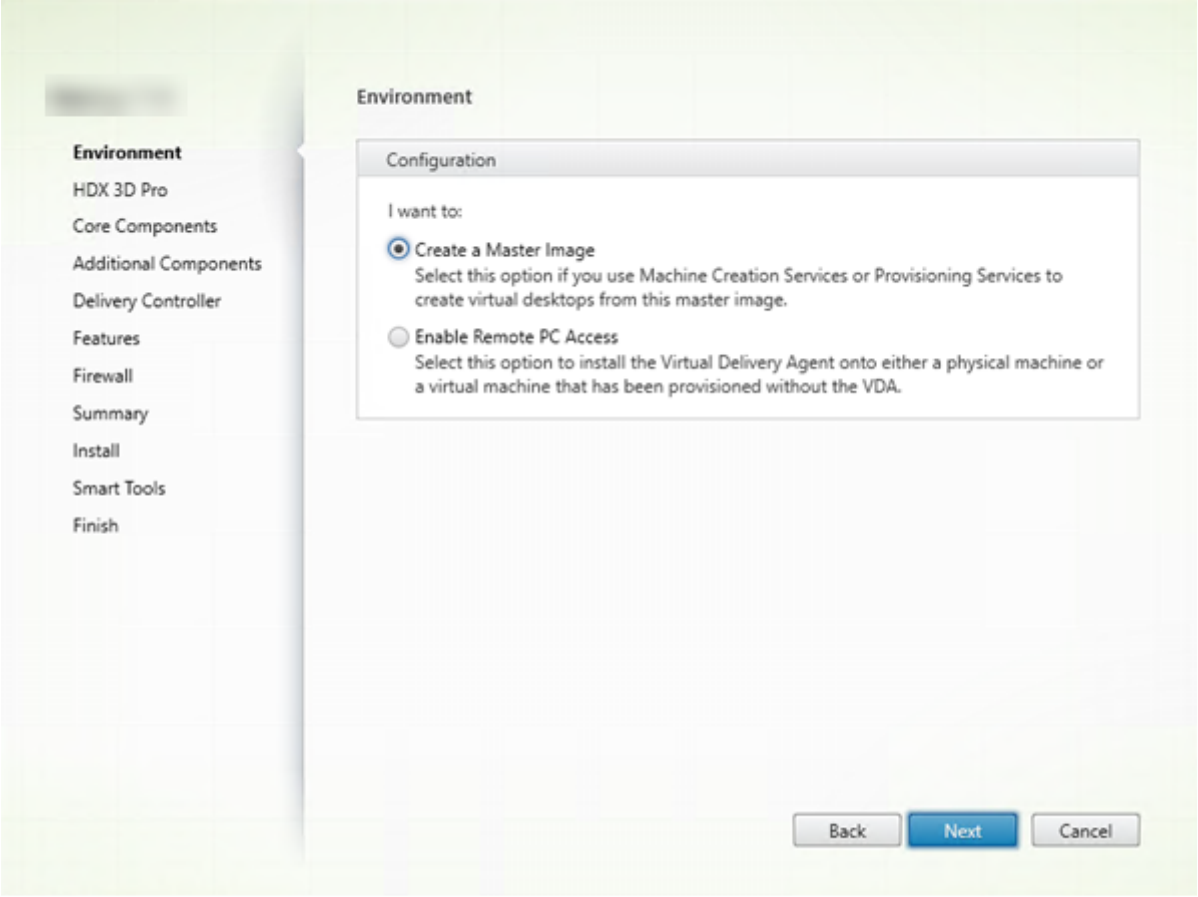
手順 **3**：**VDA** を選択する



Virtual Delivery Agent エントリを選択します。インストーラーはデスクトップ OS とサーバー OS のいずれの上で実行されているかを認識しているので、適切な種類の VDA のみが提示されます。

たとえば、Windows 10 マシンでインストーラーを実行すると、VDA for Desktop OS のオプションが利用可能になります。VDA for Server OS のオプションは提示されません。

手順 **4**：**VDA** の使用方法を指定する



［環境］ページで、VDA の使用方法を指定します。次のいずれかのオプションを選択します：

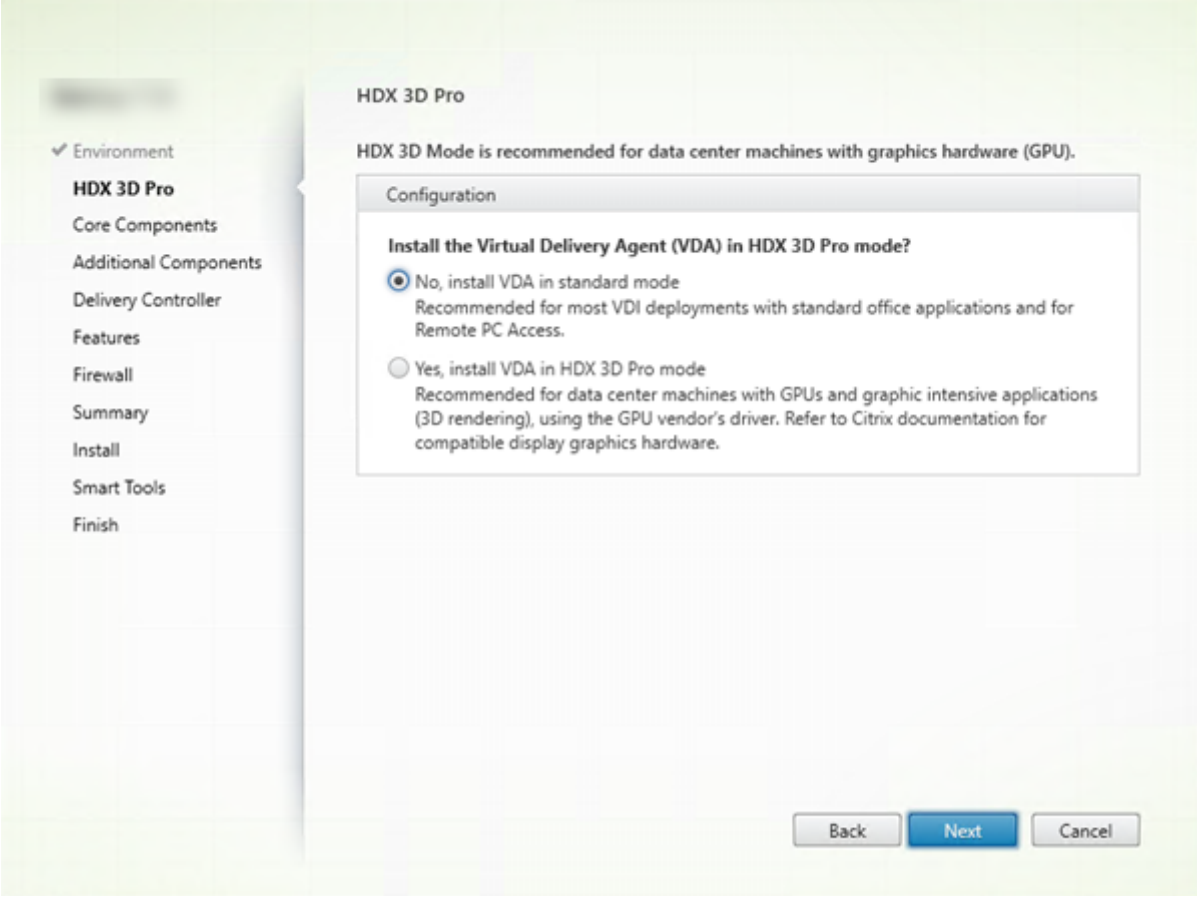
- マスターイメージ：（デフォルト）マスターイメージ上に VDA をインストールします。Citrix ツール（Machine Creation Services や Provisioning Services など）を使用して、そのマスターイメージから仮想マシンを作成することを計画しています。
- ［サーバーマシンへの接続を有効にする］（サーバー上にインストールする場合）または［リモート **PC** アクセス］（デスクトップマシン上にインストールする場合）：物理マシン上、または VDA なしでプロビジョニングした仮想マシン上に VDA をインストールします。リモート PC アクセスオプションを選択すると、以下のコンポーネントはインストールまたは有効化されません。
  - App-V
  - Profile Management
  - Machine Identity Service
  - Personal vDisk

［次へ］をクリックします。

コマンドラインオプション：/masterimage、/remotepc

VDAWorkstationCoreSetup.exe インストーラーを使用している場合、このページはウィザードに表示されず、コマンドラインオプションは無効です。

手順 **5**：**HDX 3D Pro** モードを有効にするかどうかを選択する



[**HDX 3D Pro**] ページは、VDA for Desktop OS をインストールする場合にのみ表示されます。

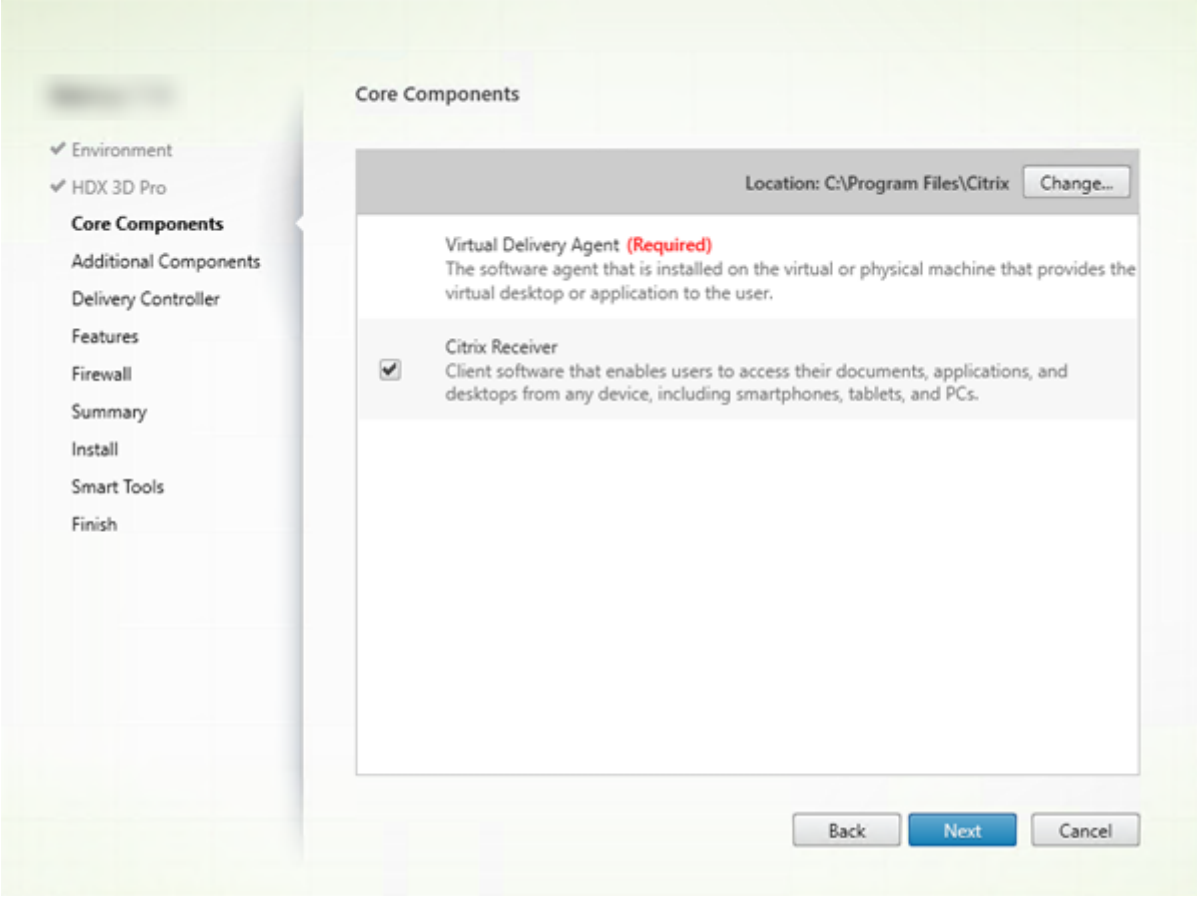
- Microsoft RemoteFX で有効にされたデスクトップを含む、ほとんどのデスクトップで、標準モードでの VDA の使用をお勧めします。デフォルトでは標準モードの VDA です。
- HDX 3D Pro VDA では、グラフィックを多用するプログラムおよびメディアを駆使したアプリケーションのパフォーマンスが最適化されます。HDX 3D Pro VDA モードは、3D レンダリングを行うためにマシンがグラフィックプロセッサにアクセスする場合にお勧めします。
- リモート PC アクセスの場合、VDA は通常、標準モードの VDA で構成されます。HDX 3D Pro で構成されているリモート PC アクセスの場合、モニターのブランキングは次でサポートされます。
  - Intel Iris Pro graphics と Intel HD graphics 5300 以上（第 5 世代 Intel Core プロセッサおよび第 6 世代 Intel Core i5 プロセッサ）
  - NVIDIA Quadro と NVIDIA GRID GPU
  - AMD RapidFire

標準モード	**HDX 3D Pro** モード
通常、グラフィックのハードウェアアクセラレーションのない仮想デスクトップおよびリモート PC アクセスに最適です。	5 つ以上のモニターが必要でない限り、通常、グラフィックハードウェアアクセラレーションのあるデータセンターデスクトップに最適です。
リモート PC アクセスには、あらゆる GPU を使用できます（アプリケーション互換性の制限あり）： **Windows 7**、**8**、**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許容しない場合、実行されないことがあります。**Windows 10** の場合、GPU アクセラレーションはウィンドウ表示の DirectX 10、11、および 12 アプリに提供されます。DX 9 アプリは WARP によってレンダリングされます。DX アプリはフルスクリーンモードでは使用できません。GPU ベンダー（現時点では NVIDIA のみ）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。	任意の GPU による GPU アクセラレーションをサポートします。ただし、コンソールのブランキング、非標準画面解像度、および True Multi Monitor サポートには NVIDIA GRID、Intel Iris Pro または AMD RapidFire グラフィックスが必要です。広範なアプリケーション互換性のためにグラフィックベンダーのドライバーを活用します：GPU がサポートするすべての **3D API**（**DirectX** または **OpenGL**）。Intel Iris Pro（Win10 のみ）、NVIDIA GRID、および AMD RapidFire での全画面 **3D** アプリケーションサポート。カスタムドライバー拡張および **API** のサポート。（CUDA や OpenCL など）。
任意のモニター解像度（上限は Windows OS およびパフォーマンスによって決まります）および最大 8 つのモニター。	最大で 4 つのモニターをサポートします。
Intel Iris Pro グラフィックプロセッサで利用可能な H.264 ハードウェアエンコーディング。	Intel Iris Pro グラフィックスプロセッサおよび NVIDIA カードを搭載して H.264 ハードウェアエンコーディングが使用可能です。

［次へ］をクリックします。

コマンドラインオプション：/enable_hdx_3d_pro

手順 **6**：インストールするコンポーネントおよびインストール場所を選択する



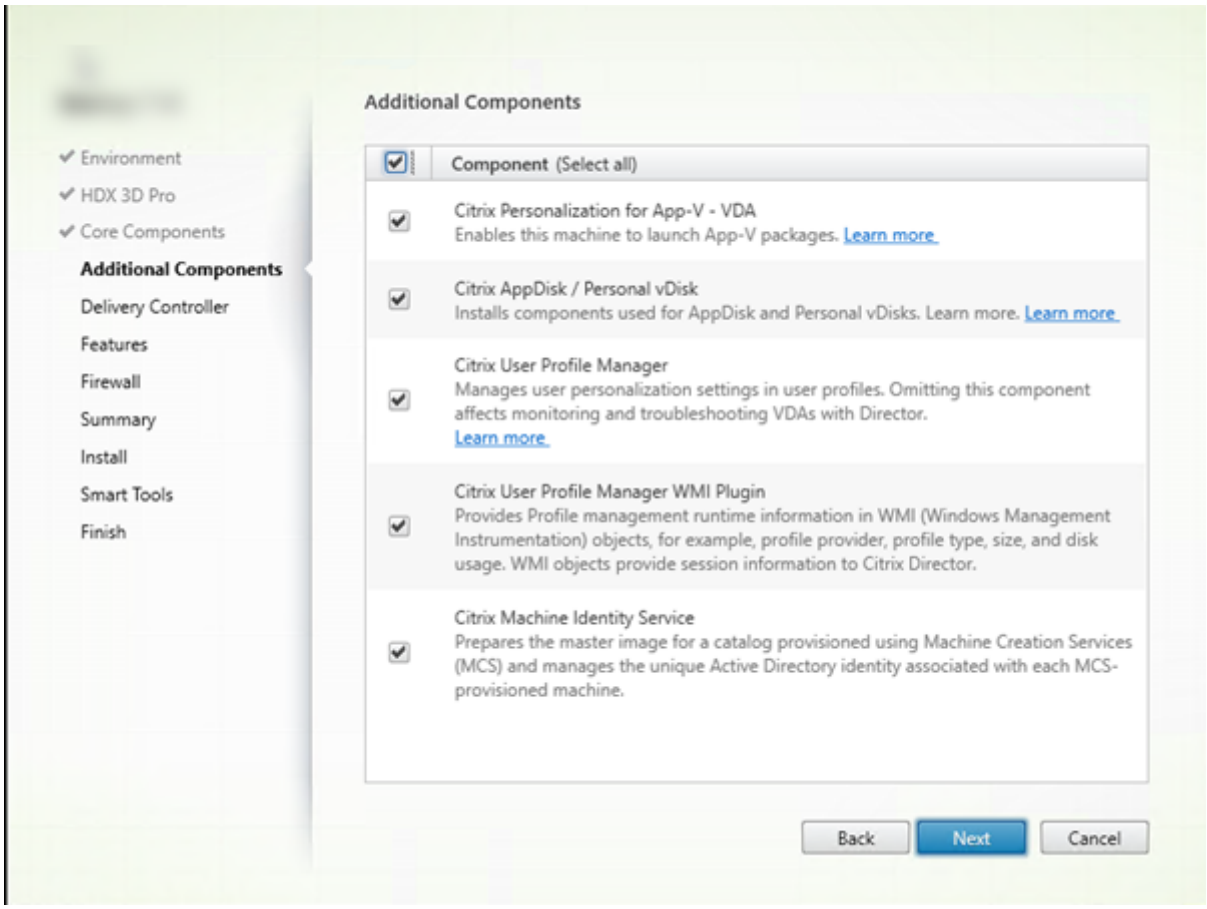
［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、C:\Program Files\Citrix に各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Service アカウントでの実行権限が必要です。
- コンポーネント：デフォルトで、Citrix Receiver for Windows は VDA とともにインストールされます（VDAWorkstationCoreSetup.exe インストーラーを使用する場合を除く）。Citrix Receiver をインストールしない場合は、チェックボックスをオフにします。VDAWorkstationCoreSetup.exe インストーラーを使用している場合、Citrix Receiver for Windows はインストールされないため、このチェックボックスは表示されません。

［次へ］をクリックします。

コマンドラインオプション：（/installdir、Citrix Receiver for Windows のインストールを阻止するには「/components vda」を使用）

手順 **7**：追加コンポーネントのインストール



［追加コンポーネント］ページには、VDA とともにほかの機能やテクノロジをインストールするかどうかを指定するチェックボックスがあります。次の場合、このページは表示されません：

- VDAWorkstationCoreSetup.exe インストーラーを使用している。また、追加コンポーネント用のコマンドラインオプションはこのインストーラーでは無効です。
- VDA をアップグレードしており、追加コンポーネントが既にすべてインストールされている。（追加コンポーネントのいくつかが既にインストールされている場合、このページにはインストールされていないものだけが表示されます。）

Citrix Personalization for App-V:

Microsoft App-V パッケージのアプリケーションを使用する場合、このコンポーネントをインストールします。詳しくは、「App-V」を参照してください。

コマンドラインオプション：/exclude “Citrix Personalization for App-V – VDA” を使用してコンポーネントがインストールされないようにする

Citrix AppDisk および **Personal vDisk**:

仮想マシン上に VDA for Desktop OS をインストールする場合にのみ有効です。AppDisk および Personal vDisk に使用されるコンポーネントがインストールされます。詳しくは、「AppDisk」および「Personal vDisk」を参照し

てください。

コマンドラインオプション：/exclude “Personal vDisk” を使用して、AppDisk と Personal vDisk のコンポーネントがインストールされないようにする

Citrix Profile Management:

このコンポーネントは、ユーザープロファイル内のユーザーの個人設定を管理します。詳しくは、「Profile Management」を参照してください。

インストールから Citrix Profile Management を除くと、Citrix Director を使った VDA の監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの［個人設定］パネル、および［エンドポイント］ページの［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management サービスをインストールして実行することをお勧めします。Citrix Profile Management サービスの有効化は、必須ではありません。

コマンドラインオプション：/exclude “Citrix User Profile Manager” を使用してコンポーネントがインストールされないようにする

Citrix User Profile Manager WMI Plugin:

このプラグインは、WMI（Windows Management Instrumentation）オブジェクトに格納して、プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用など、Profile Management のランタイム情報を提供します。WMI オブジェクトは、Director にセッション情報を提供します。

コマンドラインオプション：/exclude “Citrix User Profile Manager WMI Plugin” を使用してコンポーネントがインストールされないようにする

Citrix Machine Identity Service:

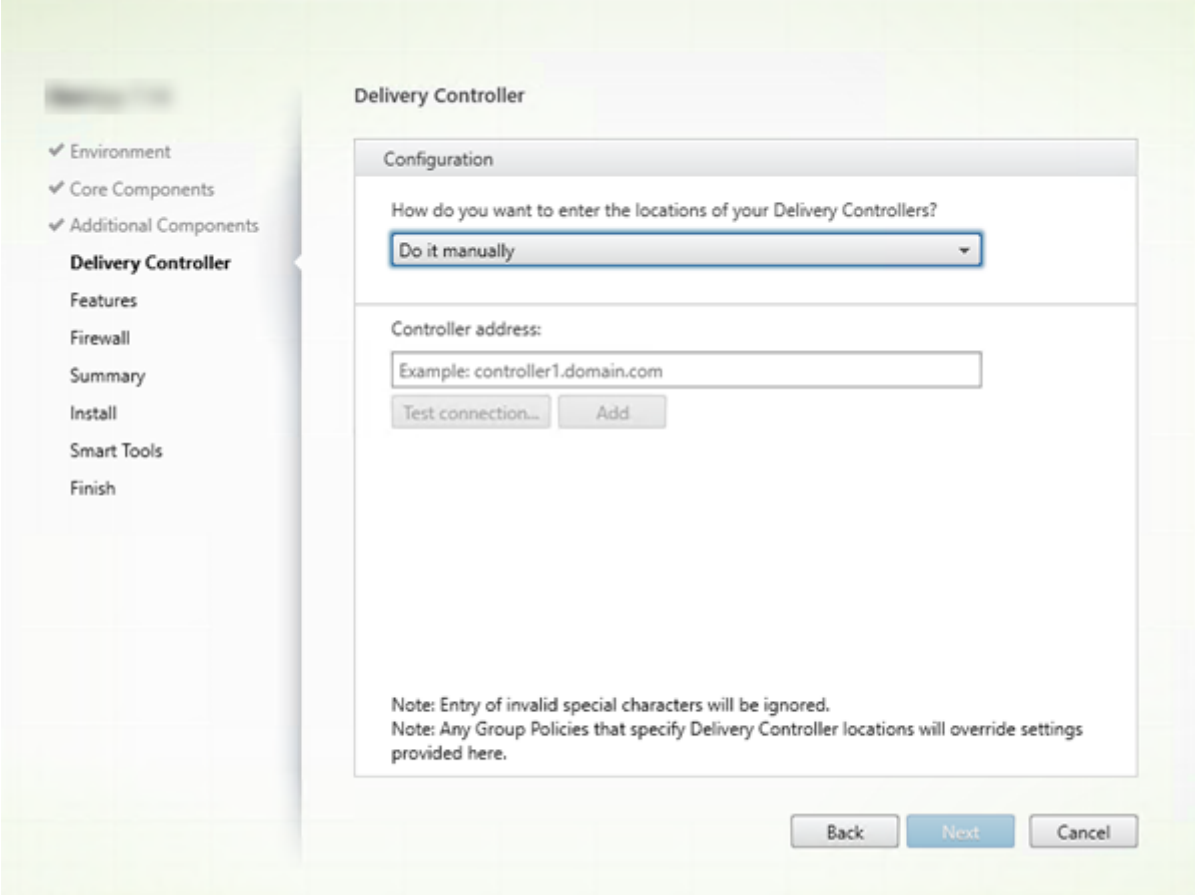
このサービスは、MCS でプロビジョニングしたカタログのマスターイメージを準備します。またプロビジョニングした各マシン固有の Active Directory ID を管理します。

コマンドラインオプション：/exclude “Machine Identity Service” を使用してコンポーネントがインストールされないようにする

グラフィカルインターフェイスでのデフォルト値：

- ［環境］ページで［マスターイメージを作成する］を選択すると（手順 4）、［追加コンポーネント］ページにある項目はデフォルトで有効になります。
- ［環境］ページで［リモート PC アクセスを有効にする］または［サーバーマシンへの接続を有効にする］を選択した場合、［追加コンポーネント］ページにある項目はデフォルトで無効になります。

手順 **8. Delivery Controller** アドレス



[**Delivery Controller**] ページで、インストール済みの Controller のアドレスを入力する方法を選択します Citrix では VDA のインストール時に、アドレスを指定することをお勧めします（[手動で指定する]）。VDA は、この情報がないと Controller に登録できません。VDA が登録されない場合、ユーザーはその VDA 上のアプリケーションやデスクトップにアクセスできません。

- 手動で指定する：（デフォルト）：インストールされている Controller の FQDN を入力し、［追加］をクリックします。追加の Controller をインストールした場合は、アドレスを追加します。
- 後で実行（上級）：このオプションを選択すると、ウィザードは続行する前に、選択を確認するよう求めてきます。後でアドレスを指定する場合は、インストーラーを再実行するか、Citrix グループポリシーを使用することができます。ウィザードは、［概要］ページでも確認を求めます。
- **Active Directory** から場所を選択する：マシンがドメインに参加していて、ユーザーがドメインユーザーである場合にのみ有効です。
- **Machine Creation Services** で自動的に指定する：MCS を使用してマシンをプロビジョニングする場合のみ有効です。

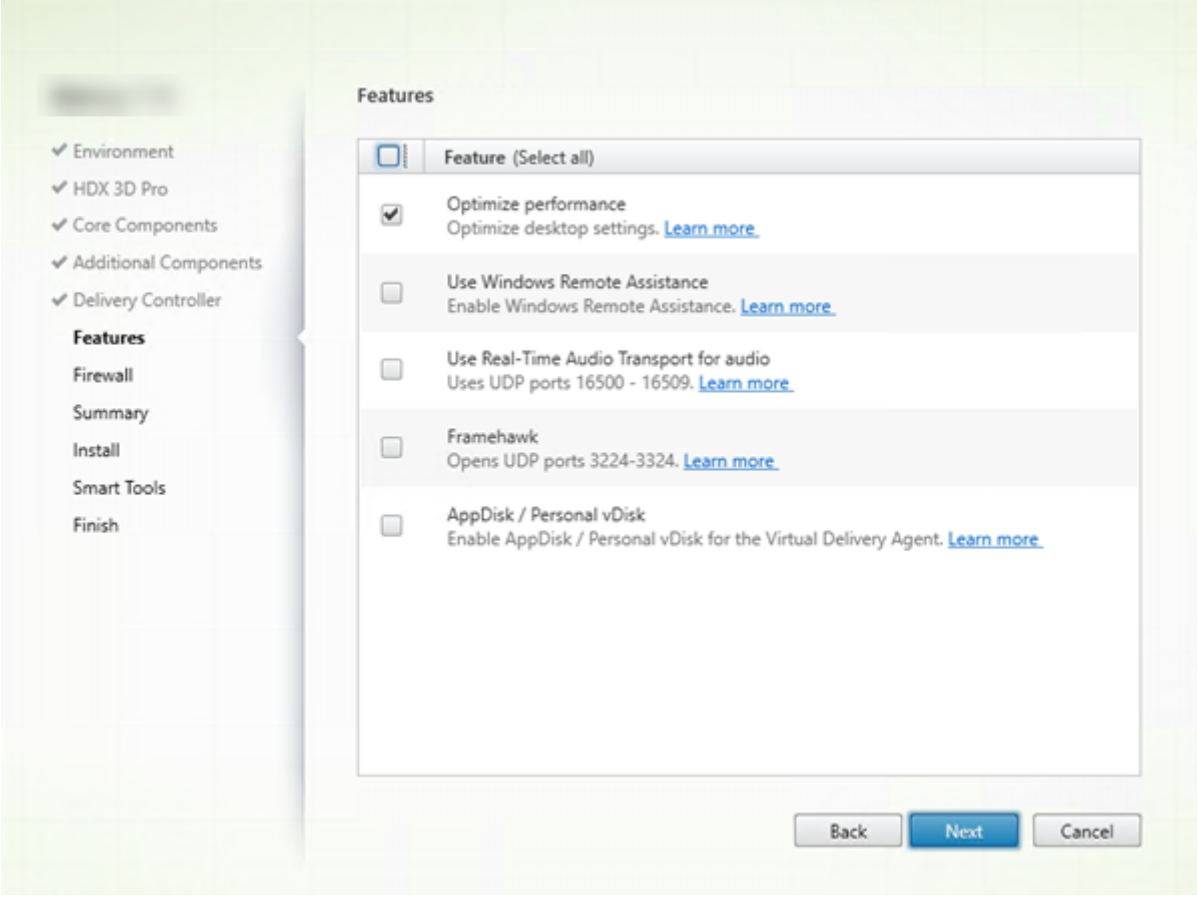
［次へ］をクリックします。［後で実行（上級）］を選択した場合、後でコントローラーのアドレスを指定することを確認するメッセージが表示されます。

そのほかの考慮事項：

- アドレスに { | } ~ [\ ] ^ ‘ : ; < = > ? & @ ! “ # $ % ( ) + / , の文字を含めることはできません。
- VDA のインストールおよびグループポリシーでアドレスを指定すると、インストール中に行われた設定がポリシーの設定によって上書きされます。
- VDA 登録を行うには、Controller を使用した通信に使用されるファイアウォールポートが開いている必要があります。デフォルトでは、ウィザードの ［ファイアウォール］ページでこのポートの開放が有効化されています。
- （VDA のインストール時またはその後に）Controller のロケーションを指定すると、Controller が追加または削除された場合に、自動更新機能を使用して VDA を更新できます。VDA による Controller の検出方法、および VDA を Controller とともに登録する方法について詳しくは、「Delivery Controller」を参照してください。

コマンドラインオプション：/controllers

手順 **9.** 機能を有効または無効にする



［機能］ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

パフォーマンス最適化：

VDA を物理マシンではなく、仮想マシンにインストールしている場合にのみ有効です。この機能を有効にすると（デフォルト）、ハイパーバイザー上の仮想マシンにインストールされる VDA が最適化されます。仮想マシンの最適化に

は、オフラインファイルの無効化、バックグラウンド最適化（デフラグ処理）の無効化、およびイベントログサイズの縮小などの操作が含まれます。詳しくは、CTX224676を参照してください。

コマンドラインオプション：/optimize

VDAWorkstationCoreSetup.exe インストーラーを使用している場合、この機能はウィザードに表示されず、コマンドラインオプションは無効です。リモート PC アクセス環境で他のインストーラーを使用している場合は、この機能を無効にします。

Windows リモートアシスタンスの使用：

この機能を有効にすると、Director のユーザーシャドウ機能で Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。（デフォルト = 無効）

コマンドラインオプション：/enable_remote_assistance

オーディオにリアルタイムオーディオ転送を使用：

ネットワークで Voice over IP が広く使われている場合、この機能を有効化します。この機能を使用すると、遅延が短縮され、損失の多いネットワーク経由の音声復元性が改善されます。オーディオデータを UDP トランスポート経由の RTP を使用して伝送することが可能になります。（デフォルト = 無効）

コマンドラインオプション：/enable_real_time_transport

Framehawk：

この機能を有効にすると、双方向の UDP ポート 3224～3324 が開放されます。（デフォルト = 無効）

ポート範囲は、Citrix ポリシー設定の［Framehawk ディスプレイチャネルポートの範囲］を使用して後で変更できます。その場合は、ローカルファイアウォールポートを開放する必要があります。UDP ネットワークパスは、内部のファイアウォール（VDA から Citrix Receiver または NetScaler Gateway）および外部のファイアウォール（NetScaler Gateway から Citrix Receiver）で開放されている必要があります。NetScaler Gateway が展開されると、Framehawk のデータグラムは DTLS（デフォルトの UDP ポート 443）を使用して暗号化されます。詳しくは、「Framehawk」を参照してください。

コマンドラインオプション：/enable_framehawk_port

AppDisk / Personal vDisk：

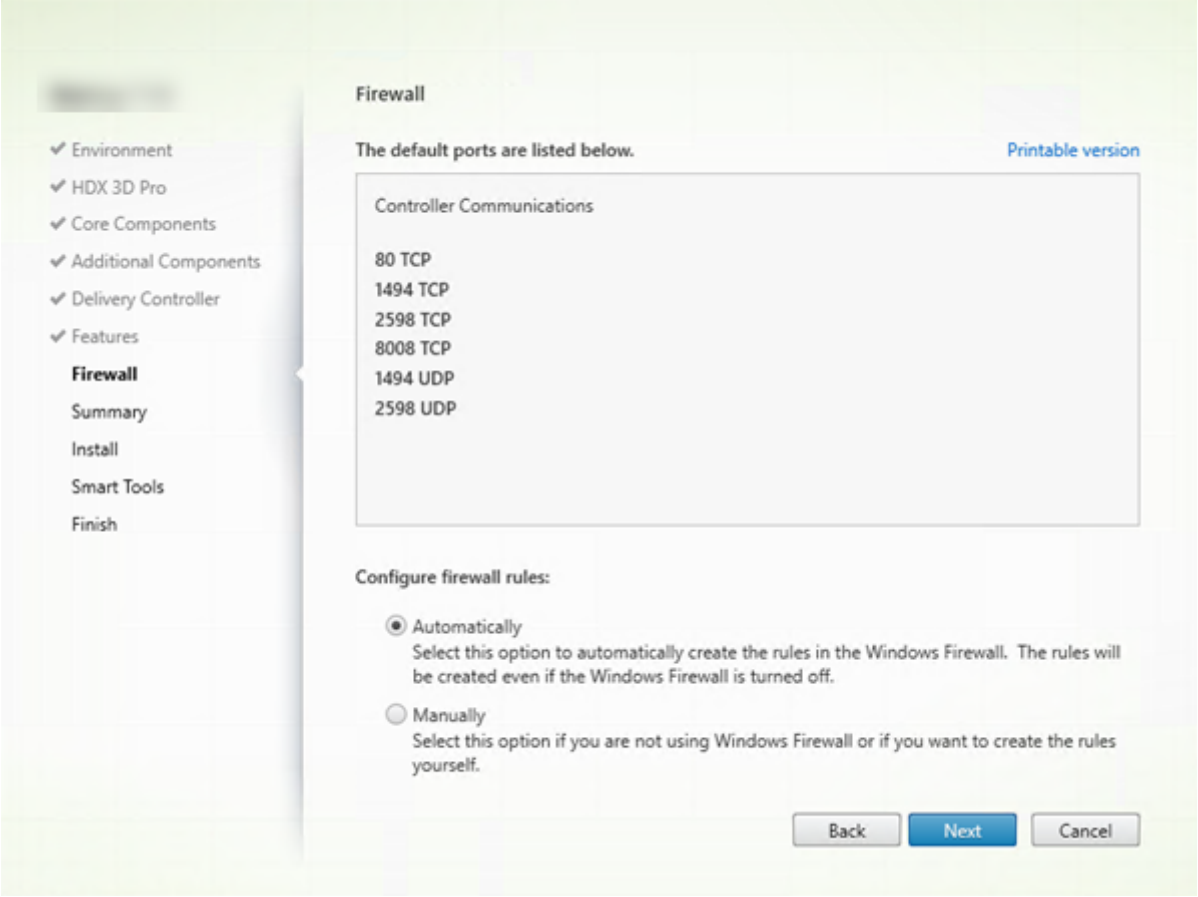
仮想マシン上に VDA for Desktop OS をインストールする場合にのみ有効です。このチェックボックスは、［追加コンポーネント］ページで［Citrix AppDisk / Personal vDisk］チェックボックスがオンになっている場合のみ利用可能です。このチェックボックスをオンにすると、AppDisk および Personal vDisk を使用できます。詳しくは、「AppDisks」および「Personal vDisks」を参照してください。

コマンドラインオプション：/baseimage

VDAWorkstationCoreSetup.exe インストーラーを使用している場合、この機能はウィザードに表示されず、コマンドラインオプションは無効です。

［次へ］をクリックします。

手順 **10.** ファイアウォールポート

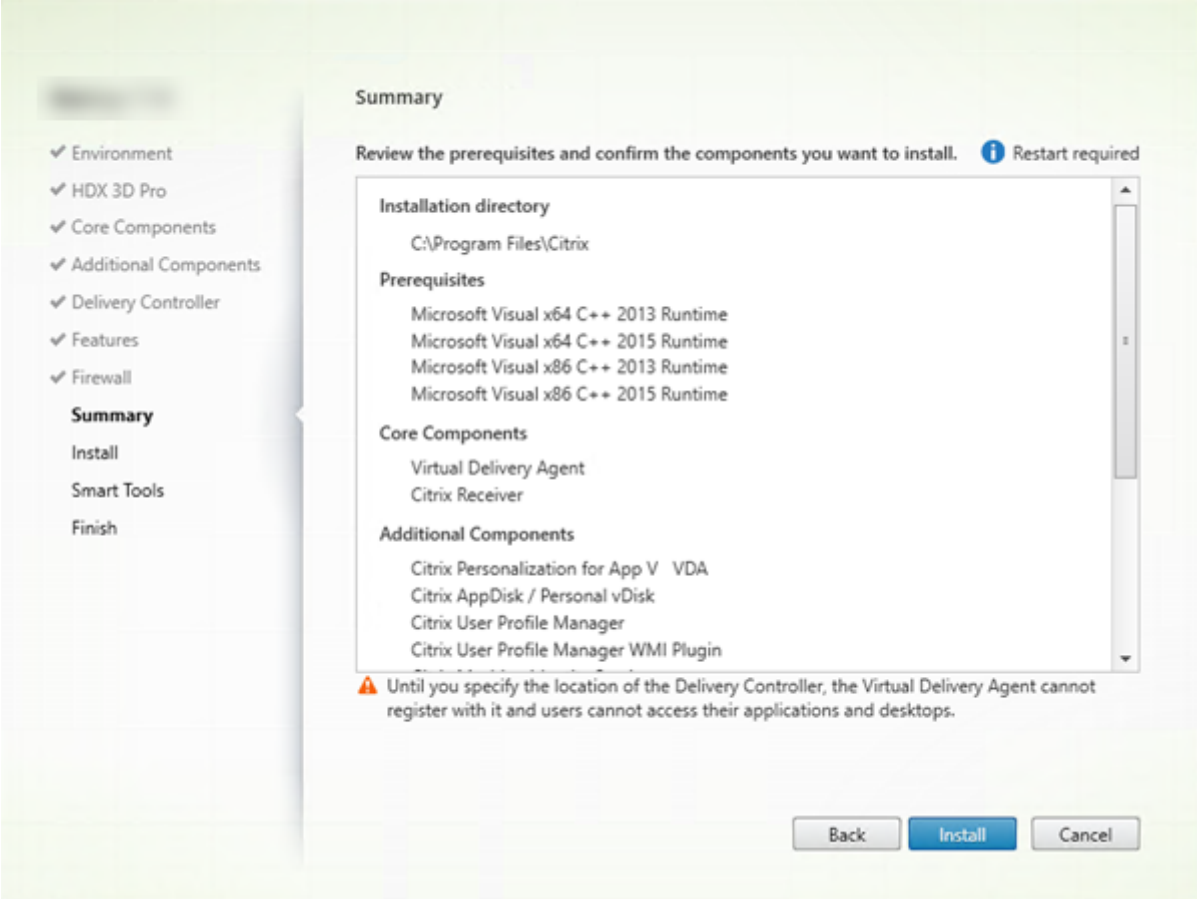


Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、［ファイアウォール］ページに示されているポートがデフォルトで開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートの詳細については、「ネットワークポート」を参照してください。

［次へ］をクリックします。

コマンドラインオプション：/enable_hdx_ports

手順 **11.** インストール前に前提条件を確認する

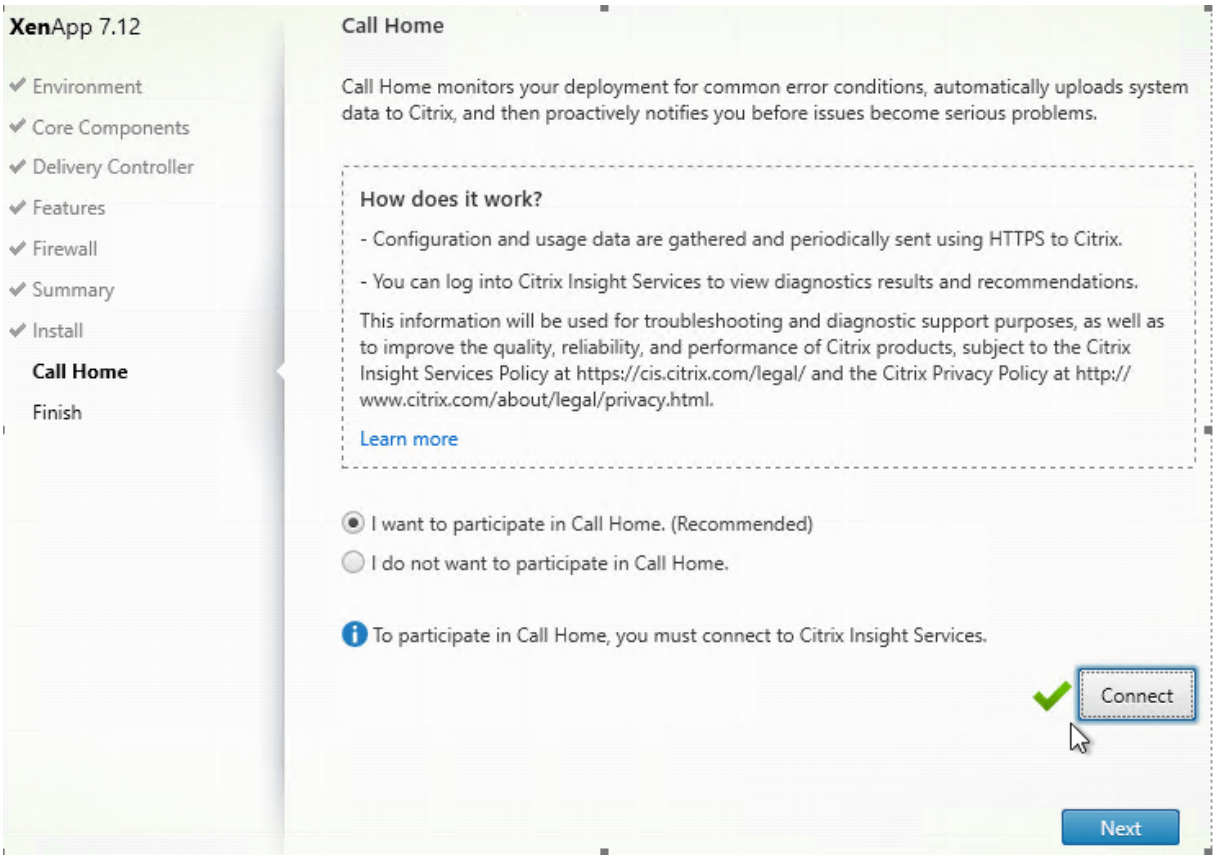


［概要］ページに、インストールされるものが表示されます。［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

準備ができたら、［インストール］をクリックします。

前提条件がまだインストール/有効化されていない場合、マシンが 1～2 回再起動する場合があります。「インストールの準備」を参照してください。

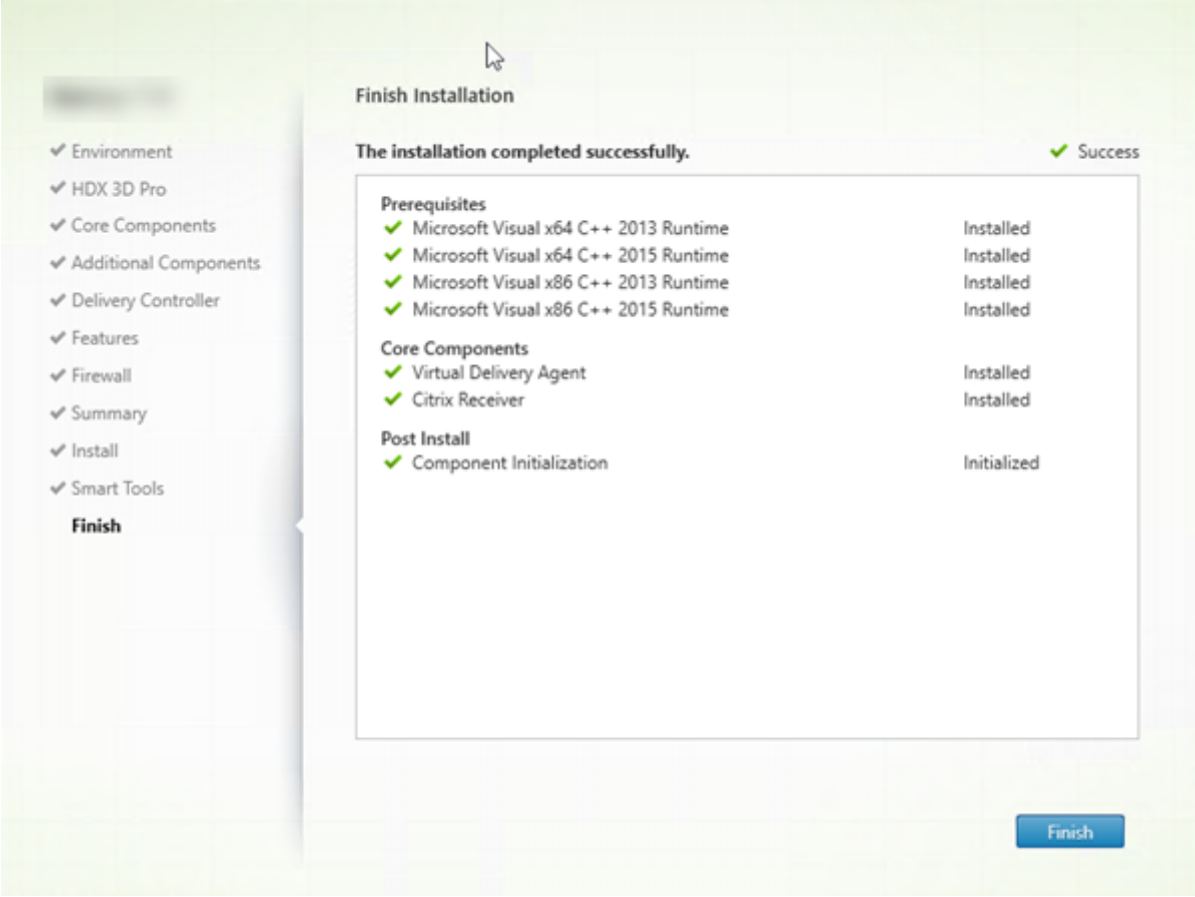
手順 **12. Call Home** に参加する



[**Call Home**] ページで、Call Home に参加するかどうかを選択します。参加することを選択する場合（デフォルト）、[接続] をクリックします。求められたら、Citrix アカウント資格情報を入力します。

資格情報が確認されたら（あるいは参加しないことを選択した場合）、[次へ] をクリックします。

手順 **13**：このインストールを完了する



［完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックします。デフォルトでは、マシンは自動的に再起動します（自動再起動を無効にすることもできますが、マシンを再起動するまで VDA は使用できません）。

次：他の **VDA** をインストールして構成を続ける

必要に応じて上の手順を繰り返し、他のマシンまたはイメージ上に VDA をインストールします。

すべての VDA をインストールしたら、Studio を起動します。サイトをまだ作成していない場合は、Studio のタスクガイドが自動的に表示されます。それが済んだら、Studio のガイドに従ってマシンカタログ、デリバリーグループを作成します。以下の情報も参照してください：

- サイトの作成
- マシンカタログの作成
- デリバリーグループの作成

インストールした後に、VDA をカスタマイズすることもできます。

1. プログラムの削除と変更を行う Windows のコントロールパネルで、[**Citrix Virtual Delivery Agent**] または [**Citrix Remote PC Access/VDI Core Services VDA**] を選択します。次に右クリックして [変更] を選択します。
2. [**Virtual Delivery Agent** 設定のカスタマイズ] を選択します。インストーラーが起動したら、次を変更できます。

- Controller のアドレス
- Controller への登録に使用される TCP/IP ポート（デフォルトは 80）
- Windows ファイアウォールポートを自動的に開放するかどうか

トラブルシューティング

Microsoft System Center Configuration Manager を使用する環境では、VDA のインストールに成功しても終了コード 3 により失敗したというメッセージが表示されることがあります。この不正なメッセージが表示されなくなるようにするには、インストールコマンドを CMD スクリプト内に記述するか、Configuration Manager パッケージの成功コードを変更してください。詳しくは、サポートフォーラムを参照してください。https://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/

デリバリーグループの Studio 表示では、[詳細] ペインの [インストール済み VDA のバージョン] エントリがマシンにインストールされているバージョンではないことがあります。マシンの Windows の [プログラムと機能] には、VDA の実際のバージョンが表示されます。

コマンドラインを使用したインストール

August 24, 2021

この記事は、Windows オペレーティングシステムがインストールされたマシンへのコンポーネントのインストールに適用されます。Linux オペレーティングシステムの VDA については、「Linux Virtual Delivery Agent」を参照してください。

> 重要:
>
> このアーティクルでは、製品のインストールコマンドの実行方法を説明します。インストールを始める前に、「インストールの準備」を読んでください。そのアーティクルには、利用できるインストーラーの説明があります。

コマンドの実行状態を確認して値を返すには、マシンの管理者であるか [管理者として実行] を使用する必要があります。詳しくは、Microsoft 社のコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用するだけでなく、製品 ISO にあるサンプルスクリプトを使用して、Active Directory で VDA マシンをインストール、アップグレード、または削除できます。詳しくは、「スクリプトを使用した VDA のインストール」を参照してください。

全製品インストーラーの使用

全製品インストーラーのコマンドラインインターフェイスへのアクセス:

1. Citrix から製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrix アカウントの資格情報が必要です。
2. ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。
3. ローカルの管理者アカウントを使って、インストール先のサーバーにログオンします。
4. DVD をドライブに挿入するか、ISO ファイルをマウントします。
5. 製品メディアの`\x64\XenDesktop Setup`ディレクトリから適切なコマンドを実行します。

コアコンポーネントのインストール

`XenDesktopServerSetup.exe`コマンドを実行します。これには、「コアコンポーネントのインストールに使用されるコマンドラインオプション」セクションに記載されているオプションを使用します。

VDA のインストール

`XenDesktopVDASetup.exe`コマンドを実行します。これには、「VDA のインストールに使用されるコマンドラインオプション」セクションに記載されているオプションを使用します。

ユニバーサルプリントサーバーのインストール

「コマンドラインを使ったユニバーサルプリントサーバーのインストール」のガイダンスに従ってください。

フェデレーション認証サービスのインストール

グラフィカルインターフェイスを使うことをお勧めします。

セルフサービスパスワードリセットサービスのインストール

セルフサービスパスワードリセットサービスのドキュメントの手順に従います。

スタンドアロン **VDA** インストーラーの使用

ダウンロードサイトにアクセスするには、Citrix アカウントの資格情報が必要です。インストールは、管理者権限（または ［管理者として実行］）で実行する必要があります。

- Citrix から適切なパッケージをダウンロードします:

ダウンロードページ上のコンポーネント名	インストーラーのファイル名
サーバー OS 用 Virtual Delivery Agent < バージョン >	VDAServerSetup.exe
デスクトップ OS 用 Virtual Delivery Agent < バージョン >	VDAWorkstationSetup.exe
デスクトップ OS 用 Core Services Virtual Delivery Agent < バージョン >	VDAWorkstationCoreSetup.exe

- まず、パッケージから既存のディレクトリにファイルを抽出して、インストールコマンドを実行するか、またはただパッケージを実行します。

インストール前にファイルを展開するには、絶対パスを指定して/extractを実行します（例：.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia）。（ディレクトリはあらかじめ存在する必要があります。そうでない場合、抽出は失敗します）。次に、新しいコマンドプロンプトを開いて、抽出先フォルダー（前述の例ではCitrixVDAInstallMedia）でXenDesktopVdaSetup.exeを実行します。「VDA のインストールに使用されるコマンドラインオプション」セクションの有効なオプションを使用してください。

ダウンロードした対象名のパッケージを実行します：VDAServerSetup.exe、VDAWorkstationSetup.exeまたはVDAWorkstationCoreSetup.exe。「VDA のインストールに使用されるコマンドラインオプション」セクションの有効なオプションを使用してください。

全製品インストーラーに慣れている場合：

- スタンドアロンのVDAServerSetup.exeまたはVDAWorkstationSetup.exeは名前以外、XenDesktopVdaSetup.exeコマンドと同じですので、同様に実行してください。
- VDAWorkstationCoreSetup.exeインストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているので異なります。

コアコンポーネントのインストールに使用されるコマンドラインオプション

次のオプションは、XenDesktopServerSetup.exeコマンドを使用してコアコンポーネントをインストールするときに有効です。オプションについて詳しくは、「コアコンポーネントのインストール」を参照してください。

/components <*component*> [,<*component*>] ...

インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します：

CONTROLLER：Controller

DESKTOPSTUDIO：Studio

`DESKTOPDIRECTOR`: Director

`LICENSESERVER`: Citrix ライセンスサーバー

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。

(7.15 LTSR CU6 より前のリリースでは、有効な値に StoreFront が含まれています。バージョン 7.15 LTSR CU6 以降では、「StoreFront のインストール」に記載の StoreFront 専用インストールコマンドを使用します)。

/configure_firewall

Windows ファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても)、インストールされるコンポーネントで使用されるポートが開放されます。サードパーティ製のファイアウォールを使用している場合は、適切なポートを手動で開く必要があります。

/disableexperiencemetrics

Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析の自動アップロードが阻止されます。

/exclude

二重引用符で囲まれた機能、サービス、またはテクノロジをインストールしません。複数の機能、サービス、またはテクノロジを指定する場合は、カンマで区切って、直線の二重引用符で囲みます。以下の値を指定します:

`Local Host Cache Storage (LocalDB)`: ローカルホストキャッシュに使用されるデータベースのインストールが阻止されますこのオプションは、サイトデータベースとして使うために SQL Server Express がインストールされているかには影響しません。

`Smart Tools Agent`: Citrix Smart Tools エージェントのインストールが阻止されます。

> 注:
>
> CU4 以降、Smart Tools はインストーラーに含まれなくなりました。以前のインストールから存在する Smart Tools のインスタンスは変更されません。

/help または /h

コマンドのヘルプを表示します。

/installdir <*directory*>

コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルトは`c:\Program Files\Citrix`です。

/logpath <*path*>

ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。デフォルト値：`"%TEMP%\Citrix\XenDesktop Installer"`

/no_remote_assistance

Director をインストールする場合にのみ有効です。Windows リモートアシスタンス機能を使用するシャドウ機能を無効化します。

/noreboot

インストール後の再起動を無効にします。（ほとんどのコアコンポーネントでは、デフォルトで再起動が無効になっています）。

/nosql

Controller のインストール先サーバーに Microsoft SQL Server Express をインストールしない場合に指定します。このオプションを指定しない場合、SQL Server Express がサイトデータベースとして使用するためにインストールされます。（このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません）。

/quiet または /passive

ユーザーインターフェイスを表示せずにインストールを実行します。インストールプロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

/remove

`/components`オプションで指定したコアコンポーネントを削除します。

/removeall

インストール済みのすべてのコアコンポーネントを削除します。

/sendexperiencemetrics

Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または`/disableexperiencemetrics`が指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

/tempdir <*directory*>

インストール時に一時ファイルを作成するディレクトリを指定します。デフォルト値：c:\Windows\Temp

/xenapp

XenApp をインストールします。このオプションを指定しない場合、XenDesktop がインストールされます。

例：コアコンポーネントのインストール

次のコマンドを実行すると、XenDesktop、Controller、Studio、Citrix ライセンスサーバー、および SQL Server Express がサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

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

次のコマンドを実行すると、XenApp、Controller、Studio、および SQL Server Express がサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

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

VDA のインストールに使用されるコマンドラインオプション

次のオプションは、次の各コマンドの 1 つ以上で使用できます: `XenDesktopVDASetup.exe`、`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、`VDAWorkstationCoreSetup.exe`

/baseimage

仮想マシン上に VDA for Desktop OS をインストールする場合にのみ有効です。マスターイメージで Personal vDisk の使用を有効にします。詳しくは、「Personal vDisk」を参照してください。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合無効です。

/components <*component*>[,<*component*>]

インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します:

`VDA`: Virtual Delivery Agent

`PLUGINS`: Citrix Receiver for Windows（`CitrixReceiver.exe`）

たとえば、Citrix Receiver ではなく、VDA をインストールするには、`/components vda`を指定します。

このオプションを指定しない場合、すべてのコンポーネントがインストールされます。

このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。そのインストーラーは Citrix Receiver をインストールできません。

/controllers “<*controller*> [<*controller*>] [...]”

VDA が通信する Controller の FQDN を、直線の二重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の両方を指定しないでください。

/disableexperiencemetrics

Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析の自動アップロードが阻止されます。

/enable_framehawk_port

Framehawk で使用される UDP ポートを開放します。デフォルト値：false

/enable_hdx_3d_pro

VDA を HDX 3D Pro モードでインストールします。

/enable_hdx_ports

Windows ファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、VDA および有効な機能（Windows リモートアシスタンスは除く）で必要なポートが開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートの詳細については、「ネットワークポート」を参照してください。

HDX アダプティブトランスポートが使用する UDP ポートを解放するには、/enable_hdx_udp_portsと/enable_hdx_portsを指定します。

/enable_hdx_udp_ports

Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、HDX アダプティブトランスポートに必要なポートが Windows ウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートの詳細については、「ネットワークポート」を参照してください。

VDA が使用する別のポートを解放するには、/enable_hdx_portsと/enable_hdx_udp_portsを指定します。

/enable_real_time_transport

オーディオパケットで UDP を使用してパフォーマンスを向上させる機能（リアルタイムオーディオ転送）を有効または無効にします。この機能を有効にすると、オーディオパフォーマンスを向上させることができます。Windows ファイアウォールサービスが検出されたときに UDP ポートが開放されるようにするには、/enable_hdx_portsを指定してください。

/enable_remote_assistance

Director で使用する Windows リモートアシスタンスのシャドウ機能を有効にします。このオプションを指定すると、Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。

/exclude “*<component>*”[,”*<component>*”]

二重引用符で囲まれた、オプションコンポーネントをインストールしません。複数のコンポーネントを指定する場合は、カンマで区切って、直線の二重引用符で囲みます。たとえば、MCS が管理していないイメージ上で VDA をインストールまたはアップグレードする場合、Personal vDisk コンポーネントや Machine Identity Service コンポーネントは必要ありません。以下の値を指定します：

- Personal vDisk
- Machine Identity Service
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization for App-V - VDA

インストール（/exclude "Citrix User Profile Manager"オプションを使用）から Citrix Profile Management を除くと、Citrix Director を使った VDA の監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの ［個人設定］パネル、および ［エンドポイント］ページの ［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと ［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか ［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management サービスをインストールして実行することをお勧めします。Citrix Profile Management サービスの有効化は、必須ではありません。

このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

/h または /help

コマンドのヘルプを表示します。

/hdxflashv2only

セキュリティを強化するため、従来の Flash リダイレクトのバイナリをインストールしません。

このオプションはグラフィカルインターフェイスでは使用できません。

/installdir <*directory*>

コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルトは`c:\Program Files\Citrix`です。

/logpath <*path*>

ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。デフォルト値: `"%TEMP%\Citrix\XenDesktop Installer"`

このオプションはグラフィカルインターフェイスでは使用できません。

/masterimage

仮想マシン上に VDA をインストールする場合にのみ有効です。VDA をマスターイメージとしてセットアップします。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合無効です。

/no_mediafoundation_ack

Microsoft の Media Foundation がインストールされていなければ、複数の HDX マルチメディア機能はインストールされず、動作しないものがあることを認識します。このオプションが省略されていて、Media Foundation がインストールされていない場合、VDA インストールは失敗します。サポートされているほとんどの Windows のエディションには、N エディションの例外を除けば、Media Foundation が既にインストールされています。

/nocitrixwddm

WDDM ドライバーを含まない Windows 7 マシン上でのみ有効です。Citrix WDDM ドライバーのインストールを無効にします。

このオプションはグラフィカルインターフェイスでは使用できません。

/nodesktopexperience

VDA for Server OS をインストールする場合にのみ有効です。デスクトップエクスペリエンス拡張機能を無効にします。この機能の有効/無効は、Citrix ポリシー設定の［デスクトップエクスペリエンス拡張］でも制御できます。

/noreboot

インストール後の再起動を無効にします。VDA は、再起動後にのみ使用できます。

/noresume

デフォルトでは、インストール中にマシンの再起動が必要になった場合、再起動が完了すると自動的にインストーラーが再開します。デフォルトを上書きするには、/noresumeを指定します。これは、メディアを再マウントする必要がある場合、または自動インストール中に情報をキャプチャする必要がある場合に役立ちます。

/optimize

仮想マシン上に VDA をインストールする場合にのみ有効です。ハイパーバイザー上の仮想マシンにインストールする VDA を最適化します。仮想マシンの最適化には、オフラインファイルの無効化、バックグラウンド最適化（デフラグ処理）の無効化、およびイベントログサイズの縮小などの操作が含まれます。リモート PC アクセスの展開では、このオプションを指定しないでください。詳しくは、CTX224676を参照してください。

/portnumber *<port>*

/reconfigオプションを指定する場合にのみ有効です。Virtual Delivery Agent と Controller 間の通信で使用されるポート番号を変更します。変更前のポートは無効になります（ポート 80 を除く）。

/quiet または /passive

ユーザーインターフェイスを表示せずにインストールを実行します。インストールおよび構成プロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

/reconfigure

インストール済みの Virtual Delivery Agent 設定をカスタマイズします。/portnumber、/controllers、または/enable_hdx_portsオプションと一緒に使用します。/quietオプションを指定しない場合は、VDA をカスタマイズするためのグラフィカルインターフェイスが開きます。

/remotepc

リモート PC アクセスの展開でのみ有効です。デスクトップ OS で次のコンポーネントのインストールを除外します。

- Citrix Personalization for App-V
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin

- Machine Identity Service
- Personal vDisk

このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。このインストーラーは、上記のコンポーネントのインストールを自動的に除外します。

/remove

/componentsオプションで指定したコンポーネントを削除します。

/removeall

インストール済みのすべてのコンポーネントを削除します。

/sendexperiencemetrics

Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

/servervdi

Windows サーバー上に VDA for Desktop OS をインストールします。Windows サーバー上に VDA for Server OS をインストールする場合は、このオプションを指定しないでください。このオプションを使用する前に、「サーバー VDI」を参照してください。

このオプションは、全製品 VDA インストーラーでのみ使用します。このオプションはグラフィカルインターフェイスでは使用できません。

/site_guid <*guid*>

サイトの Active Directory 組織単位（OU）のグローバル一意識別子（GUID）を指定します。Active Directory OU ベースの Controller 検出を使用する場合、GUID により仮想デスクトップとサイトが関連付けられます（デフォルトの検出方法である自動更新を使用することをお勧めします）。サイト GUID は、Studio に表示されるサイトプロパティです。/site_guidと/controllersの両方を指定しないでください。

/tempdir <*directory*>

インストール時に一時ファイルを作成するディレクトリを指定しますデフォルトはc:\Windows\Tempです。

このオプションはグラフィカルインターフェイスでは使用できません。

/virtualmachine

仮想マシン上に VDA をインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きして、BIOS 情報を仮想マシンに渡して物理マシンとして振る舞うようにします。

このオプションはグラフィカルインターフェイスでは使用できません。

例：**VDA** のインストール

フル製品インストーラーを使用して **VDA** をインストールする

次のコマンドを実行すると、仮想マシン上のデフォルトの場所に VDA for Desktop OS および Citrix Receiver がインストールされます。この VDA はマスターイメージとして使用されます。VDA は、まず「mydomain」ドメインの「Contr-Main」サーバー上で動作する Controller に登録され、Personal vDisk、最適化機能、および Windows リモートアシスタンスが有効になります。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins
 /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /optimize /
masterimage /baseimage /enable_remote_assistance
```

VDAWorkstationCoreSetup スタンドアロンインストーラーでデスクトップ **OS VDA** をインストールする

次のコマンドは、リモート PC アクセスまたは VDI 展開で使用するためにデスクトップ OS に Core Services VDA をインストールします。Citrix Receiver とその他の非コアサービスはインストールされません。Controller のアドレスが指定され、Windows ファイアウォールサービスのポートが自動的に開放されます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com"/
enable_hdx_ports /noreboot
```

コマンドラインを使った **VDA** のカスタマイズ

VDA をインストールした後で、いくつかの設定をカスタマイズできます。製品メディアの`\x64\XenDesktop Setup`フォルダーから、以下のオプションを指定して「`XenDesktopVdaSetup.exe`」コマンドを実行します（各オプションについては「VDA のインストールに使用されるコマンドラインオプション」を参照してください）。

- `/reconfigure`（VDA をカスタマイズする場合は必須のオプションです）
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber`：ポート
- `/enable_hdx_ports`

コマンドラインを使ったユニバーサルプリントサーバーのインストール

各プリントサーバー上で、次のいずれかのコマンドを実行します。

- サポートされている 32 ビットオペレーティングシステムで、Citrix インストールメディアの\x86\Universal Print Server\ディレクトリから、UpsServer_x86.msiを実行します。
- サポートされている 64 ビットオペレーティングシステムで、Citrix インストールメディアの\x64\Universal Print Server\ディレクトリから、UpsServer_x64.msiを実行します。

プリントサーバーにユニバーサルプリントサーバーコンポーネントをインストールした後で、「プリンターのプロビジョニング」の説明に従って、このコンポーネントを構成します。

スクリプトを使用した **VDA** のインストール

October 22, 2021

この記事は、Windows オペレーティングシステムがインストールされたマシンへの VDA のインストールに適用されます。Linux オペレーティングシステムの VDA については、「Linux Virtual Delivery Agent」を参照してください。

インストールメディアには、Active Directory 環境のマシンで Virtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが収録されています。また、このスクリプトを使って Machine Creation Services および Provisioning Services のマスターイメージを管理することもできます。

以下のアクセス権限が必要です。

- スクリプトを実行するには、VDA インストールコマンドがあるネットワーク共有に対するすべてのユーザーの読み取りアクセスが必要です。インストールコマンドはフルバージョンの製品 ISO の XenDesktopVdaSetup.exe、またはスタンドアロンインストーラーの VDAWorkstationSetup.exe または VDAServerSetup.exe です。
- ログの詳細は各ローカルマシンに保存されます。また、レビューおよび分析のために結果ログをネットワーク上に保存する場合は、そのネットワーク共有に対するすべてのユーザーの読み取りおよび書き込みアクセスが必要です。

スクリプトの実行結果をチェックするには、ネットワーク共有のログを調べます。このログには、スクリプトログ、インストーラーログ、および MSI インストールログが含まれます。各インストールまたは削除に関するログは、日時を示すフォルダー内に保存されます。フォルダー名には、操作の結果として PASS または FAIL のプレフィックスが付きます。失敗したインストールまたは削除処理を検索できるように、ネットワーク共有を使用します。これにより、ターゲットマシンのローカルドライブに代わるツールが提供されます。

> 重要:
>
> インストールを始める前に、「インストールの準備」を読んで、必要なタスクを完了しておいてください。

スクリプトを使って **VDA** をインストールまたはアップグレードする

1. インストールメディアの\Support\AdDeploy\にある InstallVDA.bat サンプルスクリプトを開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します:
   - インストールする VDA のバージョンを指定します（SET DESIREDVERSION）。Version 7 の場合はバージョンを「7.0」と指定できます。完全な値はインストールメディアの ProductVersion.txt ファイルに記述されています（7.0.0.3018 など）。ただし、完全に一致させる必要はありません。
   - 実行するインストーラーのネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指定します。スクリプトにより、適切なバージョンのインストーラー（32 ビットまたは 64 ビット）が自動的に実行されます。たとえば、SET DEPLOYSHARE=\\fileserver1\share1 と指定します。
   - オプションとして、ログを保存するためのネットワーク共有を指定します。例: SET LOGSHARE=\\fileserver1\log1。
   - 「コマンドラインを使ったインストール」の説明に従って、VDA の構成オプションを指定します。/quiet および/noreboot オプションはデフォルトでスクリプトに含まれ、必須です: SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT。
3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDA をインストールするマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、サポートされるオペレーティングシステムの各マシン上に VDA がインストールされます。

スクリプトを使って **VDA** を削除する

1. インストールメディアの\Support\AdDeploy\からサンプルスクリプトの UninstallVDA.bat を開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します。
   - 削除する VDA のバージョンを指定します（SET CHECK_VDA_VERSION）。Version 7 の場合はバージョンを「7.0」と指定できます。完全な値はインストールメディアの ProductVersion.txt ファイルに記述されています（7.0.0.3018 など）。ただし、完全に一致させる必要はありません。
   - オプションとして、ログを保存するためのネットワーク共有を指定します。
3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDA を削除するマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、各マシンから VDA が削除されます。

トラブルシューティング

スクリプトにより、スクリプトの進捗を示す内部ログファイルが生成されます。スクリプトは、展開の開始後すぐに Kickoff_VDA_Startup_Script ログをネットワーク共有にコピーします。これにより、処理全体が実行中であることを確認できます。このログがネットワーク共有にコピーされない場合は、ローカルマシンを調べることでトラブルシューティングを実行します。スクリプトにより、各マシンの%temp% フォルダーに以下の 2 つのデバッグログフ

ァイルが生成されます。

- Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
- VDA_Install_ProcessLog_<DateTimeStamp>.log

これらのログから、次の点を確認します。

- スクリプトが正しく実行されたかどうか。
- ターゲットのオペレーティングシステムが正しく検出されているかどうか。
- DEPLOYSHARE 共有で ROOT（AutoSelect.exe ファイルを含んでいるフォルダー）が正しく構成されているかどうか。
- DEPLOYSHARE および LOG で指定した両方のネットワーク共有にアクセスできるかどうか。

SCCM を使用した VDA のインストール

August 24, 2021

概要

VDA のインストールには、次の 2 つの段階があります:

- インストールの前提条件
- VDA のインストール

Microsoft System Center Configuration Manager（SCCM）または同様のソフトウェア配信ツールを使用して VDA を正常に展開するには、個別に対応することを Citrix ではお勧めします。つまり、VDA インストーラーを使用して前提条件と VDA の両方をインストールするのではなく、最初に前提条件用インストーラーを使用して前提条件をインストールしてから、VDA インストーラーを使用して VDA をインストールすることをお勧めします。

要件とタスクシーケンスの特定

VDA をインストールする前に、前提条件をマシンにインストールする必要があります。VDA の前提条件は、VDA のバージョンによって異なります。ガイダンスについては、インストールする VDA バージョンのシステム要件を参照してください。

- Citrix Virtual Apps and Desktops 最新リリース（CR）
- Citrix Virtual Apps and Desktops 1912 LTSR
- XenApp および XenDesktop 7.15 LTSR

同様に、これらの前提条件のインストールが必要かは、環境によって異なります（たとえば、ターゲットマシンのオペレーティングシステムやマシンに既にインストールされている要素によって異なります）。スクリプトまたはタスクシーケンスを作成する前に、環境固有の要件（インストールする必要のある前提条件など）を理解することが重要です。これによって、タスクシーケンスを適切に定義できます。

ヒント：この情報を収集する最適な方法は、環境内のいずれかのマシンに VDA を手動でインストールすることです。このプロセスでは、VDA のインストールプロセス全体でどの前提条件が必要か、インストール済みかを特定できます。

VDA の前提条件のインストールファイルは、**Citrix Virtual Apps and Desktops**（または **XenApp** および **XenDesktop**）リリースのインストールメディアに含まれます。これらのファイルを使用して、適切な前提条件のバージョンをインストールしていることを確認します。

再起動

前提条件および VDA のインストール中に必要な再起動回数は、環境によって異なります。たとえば、保留中の更新や、以前のソフトウェアのインストールからの再起動には、再起動が必要になる場合があります。また、以前に別のプロセスでロックされていたファイルは、更新が必要な場合があります。

- 手動インストール中に、再起動をトリガーする前提条件を特定します。
- VDA インストーラーの一部のオプションコンポーネント（Citrix User Profile Manager、Citrix Files など）は、再起動が必要な場合があります。手動インストール中に、再起動をトリガーするコンポーネントを特定します。

タスクシーケンスの定義

すべての前提条件と再起動を確認したら、SCCM のタスクシーケンサを使用して次の作業を完了します：

1. 各前提条件をインストールするために個別の SCCM ジョブを作成します。これにより、展開中に発生する問題や障害を切り分けることができ、トラブルシューティングが容易になります。
2. VDA インストールジョブを作成します。すべての前提条件が正常にインストールされるまで、このジョブを実行しないでください。これは、次の 2 つの方法のいずれかで達成できます：
    - SCCM クライアントに前提条件の GUID を監視させて、それらが存在するかどうかを判断させます。
    - VDA のインストールジョブを前提条件のジョブに依存させます。

SCCM インストールシーケンスの例

SCCM インストールシーケンスの例を次に示します。注意：前提条件のバージョンは、インストールする VDA のバージョンによって異なる場合があります。

1. SCCM ジョブ 1：Microsoft .NET Framework 4.8
2. SCCM ジョブ 2：Microsoft Visual C++ 2017 Runtime（32 ビットおよび 64 ビット）
3. SCCM ジョブ 3：VDA のインストール
    a) 要件に応じて、適切な VDA インストーラーコマンドを使用します。`/quiet`、`/noreboot`、`/noresume`オプションを追加します。（`/noresume`オプションを使用すると、インストールの続行を対話型ログインに依存しなくなるため、SCCM でインストールプロセスを実行できます）。
    b) リターンコードに注意してください。
        - `0`：成功、インストール完了、再起動が必要です。

- 3：成功、インストールが完了していません。再起動が必要です。
- 8：成功、インストール完了、再起動が必要です。

c) マシンを再起動してください。

d) リターンコードが3だった場合は、手順 3a を繰り返します。

リターンコードについて詳しくは、「Citrix インストールリターンコード」を参照してください。

VDA インストールコマンドの例

使用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、次の記事を参照してください。(Citrix Virtual Apps and Desktops 最新リリースの場所へのリンクが表示されます。LTSR 製品バージョンを使用している場合は、関連する LTSR の記事を参照してください)。

- VDA のインストール
- コマンドラインを使用したインストール

リモート PC アクセス用のインストールコマンド

- 次のコマンドでは、シングルセッションコア VDA インストーラー(スタンドアロンの VDAWorkstationCoreSetup.exe）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドでは、シングルセッション完全版 VDA インストーラー（スタンドアロンの VDAWorkstationSetup.exe）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドでは、シングルセッション完全版 VDA インストーラー（スタンドアロンの VDAWorkstationSetup.exe）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /optimize /enable_remote_assistance /noresume /noreboot
  ```

サイトの作成

August 24, 2021

「サイト」とは、XenApp または XenDesktop の展開環境に名前を付けたものを指します。サイトは、Delivery Controller などのコアコンポーネント、VDA（Virtual Delivery Agent）、ホストへの接続、およびマシンカタログやデリバリーグループで構成されます。コアコンポーネントをインストールしたら、最初のマシンカタログやデリバリーグループを作成する前に、サイトを作成します。

サイトを作成すると、Citrix のカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIP では、統計情報や使用状況が匿名で収集され、Citrix に送信されます。最初のデータパッケージは、サイトを作成してから約 7 日後に Citrix に送信されます。登録内容は、サイトの作成後いつでも変更できます。Studio のナビゲーションペインで ［構成］を選択し、［製品サポート］タブでガイダンスに従って操作します。詳しくは、「https://more.citrix.com/XD-CEIP」を参照してください。

サイトを作成する管理者には、そのサイトのすべての管理タスクの実行権限が設定されます。詳しくは「管理権限の委任」を参照してください。

サイトの作成ウィザードを開始する前に、この文書を確認してください。

サイトを作成するには

Studio が起動していない場合は起動します。サイトの作成ウィザードを開始する手順が自動的に表示されます。ウィザードページには、以下の構成が含まれます。

サイトの種類と名前

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。サイトを作成すると、その名前が Studio のナビゲーションペインの上部に表示されます：**Citrix Studio**（サイト名）。

データベース

［データベース］ページには、サイト、監視、および構成ログの各データベースを設定するための選択肢が含まれています。データベースセットアップでの選択肢および要件について詳しくは、「データベース」を参照してください。

サイトのデータベースとして使用する目的で SQL Server Express をインストールするように選択した場合（これはデフォルト設定です）、このソフトウェアのインストール後に再起動が行われます。SQL Server Express ソフトウェアをサイトのデータベースとしてインストールしない場合、再起動は行われません。

デフォルトの SQL Server Express を使用しない場合は、サイトを作成する前に、マシンに SQL Server ソフトウェアがインストールされていることを確認してください。サポートされるバージョンについては、「システム要件」を参照してください。

サイトに Controller を追加する必要があり、Controller ソフトウェアが別のサーバーに既にインストールされている場合、このページからこれらの Controller を追加できます。データベースをセットアップするスクリプトを生成する予定の場合には、スクリプトを生成する前に Controller を追加します。

ライセンス

既存のライセンスを使用するか、ライセンスファイルを後から追加できる 30 日間無料のお試し版を使用するかを決定します。サイトの作成ウィザード内で、ライセンスファイルをダウンロードしたりライセンスサーバーに追加したりすることもできます。詳しくは、Citrix ライセンスのドキュメントを参照してください。

ライセンスサーバーのアドレスを、名前:[ポート] という形式で指定します。名前は、FQDN（完全修飾ドメイン名）、NetBIOS、または IP アドレスである必要があります。推奨は FQDN です。ポート番号（<port>）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）

「リモート PC アクセス」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

ハイパーバイザーまたはクラウドサービスで仮想マシンを使用してアプリケーションおよびデスクトップを提供する場合、必要に応じて、ホストへの最初の接続を作成できます。その接続のストレージリソースとネットワークリソースも指定できます。サイトの作成後、この接続やリソースを変更したり、追加の接続を作成したりできます。詳しくは、「接続とリソース」を参照してください。

［接続］ページ：「接続の種類の情報ソース」を参照してください。

- ハイパーバイザーまたはクラウドサービスで仮想マシンを使用している場合（または Studio を使用して専用ブレード PC 上でデスクトップを管理する場合）には、接続の種類として ［なし］を選択します。
- リモート PC アクセスサイトを構成しており、Wake on LAN 機能を使用する予定の場合、［**Microsoft System Center Configuration Manager**］を選択します。

接続の種類に加え、仮想マシンの作成で Citrix のツール（Machine Creation Services など）を使用するか、その他のツールを使用するかも指定します。

［ストレージ］ページと［ネットワーク］ページ：ストレージの種類と管理方法について詳しくは、「ホストストレージ」、「ストレージの管理」、および「ストレージの選択」を参照してください。

そのほかの機能

機能を選択してサイトをカスタマイズできます。情報の入力が必要な項目のチェックボックスをオンにすると、構成ボックスが開きます。

AppDNA 統合

AppDisk を使用していて、AppDNA がインストールされている場合には有効です。AppDNA 統合では、AppDisk 内のアプリケーションを分析できます。互換性の問題を確認し、それらの問題を解決するための修復アクションを実施できます。詳しくは、「AppDisks」を参照してください。

App-V 公開

App-V サーバー上の Microsoft App-V パッケージのアプリケーションを使用する場合は、この機能を選択します。App-V 管理サーバーの URL と、App-V 公開サーバーの URL およびポート番号を入力します。

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 の構成手順を実行します。詳しくは、「Microsoft System Center Configuration Manager」を参照してください。

リモート PC アクセスサイトを作成する場合:

- Wake on LAN 機能を使用している場合、Microsoft System Center Configuration Manager のアドレス、資格情報、および接続情報を［電源管理］ページで指定します。
- ［ユーザー］ページで、ユーザーまたはユーザーグループを指定します。すべてのユーザーを自動的に追加するためのデフォルトの機能はありません。また、［マシンアカウント］ページでマシンアカウント（ドメインおよび OU）情報も指定します。

  ユーザー情報を追加するには、［ユーザーの追加］をクリックします。ユーザーと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。［**OU** 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。［**OU** の追加］をクリックします。

リモート PC アクセスサイトの作成時には、リモート PC ユーザーマシンアカウントという名前のマシンカタログが自動的に作成されます。このカタログには、サイトの作成ウィザードで追加したすべてのマシンアカウントが含まれています。リモート PC ユーザーデスクトップという名前のデリバリーグループが、自動的に作成されます。このグループには、追加したすべてのユーザーおよびユーザーグループが含まれています。

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）］を選択します。中央のペインで、［サイトのテスト］をクリックします。テスト結果は、HTML 形式のレポートで確認できます。

Windows Server 2016 にインストールされた Controller では、サイトのテスト機能がエラーになる場合があります。サイトデータベースにローカルの SQL Server Express が使用され、SQL Server Browser サービスが開始されていない場合にエラーが発生します。このエラーを回避するには、以下のタスクを行います。

1. （必要に応じて）SQL Server Browser サービスを有効にして開始します。
2. SQL Server（SQLEXPRESS）サービスを再開始します。

トラブルシューティング

サイトを成したら、Studio をインストールし、MMC を介してスナップインとしてリモートマシンに追加します。そのスナップインを後に削除しようとすると、MMC の応答が停止する場合があります。この問題が発生した場合は、MMC を再起動してください。

マシンカタログの作成

October 22, 2021

物理マシンまたは仮想マシンのグループは、「マシンカタログ」と呼ばれる単一のエンティティとして管理されます。カタログ内のマシンは、オペレーティングシステムの種類（サーバーまたはデスクトップ）がすべて同じです。サーバー OS マシンを含むカタログには、Windows マシンまたは Linux マシンのいずれかのみを含めることができ、両方を含めることはできません。

サイトを作成した後、Studio では最初のマシンカタログを作成する手順が表示されます。最初のカタログを作成した後、Studio では最初のデリバリーグループを作成する手順が表示されます。作成したカタログを後で変更したり、追加のカタログを作成したりすることができます。

概要

仮想マシンのカタログの作成時には、それらの仮想マシンのプロビジョニング方法を指定します。Machine Creation Services（MCS）や Provisioning Services（PVS）などの Citrix ツールを使用できます。または、独自のツールを使用してマシンをプロビジョニングすることもできます。

- PVS を使用してマシンを作成する場合の手順については、Provisioning Servicesのドキュメントを参照してください。
- MCS を使用して仮想マシンをプロビジョニングする場合、カタログ内に同じ仮想マシンを作成するためのマスターイメージ（またはスナップショット）を提供します。カタログを作成する前に、まずハイパーバイザーまたはクラウドサービスのツールを使用し、マスターイメージを作成して構成します。この処理には、イメージへの Virtual Delivery Agent（VDA）のインストールが含まれます。その後、Studio でマシンカタログを作成します。そのイメージ（またはイメージのスナップショット）を選択し、カタログで作成する仮想マシンの数を指定して、追加情報を構成します。
- マシンが既に提供されており、マスターイメージが必要ない場合でも、マシンに対して 1 つまたは複数のマシンカタログを作成する必要があります。

MCS または PVS を使用して最初のカタログを作成する場合、サイトの作成時に構成したホスト接続を使用します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、その接続に関する情報を変更したり、追加接続を作成したりすることができます。

カタログの作成ウィザードを完了すると、テストが自動的に実行され、正しく構成されているかどうかが検証されます。テストが完了したら、テストレポートを表示できます。Studio からテストをいつでも実行できます。

オンプレミス展開の場合のみ：MCS または PVS を使用して最初のカタログを作成する場合、サイトの作成時に構成したホスト接続を使用します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、その接続に関する情報を変更したり、追加接続を作成したりすることができます。

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。

VDA 登録

仲介セッションを起動する場合、検討対象の Delivery Controller（オンプレミス展開用）または Cloud Connector（Citrix Cloud 展開用）に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない場合がある理由にはさまざまなものがありますが、その多くは管理者がトラブルシューティングできます。Studio では、カタログ作成ウィザードで、マシンをカタログから Delivery Group に登録した後に、トラブルシューティング情報が提供されます。

カタログ作成ウィザードで、既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが示された場合は、該当のマシンを（[削除] ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（登録されたことがないなどの理由により）マシンに関する情報を取得

できないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

機能レベルに関するメッセージについては、「VDA バージョンと機能レベル」を参照してください。

VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

MCS カタログ作成の概要

以下は、カタログの作成ウィザードに情報を入力した後のデフォルトの MCS 操作の簡単な概要です。

- （スナップショットではなく）マスターイメージを選択した場合、MCS でスナップショットが作成されます。
- MCS でスナップショットの完全コピーが作成され、ホスト接続で定義されたストレージの各場所に格納されます。
- MCS によってマシンが Active Directory に追加され、そこで一意の識別子が作成されます。
- ウィザードで指定した数の仮想マシンが MCS によって作成され、各仮想マシンに対して 2 つのディスクが定義されます。1 つの仮想マシンにつき 2 つのディスクに加えて、同じストレージの場所にマスターも保存されます。ストレージの場所が複数定義されている場合、それぞれの場所に以下の種類のディスクが割り当てられます。
  - スナップショットの完全コピー（前述の説明を参照）。読み取り専用であり、作成した仮想マシン間で共有されます。
  - 各仮想マシンに一意の識別子を与える、一意の ID ディスク（16MB）。各仮想マシンに対し、1 つの ID ディスクが割り当てられます。
  - 仮想マシンへの書き込みを保存する、一意の差分ディスク。このディスクは（ホストストレージでサポートされている場合）シンプロビジョニングされ、必要に応じてマスターイメージの最大サイズまで拡大します。各仮想マシンに対し、1 つの差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保存されます。専用デスクトップの場合、この変更は無期限に保存されます。プールされたデスクトップの場合、再起動のたびにこの変更は削除され、新しい変更が作成されます。

または、仮想マシンを作成して静的デスクトップを配信する場合、（カタログの作成ウィザードの ［マシン］ページで）シックな（完全なコピーの）仮想マシンのクローンを指定できます。完全なクローンでは、すべてのデータストアにマスターイメージを保持する必要はありません。各仮想マシンに独自のファイルが存在します。

ハイパーバイザーまたはクラウドサービスでのマスターイメージの準備

ハイパーバイザーおよびクラウドプロバイダーへの接続の作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化しないアプリケーション、VDA、およびそのほかのソフトウェアをインストールしておきます。

ヒント：

- マスターイメージは、「クローンイメージ」、「ゴールデンイメージ」、「ベース仮想マシン」、または「基本イメージ」と呼ばれることがあります。ホストベンダーとクラウドサービスプロバイダーで、異なる用語を使用する場合もあります。

- PVS を使用する場合は、マスターイメージまたは物理コンピューターをマスターターゲットデバイスとして使用できます。PVS でイメージを指す用語は、MCS とは異なります。詳しくは、Provisioning Servicesのドキュメントを参照してください。
- ハイパーバイザーまたはクラウドサービスに、作成されたマシン数に対応する十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションで必要な適切な量のハードディスク領域を構成します。この値は、後で、またはマシンカタログ内で変更することはできません。
- リモート PC アクセスのマシンカタログでは、マスターイメージを使用しません。
- MCS 使用時の Microsoft KMS ライセンス認証に関する注意事項：VDA 7.x を XenServer 6.1、XenServer 6.2、vSphere、または Microsoft System Center Virtual Machine Manager ホストで使用している場合、Microsoft Windows や Microsoft Office のライセンスを手動でリセットする必要はありません。VDA 5.x を XenServer 6.0.2 ホストで使用している場合は、CTX128580を参照してください。
- マスターイメージに以下のソフトウェアをインストールして構成します。
  - ハイパーバイザー用の統合ツール（XenServer Tools、Hyper-V 統合サービス、VMware Tools など）。この手順を省略すると、アプリケーションやデスクトップが正しく動作しなくなる場合があります。
  - VDA。最新の機能を利用できるように、最新バージョンをインストールすることをお勧めします。マスターイメージに VDA をインストールできないと、カタログ作成が失敗します。
  - アンチウイルスプログラムや電子ソフトウェア配信エージェントなどのサードパーティツール（必要に応じて）。ユーザーやマシンの種類に適した設定で、サービス（更新機能など）を構成します。
  - 仮想化せずにユーザーに提供するサードパーティのアプリケーション。ただし、可能な場合はアプリケーションを仮想化することをお勧めします。仮想化することで、アプリケーションを追加したり再構成したりするたびにマスターイメージを更新する必要がなくなり、コストが削減されます。また、各デスクトップにインストールするアプリケーションが少なくなるため、マスターイメージのハードディスクのサイズを減らしてストレージコストを節約できます。
  - App-V アプリケーションを公開する場合は、推奨設定の App-V クライアント。App-V Client は、Microsoft 社から提供されます。
  - MCS で作成したマシンカタログで、ローカライズされた Microsoft Windows を配信する場合は、マスターイメージに言語パックをインストールして言語オプション（システムロケールや表示言語など）を設定しておく必要があります。これにより、プロビジョニング時にスナップショットが作成されると、その言語パックおよび言語オプションが仮想マシンで使用されます。

> 重要：
>
> PVS または MCS を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility（Sysprep）を実行しないでください。

マスターイメージを準備するには

1. ハイパーバイザーの管理ツールを使用して、マスターイメージを作成してから、オペレーティングシステムと、すべてのサービスパックおよび更新プログラムをインストールします。仮想 CPU の数を指定します。また、PowerShell を使用してマシンカタログを作成する場合、仮想 CPU の値を指定することもできます。Studio

を使用してカタログを作成する場合には、仮想 CPU の数は指定できません。デスクトップとアプリケーションで必要な量のハードディスク領域を構成します。この値は、後で、またはカタログ内で変更することはできません。

2. ハードディスクはデバイスの場所「0」で接続されている必要があります。多くの標準マスターイメージテンプレートでは、デフォルトでこの場所にハードディスクが構成されますが、カスタムテンプレートを使用する場合は注意してください。
3. マスターイメージに前述のソフトウェアをインストールして構成します。
4. PVS を使用する場合は、マスターターゲットデバイスをドメインに追加する前に、マスターターゲットデバイスから作成した vDisk の VHD ファイルを作成します。詳しくは、Provisioning Services のドキュメントを参照してください。
5. MCS を使用していない場合、マスターイメージはアプリケーションとデスクトップがメンバーとなっているドメインに統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。MCS を使用している場合、ドメインへのマスターイメージの統合は必要ありません。プロビジョニングされたマシンは、カタログの作成ウィザードで指定されたドメインに統合されます。
6. マスターイメージのスナップショットを作成して、わかりやすい名前を付けておくことをお勧めします。カタログの作成時にスナップショットの代わりにマスターイメージを指定すると、Studio によりスナップショットが作成されますが、そのスナップショットにわかりやすい名前を付けることはできません。

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には、GPU をサポートするビデオカードドライバーが必要です。仮想マシンが GPU を使用して稼働するソフトウェアによって動作できるように、GPU 対応のマシンを構成します。

1. XenCenter を使用して、標準的な VGA、ネットワーク、および vCPU を指定して仮想マシンを作成します。
2. 作成した仮想マシンの構成を変更して、GPU 機能（パススルーまたは仮想 GPU）を有効にします。
3. 仮想マシンに適切なオペレーティングシステムをインストールして、RDP を有効にします。
4. XenServer Tools と NVIDIA ドライバーをインストールします。
5. パフォーマンスを最適化するため、Virtual Network Computing（VNC）Admin Console をオフにして、仮想マシンを再起動します。
6. RDP の使用を確認するメッセージが表示されます。RDP を使用して VDA をインストールし、仮想マシンを再起動します。
7. 必要に応じて、仮想マシンのスナップショットを作成します。このスナップショットは、ほかの GPU マスターイメージのテンプレートとして使用できます。
8. RDP を使用して、XenCenter で構成され、GPU を使用する顧客固有のアプリケーションをインストールします。

Studio でのカタログの作成

カタログの作成ウィザードを開始する前に、このセクションを確認して、選択する項目および指定する情報について理解しておいてください。

マスターイメージを使用している場合、カタログを作成する前に、イメージに VDA がインストールされていることを確認してください。

Studio で以下の操作を行います。

- サイトを作成してもマシンカタログは作成していない場合は、カタログを作成するための説明が表示されます。
- 既存のマシンカタログがあり、別のマシンカタログを作成する場合は、Studio のナビゲーションペインで［マシンカタログ］を選択します。その後、［操作］ペインで ［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、ホストされた共有デスクトップおよびアプリケーションが提供されます。マシンでは、サポートされているバージョンの Windows または Linux オペレーティングシステムを実行できますが、両方をカタログに含めることはできません。（この OS について詳しくは、Linux VDA のドキュメントを参照してください）。
- デスクトップ **OS**：デスクトップ OS のカタログでは、さまざまなユーザーに割り当て可能な VDI デスクトップやアプリケーションが提供されます。
- リモート **PC** アクセス：リモート PC アクセスのカタログでは、オフィスにあるユーザーの物理デスクトップマシンへのリモートアクセスが提供されます。リモート PC アクセスでは、セキュリティを保護するための VPN が不要です。

マシン管理

このページは、リモート PC アクセスカタログを作成するときには表示されません。

［マシン管理］ページでは、マシンの管理方法と、マシンの展開に使用するツールが示されます。

Studio を使用してカタログ内のマシンの電源を管理するかどうかを選択します。

- Studio で電源管理したりクラウド環境でプロビジョニングしたりするマシン（仮想マシンやブレード PC など）。このオプションは、ハイパーバイザーやクラウドサービスへの接続が構成済みの場合にのみ使用可能です。
- Studio で電源管理しないマシン（物理マシンなど）。

マシンが Studio で電源管理されるか、クラウド環境でプロビジョニングされるよう指定した場合、仮想マシンの作成に使用するツールを選択します。

- **Citrix MCS**（**Machine Creation Services**）：マスターイメージを使用して仮想マシンを作成および管理します。クラウド環境内のマシンカタログでは MCS が使用されます。MCS は物理マシンでは使用できません。

- **Citrix PVS**（**Provisioning Services**）：複数のターゲットデバイスを単一のデバイスコレクションとして管理します。マスターターゲットデバイスからイメージ作成された PVS vDisk を使用して、デスクトップとアプリケーションを配信します。このオプションはクラウド展開では使用できません。
- その他：上記以外のツールでデータセンター内の既存のマシンを管理します。この場合、Microsoft System Center Configuration Manager またはほかのサードパーティアプリケーションを使用してカタログ内のマシン構成の一貫性を保つことをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

このページは、デスクトップ OS マシンを含むカタログを作成しているときにのみ表示されます。

［デスクトップエクスペリエンス］ページでは、ユーザーのログオンのたびに行われる処理を指定できます。次のいずれかを選択します。

- ユーザーは、ログオンするたびに新しい（ランダムの）デスクトップに接続されます。
- ユーザーは、ログオンするたびに同じ（静的な）デスクトップに接続されます。

ログイン時に静的デスクトップに接続することを選択した場合、デバイスコレクション画面が表示されます。この接続の種類を確立すると、カタログはマシンの種類のユーザーデータフィールドに Personal vDisk を表示します。

マスターイメージ

このページは、MCS を使用して仮想マシンを作成するときにのみ表示されます。

ホストハイパーバイザーまたはクラウドサービスへの接続を選択してから、過去に作成したスナップショットまたは仮想マシンを選択します。最初のカタログを作成する場合、サイトの作成時に構成した接続のみを使用できます。

注意事項:

- MCS（または PVS）を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility（Sysprep）を実行しないでください。
- スナップショットの代わりにマスターイメージを指定すると、Studio でスナップショットが作成されますが、そのスナッ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。デフォルトで選択されている最小 VDA は変更しないでください。ただし、以前のバージョンの VDA を使用する必要がある場合には、「VDA バージョンと機能レベル」を参照してください。

ウィザードで過去に選択したマシン管理テクノロジとの互換性がないスナップショットまたは仮想マシンを選択すると、エラーメッセージが表示されます。

クラウドプラットフォームとサービス環境

仮想マシンをホストするのにクラウドサービスやプラットフォームを使用している場合（Azure Resource Manager、Nutanix、Amazon Web Services など）、カタログの作成ウィザードにホストに特有の追加ページが含まれることがあります。

詳しくは、「接続の種類に関する情報の参照先」を参照してください。

デバイスコレクション

このページは、PVS を使用して仮想マシンを作成するときにのみ表示されます。このページには、まだカタログに追加されていないデバイスコレクションおよびデバイスが表示されます。

使用するデバイスコレクションを選択してください。詳しくは、Provisioning Services のドキュメントを参照してください。

マシン

このページは、リモート PC アクセスカタログを作成するときには表示されません。

このページのタイトルは、［マシン管理］ページで選択した項目：［マシン］、［仮想マシン］、［仮想マシンとユーザー］によって変わります。

MCS を使ってマシンを作成する場合：

- 作成する仮想マシンの数を指定します。
- 各仮想マシンのメモリ量（MB 単位）を選択します。
- 重要：作成された各仮想マシンにハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- ［デスクトップエクスペリエンス］ページでユーザーによる静的デスクトップへの変更を専用の Personal vDisk に保存することを指定した場合は、vDisk サイズ（GB 単位）とドライブ文字を指定します。
- 環境に複数のゾーンがある場合は、カタログのゾーンを選択できます。
- 静的なデスクトップ仮想マシンを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- Personal vDisk を使用しないランダムなデスクトップ仮想マシンを作成する場合は、各マシンの一時データに対して使用するキャッシュを構成できます。「一時データ用キャッシュの構成」を参照してください。

PVS を使ってマシンを作成する場合：

［デバイス］ページには、前のウィザードページで選択したデバイスコレクションにあるマシンが一覧表示されます。このページでは、マシンを追加または削除することができません。

他のツールを使ってマシンを配信する場合：

Active Directory マシンアカウント名の追加（またはアカウント名一覧のインポート）仮想マシンの Active Directory アカウント名は、追加またはインポートした後に変更できます。［デスクトップエクスペリエンス］ウィザードページで静的なマシンを指定すると、追加する各仮想マシンにオプションで Active Directory ユーザー名を指定できます。

名前を追加またはインポートした後で、［削除］ボタンを使用して、ユーザーはウィザードページ上のままで一覧から名前を削除できます。

PVS または他のツール（**MCS** 以外）を使う場合：

追加（または PVS デバイスコレクションからインポート）される各マシンのアイコンとツールチップは、カタログに追加できない可能性のあるマシン、または Delivery Controller で登録できない可能性のあるマシンの特定に役立ちます。詳しくは、「VDA バージョンと機能レベル」を参照してください。

仮想マシンコピーモード

［マシン］ページで指定するコピーモードによって、MCS がマスターイメージからシン（簡易コピー）クローンまたはシック（完全なコピー）クローンのどちらを作成するかが決まります。（デフォルトはシンクローン）

- 簡易コピークローンは、効率的にストレージを使用し、すばやくマシンを作成したい場合に使います。
- 完全コピークローンは、マシン作成後に IOPS が潜在的に低下した場合に、質の高いデータの復元と移行サポートが必要な場合に使います。

VDA バージョンと機能レベル

カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しい VDA が必要な場合があります。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能がカタログで利用できるようになります。ただし、以前の VDA バージョンのカタログにあるマシンは登録できません。

［マシン］（または ［デバイス］）ページの下部近くにあるドロップダウンを使って、登録できる最小 VDA レベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトで、オンプレミスの展開には最新の機能レベルが選択されます。Citrix の推奨事項に従って VDA とコアコンポーネントを常に最新のバージョンでインストールおよびアップグレードする場合は、この選択を変更する必要がありません。以前の VDA バージョンを使用し続ける必要がある場合は、正しい値を選択してください

XenApp および XenDesktop リリースには、新しい VDA バージョンが含まれないことがあります。または、新しい VDA は、機能レベルに影響を与えません。このような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントより以前の VDA バージョンであることを示します。たとえば、XenApp および XenDesktop 7.15 LTSR には、7.15 VDA が含まれますが、デフォルトの機能レベル（7.9 以降）が最新のまま保持されます。このため、コンポーネントのインストール、または 7.9～7.14 から 7.15 LTSR へのアップグレード後にデフォルトの機能レベルを変更する必要はありません。

(Citrix Cloud の展開では、Studio は最新の機能レベルより古い可能性のあるデフォルトの機能レベルを使用します)。

選択した機能レベルは、このレベルのマシンの一覧に影響します。一覧で、各エントリの横にあるツールチップは、マシンの VDA がその機能レベルでカタログと互換性があるかどうかを示します。

各マシンの VDA が選択した最小機能レベルを満たさない、または超過している場合、ページにメッセージが表示されます。ウィザードは続行できますが、これらのマシンは後で Controller によって登録できない可能性があります。代わりに、以下を行うことができます。

- 古い VDA が含まれるマシンを一覧から削除し、VDA をアップグレードしてからマシンをカタログに追加し直します。
- 低い機能レベルを選択します。ただし、これによって最新の製品機能にアクセスできなくなります。

マシンの種類が正しくないためにマシンがカタログに追加されなかった場合には、メッセージも表示されます。たとえば、デスクトップ OS カタログにサーバーを追加しようとした場合、ランダム割り当て用に作成されたデスクトップ OS マシンを静的マシンのカタログに追加した場合などです。

一時データ用キャッシュの構成

仮想マシンでローカルに行う一時データのキャッシュはオプションです。MCS を使用してカタログ内のプールされた（専用ではない）マシンを管理するときに、マシンの一時データキャッシュの使用を有効にできます。カタログで一時データのストレージを指定する接続を使用する場合は、カタログ作成時に一時データキャッシュ情報を有効にして構成できます。

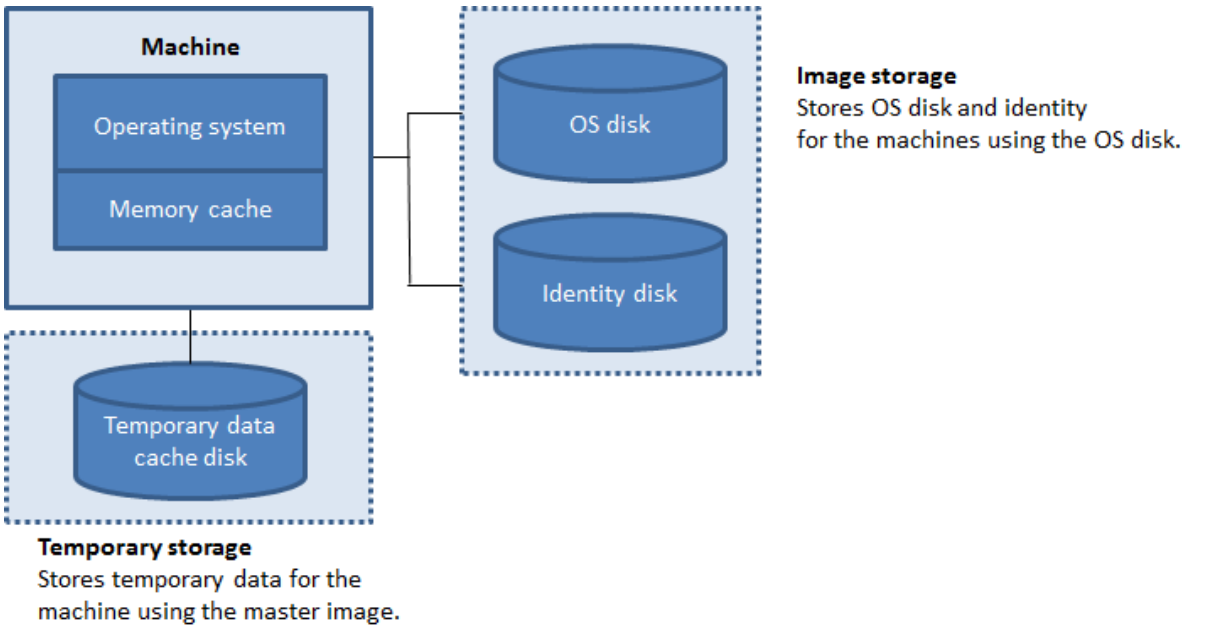
一時データのキャッシュを有効にするには、カタログの各マシンの VDA をバージョン 7.9 以上にする必要があります。

カタログで使用する接続を作成するときに、一時データで共有ストレージとローカルストレージのどちらを使用するかを指定します。詳しくは「接続とリソース」を参照してください。カタログでの一時キャッシュの有効化と構成には、2 つのチェックボックスと値、［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**）］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、構成された制限（［キャッシュに割り当てられたメモリ］の値）に達すると、最も古いデータは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することがあります。サイズはユーザー要件とマシンの負荷に合わせる必要があります。

> 重要：
>
> ディスクキャッシュの容量が不足すると、ユーザーセッションは利用できなくなります。

［ディスクキャッシュサイズ］チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合は、［キャッシュに割り当てられたメモリ］にすべての一時データを格納できる十分に大きい値を指定します。この設定ができるのは、大容量の RAM を各仮想マシンに割り当てられる場合だけです。

両方のチェックボックスをオフにすると、一時データはキャッシュされず、各仮想マシンの差分ディスク（OS ストレージにあります）に書き込まれます。（これは、7.9 より前のリリースでは、プロビジョニングアクションです。）

このカタログを使用して AppDisk を作成しようとしている場合は、キャッシュを有効にしないでください。

Nutanix ホスト接続を使用している場合、この機能は使用できません。

マシンカタログの作成後は、キャッシュ値を変更できません。

ネットワークインターフェイスカード（**NIC**）

このページは、リモート PC アクセスカタログを作成するときには表示されません。

複数の NIC を使用する場合は、各 NIC に仮想ネットワークを関連付けます。たとえば、特定のセキュアネットワークへのアクセスに 1 枚の NIC を割り当てて、より一般的なネットワークへのアクセスに別の NIC を割り当てることができます。また、このページで NIC を追加または削除することもできます。

マシンアカウント

このページは、リモート PC アクセスカタログを作成するときにのみ表示されます。

ユーザーまたはユーザーグループに対応する Active Directory マシンアカウントまたは組織単位（OU）を指定して追加します。組織単位名にはスラッシュ（/）を使用しないでください。

構成済みの電源管理接続を選択するか、電源管理を使用しないことを選択します。電源管理に必要な接続が構成済みでない場合は、マシンカタログの作成後に新しい接続を作成してから、そのマシンカタログを編集して電源管理設定を更新できます。

コンピューターアカウント

このページは、MCS を使用して仮想マシンを作成するときにのみ表示されます。

カタログ内の各マシンには、対応する Active Directory コンピューターアカウントを割り当てる必要があります。新しいアカウントを作成するか既存のものを選択して、アカウントの場所を指定します。

- 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が含まれる 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
…
<!--NeedCopy-->
```

追加するマシンに十分な数のアカウントをインポートする必要があります。これらのアカウントは Studio で管理されるため、すべてのアカウントのパスワードのリセットを Studio に許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

物理マシンまたは既存のマシン用のカタログでは、既存のアカウントを選択またはインポートして、各マシンを Active Directory コンピューターアカウントおよびユーザーアカウントに割り当てます。

PVS で作成されたマシンでは、ターゲットデバイスのコンピューターアカウントは異なる方法で管理されます。詳しくは、Provisioning Services のドキュメントを参照してください。

概要、名前、および説明

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。

トラブルシューティング

サポートチームが解決策を提供するのに役立つログを Citrix で収集することをお勧めします。PVS を使用する場合、以下の手順でログファイルを生成します。

1. マスターイメージで次のレジストリキーを作成し、値（DWORD（32 ビット）の値）を 1 に設定します。

   ```
   HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING
   ```

2. マスターイメージを閉じて、新しいスナップショットを作成します。
3. Delivery Controller で、以下のコマンドを実行します:

   ```
   Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
    -Value $True
   ```

4. このスナップショットに基づいて新しいカタログを作成します。
5. ハイパーバイザーで準備用仮想マシンが作成されたら、ログインして C:\ドライブのルートから次のファイルを抽出します:
   - Image-prep.log
   - PvsVmAgentLog.txt
6. マシンをシャットダウンすると、その時点でエラーが報告されます。
7. 次の PowerShell コマンドを実行して、イメージ準備マシンの自動シャットダウンを再度有効にします。

   ```
   Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
   ```

マシンカタログの管理

November 9, 2020

はじめに

マシンカタログにマシンを追加したり、カタログからマシンを削除したり、マシンカタログの名前や説明を変更したりすることができます。また、カタログの Active Directory コンピューターアカウントを管理できます。

カタログの管理には、最新の OS アップデート、アンチウイルスプログラムのアップデート、オペレーティングシステムのアップグレード、または構成の変更が、各マシンに適用されていることの確認も含めることができます。

- Machine Creation Services（MCS）を使用して作成されたプール（ランダム）マシンが含まれるカタログの場合は、カタログで使用されるマスターイメージを更新してマシンを管理します。マスターイメージの更新後に、マシンを更新します。このプロセスによって、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。

永続インスタンスについて

永続インスタンスまたは専用インスタンスを使用して作成された MCS カタログを更新する場合、カタログで作成された新しいマシンは更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。これを確実にするには、PowerShell コマンドを使用してマスターイメージを更新する必要があります。詳しくは、Knowledge Center の記事CTX129205を参照してください。

他の種類のカタログでも、イメージの更新プロセスは同様です。以下に注意してください:

- 永続ディスクカタログでは、既存のマシンは新しいイメージに更新されませんが、追加されたマシンは新しいイメージを使用します。
- 永続ディスクカタログではない場合、次回のマシンのリセット後にマシンイメージが更新されます。
- 永続マシンカタログでは、イメージを更新するとそのイメージを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、マシンごとに異なるイメージを使用するには、個別のカタログ内にイメージが存在する必要があります。

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。Studio はこれらのアカウントを管理します。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

展開に複数のゾーンがある場合、カタログをゾーン間で移動させることができます。

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ることに注意してください。

1. **Studio** のナビゲーションペインで ［マシンカタログ］を選択します。
2. カタログを選択し、［操作］ペインの ［移動］を選択します。
3. カタログの移動先ゾーンを選択します。

マシンカタログの削除

カタログを削除する前に、以下の点について確認してください：

- すべてのユーザーがログオフしており、実行中の切断セッションがないこと。
- カタログ内のすべてのマシンのメンテナンスモードがオンで、新たに接続できないこと。
- カタログ内のすべてのマシンの電源がオフになっていること。
- そのカタログがデリバリーグループに関連付けられていないこと。すなわち、そのカタログのマシンがデリバリーグループに含まれていないこと。

カタログを削除するには、以下の手順に従います：

1. **Studio** のナビゲーションペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、［操作］ペインの ［マシンカタログの削除］を選択します。
3. カタログ内のマシンを削除するかどうかを指定します。マシンを削除する場合は、マシンの Active Directory コンピューターアカウントを残すか、無効にするか、削除するかを指定します。

マシンカタログにおける **Active Directory** コンピューターアカウントの管理

マシンカタログの Active Directory アカウントについて、次の操作を行えます：

- デスクトップ OS カタログおよびサーバー OS カタログから Active Directory コンピューターアカウントを削除して未使用のマシンアカウントを解放する。解放したアカウントは、ほかのマシンで使用可能になります。

- 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。

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マスターイメージの作成

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. 仮想マシンの電源を切ります。
6. 仮想マシンのスナップショットを作成してわかりやすい名前を付けます。この名前は、Studio でのカタログの更新時に使用されます。Studio でスナップショットを作成することもできますが、ハイパーバイザー側の

管理コンソールでスナップショットを作成し、それを Studio で選択することをお勧めします。これにより、スナップショットに自動生成される名前を付けるのではなく、わかりやすい名前と説明を指定できます。GPU の仮想化機能を使用したマスターイメージを更新する場合は、XenServer の XenCenter を使用する必要があります。

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］ページの情報を確認し、［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。メンテナンスモードの VDA を再起動することはできません。

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

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションのないマシンにも即座に反映されます。現在アクティブなセッションが終了すると、使用中のシステムも更新を受け取ります。以下に注意してください:

- 新しいセッションは、該当するマシンで更新が完了するまで起動できません。
- デスクトップ OS マシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、即座にマシンが更新されます。
- 子マシンがあるサーバー OS の場合、再起動は自動的に行われません。手動でシャットダウンし、再起動する必要があります。

> ヒント:
>
> ホスト接続の詳細設定を使用して、再起動するマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

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。

- 分散時間：すべてのマシンを同時に更新するか、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］ドロップダウンで、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になることがあります。ロールバックした場合、カタログ内のマシンは前回の動作イメージまでロールバックされます。より新しいイメージを必要とする新機能は、利用できなくなります。ロールアウトと同様に、ロールバックでもマシンは再起動されます。

1. **Studio** のナビゲーションペインで ［マシンカタログ］を選択します。
2. 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、VDA をアップグレードします。プロビジョニングコンソールは VDA バージョンを保持しません。Provisioning Services は、XenApp および XenDesktop セットアップウィザードと直接通信して、作成されたカタログに VDA バージョンを設定します。
- アップグレードしたマシンを起動します。これにより、マシンが Controller に登録されます。このときに、そのマシンカタログ内のマシンについてアップグレードが必要かどうかが Studio によりチェックされます。

マシンカタログをアップグレードするには、以下の手順に従います:

1. **Studio** のナビゲーションペインで ［マシンカタログ］を選択します。
2. カタログを選択します。下ペインの ［詳細］タブにバージョン情報が表示されます。
3. ［カタログのアップグレード］を選択します。Studio によりアップグレードが必要なことが検出されると、メッセージが表示されます。画面の指示に従って操作します。アップグレードできないマシンがある場合は、その理由を説明するメッセージが示されます。すべてのマシンを適切に動作させるため、マシンカタログをアップグレードする前にマシンの問題を解決しておくことをお勧めします。

カタログをアップグレードした後でマシンを以前の VDA バージョンに戻すには、カタログを選択し、［操作］ペインの ［元に戻す］を選択します。

トラブルシューティング

マシンの状態が「Power State Unknown」の場合、CTX131267を参照してください。

デリバリーグループの作成

August 24, 2021

デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。デリバリーグループでは、それらのマシンを使用できるユーザーと、そのユーザーに提供するアプリケーションまたはデスクトップ（もしくはその両方）を指定します。

サイトおよびマシンカタログを作成した後、展開の構成における次の手順となるのが、デリバリーグループの作成です。その後、最初のデリバリーグループにおける初期設定を変更し、別のデリバリーグループを作成することができます。また、デリバリーグループの作成時ではなく、その編集時にのみ構成できる機能と設定もあります。

リモート PC アクセスでサイトを作成すると、リモート **PC** アクセスデスクトップという名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには、次の手順に従います：

1. サイトおよびマシンカタログを作成した後でデリバリーグループを作成していない場合は、デリバリーグループを作成するための説明が表示されます。既存のデリバリーグループがあり、別のデリバリーグループを作成する場合は、Studio のナビゲーションペインで ［デリバリーグループ］を選択し、［操作］ペインの ［デリバリーグループの作成］を選択します。
2. デリバリーグループの作成ウィザードが起動され、［はじめに］ページが開きます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、以下のページの操作を行います。各ページの操作を終えたら、最後のページに到達するまで ［次へ］をクリックします。

手順 **1**：マシン

マシンカタログを選択して、そのマシンカタログから使用するマシンの数を選択します。

ヒント：

- マシンカタログに未使用のマシンが残っていない場合、そのカタログを選択することはできません。
- 同じマシンカタログを複数のデリバリーグループで選択することができます。ただし、同じマシンを複数のデリバリーグループで使用することはできません。
- 1 つのデリバリーグループで、複数のマシンカタログのマシンを使用できますが、これらのマシンカタログに同じ種類のマシン（サーバー OS、デスクトップ OS、リモート PC アクセス）が含まれている必要があります。つまり、異なる種類のマシンをデリバリーグループに混在させることはできません。同様に、展開に

Windows マシンのカタログと Linux マシンのカタログが含まれている場合、デリバリーグループには、両方ではなくいずれかの種類のオペレーティングシステムのマシンのみを含めることができます。

- すべてのマシンに最新の VDA バージョンをインストールするか、またはすべてのマシンにおいて VDA を最新バージョンにアップグレードしてから、必要に応じてマシンカタログおよびデリバリーグループをアップグレードすることをお勧めします。デリバリーグループの作成時に、異なる VDA バージョンがインストールされたマシンを選択した場合、デリバリーグループは最も古いバージョンと互換性を持ちます（これは、グループの機能レベルと呼ばれます）。たとえば、選択したマシンの 1 つに VDA Version 7.1 がインストールされており、ほかのマシンには最新バージョンがインストールされている場合、グループ内のすべてのマシンで使用できるのは、VDA 7.1 でサポートされていた機能のみです。すなわち、より新しい VDA バージョンを必要とする機能を、このデリバリーグループで利用できない可能性があります。たとえば、AppDisk の機能を使用するには、VDA（およびグループの機能レベル）のバージョンは 7.8 以上である必要があります。
- リモート PC アクセスマシンカタログの各マシンは、デリバリーグループに自動的に関連付けられます。リモート PC アクセスサイトを作成すると、「リモート **PC** アクセスマシン」という名前のマシンカタログと、「リモート **PC** アクセスデスクトップ」という名前のデリバリーグループが自動的に作成されます。

手順 **2**：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。

手順 **3**：**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（右の列の上にある ［アプリケーション］タブを選択すると、［スタート］メニューと同様の形式でアプリケーションが一覧表示されます。［インストール済みパッケージ］タブを選択すると、［プログラムと機能］リストと同様の形式でアプリケーションが一覧表示されます。）1 つまたは複数のチェックボックスをオンにします。

AppDisks は廃止されました。

手順 **4**：ユーザー

このデリバリーグループで配信されるアプリケーションやデスクトップを使用できるユーザーおよびユーザーグループを指定します。

ユーザー一覧の指定場所

以下の作成時または編集時に、Active Directory ユーザー一覧を指定します。

- サイトのユーザーアクセス一覧（Studio では構成しません）。デフォルトでは、アプリケーション資格ポリシー規則には全ユーザーが含まれます。詳しくは、PowerShell SDK の BrokerAppEntitlementPolicyRule コマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront 経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーション A の使用を構成するには次のように設定します：

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- （アプリケーショングループが構成されている場合）アプリケーション A～L に管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーション A のプロパティを構成します。

認証が必要なユーザーおよび認証が不要なユーザー

ユーザーには、認証が必要なユーザーと認証が不要なユーザーの 2 種類があります（認証が不要なユーザーは「匿名ユーザー」とも呼ばれます）。いずれか一方または両方の種類のユーザーをデリバリーグループ内に構成できます。

認証済み

特定のアカウント名で指定するユーザーおよびグループメンバーは、アプリケーションおよびデスクトップにアクセスするときに StoreFront または Citrix Receiver で資格情報（スマートカード、またはユーザー名とパスワードなど）による認証が必要です（デスクトップ OS マシン用のデリバリーグループでは、デリバリーグループを編集することにより、後でユーザーデータ（ユーザーの一覧）をインポートすることができます）。

認証が不要なユーザー（匿名ユーザー）

サーバー OS マシン用のデリバリーグループでは、StoreFront または Citrix Receiver での認証が不要な匿名アクセスを許可できます。たとえば、キオスクでは、アプリケーション自体での認証が必要な場合がありますが、Citrix のアクセスポータルやツールでは資格情報が要求されません。最初の Delivery Controller をインストールすると、匿名のユーザーグループが作成されます。

認証が不要なユーザーのアクセスを許可するには、デリバリーグループの各マシンに VDA for Windows Server OS (Version 7.6 以降）がインストールされている必要があります。認証が不要なユーザーのアクセスを有効にする場合は、認証が不要な StoreFront ストアを作成しておく必要があります。

認証が不要なユーザーアカウントはセッション開始時にオンデマンドで作成され、AnonXYZ（XYZ は一意の 3 桁の値）という名前が付けられます。

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。

次の表に、［ユーザー］ページでの選択肢を示します：

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

手順 **5**：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。
- アプリケーションを追加すると、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配置されます。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、[**OK**] をクリックします。
- 既存：過去にサイトに追加された、おそらく別のデリバリーグループのアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して [**OK**] をクリックします。
- **App-V**： App-V パッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページで App-V サーバーまたはアプリケーションライブラリを選択します。表示結果からグループに追加するアプリケーションを選択し、[**OK**] をクリックします。詳しくは、「App-V」を参照してください。

あるアプリケーションのソースまたはアプリケーションが選択できない、または無効な場合、そのアプリケーションは見ることができないか、選択できないかのどちらかです。たとえば、サイトに追加されたアプリケーションがない場合、[既存] 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。

手順 **6**：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。

[追加] をクリックします。ダイアログボックスで次の操作を実行します。

- [表示名] と [説明] フィールドで、Citrix Receiver に表示される情報を入力します。
- デスクトップにタグ制約を追加するには、[このタグでマシンの起動を制限します:] を選択し、ドロップダウンからタグを選択します。（詳しくは、「タグ」を参照してください）。
- 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。

手順 **7**：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

August 24, 2021

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. ［ユーザー設定］（または ［基本設定］）ページで、次の表のいずれかの設定を変更します。
4. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

設定	説明
説明	StoreFront でユーザーに表示される説明です。
デリバリーグループの有効化	このデリバリーグループを有効にするかどうかを設定します。
タイムゾーン	タイムゾーンを調整します。

設定	説明
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、ICA プロトコルを暗号化する SecureICA を使用してセキュリティで保護します。デフォルトレベルは 128 ビットです。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. ユーザーを追加する場合は、［ユーザー］ページで ［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 ［一覧のエクスポート］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. ［配信の種類］ページで、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. ［**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。

デスクトップのタグ制約の追加、変更、または削除

タグ制約を追加、変更、および削除すると、どのデスクトップが起動の対象となるかについて、予期しない効果を招くことがあります。「タグ」の記事に記載されている考慮事項と注意を確認してください。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［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］ページでデスクトップを選択し、［編集］をクリックします。
4. タグ制約を追加するには、［次のタグを持つマシンに起動を制約する:］を選択し、タグを選択します。
5. タグ制約を変更または削除するには、異なるタグを選択するか、［次のタグを持つマシンに起動を制約する:］をオフにして、タグ制約を完全に削除します。
6. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

デリバリーグループのアップグレード、またはアップグレードの取り消し

デリバリーグループのアップグレードは、マシン上の VDA、およびデリバリーグループで使用されているマシンを含むマシンカタログをアップグレードしてから行ってください。

デリバリーグループのアップグレードを開始する前に、以下の操作を行います。

- Provisioning Services を使用する環境では、Provisioning Services コンソールで VDA のバージョンをアップグレードします。
- アップグレードした VDA がインストールされているマシンを起動して、Delivery Controller に登録します。この処理によって、デリバリーグループで必要なアップグレードが Studio で特定されます。
- VDA をアップグレードせずに使用を継続すると、新しい製品機能を使用できなくなる場合があります。詳しくは、アップグレードに関連する記事を参照してください。

デリバリーグループをアップグレードするには、次の手順に従います。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［操作］ペインの ［デリバリーグループのアップグレード］を選択します。［配信グループのアップグレード］操作は、Studio がアップグレード済み VDA を検出した場合にのみ表示されます。

アップグレードできないマシンがある場合は、そのマシンとアップグレードできない理由が表示されます。この場合はアップグレードをキャンセルし、マシンの問題を解決してから、アップグレードを再度開始できます。

アップグレードが完了した後でマシンを元の状態に戻すには、デリバリーグループを選択し、［操作］ペインの ［元に戻す］を選択します。

リモート **PC** アクセスのデリバリーグループの管理

リモート PC アクセス用のマシンカタログでユーザーに割り当てられていないマシンは、そのカタログに関連付けられたデリバリーグループに一時的に割り当てられます。この一時的な割り当てにより、そのマシンを後でユーザーに割り当てられるようになります。

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動で割り当てられたマシンを除く）。ユーザーが接続すると、マシンが永続的に割り当てられます。静的なデリバリーグループでは未割り当てマシンの電源を完全に管理できますが、永続的に割り当てられたマシンでは一部の電源管理のみを実行できます。

プールおよびバッファー：未割り当てマシンが含まれる静的なデリバリーグループ、およびプールされたデリバリーグループの場合、（ここでの）「プール」は、電源が入っていてユーザーが接続可能な、未割り当てまたは一時的に割り当てられたマシンのセットを指し、ユーザーがログオンすると直ちにマシンが割り当てられます。プールサイズ（電源が入った状態のマシンの数）は時刻によって構成できます。静的なデリバリーグループでは、SDK を使用してプールを構成します。

「バッファー」は追加の未割り当てマシンの「待機」セットを指し、プール内のマシンの数がデリバリーグループのサイズに対する割合により設定されたしきい値を下回ると、バッファーのマシンの電源がオンになります。大規模なデリバリーグループの場合、このしきい値により多数のマシンの電源がオンになることがあります。このため、デリバリーグループのサイズを小さくするか、SDK を使ってデフォルトのバッファーサイズを調節してください。

電源状態タイマー：電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にすることができます。たとえば、業務時間終了後にユーザーが切断してから 10 分が経過したマシンを自動的に一時停止状態にできます。ランダムなマシンまたは Personal vDisks を使用しているマシンは、ユーザーがログオフすると自動的にシャットダウンします（SDK でデリバリーグループの ShutdownDesktopsAfterUse プロパティを構成している場合を除く）。

平日と週末、ピーク期間とオフピーク期間のタイマーを構成できます。

永続的に割り当てられたマシンの部分的な電源管理：永続的に割り当てられたマシンでは、電源の状態タイマーを設定することはできますが、プールまたはバッファーを設定することはできません。各ピーク時間の開始時にマシンの電源がオンになり、各オフピーク時間の開始時に電源がオフになります。このため、未割り当てマシンの場合とは異なり、使用中のマシンを補うためのマシンの数を詳細に調整できません。

仮想デスクトップ OS マシンの電源を管理するには、次の手順に従います。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［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. ［電源管理］ページの［マシンの電源管理］ボックスで ［**1 -** 平日］を選択します。平日は、デフォルトで月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、［電源をオンするマシン］で ［編集］をクリックして、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. ［ピーク時］で、平日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間およびオフピーク時間の電源状態タイマーを設定します：［ピーク時の電源管理］**>** ［切断時］で、ユーザーが切断してからマシンを一時停止状態にするまでの時間（分）を指定して［一時停止］を選択します。［オフピーク時の電源管理］**>** ［切断時］で、ユーザーがログオフしてからマシンの電源をオフにするまでの時間を指定して ［シャットダウン］を選択します。このタイマーはランダムマシンのデリバリーグループでは使用できません。

7. ［マシンの電源管理］ボックスで ［**2 -** 週末］を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

SDK を使用すると、以下の設定が可能です。

- 電源状態タイマーの設定に基づいてマシンを（一時停止ではなく）シャットダウンする場合や、ユーザーの（切断時ではなく）ログオフ時にタイマーが起算されるように設定する。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にする。CTX217289を参照してください。

デリバリーグループのマシンに対する再起動スケジュールの作成

このセクションでは、Studio で単一の再起動スケジュールを構成する方法について説明します。または、PowerShell を使用して、デリバリーグループ内のマシンの異なるサブセットに対して複数の再起動スケジュールを構成できます。詳しくは、次のセクションを参照してください。

再起動のスケジュールにより、デリバリーグループ内のすべてのマシンを定期的に再起動するタイミングが指定されます。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［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. ［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］ドロップダウンで、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。再起動するまでの分数をメッセージに含める場合は、変数 **<%m%>** を使用します（例：警告：コンピューターは、%*m*%分後に自動で再起動します。）繰り返し通知の間隔を選択すると、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は 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に対する複数の再起動スケジュールの作成

PowerShell コマンドレットを使用して、デリバリーグループ内のマシンに対して複数の再起動スケジュールを作成できます。各スケジュールは、指定されたタグを持つグループ内のマシンだけを対象とするように構成できます。このタグ制約機能を使用すると、デリバリーグループ内のマシンの異なるサブセットに対して複数の再起動スケジュールを簡単に作成できます。

たとえば、社内のすべてのマシンに対して 1 つのデリバリーグループを使用しているとします。すべてのマシンを毎週少なくとも 1 回（日曜日の夜）再起動するようにしたいのですが、経理チームが使用するマシンは毎日再起動する必要があります。すべてのマシンに対して週次スケジュール、および経理チームが使用するマシンだけに日次スケジュールを設定できます。

スケジュールの重複：

複数のスケジュールが重複することがあります。上の例で、経理が使用するマシンは、両方のスケジュールの対象となり、日曜日に二回再起動される可能性があります。

スケジュールコードは、同じマシンを必要以上に再起動しないよう設計されていますが、保証はされません。両方のスケジュールで開始時刻と処理時間が正確に一致する場合、マシンが一度のみ再起動される可能性の方が高そうです。ただし、スケジュールの開始時刻や処理時間が異なるほど、再起動が 2 回起きる可能性が高くなります。また、スケジュールの対象となるマシン数も、重複の可能性に影響します。例では、すべてのマシンを再起動する週次スケジュールは、日次スケジュールより大幅に高速の再起動を開始できました（それぞれについて構成された処理期間により異なる）。

要件：

複数の再起動スケジュールの作成と、再起動スケジュールでのタグ制約の使用のサポートは、現在、XenApp および XenDesktop 7.12 に新しく搭載された RebootScheduleV2 PowerShell コマンドレットを使用する PowerShell コマンドラインでのみ利用できます（これらはこの記事では「V2」コマンドレットと呼ばれます）。

V2 コマンドレットの使用に必要な条件：

- Delivery Controller Version 7.12（最小要件）。
  - 最新の SDK プラグインを 7.12 より前の Controller とともに使用する場合、作成する新しいスケジュールはいずれも意図どおりに機能しません。
  - 混在サイト（一部の、ただしすべてではない Controller がアップグレード済み）では、V2 コマンドレットはデータベースがアップグレードされるまで機能せず、少なくとも 1 つの Controller がアップグレードされ、使用されています（V2 コマンドレットで–adminaddress <controller> パラメーターを指定）。

  - ベストプラクティス：すべてのサイトの Controller がアップグレードされるまで、新しいスケジュールをいっさい作成しません。
- XenApp および XenDesktop 7.12（最小）とともに提供される PowerShell SDK スナップイン。コンポーネントおよびサイトをインストールまたはアップグレードした後、asnp Citrix.* を実行して、最新のコマンドレットをロードします。

Studio は現在、以前の V1 RebootSchedule PowerShell コマンドレットを使用しており、V2 コマンドレットで作成されたスケジュールは表示しません。

タグ制約を使用する再起動スケジュールを作成し、後から Studio を使用して再起動間隔（サイクル）中に対象のマシンからタグを削除するか、再起動サイクル中に追加のマシンにタグを追加した後、それらの変更は次の再起動サイクルまで有効ではありません（変更は現在の再起動サイクルには影響しません）。

PowerShell コマンドレット：

次の RebootScheduleV2 コマンドレットをコマンドラインから使用して複数のスケジュールを作成し、スケジュールでタグ制約を使用します。

- New-BrokerRebootScheduleV2（New-BrokerRebootSchedule を置き換えます）
- Get-BrokerRebootScheduleV2（Get-BrokerRebootSchedule を置き換えます）
- Set-BrokerRebootScheduleV2（Set-BrokerRebootSchedule を置き換えます）
- Remove-BrokerRebootScheduleV2（Remove-BrokerRebootSchedule を置き換えます）
- Rename-BrokerRebootScheduleV2（新しいもの、置き換えられないもの）

完全なコマンドレットの構文およびパラメーターの説明を見るには、「**Get-Help –full** <*cmdlet-name*」と入力します。

用語に関する注意：PowerShell SDK では、DesktopGroup パラメーターは、デリバリーグループを識別します。

再起動スケジュールを作成するための Studio インターフェイスをよく知っている場合、V2 コマンドレットを使用してスケジュールを作成または更新する場合、それらのパラメーターのすべてを利用できます。さらに、以下のことが可能です：

- スケジュールを、指定されたタグを持つマシンに制限する。
- その間は新しいセッションが対象のマシンに仲介されない、最初の警告メッセージを送信するまでの間隔を指定する。

構成：

タグ制約を使用する再起動スケジュールを構成する場合、スケジュールの対象とするマシンにそのタグを追加（適用）する必要もあります（詳しくは、「タグ」を参照してください）。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. スケジュールの対象となるマシンを含むデリバリーグループを選択します。
3. ［マシンの表示］を選択し、タグを追加するマシンを選択します。
4. ［操作］ペインの ［タグの管理］を選択します。

5. タグが既に存在する場合、タグ名の隣にあるチェックボックスをオンにします。タグが存在しない場合は、［作成］をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成したタグ名の隣にあるチェックボックスをオンにします。
6. ［タグの管理］ダイアログボックスの ［保存］をクリックします。

タグを作成、追加（適用）したら、V2 コマンドレットでスケジュールを作成または編集するときに、-RestrictToTag パラメーターを使用してタグ名を指定します。

XenApp または **XenDesktop** の以前のバージョンで再起動スケジュールを作成する場合：

Studio は、現在 V1 RebootSchedule コマンドレットを使用しています。7.12（最小）にアップグレードする前に作成された再起動スケジュールがある場合、引き続き V1 コマンドレットを使用して Studio で管理することができますが、Studio を使用してそのスケジュールにタグ制約を追加したり、追加のスケジュールを作成したりすることはできません（Studio が V2 コマンドレットをサポートしないため）。既存のスケジュールに V1 コマンドレットを使用する限り、再起動スケジュールに関して正しい情報が表示されます。

または、新しい V2 RebootSchedule コマンドレットを使用して、コマンドラインから既存のスケジュールを編集できます。新しい V2 コマンドレットを使用すると、そのスケジュールでタグ制約パラメーターを使用したり、追加の再起動スケジュールを作成したりできます。ただし、V2 コマンドレットを使用して既存のスケジュールを変更すると、Studio には完全なスケジュール情報が表示されません（V1 情報しか認識できないため）。タグ制約が使用されているかどうか、またはスケジュールの名前と説明は表示されません。

```
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
```

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ルール］ページで、ユーザーあたりのデスクトップの最大値を設定します。
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、［サーバー負荷指数］列は表示されません。［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］カテゴリの［負荷指数］を選択します。

SDK では Get-BrokerMachine コマンドレットを使用します。詳しくは、CTX202150を参照してください。

［負荷指数］列に値 10000 が表示される場合、そのサーバーが負荷限界状態であることを示しています。ほかに使用可能なサーバーがない場合は、ユーザーがセッションを起動したときに、デスクトップまたはアプリケーションを使用できないという内容のメッセージが表示されます。

同時ログオントレランスのポリシー設定：サーバーが同時に処理できるログオン要求の最大数です。この設定項目は、Version 7.5 より前の XenApp の「負荷調整」に相当します。

すべてのサーバーが同時ログオントレランスの設定値に達した場合、それ以降のログオン要求は保留中のログオン数が最も少ないサーバーに割り当てられます。同時ログオントレランスの設定値に達しないサーバーがいくつか存在する場合は、負荷指数が最小のサーバーにログオン要求が割り当てられます。

デリバリーグループからのマシンの削除

デリバリーグループからマシンを削除しても、そのデリバリーグループで使用するマシンカタログからは削除されません。このため、そのマシンをほかのデリバリーグループに割り当てることができます。

マシンを削除する前に、マシンをシャットダウンする必要があります。デリバリーグループから削除せずにマシンを一時的に使用できなくする場合は、そのマシンをメンテナンスモードにしてからシャットダウンしてください。

マシンには個人データが保存されている可能性があります。このため、そのマシンを別のユーザーに割り当てる場合は注意が必要です。マシンをイメージから再作成することをお勧めします。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択し、［操作］ペインの ［マシンの表示］を選択します。
3. マシンがシャットダウン状態であることを確認します。
4. ［操作］ペインの ［デリバリーグループから削除］を選択します。

マシンが使用する接続からも、デリバリーグループからマシンを削除できます。詳しくは、「接続とリソース」を参照してください。

デリバリーグループのマシンへのアクセス制限

デリバリーグループでマシンへのアクセス制限を変更した場合、使用する方法にかかわらず既存の設定より優先されます。次の操作を実行できます:

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次のコマンドを使用します: **Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -**

ワイルドカード文字としてアスタリスク（*）を使用し、同じポリシー式で始まるタグをすべて一致させることもできます。たとえば、タグ「VPDesktops_Direct」が追加されたマシンと、タグ「VPDesktops_Test」が追加されたマシ

ンの両方をフィルターの対象にする場合は、Set-BrokerAccessPolicy スクリプトでタグとして「VPDesktops_*」を指定します。

Web ブラウザーを使用している、またはストアで統合 Citrix Receiver ユーザーエクスペリエンス機能を有効にして接続している場合、クライアント名除外フィルターは使用できません。

デリバリーグループのマシンの更新

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択し、［操作］ペインの ［マシンの表示］を選択します。
3. マシンを選択して、［操作］ペインの ［マシンの更新］を選択します。

別のマスターイメージを選択するには、［マスターイメージ］を選択し、スナップショットを選択します。

変更内容を適用し、マシンのユーザーに通知するには、［エンドユーザーへのロールアウト通知］を選択します。次に、マスターイメージの更新タイミング（即時または次回再起動時）、再起動を分散させる時間（グループのすべてのマシンの更新を開始するまでの合計時間）、ユーザーに再起動を通知するかどうか、およびユーザーに送信されるメッセージを指定します。

セッションをログオフまたは切断する

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 ［マシンの表示］を選択します。
3. 中央のペインでマシンを選択し、［操作］ペインで［セッションの表示］を選択して、セッションを選択します。
    - または、中央のペインで ［セッション］タブを選択し、セッションを選択します。
4. ユーザーをセッションからログオフするには、［操作］ペインの ［ログオフ］をクリックします。セッションが終了し、ユーザーがログアウトされます。ほかのユーザーがそのマシンを使用できるようになります（そのマシンが特定のユーザーに割り当てられてない場合）。
5. セッションを切断するには、［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引き続きセッション内で実行され、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。

デスクトップ OS マシンでは、電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にしたりシャットダウンしたりすることができます。詳しくは、「マシンの電源管理」セクションを参照してください。

デリバリーグループへのメッセージの送信

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. デリバリーグループを選択して、［操作］ペインの ［マシンの表示］を選択します。
3. 中央のペインで、メッセージを送信するマシンを選択します。
4. ［操作］ペインで ［セッションの表示］を選択します。

5. 中央のペインですべてのセッションを選択し、［操作］ペインで ［メッセージの送信］を選択します。
6. メッセージを入力して ［**OK**］をクリックします。必要に応じて、重要度のレベルを指定できます。オプションには ［重要］、［質問］、［警告］、［情報］があります。

または、Citrix Director を使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」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。

注意事項:

- これらの機能を使用するには、デリバリーグループでアプリケーションが配信されている必要があります。また、マシンで VDA for Server OS 7.6 以降が動作している必要があります。
- これらの機能は Citrix Receiver for Windows を使用している場合にのみサポートされ、Citrix Receiver 側での構成も必要です。詳しくは、適切なバージョンの Receiver for Windows の eDocs ドキュメントで「セッションの事前起動」を検索してください。
- Citrix Receiver for HTML5 はサポートされないことに注意してください。
- セッションの事前起動を使用するときに、ユーザーのマシンが「一時停止」または「休止」状態の場合は、（セッションの事前起動設定にかかわらず）事前起動が機能しません。ユーザーはマシンやセッションをロックできますが、ユーザーが Citrix Receiver からログオフすると、セッションが終了し、事前起動は適用されません。
- セッションの事前起動を使用するときは、物理クライアントマシンでは一時停止または休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックすることはできますが、ログオフすることはできません。
- 事前起動セッションと残留セッションは、接続されている間のみライセンスを消費します。使用されない事前起動セッションと残留セッションは、デフォルトで 15 分後に切断されます。この値は PowerShell（New/Set-BrokerSessionPreLaunch コマンドレット）で構成できます。
- これらの機能が相互に補完し合うよう調整するには、ユーザーの使用状況を監視して慎重に計画することが重要です。最適に構成することで、ライセンス消費やリソース割り当ての効率化とユーザーの利便性を両立させることができます。
- Citrix Receiver 側では、セッションの事前起動を有効にする時間帯を構成できます。

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 や ［デリバリーグループの編集］ページにそのデリバリーグループのタイムアウトが表示されなくなります。

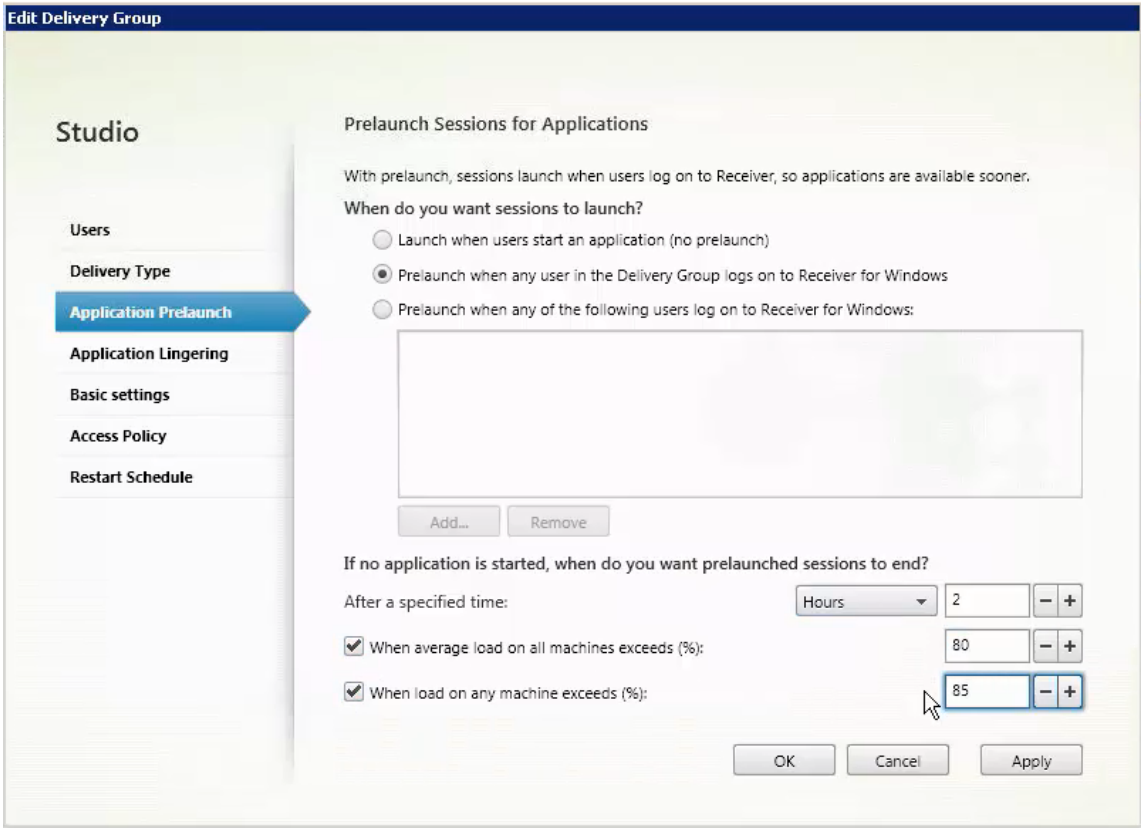
- しきい値：サーバーの負荷が高くなったときに事前起動セッションや残留セッションを自動的に終了することができます。これにより、サーバーの負荷が低い間は可能な限りセッションが保持されます。新しいユーザーセッション用のリソースが必要になったときに事前起動セッションや残留セッションが自動的に終了するため、これらのセッションが原因で接続が拒否されることはありません。

  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 1 つずつセッションが終了します。しきい値を超えている間は、新たな事前起動セッションは開始されません。

Controller に登録されていない VDA が動作するサーバーやメンテナンスモードのサーバーは、負荷限界状態として認識されます。サーバーで計画外の停止状態が発生した場合、事前起動セッションや残留セッションは自動的に終了してリソースが解放されます。

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。



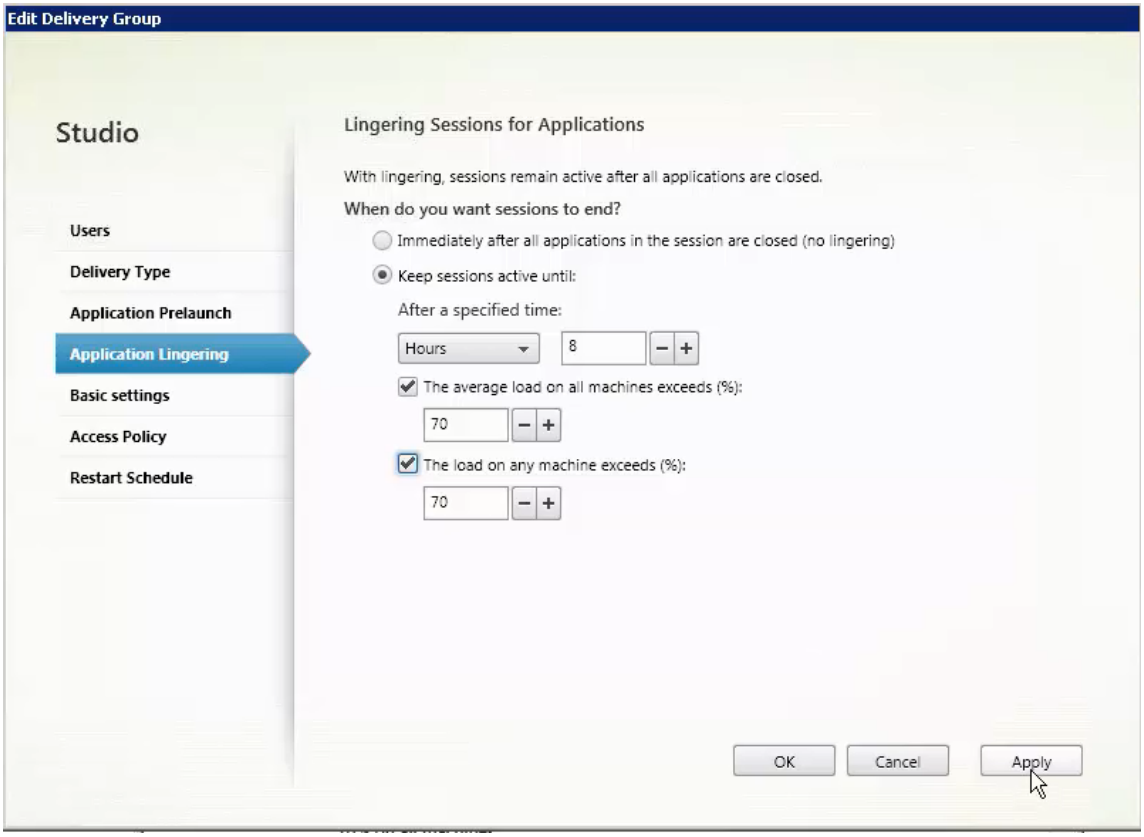
4. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。

    - 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。

    要約：残留セッションは、次のいずれかの状態が発生するまで保持されます：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。

トラブルシューティング

- Delivery Controller で登録されていない VDA は、仲介されたセッションの起動時に考慮されず、利用可能なリソースが十分に活用されなくなります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Studio ではカタログ作成ウィザードで、またはカタログをデリバリーグループに登録した後に、トラブルシューティング情報を提供します。

  デリバリーグループを作成すると、そのグループと関連付けられているマシンの詳細が Studio に表示されます。デリバリーグループの［詳細］ペインに、登録の必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードでないはないのに、Controller に現在登録されていないマシンが 1 台または複数台存在することが考えられます。「未登録だが登録する必要がある」のマシンが表示された

場合は、［詳細］ペインの［トラブルシューティング］タブで、考えられる原因と推奨される修正アクションを確認します。

機能レベルに関するメッセージについては、「VDA バージョンと機能レベル」を参照してください。VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

- デリバリーグループの Studio の表示では、［詳細］パネルの［インストール済み VDA のバージョン］が、マシンにインストールされている実際のバージョンと異なる可能性があります。マシンの Windows の［プログラムと機能］には、VDA の実際のバージョンが表示されます。
- マシンの状態が「Power State Unknown」の場合、CTX131267を参照してください。

アプリケーショングループの作成

August 24, 2021

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代わりの手段となります。デリバリーグループは複数のアプリケーショングループに関連付けることができ、アプリケーショングループは複数のデリバリーグループに関連付けることができます。

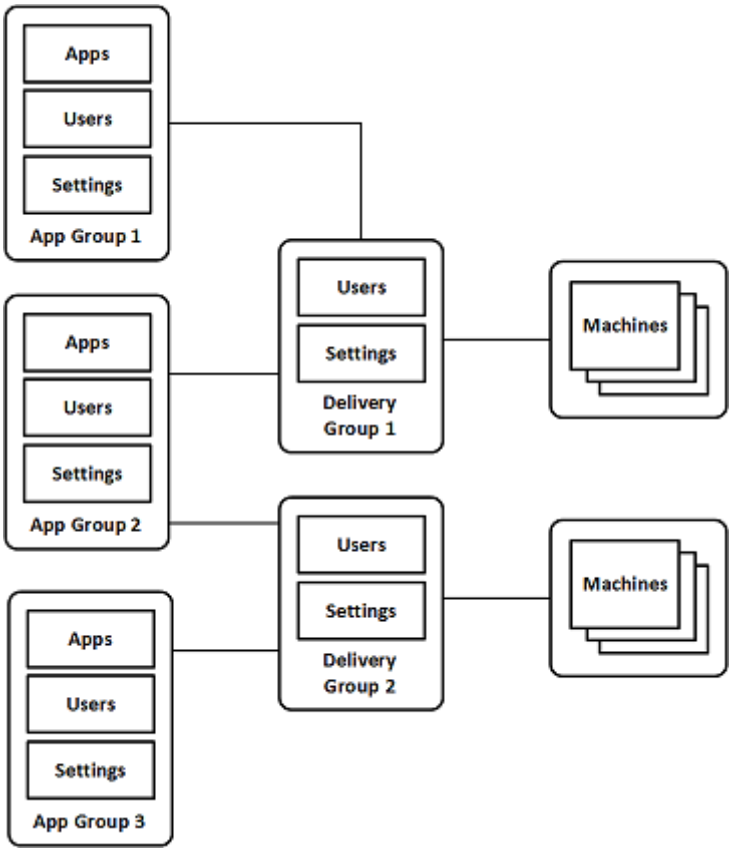
アプリケーショングループの使用は、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします。

- アプリケーションおよびその設定を論理的にグループ化することで、アプリケーションを 1 つの単位として管理することができます。たとえば、同じアプリケーションをそれぞれのデリバリーグループに 1 つずつ追加（公開）する必要はありません。
- アプリケーショングループ間でのセッション共有により、リソースの消費を削減できます。また、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループからアプリケーションを公開できます。タグ制約で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制約は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。タグ制限のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

構成例

例 **1**

次の図は、アプリケーショングループを含む XenApp または XenDesktop 環境を示しています:



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。)

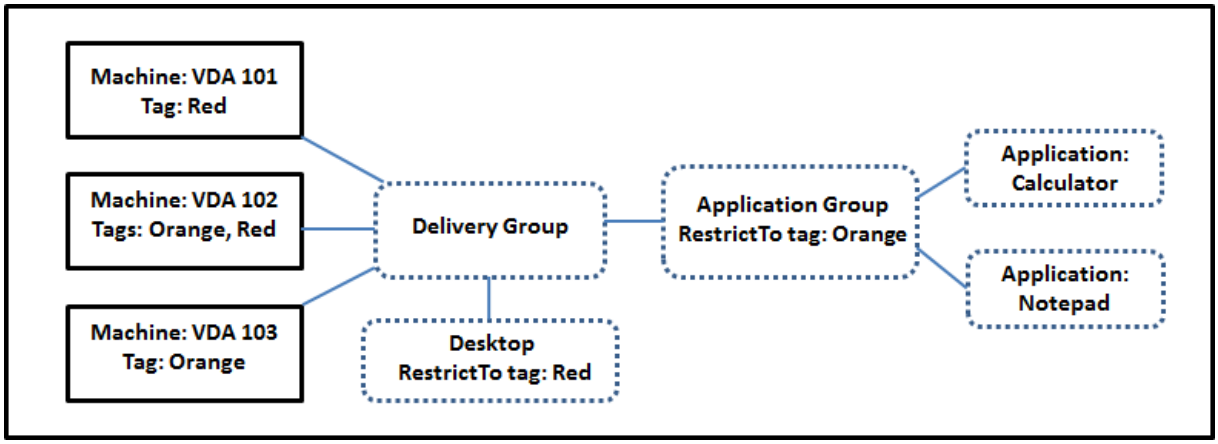
アプリケーショングループ 1 はデリバリーグループ 1 に関連付けられています。アプリケーショングループ 1 のアプリケーションには、アプリケーショングループ 1 で指定されているユーザーが、デリバリーグループ 1 のユーザー一覧にも含まれている限り、アクセスできます。これは、アプリケーショングループのユーザー一覧は関連付けられているデリバリーグループのユーザー一覧のサブセット(制限)でなければならないというガイダンスに従っています。アプリケーショングループ 1 の設定(アプリケーショングループ間で共有されるアプリケーションセッション、関連付けられているデリバリーグループなど)は、このグループ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。

例 **2**

この単純なレイアウトでは、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグ制約を使用して制限します。サイトには、1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



3 台のマシン（VDA 101～103）それぞれにタグが追加されています。

アプリケーショングループは「Orange」のタグ制約で作成されているので、各アプリケーション（計算機とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン：VDA 102 および 103 上でのみ起動できます。

アプリケーショングループ（およびデスクトップ）でのタグ制限の使用に関する包括的な例やガイダンスは、「タグ」を参照してください。

ガイダンスおよび考慮事項

Citrix は、アプリケーショングループとデリバリーグループの両方にではなく、どちらか一方にアプリケーションを追加することをお勧めします。両方に追加すると、アプリケーションを 2 種類のグループに追加することにより複雑度が増加し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループが有効になっています。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間でのアプリケーションセッションの共有が有効になっています。「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。「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに関連付けると表現することで、このアクションと、利用可能なソースからアプリケーションの新しいインスタンスを追加することを区別しています。同様に、デリバリーグループはアプリケーショングループに関連付けられ、アプリケーショングループはデリバリーグループに関連付けられます。追加されるのでも、お互いのコンポーネントになるのでもありません。

アプリケーショングループを使用したセッション共有

アプリケーションセッション共有を有効にすると、すべてのアプリケーションが同一のアプリケーションセッションで起動されるようになります。これにより、追加のアプリケーションセッションの起動にかかるコストが抑えられるとともに、クリップボードを使用するアプリケーション機能（コピーアンドペーストなど）を使用できます。ただし、セッション共有の無効化が必要になる場合もあります。

アプリケーショングループを使用する場合、以下の 3 通りの方法でアプリケーションセッション共有を構成して、デリバリーグループのみを使用ときに利用できる標準的なセッション共有の動作を拡張できます。

- アプリケーショングループ間でセッション共有を有効にする。
- 同一のアプリケーショングループに含まれるアプリケーション間でのみセッション共有を有効にする。
- セッション共有を無効にする。

アプリケーショングループ間のセッション共有

アプリケーショングループ間のアプリケーションセッション共有を有効にすることも、この共有を無効化して、アプリケーションセッション共有を同一のアプリケーショングループに含まれるアプリケーションのみに限定することもできます。

アプリケーショングループ間のセッション共有を有効にすることが役立つ例:

- アプリケーショングループ 1 には、Word や Excel などの Microsoft アプリケーションが含まれています。アプリケーショングループ 2 にはメモ帳や電卓などその他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーションへのアクセス権を持つユーザーが、Word を起動してアプリケーションセッションを開始してから、メモ帳を起動するとします。Controller により、このユーザーの Word が実行されている既存のセッションがメモ帳の実行にも適していると判断されると、メモ帳は既存のセッション内で起動されます。メモ帳を既存のセッションで実行できない場合（タグ制約によりセッションの実行元のマシンが除外されている場合など）、セッション共有を使用せず適切なマシン上に新しいセッションが作成されます。

アプリケーショングループ間のセッション共有を無効にすることが役立つ例:

- 同じソフトウェアスイートの 2 つの異なるバージョンや、同じ Web ブラウザーの 2 つの異なるバージョンなど、同時に使用することがあまりない一連のアプリケーションが同じマシンにインストールされています。管理者は、同じセッションで両方のバージョンを起動することをユーザーに許可しないほうがいいと考えました。

ソフトウェアスイートの各バージョン用にアプリケーショングループを 1 つ作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追加しました。これらの各アプリケーショングループでグループ間のセッション共有を無効にすると、各グループで指定されたユーザーは同じセッションで同じバージョンのアプリケーションを実行でき、同時に他のアプリケーションを別のセッションで実行できます。ユーザーが異なるバージョンのアプリケーション（異なるアプリケーショングループに含まれるアプリケーション）を起動するか、アプリケーショングループには含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。完全に信頼することはできず、ユーザーが別の手段（Windows エクスプローラーなど）を使用してセッションにアプリケーションを起動することは防げません。

マシンがフル稼働の場合、そのマシンで新しいセッションは開始されません。新しいアプリケーションは、必要に応じてセッション共有を使用し、既存のセッション内で起動されます（この動作が、ここで説明するセッション共有の制限に従っている場合）。

事前起動セッションは、アプリケーションセッション共有が許可されているアプリケーショングループでのみ利用できます（残留セッション機能を使用するセッションは、すべてのアプリケーショングループで利用できます）。これらの機能は、アプリケーショングループに関連付けるデリバリーグループごとに有効にして構成する必要があります。これらの機能をアプリケーショングループで構成することはできません。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は、アプリケーショングループ作成時に有効にされます。グループを作成しているときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内でのセッション共有の無効化

同一のアプリケーショングループに含まれるアプリケーション間で、アプリケーションセッション共有を無効にすることができます。

アプリケーショングループ内のセッション共有を無効にすることが役立つ例:

- ユーザーが別々のモニターで、アプリケーションの複数の全画面セッションへ同時にアクセスできるようにする場合。

  アプリケーショングループを作成して、そのグループにアプリケーションを追加する場合。アプリケーショングループ内のアプリケーション間でのセッション共有が禁止されている場合、グループ内で指定されたユーザーは別々のセッションでアプリケーションを 1 つずつ起動することになり、各アプリケーションを個別のモニターに移動することができます。

デフォルトでは、アプリケーションセッション共有はアプリケーショングループの作成時に有効にされます。グループを作成しているときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループの作成

アプリケーショングループを作成するには:

1. Studio のナビゲーションペインで ［アプリケーション］を選択し、次に［操作］ペインで ［アプリケーショングループの作成］を選択します。
2. アプリケーショングループの作成ウィザードが起動され、［はじめに］ページが開きます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、以下のページの操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。

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］リストには、選択可能なデリバリーグループが含まれています。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］リストには、選択できないデリバリーグループが含まれています。各エントリで、静的に割り当てられたマシンを含む、などの互換性がない理由が説明されます。

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

また、(1) デリバリーグループに共有マシンが含まれていてこのグループが XenDesktop 7.x バージョンで作成されており、かつ (2) ［デリバリーグループの編集］権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれるデリバリーグループを選択することもできます。アプリケーショングループの作成ウィザードをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

おそらくはアプリケーションを整理したり現在は使用されていないアプリケーションのストレージとして使用したりするために、デリバリーグループに関連付けないアプリケーショングループを作成することができますが、アプリケーショングループで少なくとも 1 つのデリバリーグループを指定するまでは、そのアプリケーショングループを使用してアプリケーションを配信することはできませんまた、デリバリーグループが指定されていない場合は、［［スタート］メニューから］ソースからアプリケーショングループにアプリケーションを追加することもできません。

選択するデリバリーグループで、アプリケーションの配信に使用するマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制約を追加するには、［タグでマシンの起動を制限します:］を選択し、ドロップダウンからタグを選択します。詳細については、「タグ」を参照してください。

ユーザー

アプリケーショングループのアプリケーションを使用できるユーザーを指定します。1 つ前のページで選択したデリバリーグループのすべてのユーザーとユーザーグループに許可するか、このデリバリーグループの特定のユーザーと

ユーザーグループを選択することができます。指定したユーザーの使用を制限した場合は、デリバリーグループとアプリケーショングループで指定したユーザーだけが、このアプリケーショングループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザー一覧は、デリバリーグループのユーザー一覧のフィルターとして機能します。

認証されていないユーザーによるアプリケーション使用の有効化または無効化は、デリバリーグループでのみ行えます。アプリケーショングループではできません。

ユーザー一覧の指定場所

以下の作成時または編集時に、Active Directory ユーザー一覧を指定します。

- デリバリーグループの使用権を持つユーザーの一覧。この一覧は Studio では構成されません。デフォルトでは、アプリケーション資格ポリシー規則には全ユーザーが含まれます。詳しくは、PowerShell SDK の BrokerAppEntitlementPolicyRule コマンドレットを参照してください。
- アプリケーショングループのユーザー一覧。
- デリバリーグループのユーザー一覧。
- アプリケーション可視性プロパティ。

StoreFront 経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーション A の使用を構成するには次のように設定します。

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- アプリケーション A～L に管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーション A のプロパティを構成します。

アプリケーション

ヒント：

- アプリケーションを追加すると、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配置されます。別のフォルダーを指定することもできます。アプリケーションの追加時に、そのフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された一意の名前を受け入れると、アプリケーションにその新しい名前が追加されます。受け入れない場合は、提案された名前を自分で変更して、追加できるようにする必要があります。詳しくは、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。「アプリケーションプロパティの変更」を参照してください。2 つのアプリケーションを同じ名前で同じユーザーに公開する場合は、Studio

で［アプリケーション名（ユーザー用）］プロパティの名前を変更します。これを行わないと、ユーザーの Citrix Receiver に同じ名前が 2 つ表示されます。

- アプリケーションを複数のアプリケーショングループに追加する場合、そのすべてのアプリケーショングループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したグループをすべて含めるようにします。

［追加］ボックスをクリックして、アプリケーションのソースを表示します。

- ［スタートから］メニュー：選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。このソースは、（1）デリバリーグループが関連付けられていないアプリケーショングループを選択した、（2）マシンを含まないデリバリーグループが関連付られているアプリケーショングループを選択した、（3）マシンを含まないデリバリーグループを選択した、のいずれかの場合には選択できません。
- 手動で定義：サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。これらの情報を入力したら、［**OK**］をクリックします。
- 既存：以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。このソースは、サイトにアプリケーションが含まれていない場合は選択できません。
- **App-V**： App-V パッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページで App-V サーバーまたはアプリケーションライブラリを選択します。結果表示で、追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。詳しくは、App-Vを参照してください。このソースは、サイトで App-V を構成していない場合は選択できません（表示されないこともあります）。

上述のとおり、［追加］ボックスの特定のエントリは、そのタイプの有効なソースがない場合は選択できません。互換性のなソースは、一切表示されません。たとえば、アプリケーショングループにアプリケーショングループは追加できないため、このソースはアプリケーショングループ作成時には表示されません。

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、すべてのスコープが選択されています。詳しくは、「管理者権限の委任」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

August 24, 2021

はじめに

この記事では、作成済みのアプリケーショングループの管理手順について説明します。

以下の操作方法を含む、アプリケーショングループまたはデリバリーグループでのアプリケーションの管理について詳しくは、「アプリケーション」を参照してください:

- アプリケーショングループのアプリケーションの追加または削除
- アプリケーショングループの関連付けの変更

アプリケーショングループの管理には、組み込みの役割であるデリバリーグループ管理者の委任管理権限が必要です。詳しくは、「委任管理」を参照してください。

アプリケーショングループの有効化または無効化

アプリケーショングループを有効にすると、このグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、グループ内のアプリケーションもすべて無効になります。ただし、これらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合は、これらの他のアプリケーショングループから配信できます。同様に、アプリケーションが（アプリケーショングループへの追加に加えて）アプリケーショングループに関連付けられているデリバリーグループに明示的に追加されている場合は、アプリケーショングループを無効にしても、これらのデリバリーグループに追加されたアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。これをグループの作成時に変更することはできません。

1. Studio のナビゲーションペインで ［アプリケーション］を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループを有効にする］チェックボックスをオンまたはオフにします。
4. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループ間でのアプリケーションセッション共有の有効化または無効化

アプリケーショングループ間でのセッション共有は、アプリケーショングループの作成時に有効になります。これをグループの作成時に変更することはできません。アプリケーションセッション共有について詳しくは、「アプリケーション間のセッション共有」を参照してください。

1. Studio のナビゲーションペインで ［アプリケーション］を選択します。

2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループ間のアプリケーションのセッション共有を有効にします］チェックボックスをオンまたはオフにします。
4. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループ内のアプリケーションのセッション共有を無効にします

同じアプリケーショングループのアプリケーション間のセッション共有は、アプリケーショングループを作成した場合、デフォルトで有効です。アプリケーショングループ間でのアプリケーションセッション共有を無効化しても、同じアプリケーショングループのアプリケーション間のセッション共有は引き続き有効です。Broker PowerShell SDK を使用して、所属するアプリケーション間のセッション共有を無効化したアプリケーショングループを構成できます。状況によっては、この機能が望ましい場合もあります：たとえば、ユーザーが複数の非シームレスアプリケーションを個別のモニターのフルサイズのアプリケーションウィンドウで起動できるようにする場合などです。アプリケーションセッション共有について詳しくは、「アプリケーション間のセッション共有」を参照してください。

アプリケーショングループ内でのアプリケーションセッション共有を無効にした場合、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。適切な切断されたセッションで同じアプリケーションが動作中の利用可能なセッションがあれば、そのセッションが再接続されます。たとえば、Notepad を起動する場合、Notepad が動作中の切断されたセッションがあれば、新しいセッションを作成しないでそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、そのうちの 1 つのセッションが再接続先として、ランダムだが決定的な方法で選択されます。同じ状況で同じ状態が再現した場合は、同じセッションが選択されます。しかし、そうでない場合は再接続されるセッションは、予測できるとは限りません。
Broker PowerShell SDK を使用して、既存のアプリケーショングループのすべてのアプリケーションでアプリケーションセッション共有を無効化するか、アプリケーションセッション共有を無効化したアプリケーショングループを作成できます。

PowerShell コマンドレット例

セッション共有を無効化するには、Broker PowerShell コマンドレットの **New-BrokerApplicationGroup**、または **Set-BrokerApplicationGroup** を **-SessionSharingEnabled** パラメーターを False に、**-SingleApp-PerSession** パラメーターを True に設定して実行します。

たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効のアプリケーショングループを作成するには、以下を実行します。

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession
 $True
```

たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効化するには、以下を実行します。


```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession
 $True
```

> メモ:
>
> - SingleAppPerSession プロパティを有効化するには、SessionSharingEnabled プロパティを False に設定する必要があります。この 2 つのプロパティは、同時に有効化してはなりません。Session-SharingEnabled パラメーターは、アプリケーショングループ間のセッション共有に関するものです。
> - アプリケーションセッション共有は、アプリケーショングループに割り当てられているが、デリバリーグループには割り当てられていないアプリケーションに対してのみ有効です。(デリバリーグループに直接割り当てられているアプリケーションはすべてデフォルトでセッションを共有します)。
> - 1 つのアプリケーションが複数のアプリケーショングループに割り当てられている場合、グループどうしで設定が矛盾(たとえば、同じオプションを一方は True に、他方は False に設定しているような場合)しないようにしてください。予想のつかない動作を引き起こします。

アプリケーショングループ名の変更

1. Studio のナビゲーションペインで [アプリケーション] を選択します。
2. 中央ペインでアプリケーショングループを選択し、[操作] ペインで [アプリケーショングループ名を変更します] を選択します。
3. 新しい一意の名前を指定し、[**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。優先順位（0 が最高）を入力し、[**OK**]をクリックします。
7. [適用]をクリックして行った変更を適用しウィンドウを開いたままにするか、[**OK**]をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのタグ制約の追加、変更、または削除

重要：タグ制約を追加、変更、および削除すると、どのマシンがアプリケーション起動の対象となるかについて、予期しない効果を招くことがあります。「タグ」に記載されている考慮事項と注意を必ず確認してください。

1. Studio のナビゲーションペインで [アプリケーション]を選択します。
2. 中央ペインでアプリケーショングループを選択し、[操作]ペインで [アプリケーショングループを編集します]を選択します。
3. [デリバリーグループ]ページを選択します。
4. タグ制約を追加するには、[タグでマシンの起動を制限します:]を選択し、ドロップダウンからタグを選択します。
5. タグ制約を変更または削除するには、異なるタグをドロップダウンから選択するか、[次のタグを持つマシンに起動を制約する:]をオフにして、タグ制約を完全に削除します。
6. [適用]をクリックして行った変更を適用しウィンドウを開いたままにするか、[**OK**]をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのユーザーの追加または削除

ユーザーについて詳しくは、「アプリケーショングループの作成」の記事で「ユーザー」のセクションを参照してください。

1. Studio のナビゲーションペインで [アプリケーション]を選択します。
2. 中央ペインでアプリケーショングループを選択し、[操作]ペインで [アプリケーショングループを編集します]を選択します。
3. [ユーザー]ページを選択します。アプリケーショングループ内のアプリケーションの使用を、関連付けられたデリバリーグループ内のすべてのユーザーに許可するか、特定のユーザーおよびグループにのみ許可するかを指定します。ユーザーを追加するには、[追加]をクリックし、追加するユーザーを指定します。ユーザーを削除する場合は、1 人または複数のユーザーを選択し、[削除]をクリックします。
4. [適用]をクリックして行った変更を適用しウィンドウを開いたままにするか、[**OK**]をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのスコープの変更

スコープの変更は、スコープを作成済みの場合のみ行うことができます（[すべて］のスコープを編集することはできません)。詳しくは、「委任管理」を参照してください。

1. Studio のナビゲーションペインで ［アプリケーション］を選択します。
2. 中央ペインでアプリケーショングループを選択し、［操作］ペインで ［アプリケーショングループを編集します］を選択します。
3. ［スコープ］ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループの削除

アプリケーションは、デリバリーグループかアプリケーショングループの少なくとも 1 つに割り当てる必要があります。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］を選択します。
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

October 22, 2021

リモート PC アクセスは Citrix Virtual Apps and Desktops の機能であり、組織で従業員が安全な方法でリモートから企業リソースに簡単にアクセスできるようにします。Citrix プラットフォームでは、ユーザーが社内の物理的な PC にアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーが社内 PC にアクセスできる場合、作業に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモート PC アクセスにより、テレワークに対応するために他のツールを導入したり提供したりする必要がなくなります。たとえば、仮想デスクトップまたはアプリケーション、および関連するインフラストラクチャなどです。

リモート PC アクセスでは、仮想デスクトップとアプリケーションを配信するのと同じ Citrix Virtual Apps and Desktops コンポーネントが使用されます。その結果、リモート PC アクセスの展開と構成の要件およびプロセスは、仮想リソースの配信のために Citrix Virtual Apps and Desktops の展開に必要なものと同じです。この統一性により、一貫性のある統一された管理エクスペリエンスが実現されます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

この機能は、種類がリモート **PC** アクセスのマシンカタログで構成され、提供されます:

- OU を指定してマシンを追加する機能。この機能によって PC の一括追加を円滑に実行できます。
- 社内の Windows PC にログインするユーザーに基づいた自動ユーザー割り当て。単一ユーザーおよび複数ユーザーの割り当てをサポートしています。

Citrix Virtual Apps and Desktops では、他の種類のマシンカタログを使用することで、物理 PC のユースケースが増えます。これらのユースケースには次のようなものがあります:

- 物理 Linux PC
- プールされた物理 PC（ランダムに割り当てられ、専用ではありません）

> 注:
>
> サポートされている OS バージョンについて詳しくは、「Virtual Delivery Agent（VDA）for Desktop OS」と「Linux VDA」のシステム要件を参照してください。
>
> オンプレミス展開の場合、リモート PC アクセスは、Citrix Virtual Apps and Desktops の Advanced または Premium ライセンスでのみ有効です。セッションでは、他の Citrix Virtual Desktops セッションと同様にライセンスが消費されます。Citrix Cloud の場合、Citrix Virtual Apps and Desktops サービスおよび Workspace Premium Plus で有効です。

注意事項

Citrix Virtual Apps and Desktops 全般に適用される技術的要件および考慮事項はすべて、リモート PC アクセスにも適用されますが、一部は物理 PC のユースケースに対してより関連性があるか、または排他的な場合もあります。

展開に関する考慮事項

リモート PC アクセスの導入を計画する際は、以下の全般的な項目について判断してください。

- 既存の Citrix Virtual Apps and Desktops 展開にリモート PC アクセスを追加できます。このオプションを選択する前に、以下の点を考慮してください:
  - リモート PC アクセスの VDA に関連する追加の負荷をサポートするために、現在の Delivery Controller または Cloud Connector のサイズは適切か?
  - オンプレミスのサイトデータベースとデータベースサーバーは、リモート PC アクセスの VDA に関連する追加の負荷をサポートするために適切なサイズか?
  - 既存の VDA と新しいリモート PC アクセスの VDA は、サイトあたりサポートされる VDA の最大数を超えているか?
- VDA は、自動プロセスによって社内 PC に展開する必要があります。使用可能な 2 つのオプションは次のとおりです:
  - SCCM などの電子ソフトウェア配信（ESD）ツール：SCCM を使用した VDA のインストール。
  - 展開スクリプト：スクリプトを使用した VDA のインストール。
- 「リモート PC アクセスのセキュリティに関する考慮事項」を確認してください。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります:

- リモート PC アクセス
  - Windows 専用 PC
  - Windows 専用のマルチユーザー PC
- シングルセッション OS
  - 静的 - 専用 Linux PC
  - ランダム - プールされた Windows および Linux PC

マシンカタログの種類を特定したら、次の点を考慮してください:

- 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に同時に関連付けることはできません。
- 委任管理を円滑に進めるために、各カタログの管理を適切な管理者に容易に委任できる地理的な場所、部署、またはその他のグループに基づいて、マシンカタログを作成することを検討してください。
- マシンアカウントが存在する OU を選択する場合は、より細分化するために下位レベルの OU を選択します。このような細分性が必要ない場合は、上位レベルの OU を選択できます。たとえば、Bank/Officers/Tellers の場合、より細分性を高めるために **Tellers** を選択します。それ以外の場合は、要件に基づいて ［役員］または ［銀行］を選択できます。
- リモート PC アクセスマシンカタログに割り当てた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。したがって、マシンカタログの OU 割り当ての更新が Active Directory 変更計画で考慮されるように、適切な計画を立ててください。
- OU 構造のため、マシンカタログにマシンを追加する OU を選択することが容易でない場合は、OU を選択する必要はありません。後で PowerShell を使用してマシンをカタログに追加できます。デリバリーグループでデスクトップ割り当てが正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てと併せてマシンカタログにマシンを追加するサンプルスクリプトについては、「GitHub」を参照してください。
- 統合された Wake on LAN は、リモート **PC** アクセスタイプのマシンカタログでのみ使用できます。

Linux VDA に関する考慮事項

次の考慮事項は、Linux VDA に固有のものです:

- Linux VDA は、非 3D モードの物理マシンでのみ使用します。NVIDIA のドライバーの制限により、HDX 3D モードが有効になっている場合、PC のローカル画面はブラックアウトせず、画面にはセッションのアクティビティが表示されます。この画面の表示は、セキュリティ上のリスクです。
- 物理 Linux マシンには、シングルセッション OS タイプのマシンカタログを使用します。
- 統合された Wake on LAN 機能は、Linux マシンでは使用できません。

技術的な要件および考慮事項

このセクションでは、物理 PC の技術要件と考慮事項について説明します。

- 以下はサポートされていません:
  - KVM スイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。
  - ハイブリッド PC（オールインワンおよび NVIDIA Optimus ノートブックおよび PC を含む）。
- キーボードとマウスを PC に直接接続します。電源を切ったり接続を切断したりできるモニターなどのコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。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、それらのコンポーネントの電源をオフにしないでください。
- PC は Active Directory ドメインサービスドメインに参加している必要があります。
- セキュアブートは Windows 10 でのみサポートされています。
- PC にはアクティブなネットワーク接続が必要です。信頼性と帯域幅を高めるには、有線接続をお勧めします。
- Wi-Fi を使用する場合、以下の点を確認します:
  1. 電源設定でワイヤレスアダプターの電源を入れたままにするようにします。
  2. ユーザーがサインインする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまで VDA は登録されません。ユーザーがログオンするまで、PC ではリモートアクセスを使用できません。
  3. Wi-Fi ネットワークから Delivery Controller または Cloud Connector にアクセスできることを確認してください。
- リモート PC アクセスはノートブックコンピューターで使用できます。ノートブックがバッテリーで動作しているのではなく、電源に接続されていることを確認します。デスクトップ PC のオプションに合わせて、ノートブックの電源オプションを構成します。次に例を示します:
  1. 休止機能を無効にする。
  2. スリープ機能を無効にする。
  3. カバーを閉じた場合の動作を ［何もしない］ に設定する。
  4. 電源ボタンを押したときの操作を ［シャットダウン］ に設定する。
  5. ビデオカードおよび NIC の省電力設定を無効にする。
- リモート PC アクセスは、Surface Pro デバイス上の Windows 10 でサポートされます。前述のノートブックと同じガイドラインに従います。
- ドッキングステーションを使用している場合、ノートブックをドッキング解除して再接続できます。ドッキング解除すると、VDA は Wi-Fi で Delivery Controller または Cloud Connector に再登録されます。ただし、ノートブックを再接続した場合、ワイヤレスアダプターを外さない限り、VDA は有線接続を使用するように切り替わりません。有線接続が確立されると、組み込まれた機能がワイヤレスアダプターを切断するデバイスもあります。それ以外のデバイスでは、ワイヤレスアダプターを切断するためのカスタムソリューションかサードパーティ製のユーティリティが必要です。前述の Wi-Fi に関する考慮事項を確認してください。

  デバイスのリモート PC アクセスでドッキングとドッキング解除を有効にするには、以下の操作を実行します:

1. ［スタート］メニューの ［設定］**>** ［システム］**>** ［電源とスリープ］で ［スリープ］を ［なし］に設定します。
2. ［デバイスマネージャー］**>** ［ネットワークアダプター］**>** ［イーサネットアダプター］の［電源管理］で［電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする］に移動します。［このデバイスで、コンピューターのスタンバイ状態を解除できるようにする］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。

- 同じ社内 PC にアクセスする複数のユーザーには、Citrix Workspace で同じアイコンが表示されます。ユーザーが Citrix Workspace にログオンすると、そのリソースが他のユーザーによって既に使用されている場合は使用不可と表示されます。
- 社内 PC へアクセスする各クライアントデバイス（自宅の PC など）に、Citrix Workspace アプリをインストールします。

構成の順序

このセクションでは、リモート **PC** アクセスタイプのマシンカタログを使用する場合にリモート PC アクセスを構成する方法の概要について説明します。他のタイプのマシンカタログを作成する方法については、「マシンカタログの作成」を参照してください。

1. オンプレミスサイトのみ - 統合された Wake on LAN 機能を使用するには、「Wake on LAN」で説明されている前提条件を構成します。
2. リモート PC アクセス用に新しい Citrix Virtual Apps and Desktops サイトが作成された場合：

   a) リモート **PC** アクセスサイトの種類を選択します。
   b) 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。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LAN の構成について詳しくは、「Wake on LAN」を参照してください。
   c)「ユーザー」ページと「マシンアカウント」ページの情報を入力します。

   これらの手順を完了すると、「リモート **PC** アクセスマシン」という名前のマシンカタログと、「リモート **PC** アクセスデスクトップ」という名前のデリバリーグループが作成されます。
3. 既存の Citrix Virtual Apps and Desktops サイトに追加する場合：

   a) リモート **PC** アクセスタイプのマシンカタログを作成します（ウィザードの［オペレーティングシステム］ページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してください。ターゲットの PC をリモート PC アクセスで使用できるように、正しい組織単位が割り当てられていることを確認します。
   b) デリバリーグループを作成して、ユーザーがマシンカタログの PC にアクセスできるようにします。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。PC へのアクセスが必要なユーザーが含まれる Active Directory グループにこのデリバリーグループを割り当てます。
4. VDA を社内 PC に展開します。

- シングルセッション OS コア VDA インストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションのフル VDA インストーラー（VDAWorkstationSetup.exe）を /remotepcオプションで使用することもできます。これにより、コア VDA インストーラーを使用する場合と同じ結果が得られます。
- ヘルプデスクチームが Citrix Director を通じてリモートサポートを提供できるように、Windows リモートアシスタンスを有効にすることを検討してください。そのために、/enable_remote_assistanceオプションを使用します。詳しくは、「コマンドラインを使ったインストール」を参照してください。
- Director でログオン時間情報を表示するには、シングルセッション完全版 VDA インストーラーを使用して **Citrix User Profile Manager WMI Plugin** コンポーネントを含める必要があります。/includeadditionalオプションを使用してこのコンポーネントを含めます。詳しくは、「コマンドラインを使ったインストール」を参照してください。
- SCCM を使用した VDA の展開については、「SCCM を使用した VDA のインストール」を参照してください。
- 展開スクリプトを使用した VDA の展開については、「スクリプトを使用した VDA のインストール」を参照してください。

手順 2〜4 を正常に完了すると、ユーザーが PC にローカルでログインしたときに、自動的にマシンが割り当てられます。

5. 社内 PC へのリモート接続で使用する各クライアントデバイスに、Citrix Workspace アプリをダウンロードしインストールするようユーザーに指示します。Citrix Workspace アプリはhttps://www.citrix.com/downloads/から、またはサポートされるモバイルデバイス向けのアプリストアから入手できます。

レジストリで管理される機能

> 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、シトリックス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。

複数ユーザーの自動割り当てを無効化

Delivery Controller ごとに、次のレジストリ設定を追加します:

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

- 値の名前：AllowMultipleRemotePCAssignments
- 種類：DWORD
- データ：0

スリープモード（バージョン **7.16** 以降）

リモート PC アクセスマシンがスリープ状態に入ることを許可するには、このレジストリ設定を VDA に追加してからマシンを再起動します。再起動後は、オペレーティングシステムの省電力設定が優先されます。設定済みのアイドルタイマー間隔が経過すると、マシンはスリープモードに入ります。マシンがスリープモードから復帰すると、Delivery Controller に再登録されます。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

- 値の名前：DisableRemotePCSleepPreventer
- 種類：DWORD
- データ：1

セッション管理

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。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

- 値の名前：SasNotification
- 種類：DWORD
- データ：1

デフォルトでは、接続メッセージがタイムアウト期間内に承認されなかった場合にリモートユーザーがローカルユーザーより優先されます。この動作を構成するには、次の設定を使用します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

- 値の名前：RpcaMode
- 種類：DWORD
- データ：
  - 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優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

リモート PC アクセスモードを強制するまでのタイムアウト期間はデフォルトでは 30 秒です。このタイムアウト期間は変更できますが、30 秒より短く設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します：

HKLM\SOFTWARE\Citrix\PortICA\RemotePC

- 値の名前：RpcaTimeout
- 種類：DWORD
- データ：10 進数のタイムアウト値（秒単位）

ユーザーがコンソールに強制的にアクセスできるようにするには：ローカルユーザーが Ctrl+Alt+Del キーを 10 秒以内に 2 回押すことによって、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的に発生します。

レジストリを変更してマシンを再起動した後に、リモートユーザーが使用中の PC にローカルユーザーが Ctrl+Alt+Del キーを押してログオンすると、プロンプトがリモートユーザーに表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。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。

Wake-on-LAN

統合された Wake on LAN は、オンプレミスの Citrix Virtual Apps and Desktops でのみ使用でき、Microsoft System Center Configuration Manager（SCCM）が必要です。

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、電源が突然オフになった PC にもリモートアクセスできるようになります。たとえば、停電でオフになった場合などです。

リモート PC アクセスの Wake on LAN 機能は、BIOS/UEFI で Wake on LAN オプションが有効になっている PC でサポートされてます。

CCM およびリモート 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 VDA を展開します。

- 組織内で SCCM 2012 R2、2016、または 2019 を構成します。リモート PC アクセス用のすべてのマシンに SCCM クライアントを展開し、スケジュールされている SCCM インベントリサイクルが実行されるのを待ちます（必要に応じて、手動で強制的に実行することもできます）。
- SCCM 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/UEFI 設定で、Wake on LAN 機能を有効にします。
  - ウェイクアッププロキシの場合は、SCCM 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マシンが 3 台以上あることを確認します。
  - マジックパケットの場合は、サブネット宛てのブロードキャストまたはユニキャストを使用して、ネットワーク経路およびファイアウォールでパケットの転送がブロックされないようにします。

社内 PC 上に VDA をインストールしたら、接続とマシンカタログを作成するときに電源管理機能を有効または無効にします。

- カタログで電源管理機能を有効にする場合は、接続の詳細として SCCM のアドレス、アクセス資格情報、および接続名を指定します。このアクセス資格情報は、スコープのコレクションおよびリモートツールオペレーターの役割にアクセスできる必要があります。
- 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電源管理機能を有効にできます。

電源管理接続を編集して、詳細設定を変更できます。以下の機能を有効にできます。

- SCCM 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

診断情報

リモート PC アクセスの診断情報は、Windows のアプリケーションイベントログに書き込まれます。情報メッセージは調整されません。エラーメッセージは重複メッセージの破棄により調整されます。

- 3300（情報）：マシンカタログへのマシンの追加
- 3301（情報）：デリバリーグループへのマシンの追加
- 3302（情報）：ユーザーへのマシンの割り当て
- 3303（エラー）：例外の発生

電源の管理

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。

その他のリソース

リモート PC アクセスのその他のリソースは次のとおりです：

- ソリューション設計ガイダンス：「リモート PC アクセス設計の決定」。
- リモート PC アクセスアーキテクチャの例：「Citrix のリモート PC アクセスソリューションのリファレンスアーキテクチャ」。

App-V

August 24, 2021

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 以降
5.0 SP2	XenDesktop 7 以降、XenApp 7.5 以降	7.1 以降
5.0 SP3 および 5.1	XenDesktop 7.6 以降、XenApp 7.6 以降	7.6.300～最新バージョン
Windows Server 2016 での App-V	XenDesktop 7.12 以降、XenApp 7.12 以降	7.12 以降

App-V クライアントは、アプリケーションへのオフラインアクセスをサポートしません。App-V の統合機能により、アプリケーションでの SMB 共有の使用がサポートされます。HTTP プロトコルはサポートされません。

App-V について詳しくは、Microsoft 社のドキュメントを参照してください。以下に、本書で説明する App-V コンポーネントの概要を示します。

- 管理サーバー App-V インフラストラクチャを管理したり、App-V デスクトップクライアントやリモートデスクトップサービスクライアントに仮想アプリケーションを配信したりするための中央管理コンソールです。App-V 管理サーバーは、セキュリティ、測定、監視、および管理者によって要求されるデータ収集を認証、要求、および提供します。このサーバーは、Active Directory といくつかのツールを使用してユーザーとアプリケーションを管理します。
- 公開サーバー。App-V クライアントに特定ユーザー用のアプリケーションを提供し、ストリーム配信用の仮想アプリケーションパッケージをホストします。これらのパッケージは、管理サーバーから取得されます。
- 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 クライアントは 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 サーバー上のパッケージからアプリケーションを使用するには、検出、構成、および VDA へのダウンロードのために Studio と App-V サーバー間の通信を継続する必要があります。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、App-V パッケージとアプリケーションアクセスに Studio と App-V サーバーコンソールの両方が必要なため、デュアル管理の管理方式と呼ばれています。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）。

  App-V パッケージとアプリケーションの使用には Studio コンソールのみが必要なため、これはシングル管理の管理方法と呼ばれます。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とは、App-V パッケージに関する情報を保存するキャッシングリポジトリを表す Citrix の用語です。またアプリケーションライブラリでは、ほかの Citrix アプリケーションの配信テクノロジに関する情報も保存されます。

いずれかの管理方式を使用することも、両方の管理方式を同時に使用することもできます。つまり、アプリケーションをデリバリーグループに追加する場合、App-V サーバーとネットワーク共有に置かれた App-V パッケージのどちらからもアプリケーションを追加できます。

Studio のナビゲーションペインで、［構成］**>** ［**App-V** 公開］の順に選択すると、App-V パッケージの名前とソースが表示されます。ソースの列には、パッケージが App-V サーバーにあるか、またはアプリケーションライブラリにキャッシュされているかが表示されます。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションが一覧表示されます。

負荷分散 **App-V** サーバー

デュアル管理方式を使用している場合は、DNS ラウンドロビンを使用した負荷分散管理および公開サーバーがサポートされています。Netscaler、F5（または同様の）仮想 IP を使用する管理サーバーの負荷分散は、Studio がリモート PowerShell 経由で管理サーバーと通信する必要があるため、サポートされていません。詳しくは、Citrixブログの記事を参照してください。

分離グループ

App-V シングル管理方式を使用するときは、分離グループを作成して、サンドボックスで実行する必要がある相互依存のアプリケーションのグループを指定できるようにします。この機能は、App-V 接続グループと大きな違いはありませんが、同一ではありません。App-V 管理サーバーで使用する必須またはオプションのパッケージ用語の代わりに、自動の明示的なパッケージ展開オプションが使用されます。

- ユーザーが App-V アプリケーション（プライマリアプリケーション）を起動すると、自動包含対象としてマークされている他のアプリケーションパッケージ用に分離グループが検索されます。それらのパッケージは自動的にダウンロードされ、分離グループに含められます。それらのパッケージを、プライマリアプリケーションを含むデリバリーグループに追加する必要はありません。
- 明示的包含対象としてマークされている分離グループのアプリケーションパッケージは、プライマリアプリケーションが含まれる同じデリバリーグループにそのアプリケーションを明示的に追加した場合に限りダウンロードされます。

これにより、すべてのユーザーがグローバルに使用できる自動包含アプリケーションが混在する分離グループの作成が可能となります。さらにこのグループには、一連のプラグインと（特定のライセンス制約のある）その他のアプリケーションを含めることができます。それにより、追加の分離グループを作成することなく特定のユーザー（デリバリーグループを通して特定）に制限できます。

たとえば、アプリケーション「app-a」を実行するには JRE 1.7 が必要です。（明示的展開の種類の）app-a と（自動展開の種類の）JRE 1.7 を含む分離グループを作成できます。その後、それらの App-V パッケージを 1 つまたは複数のデリバリーグループに追加します。ユーザーが app-a を実行すると、JRE 1.7 が自動的に app-a で展開されます。

アプリケーションは複数の App-V 分離グループに追加することができます。ただし、ユーザーがそのアプリケーションを起動したときは、アプリケーションが追加された最初の分離グループが常に使用されます。そのアプリケーションを含む他の分離グループに順位を付けすること、またはこれらを優先することはできません。

セットアップ

次の表は、XenApp および XenDesktop で App-V を使用する場合のセットアップ作業の順序をまとめたものです。

シングル管理	デュアル管理	タスク
○	○	App-V を展開する
○	○	パッケージングと配置

シングル管理	デュアル管理	タスク
	○	Studio での App-V サーバーアドレスの構成
○	○	VDA マシンへのソフトウェアのインストール
○		アプリケーションライブラリへの App-V パッケージの追加
○		App-V 分離グループの追加（オプション）
○	○	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、https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/?redirectedfrom=MSDN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。

GPO ポリシーを使って公開サーバー設定を管理していた環境では、コマンドレットでの設定を含めて、すべての App-V 統合設定よりも GPO での設定が優先されてしまいます。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権限を保有していることを確認します。
- デュアル管理方式では、UNC パスから App-V 管理サーバーにパッケージを公開します。（HTTP URL からの公開はサポートされていません。）

パッケージが App-V サーバーにあるか、ネットワーク共有上にあるかにかかわらず、Studio 管理者がアクセスできるよう、そのパッケージに適切なセキュリティ権限が付与されていることを確認します。ネットワーク共有は「認証ユーザー」と共有し、デフォルトで、VDA と Studio の両方に読み取りアクセス権限が付与される必要があります。

Studio での **App-V** サーバーアドレスの構成

> 重要:
>
> それらのサーバーで非デフォルトのプロパティ値を使用する場合、Controller の PowerShell コマンドレットを使用して App-V サーバーのアドレスを指定することをお勧めします。詳しくは、SDK のドキュメントを参照してください。Studio で App-V サーバーのアドレスを変更すると、指定したサーバー接続プロパティの一部がデフォルト値にリセットされることがあります。VDA では、これらのプロパティが App-V 公開サーバーへの接続に使用されます。この事象が発生した場合、サーバーで、リセットされたプロパティの非デフォルト値を再構成してください。

この手順は、デュアル管理方式にのみ適用されます。

デュアル管理方式では、サイトの作成中または作成後に、App-V Management server および公開サーバーのアドレスを指定します。この作業は、サイトの作成中または作成後に実行できます。

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. 以前に App-V サーバーアドレスを指定していない場合は、［操作］ウィンドウで ［**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］ウィンドウで ［**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 管理サーバーと公開サーバーへのすべてのリンクを削除し、それらのサーバーから Studio が App-V パッケージを検出しないようにするには、［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 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、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 クライアントには、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 クライアントを、VDA がインストールされた各マシン、または仮想マシンを作成するためにマシンカタログで使用されるマスターイメージにインストールします。注: Windows 10（1607 以降）および Windows Server 2016 には、App-V Client が既に含まれています。これらの OS でのみ、PowerShell コマンドレットの **Enable-AppV**（パラメーターなし）を実行して App-V クライアントを有効にします。**Get-AppVStatus** コマンドレットは現在の有効性の状態を取得します。

ヒント: App-V Client をインストールしたら、管理者権限で PowerShell の **Get-AppvClientConfiguration** コマンドレットを実行し、EnablePackageScripts が 1 に設定されていることを確認します。1 に設定されていない場合は、**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。

VDA のインストール時にこのデフォルトの操作を制御することもできます。グラフィカルインターフェイスの場合は、［追加コンポーネント］ページの ［**Citrix Personalization for App-V - VDA**］チェックボックスをオフにします。コマンドラインインターフェイスの場合は、「**/exclude “Citrix Personalization for App-V - VDA”**」オプションを追加します。

VDA のインストール中に Citrix App-V コンポーネントのインストールを意図的に無効化し、後で App-V アプリケーションを使用する必要が生じた場合: 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での **App-V** パッケージの追加または削除

これらの手順は、シングル管理方式にのみ適用されます。

少なくとも、App-V パッケージが置かれたネットワーク共有への読み取りアクセスを保有している必要があります。

アプリケーションライブラリへの **App-V** パッケージの追加

1. Studio のナビゲーションペインで、［構成］**>**［**App-V** 公開］の順に選択します。
2. ［操作］ペインで ［パッケージの追加］を選択します。
3. App-V パッケージの置かれたネットワーク共有を検索し、1 つまたは複数のパッケージを選択します。
4. ［追加］をクリックします。

アプリケーションライブラリからの **App-V** パッケージの削除

アプリケーションライブラリから App-V パッケージを削除すると、Studio App-V 公開ノードの表示から App-V パッケージが削除されます。ただし、App-V パッケージのアプリケーションはデリバリーグループから削除されません。それらのアプリケーションは起動されたままになります。パッケージは、物理ネットワーク上に残ります（これは、App-V アプリケーションをデリバリーグループから削除した場合とは異なります）。

1. Studio のナビゲーションペインで、［構成］**>**［**App-V** 公開］の順に選択します。
2. 削除するパッケージを 1 つまたは複数選択します。
3. ［操作］ペインで ［パッケージの削除］を選択します。

App-V 分離グループの追加、編集、削除

App-V 分離グループの追加

1. Studio のナビゲーションペインで、［**App-V** 公開］を選択します。
2. ［操作］ウィンドウで ［分離グループの追加］を選択します。
3. ［分離グループ設定の追加］ダイアログボックスで、分離グループの名前と説明を入力します。
4. ［利用可能なパッケージ］の一覧で、分離グループに追加するアプリケーションを選択して右向き矢印をクリックします。選択したアプリケーションが［分離グループ］一覧の［パッケージ］に表示されます。各アプリケーションの横にある ［展開］ドロップダウンで ［明示］または ［自動］を選択します。この一覧では、上向き矢印と下向き矢印を使用して、アプリケーションの順番を変更できます。
5. 完了したら、［**OK**］をクリックします。

App-V 分離グループを編集する

1. Studio のナビゲーションペインで、［**App-V** 公開］を選択します。
2. 中央ペインで ［分離グループ］タブを選択し、編集する分離グループを選択します。
3. ［操作］ペインの ［分離グループの編集］を選択します。
4. ［分離グループ設定の編集］ダイアログボックスで、分離グループの名前または説明の変更、アプリケーションの追加または削除、展開タイプの変更、またはアプリケーションの順序の変更を行います。
5. 完了したら、［**OK**］をクリックします。

App-V 分離グループの削除

分離グループを削除しても、アプリケーションパッケージは削除されません。グループ化のみが解除されます。

1. Studio のナビゲーションペインで、[**App-V** 公開] を選択します。
2. 中央ペインで [分離グループ] タブを選択し、削除する分離グループを選択します。
3. [操作] ペインの [分離グループの削除] を選択します。
4. 削除を確認します。

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、App-V アプリケーションを既存のデリバリーグループに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] ペインで [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 App-V 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] ウィンドウで [アプリケーションの追加] を選択します。
3. App-V アプリケーションを追加する 1 つまたは複数のデリバリーグループを選択します。

手順 **2**: ウィザードの [アプリケーション] ページで、[追加] ドロップダウンをクリックしてアプリケーションのソースを表示します。**App-V** を選択します。

手順 **3**: [**App-V** アプリケーションの追加] ページで、App-V ソースの App-V サーバーまたはアプリケーションライブラリを選択します。アプリケーションの名前と、そのパッケージの名前とバージョンが表示されます。追加するアプリケーションの横にあるチェックボックスをオンにします。[**OK**] をクリックします。

手順 **4**: ウィザードを完了します。

ヒント:

- App-V アプリケーションをデリバリーグループに追加するときに App-V アプリケーションのプロパティを変更すると、変更はそのアプリケーションの起動時に適用されます。たとえば、アプリケーションをデリバリーグループに追加するときにアプリケーションの表示名やアイコンを変更した場合、ユーザーがそのアプリケーションを起動すると変更が反映されます。
- App-V アプリケーションを含むデリバリーグループを後で編集した場合、デリバリーグループの配信のタイプを「デスクトップとアプリケーション」から「アプリケーションのみ」に変更しても、App-V アプリケーションのパフォーマンスは変わりません。
- 以前に公開された（シングル管理の）App-V パッケージをデリバリーグループから削除すると、Citrix App-V クライアントコンポーネントは、シングル管理方式で使用されなくなったパッケージをクリーンアップし、非公開にして、削除しようとします。

- ハイブリッド展開では、パッケージはシングル管理方式で配信され、App-V 公開サーバーはデュアル管理方式か、他のメカニズム（グループポリシーなど）で管理されています。ハイブリッド展開を使用している場合、どの（冗長性があると思われる）パッケージがどのソースに由来するか判断することはできません。この場合、クリーンアップは試行されません。
- 公開サーバーを使用していないが、VDA 上のパッケージを別のメカニズムで管理している場合（SCCM、カスタムスクリプト、またはサードパーティの App-V 管理ソリューション）、クリーンアップルーチンが必要なパッケージを削除する可能性があります。このような場合、ダミーの App-V Management server を VDA に登録して、クリーンアップが試行されないようにします。

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 のナビゲーションペインで ［構成］**>** ［**App-V** 公開］を選択すると、PowerShell 接続エラーが発生します。

- Studio の管理者は App-V サーバーの管理者でもありますか。Studio の管理者は、Studio と通信できるように、App-V 管理サーバーの「管理者」グループに属している必要があります。

(デュアル）Studio で App-V サーバーのアドレスを指定するときに行う「接続テスト」に失敗します。

- App-V サーバーの電源は入っていますか。ping コマンドを送信するか IIS マネージャーを使用して、各 App-V サーバーの状態が開始済みかつ実行中であることを確認します。
- App-V サーバーの PowerShell リモート処理は有効ですか。そうでない場合は、https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)?redirectedfrom=MSDNを参照してください。
- Studio の管理者は App-V サーバーの管理者でもありますか。Studio の管理者は、Studio と通信できるように、App-V 管理サーバーの「管理者」グループに属している必要があります。
- App-V サーバーのファイル共有は有効ですか。Windows エクスプローラーまたは［ファイル名を指定して実行］ダイアログボックスに、「***<App-V server FQDN>***」と入力します。
- App-V サーバーには、App-V 管理者と同じファイル共有権限が付与されていますか。App-V サーバーで、［ユーザー名およびパスワードの保存］ダイアログボックスに「*<App-V Server FQDN>*」のエントリを追加して、その App-V サーバーの管理者権限を持つユーザーの資格情報を指定します。ガイダンスについては、https://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 マシン上の 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。」この場合は、

GPO の TrustedHosts ポリシー（[管理用テンプレート] > [**Windows** コンポーネント] > [**Windows** リモート管理（**WinRM**）] > [**WinRM** クライアント]）に App-V サーバーの名前を追加します。

（デュアル）App-V アプリケーションをデリバリーグループに追加するとき、検出が失敗します。

- Studio の管理者は App-V Management server の管理者でもありますか。Studio の管理者は、Studio と通信できるように、App-V 管理サーバーの「管理者」グループに属している必要があります。
- App-V Management server は実行中ですか。ping コマンドを送信するか IIS マネージャーを使用して、各 App-V サーバーの状態が開始済みかつ実行中であることを確認します。
- 両方の App-V サーバーの PowerShell リモート処理は有効ですか。そうでない場合は、https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)?redirectedfrom=MSDNを参照してください。
- Studio 管理者がアクセスできるように、パッケージに適切なセキュリティ権限が設定されていますか。

App-V アプリケーションが起動しません。

- （デュアル）公開サーバーは実行中ですか。
- （デュアル）App-V パッケージに適切なセキュリティ権限が設定されており、ユーザーがアクセスできるようになっていますか。
- （デュアル）VDA で、Temp ディレクトリの参照が正しく、Temp ディレクトリに十分な空き領域があることを確認してください。
- （デュアル）App-V 公開サーバーで`Get-AppvPublishingServer \*`を実行して、公開サーバーの一覧を表示します。
- （デュアル）App-V 公開サーバーで、UserRefreshonLogon が False に設定されていることを確認します。
- （デュアル）App-V 公開サーバーで、管理者として **Set-AppvPublishingServer** を実行して、UserRefreshonLogon を False に設定します。
- VDA に、サポート対象バージョンの App-V クライアント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 クライアントと 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 キーが次のフォーマットであることを確認します：<AppVManagementServer>+<metadata>;<PublishingServer>（例：`http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`）。
- App-V クライアントと VDA がインストールされたマシンまたはマスターイメージで、PowerShell ExecutionPolicy が RemoteSigned に設定されていることを確認します。Microsoft 社から提供される App-V クライアントは署名されてないため、この ExecutionPolicy で、PowerShell で無署名のローカルのスクリプトとコマンドレットを実行できるようにします。次のいずれかの方法を使用して ExecutionPolicy を設定します：（1）管理者として、コマンドレット：「**Set-ExecutionPolicy RemoteSigned**」を入力するか、（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:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1 に移動します。テキストエディターで CtxAppvCommon.dll.config を開き、次の行のコメントを解除します: <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Broker Service を再起動してログの記録を開始します。

VDA のログを有効にするには、次の手順に従います。

1. C:\CtxAppvLogs フォルダーを作成します。
2. C:\Program Files\Citrix\Virtual Desktop Agent に移動します。テキストエディターで CtxAppvCommon.dll.config を開き、次の行のコメントを解除します: <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. 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: <add key =”EnableLauncherLogs” value=”1”/>
4. マシンを再起動してログの記録を開始します。

AppDisk

August 24, 2021

概要

アプリケーションに加えて、アプリケーションのインストール元となるイメージも管理することは非常に困難です。Citrix の AppDisk 機能により、こうした問題を解決できます。AppDisk では、アプリケーションとアプリケーションのグループはオペレーティングシステムから分離されるため、アプリケーションを個別に管理できます。

個々のユーザーグループ向けに設計されたアプリケーションを含むさまざまな AppDisk を作成し、任意のマスターイメージ上で組み立てることができます。このようにアプリケーションをグループ化して管理することで、アプリケーションをより詳細に管理できるようになり、保守するマスターイメージの数が削減されます。これにより、IT 管理が簡素化されるとともに、ユーザーのニーズにより迅速に対応できるようになります。AppDisk に含まれるアプリケーションは、デリバリーグループ経由で提供します。

自身の環境で Citrix AppDNA も使用している場合、AppDisk の機能を AppDNA と統合すると、XenApp と XenDesktop では AppDisk ごとにアプリケーションの自動分析を実行できるようになります。AppDNA を使用することで、AppDisk の機能を最大限に活用できます。AppDNA を使用しない場合は、アプリケーション互換性のテストと報告は行われません。

AppDisk は、隔離と変更管理という 2 つの面において、ほかのアプリケーションプロビジョニングテクノロジとは異なります。

- Microsoft App-V では、互換性のないアプリケーションどうしを隔離することで、共存できるようにします。AppDisk の機能では、アプリケーションどうしは隔離されません。アプリケーション（および関連ファイルとレジストリキー）は、OS から分離されます。OS とユーザーには、AppDisk はマスターイメージに直接インストールされているかのように見え、そのように動作します。
- 変更管理（マスターイメージを更新し、その更新がインストール済みのアプリケーションと互換性があるかどうかをテストすること）には、非常にコストがかかる可能性があります。AppDNA レポートは、問題の特定と修復手順の提案に役立ちます。たとえば、AppDNA では、.NET など共通の依存関係を持つアプリケーションを特定できるため、そのようなアプリケーションを 1 つの共通基本イメージにインストールできます。また、OS 起動シーケンスで早期にロードされるアプリケーションも特定できるため、アプリケーションが予想通りに動作することを保証できます。

ヒント:

- イメージの更新後、一部のアプリケーションが、以前にインストールされたライセンスを検証する機能が原因で、正しく機能しない場合があります。たとえば、イメージアップグレード後に Microsoft Office を起動すると、以下のようなエラーメッセージが表示される場合があります。

  「Microsoft Office Professional Plus 2010 ではこのアプリケーションのライセンスを確認できませんでした。修復できなかったか、ユーザーによって中止されました。アプリケーションがシャットダウンしません。」

この問題を解決するには、基本イメージ上で Microsoft Office をアンインストールし、新しいバージョンをインストールします。

- Windows ストアから公開カタログの仮想マシンに Metro アプリをダウンロードすると、時間がたってから失敗することがあります。
- すべての Microsoft Office コンポーネントを常に同じ AppDisk に配置することをお勧めします。たとえば、ある AppDisk には Microsoft Office と Project を、別の AppDisk には Microsoft Office、Project、および Visio を配置するなどです。
- 一部のシステムで、イメージを更新するときに SCCM がクラッシュします。このシナリオは、基本イメージが更新、適用されるときに発生し、SCCM クライアントの障害を招きます。この問題を解決するには、先に基本イメージに SCCM クライアントインスタンスをインストールします。
- AppDisk 上でインストールされたアプリケーションが、デリバリーグループに割り当てられて、ユーザーの仮想マシンを割り当てられた後、Windows の［スタート］メニューに表示されない場合があります。詳しくは、「［スタート］メニューにアプリケーションを表示する方法」を参照してください。
- ユーザーは、アプリケーションと OS の分離や、AppDisk によって提供されるほかの機能を意識することはありません。アプリケーションは、イメージにインストールされているかのように動作します。AppDisk に

複雑なアプリケーションが含まれる場合、デスクトップの起動がわずかに遅れる場合があります。

- AppDisk は、ホストされる共有およびプールデスクトップとともにのみ使用できます。
- AppDisk は、ホストされる共有デスクトップとともに使用できます。
- 複数のマスターイメージや OS プラットフォームで（アプリケーションごとに）AppDisk を共有することもできますが、この方法はすべてのアプリケーションで機能するわけではありません。デスクトップ OS のインストールスクリプトが搭載されたアプリケーションが複数あり、そのデスクトップ OS により、それらのアプリケーションが 1 つのサーバー OS で機能できない場合、この 2 つの OS 向けにアプリケーションを別々にパッケージ化することが推奨されます。
- 多くの場合、AppDisk は複数の OS で機能します。たとえば、Windows 7 の仮想マシンで作成された AppDisk を、Windows 2008 R2 マシンを含むデリバリーグループに追加する操作は、どちらの OS も同じビット数（32 ビットまたは 64 ビット）であり、アプリケーションがどちらの OS でもサポートされる限りは可能です。ただし、新しい OS のバージョン（Windows 10 など）で作成された AppDisk を、古い OS バージョン（Windows 7 など）を実行するマシンを含むデリバリーグループに追加することは、正常に機能しない場合もあるため、推奨されません。
- デリバリーグループのユーザーのサブセットのみが AppDisk のアプリケーションにアクセスできるようにする必要がある場合、グループポリシーを使用して、AppDisk のアプリケーションをほかのユーザーから見えないようにすることが推奨されます。非表示にしたアプリケーションの実行可能ファイルは使用できる状態のままですが、ほかのユーザーは実行できません。
- Windows 7 OS が稼働するロシア語および中国語の環境では、再起動ダイアログが自動的に消えません。そのような場合、提供されたデスクトップにログオンすると、再起動ダイアログが表示されてから、すぐに消えます。
- **Upload-PvDDiags** スクリプトツールを使用している場合、ユーザーのドライブ指定が「P」に設定されていないと、PVD ユーザーレイヤーに関連するログ情報が欠落します。
- バスク語を表示する環境では、Windows 7 OS で、再起動プロンプト画面に言語が適切に表示されない場合があります。言語をバスク語に設定している場合には、フランス語かスペイン語が親言語としてインストールされていることを確認した後、バスク語をインストールし、それを現在の言語に設定してください。
- コンピューターをシャットダウンすると、PVD ディスクが読み取り専用モードに設定されていても、PVD は通知ポップアップを更新します。
- インプレースアップグレード中でもレジストリファイル（DaFsFilter）を削除できますが、それによりアップグレードは失敗します。

> ヒント：
>
> AppDisk を作成するには、OS のみがインストールされた（つまり、他のアプリをインストールしていない）仮想マシンを使用します。AppDisk の作成前に、OS のすべての更新を実行する必要があります。

展開の概要

次の一覧は、AppDisk の展開手順をまとめたものです。詳しくは、この文書の後半部分を参照してください。

1. ハイパーバイザー管理コンソールから、仮想マシンに Virtual Delivery Agent（VDA）をインストールします。

2. AppDisk を作成します。この作業には、ハイパーバイザー管理コンソールと Studio から実行する手順が含まれます。
3. ハイパーバイザー管理コンソールから、アプリケーションを AppDisk にインストールします
4. （ハイパーバイザー管理コンソールまたは Studio で）AppDisk を封印します。封印により、XenApp および XenDesktop で、AppDisk のアプリケーションと関連ファイルをアプリケーションライブラリ（AppLibrary）に記録できるようになります。
5. Studio において、デリバリーグループを作成または編集し、そのデリバリーグループに含める AppDisk を選択します。この手順は *AppDisk* の割り当てと呼ばれます（ただし、Studio では［**AppDisk** の管理］を使用します）。デリバリーグループの仮想マシンの起動時に、XenApp および XenDesktop は、AppLibrary と連携し、Creation Services（MCS）または Provisioning Services（PVS）、および Delivery Controller で動作して、AppDisk が構成された後でブートデバイスをストリーム配信します。

要件

AppDisk の使用には、「システム要件」に記載された要件のほかにもいくつかの要件があります。

AppDisk の機能がサポートされるのは、（最低でも）XenApp および XenDesktop 7.8 のダウンロードファイルで提供されるバージョンの Delivery Controller と Studio が動作する環境のみです。これには、インストーラーが自動的に展開する前提条件（.NET 4.5.2 など）も含まれます。

AppDisk は、VDA でサポートされる同じバージョンの Windows OS 上で作成できます。AppDisk を使用するデリバリーグループ用に選択されたマシンには、最低でも VDA 7.8 がインストールされている必要があります。

すべてのマシンに最新の VDA バージョンをインストールするか、またはすべてのマシンにおいて VDA を最新バージョンにアップグレードしてから、必要に応じてマシンカタログおよびデリバリーグループをアップグレードすることをお勧めします。デリバリーグループの作成時に、異なる VDA バージョンがインストールされたマシンを選択した場合、デリバリーグループは最も古いバージョンと互換性を持ちます（これは、グループの機能レベルと呼ばれます）。機能レベルについて詳しくは、「デリバリーグループの作成」を参照してください。

AppDisk の作成に使用される仮想マシンをプロビジョニングするには、以下を使用できます：

- 7.8 Controller 以上で提供される MCS。
- 使用中の XenApp および XenDesktop のバージョンのダウンロードページで提供される PVS のバージョン。
- サポートされるハイパーバイザー：
  - XenServer
  - VMware（バージョン 5.1 以上）
  - Microsoft System Center Virtual Machine Manager

AppDisk は、XenApp および XenDesktop 用にサポートされるほかのホストハイパーバイザーやクラウドサービスとともに使用することはできません。

一時データのキャッシュを使用する MCS カタログのマシンでは、AppDisk の作成はサポートされません。

> 注:
>
> 書き込みキャッシュを使用して、AppDisk を MCS プロビジョニングマシンに接続できますが、AppDisk の作成には使用できません。

リモート PC アクセスカタログでは、AppDisk はサポートされません。

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、デフォルトで有効になっています。

AppDisk で使用されるデリバリーグループには、サーバー OS またはデスクトップ OS マシンがインストールされたプール（ランダム）マシンカタログのマシンを含めることができます。AppDisk を、プール（静的）または専用（割り当て済み）など、ほかのカタログタイプのマシンとともに使用することはできません。

Studio がインストールされているマシンには、（インストール済みのほかの.NET のバージョンに加えて）.NET Framework 3.5 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。

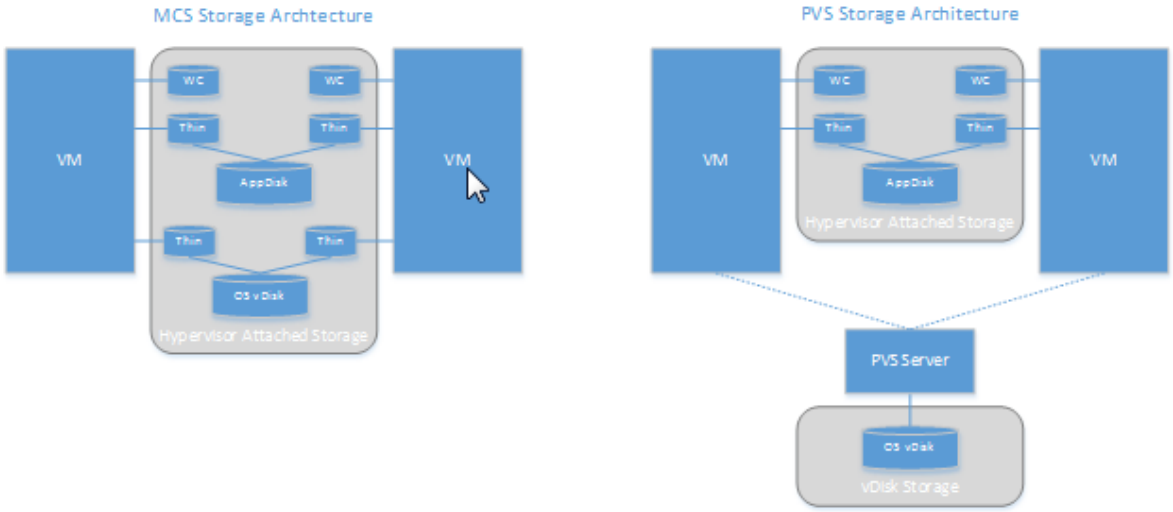
AppDNA を使用するには、以下の手順に従います:

- AppDNA のドキュメントと [AppDisk についてよくある質問]（/en-us/xenapp-and-xendesktop/7-15-ltsr/downloads/AppDisk FAQ.pdf）を参照してください。
- AppDNA ソフトウェアは、Controller とは別のサーバーにインストールする必要があります。この XenApp および XenDesktop のリリースで提供される AppDNA のバージョンを使用します。AppDNA のほかの要件について詳しくは、AppDNA のドキュメントを参照してください。
- AppDNA サーバーで、デフォルトポート 8199 にファイアウォールの例外規則があることを確認します。
- AppDisk の作成中、AppDNA 接続を無効にしないでください。
- XenApp または XenDesktop サイトを作成する場合、サイト作成ウィザードの ［追加機能］ページで、AppDNA との互換性分析を有効にできます。この機能は、Studio のナビゲーションペインの ［構成］**>** [**AppDNA**］を選択することで、後で有効または無効にできます。
- Studio の［問題レポートの表示］リンクをクリックすると AppDNA レポートが表示されます。ただし、AppDNA がデフォルトで使用する OS の組み合わせは、デスクトップデリバリーグループ向け Window 7（64 ビット）とサーバーデリバリーグループ向け Windows Server 2012 R2 です。デリバリーグループが異なるバーションの Windows で構成されている場合、Studio が表示するレポートのデフォルトのイメージの組み合わせが正しくありません。この問題を回避するには、Studio がソリューションを作成した後で、AppDNA でそのソリューションを手動で編集します。
- Studio と AppDNA サーバーのバージョンには依存関係があります。
  - バージョン 7.12 からは、Studio のバージョンは AppDNA サーバーと同じかそれ以降である必要があります。
  - バージョン 7.9 と 7.11 では、Studio と AppDNA サーバーのバージョンは一致する必要があります。
  - 次の表は、どのバージョンが連携して動作するかの概要を示しています（はい＝連係して動作する、- ＝連係して動作しない）:

製品バージョン	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	はい	–	–	–	–	–
AppDNA 7.11	–	はい	–	–	–	–
AppDNA 7.12	–	–	はい	はい	はい	はい
AppDNA 7.13	–	–	はい	はい	はい	はい
AppDNA 7.14	–	–	–	–	はい	はい
AppDNA 7.15	–	–	–	–	–	はい

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、自動的に分析が開始されます。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［概要］ページの情報を確認し、［次へ］をクリックします。
3. ［**AppDisk** の作成］ページで、［新しい **AppDisk** を作成する］ラジオボタンを選択します。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。［次へ］をクリックします。
4. ［準備用マシン］ページで、AppDisk を構築するマスターイメージとして使用する、ランダムにプールされた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 VM を選択し、［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（そのほかの注意事項：ハイパーバイザー管理コンソールからアプリケーションを AppDisk にインストールする必要があります。Studio の［操作］ペインの［アプリケーションのインストール］タスクは使用しないでください）。

AppDisk の封印

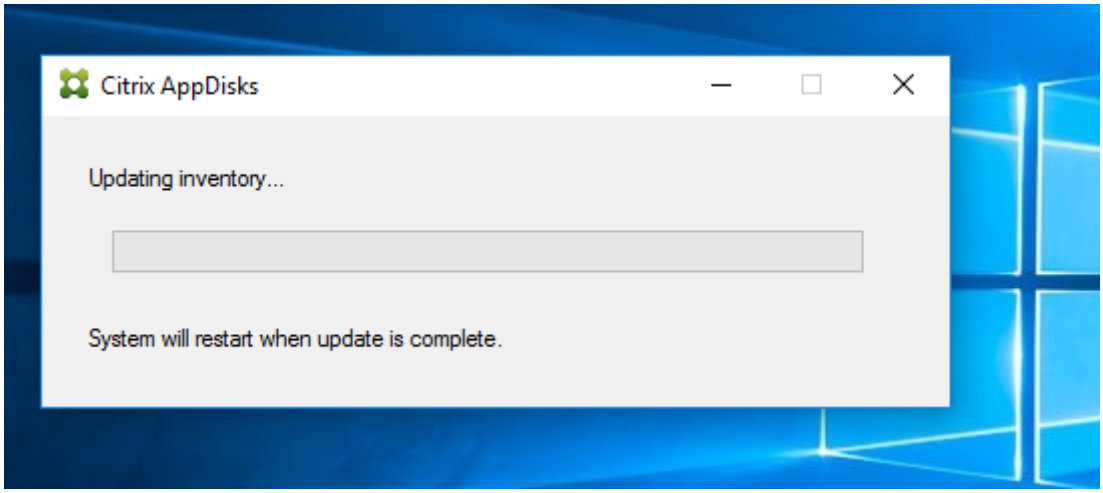
1. Studio のナビゲーションペインで ［**AppDisks**］を選択します。
2. 作成した AppDisk を選択し、［操作］ペインで ［**AppDisk** の封印］を選択します。

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。

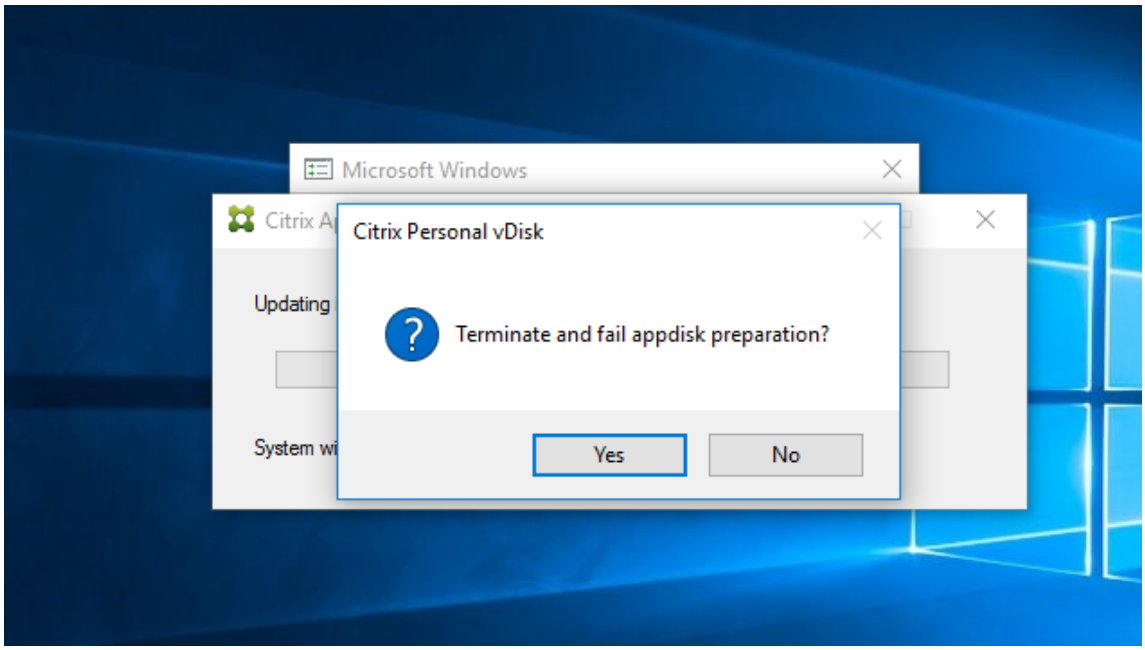
AppDisk の準備と封印の取り消し

管理者による AppDisk の作成や封印の取り消しが必要な場合があります：

1. VM にアクセスします。
2. ダイアログを閉じます：



3. ダイアログを閉じると、ポップアップメッセージが表示され、選択した操作の取り消しの確認を求められますので、［はい］をクリックします。



> 注:
>
> AppDisk の準備を取り消した場合、マシンを再起動すると初期状態に戻ります。再起動しない場合は、新しい VM を作成する必要があります。

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］を選択します。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にない場合は、C:¥Program Files¥Citrix¥personal vDisk¥bin にあるコマンドプロンプトを開き、次を入力します：**CtxPvD.Exe -s LayerCreationBegin** マシンが再起動し、ディスクを準備します。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の ［**AppDisk** のパッケージ化］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］ページで情報を確認し、［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］ラジオボタンを選択します。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、マシンを参照してディスクを選択し、［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 を追加する場合は、デリバリーグループの作成ウィザードの ［**AppDisks**］ページで次のガイダンスを使用します。（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、［操作］ペインの ［**AppDisks** 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

［**AppDisks**］ページ（デリバリーグループの作成ウィザードまたは［AppDisks の管理］フロー）には、デリバリーグループ用にすでに配備されている 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. ［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、左側の列にすべての AppDisk が一覧表示されます。既にこのデリバリーグループに割り当てられている AppDisk のチェックボックスはオンになっており、選択することはできません。
2. 左側の列で、選択可能な AppDisk のチェックボックスを 1 つまたは複数オンにします。右側の列に AppDisk のアプリケーションが一覧表示されます（右の列の上にある ［アプリケーション］タブを選択すると、［スタート］メニューと同様の形式でアプリケーションが一覧表示され、［インストール済みパッケージ］タブを選択すると、［プログラムと機能］リストと同様の形式でアプリケーションが一覧表示されます。
3. 1 つまたは複数の使用可能な AppDisk を選択したら、［**OK**］をクリックします。
4. ［AppDisks］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、［**AppDisks**］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、AppDisk の管理の表示）に AppDisk が降順で表示されます。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。

AppDisk 作成のウイルス対策に関する考慮事項

場合によっては、ベース仮想マシンにウイルス対策（A/V）エージェントがインストールされているシナリオで、AppDisk の作成時に問題が発生する場合があります。そのような場合、A/V エージェントがいくつかのプロセスにフラグを立てると AppDisk 作成が失敗する場合があります。これらのプロセス、**CtxPvD.exe** および **CtxPvDSrv.exe** は、ベース仮想マシンが使用する A/V エージェントの例外リストに追加する必要があります。

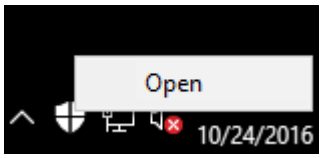
このセクションでは、次のウイルス対策アプリケーションでの例外の追加について説明します。

- Windows Defender（Windows 10 用）
- OfficeScan（バージョン 11.0）
- Symantec（バージョン 12.1.16）
- McAfee（バージョン 4.8）

Windows Defender

ベース仮想マシンが Windows Defender（バージョン 10）を使用している場合：

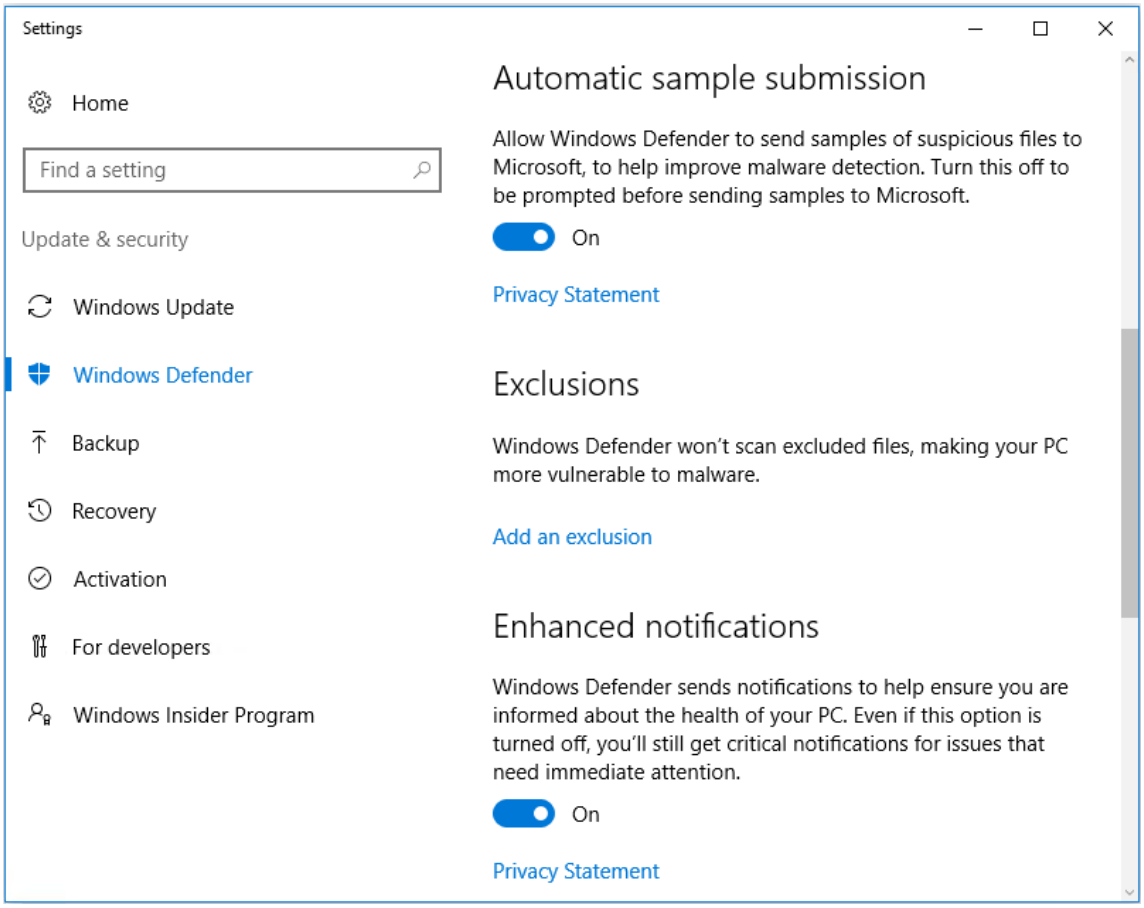
1. ローカル管理者権限でコンピューターにログオンします。
2. Windows Defender のアイコンを選択して右クリックし、［開く］ボタンを表示します：

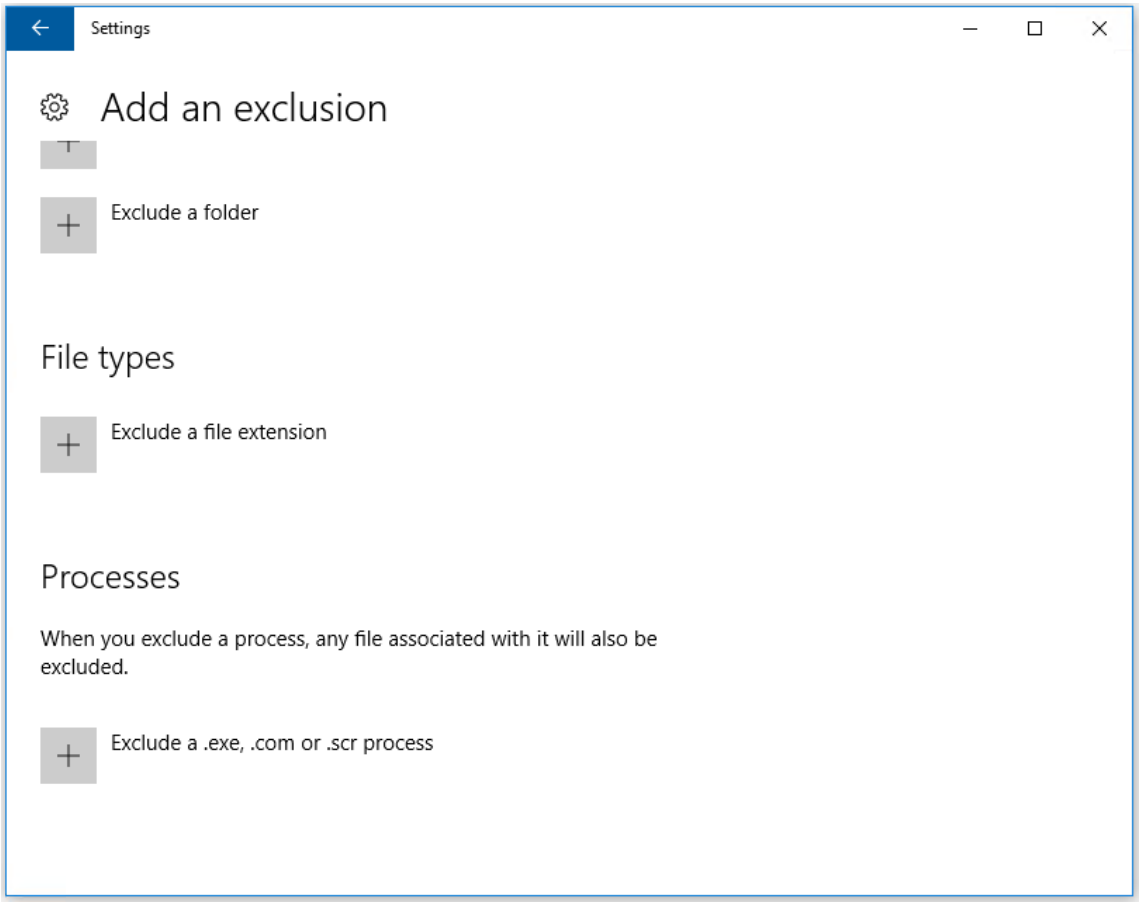
3. Windows Defender コンソールで、インターフェイスの右上部分の ［設定］を選択します：

   ローカライズされた画像］（/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-main-page.png）

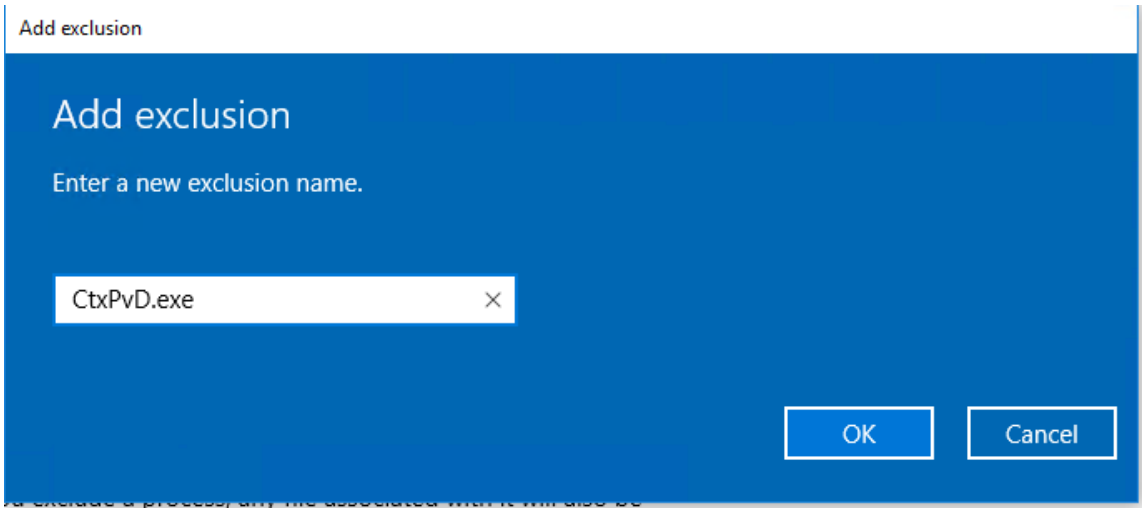
4. ［設定］画面の ［除外］部分で、［除外の追加］をクリックします：



5. ［除外の追加］画面で、［**.exe**、**.com**、または**.scr** プロセスを除外します］をクリックします：



6. ［除外の追加］画面で除外の名前を入力します。AppDisk 作成時の競合を避けるため、**CtxPvD.exe** と **CtxPvDSvc.exe** を追加する必要があります。除外名を入力したら、［**OK**］をクリックします:



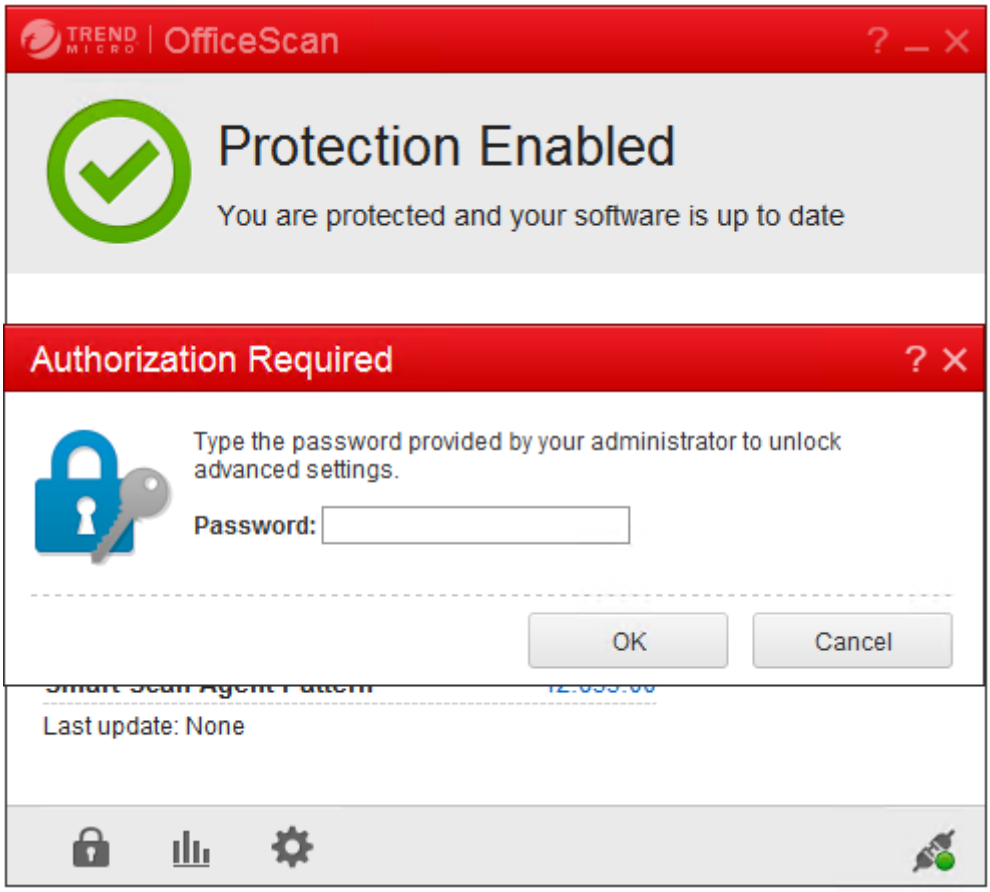
除外項目を追加すると、［設定］画面にある除外されたプロセスのリストに表示されます:

```
1 ![localized image](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-
    process-added.png)
```

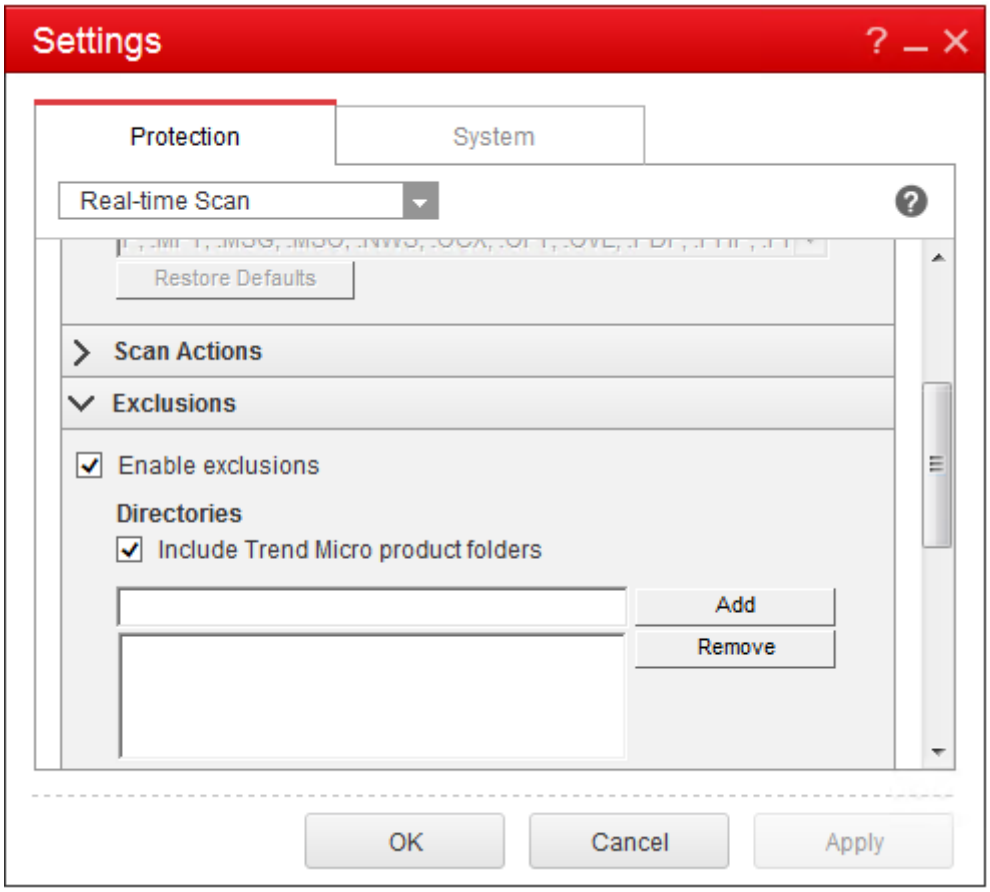

OfficeScan

ベース仮想マシンが OfficeScan（バージョン 11）を使用している場合：

1. OfficeScan コンソールを起動します。
2. インターフェイスの左下部分にあるロックアイコンをクリックして、パスワードを入力します：

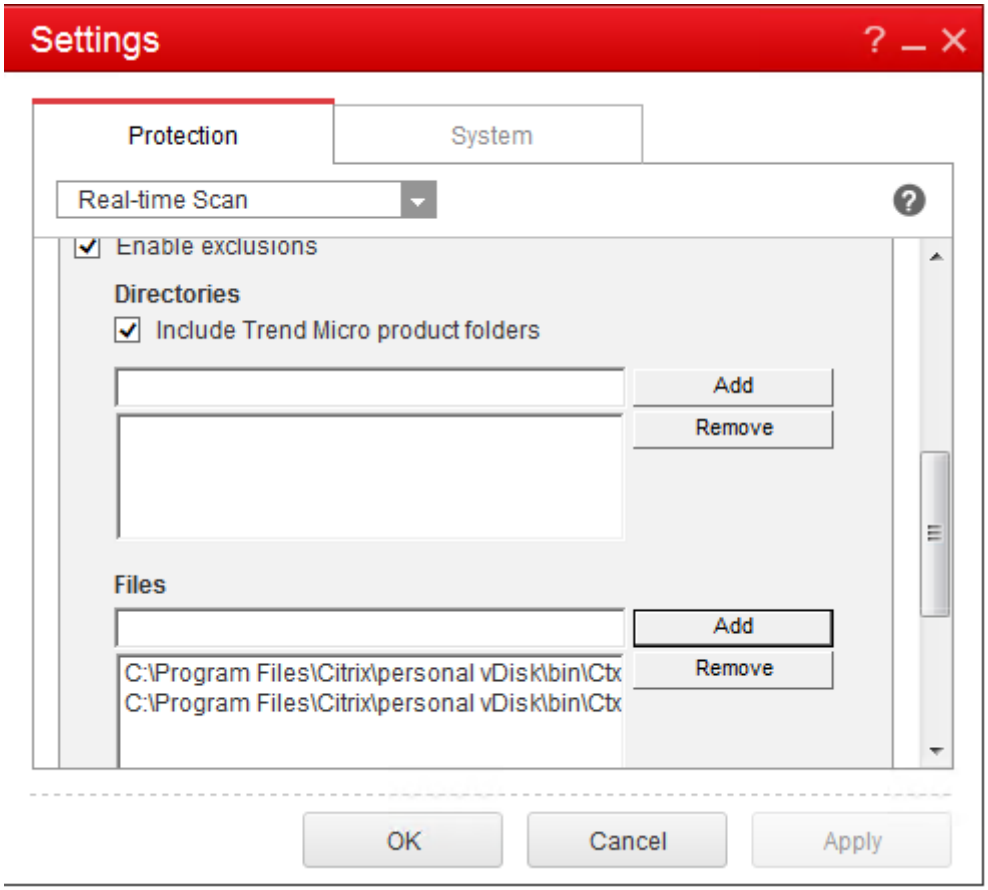


3. ［設定］アイコンをクリックして、構成オプションを表示します。
4. ［設定］画面で、［保護］タブを選択します。
5. ［保護］タブで、［除外］セクションが見つかるまでスクロールダウンします。



6. ［ファイル］セクションで、［追加］をクリックし、次の AppDisk プロセスを例外一覧に入力します:

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```

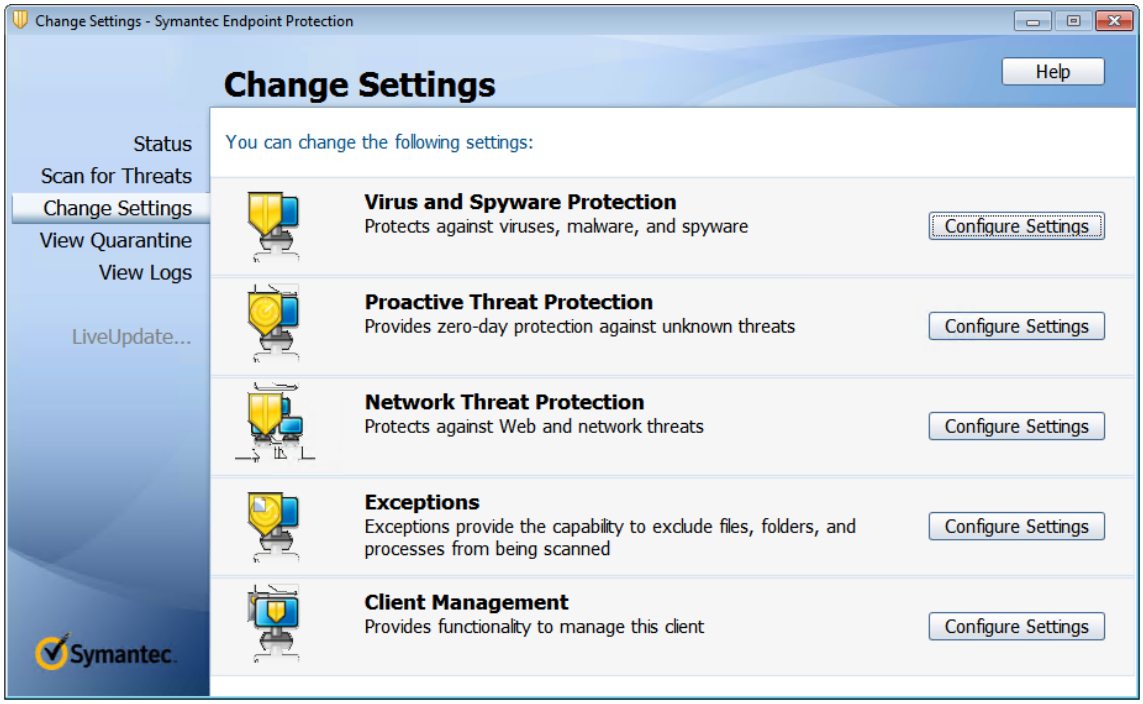



［適用］をクリックし、［**OK**］をクリックして除外を追加します。

Symantec

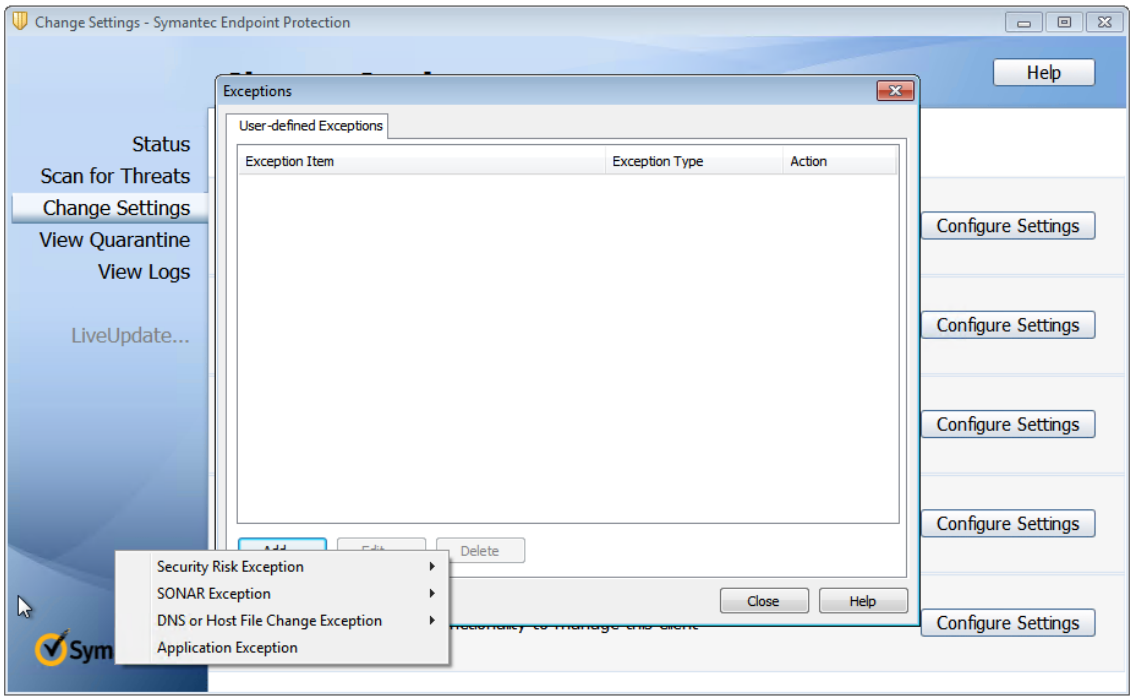
ベース仮想マシンが Symantec （バージョン 12.1.16）を使用している場合：

1. Symantec コンソールを起動します。
2. ［設定の変更］をクリックします。
3. ［例外］セクションで ［設定の構成］をクリックします：



4. ［オプションの設定］画面で ［追加］をクリックします。

5. ［追加］をクリックすると、表示されたコンテキストメニューで、アプリケーションのタイプを指定できます。［アプリケーション例外］を選択します:

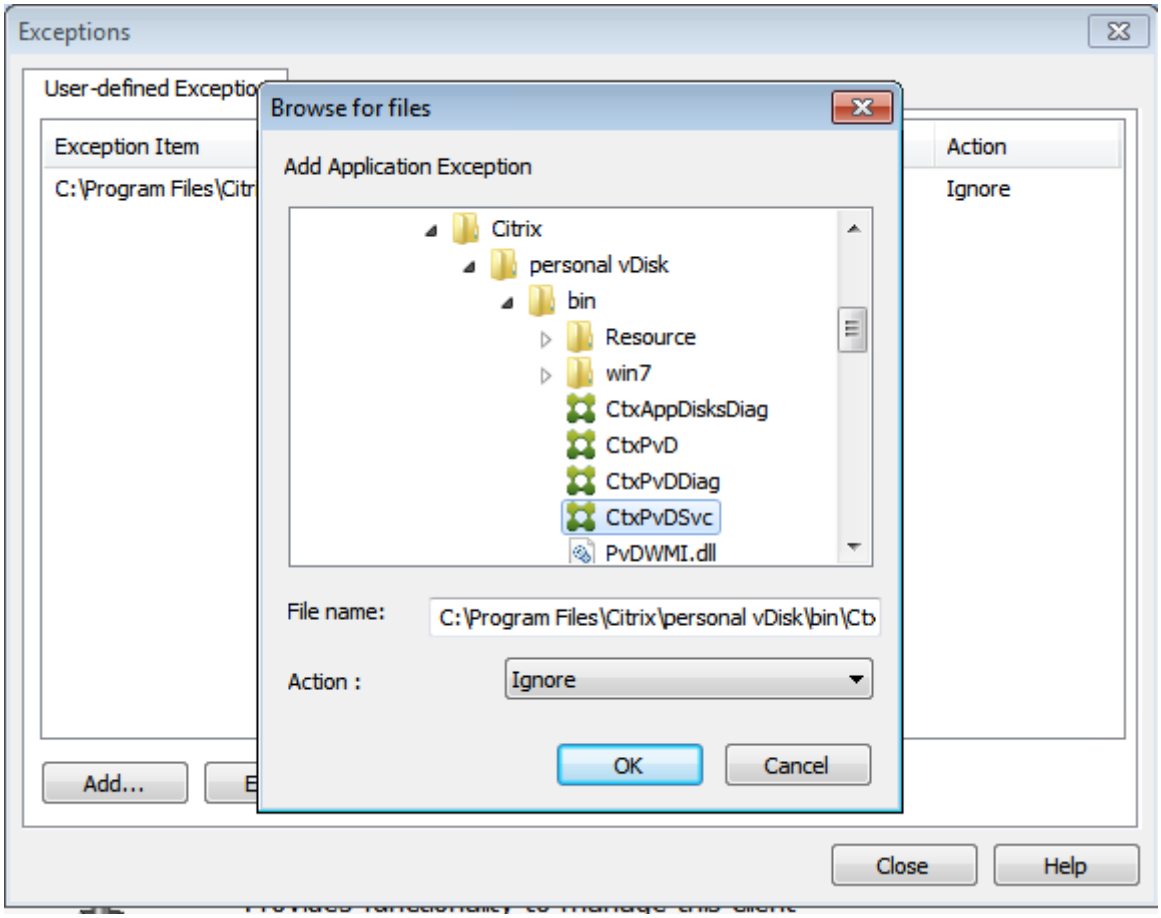


6. ［例外］画面で、次の AppDisk ファイルパスを入力し、操作を ［無視］に設定します:

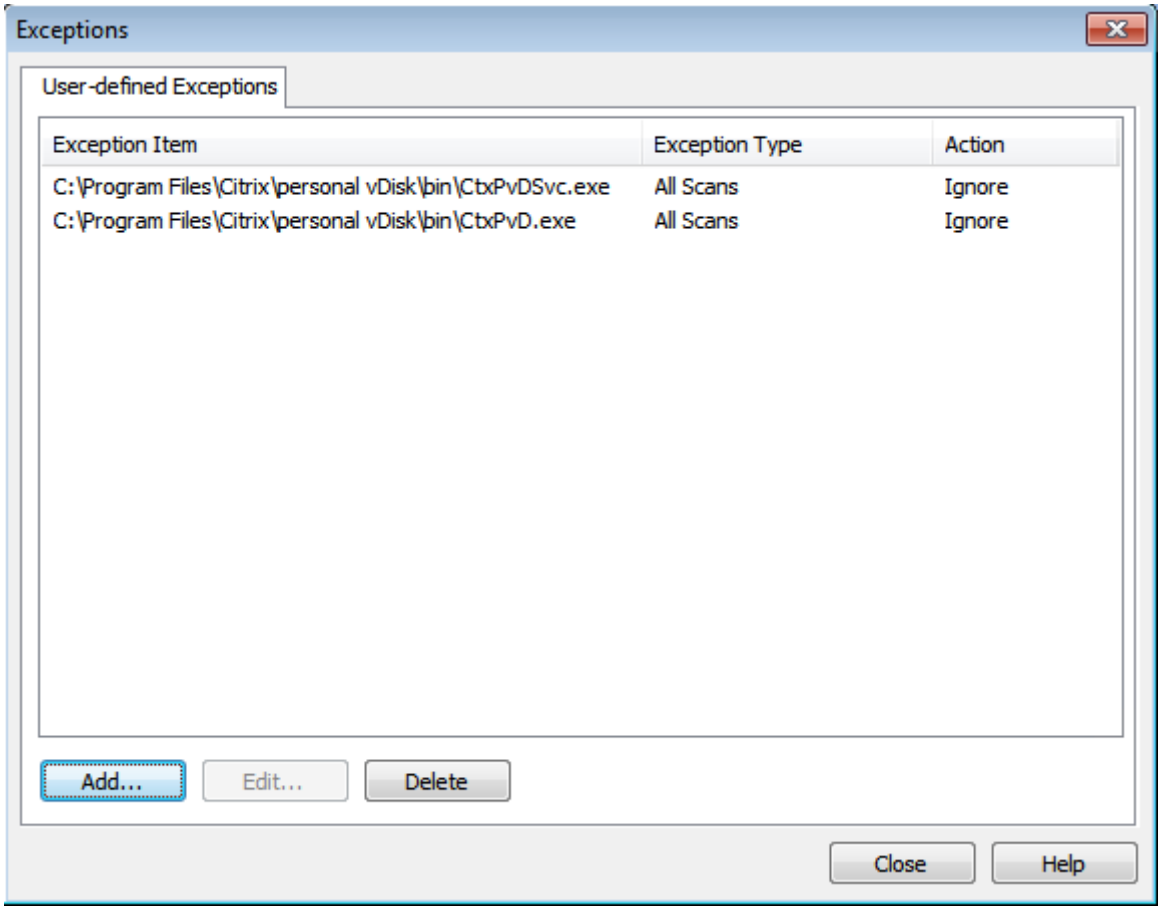
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```



```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```



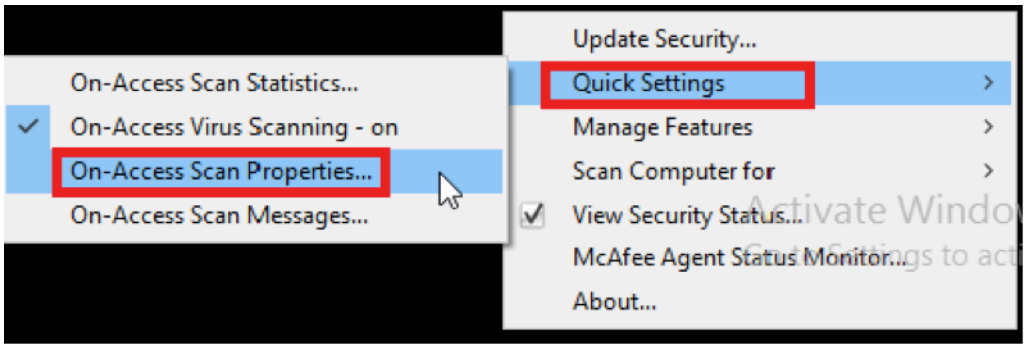
書きとめられた例外が一覧に追加されます。ウィンドウを閉じて変更を適用します。



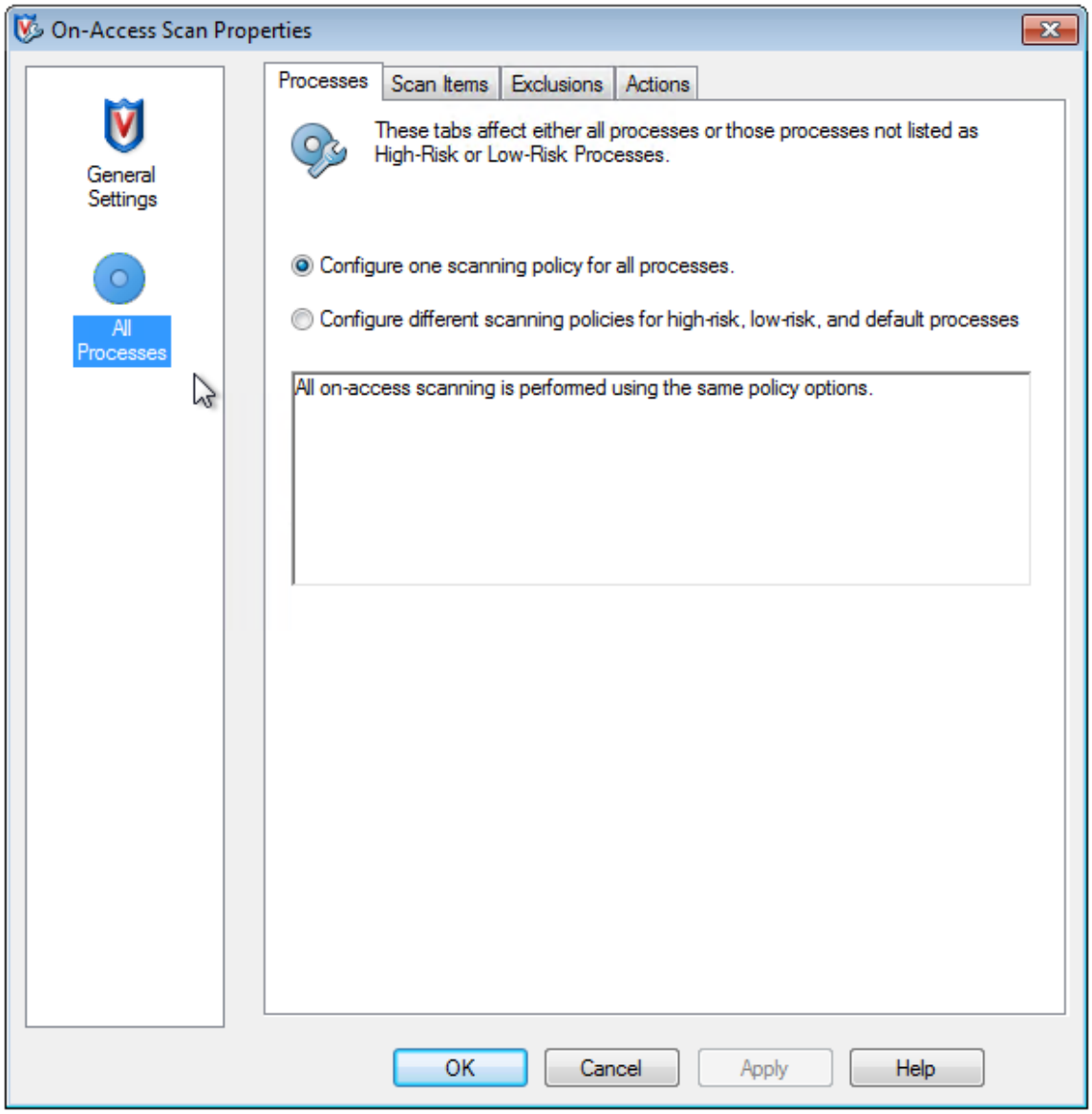
McAfee

ベース仮想マシンが McAfee（バージョン 4.8）を使用している場合：

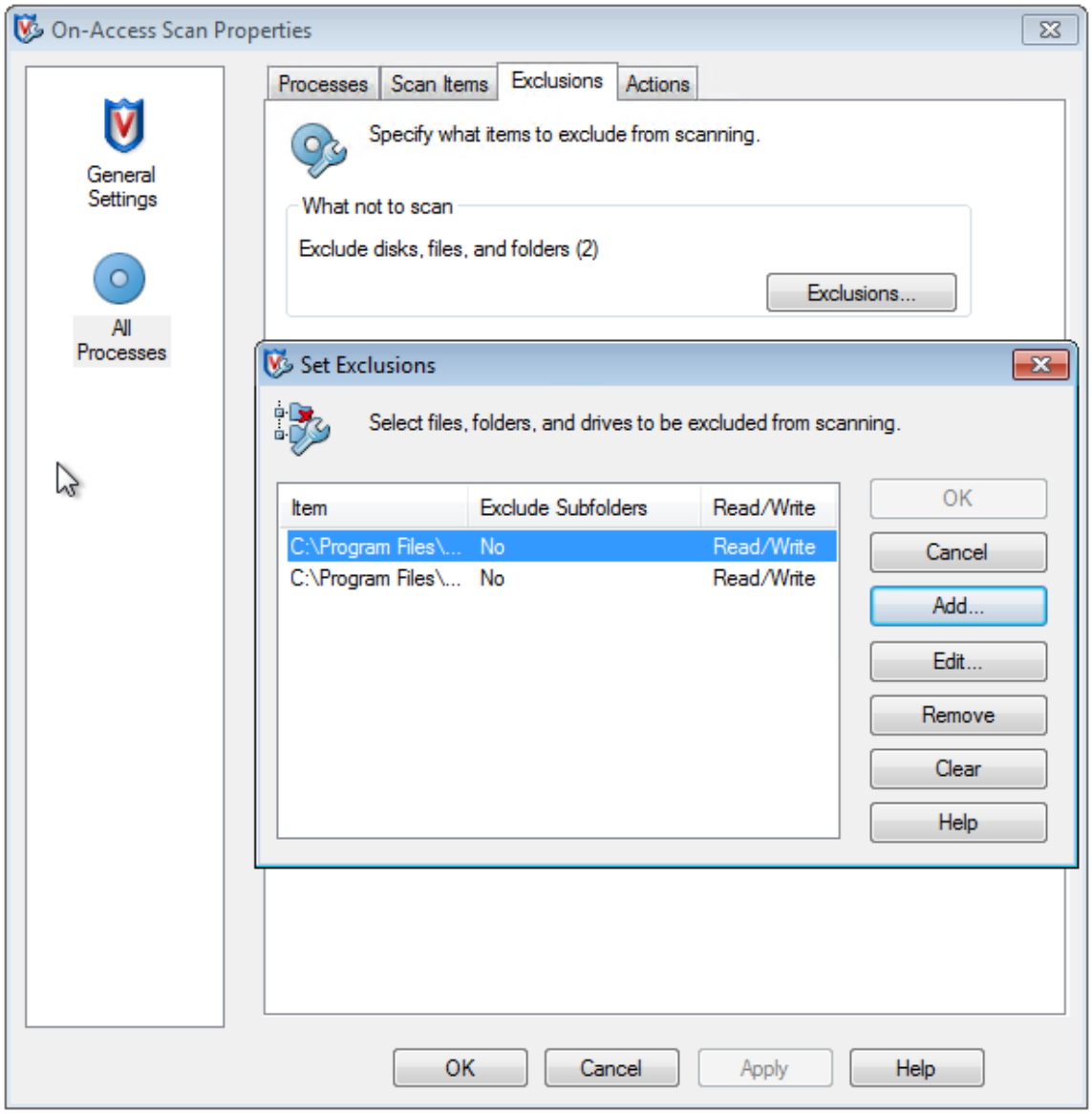
1. McAfee アイコンを右クリックし、［クイック設定］オプションを展開します。
2. 拡張メニューで、［オンアクセススキャンのプロパティ］を選択します：



3. ［オンアクセススキャンのプロパティ］画面で、［すべてのプロセス］をクリックします：



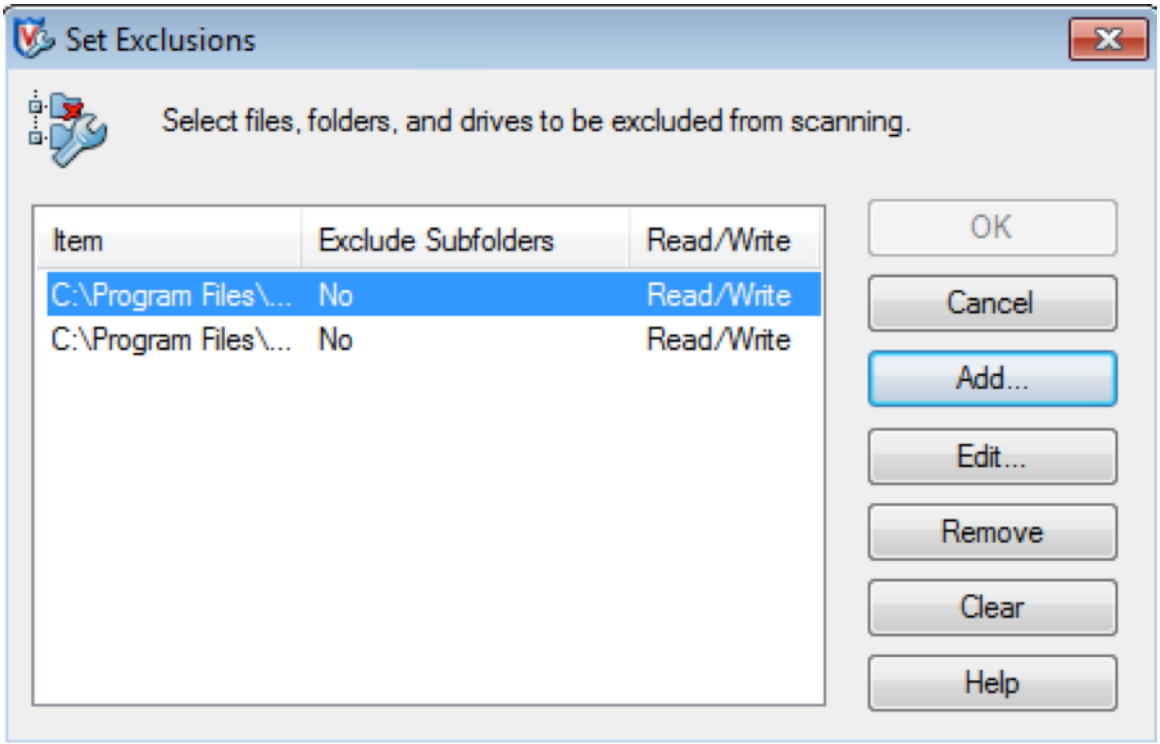
4. ［除外］タブを選択します。
5. ［除外］ボタンをクリックします。
6. ［除外の設定］画面で ［追加］をクリックします:



7. ［除外項目の追加］画面で、［名前/場所（ワイルドカード ***** または**?** を使用可能）］を選択します。［参照］をクリックして、除外実行ファイルを見つけます:

```
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```

［**OK**］をクリックします。［除外の設定］画面に、追加された除外が表示されます。［**OK**］をクリックして変更を適用します:



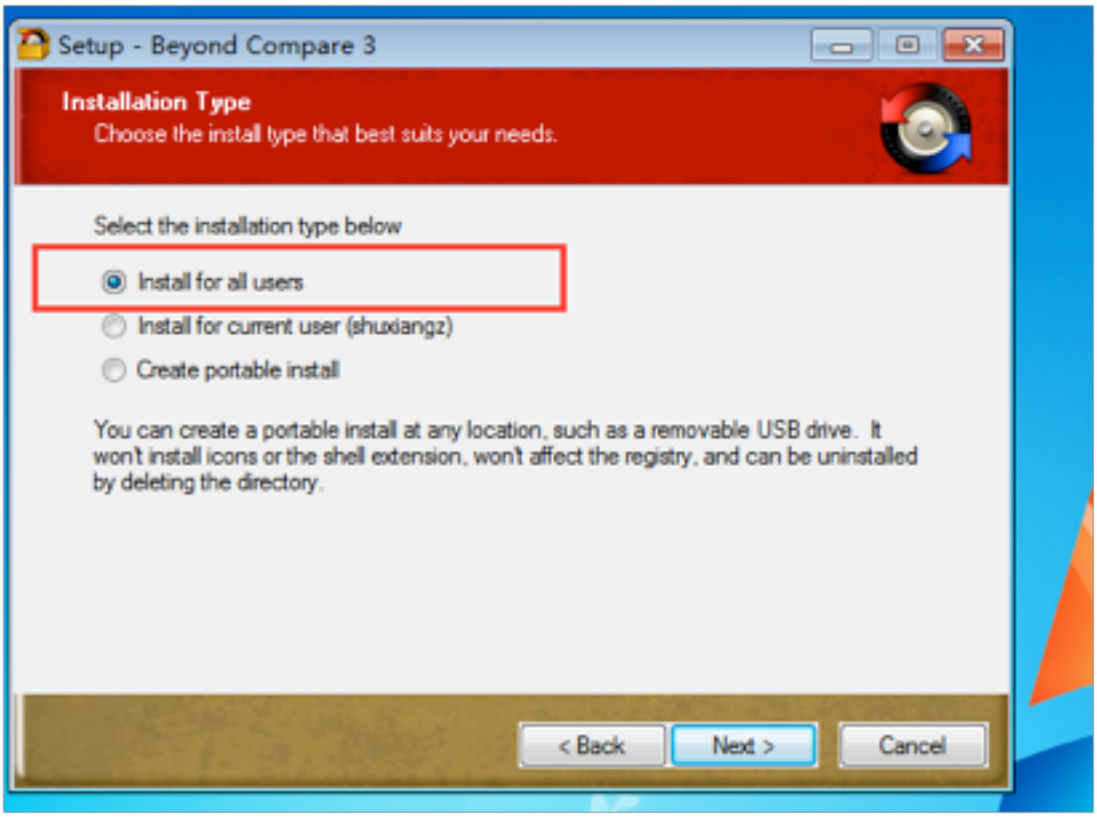
> 注:
>
> これらの除外を構成したら、AppDisk を作成します。

［スタート］メニューにアプリケーションを表示する方法

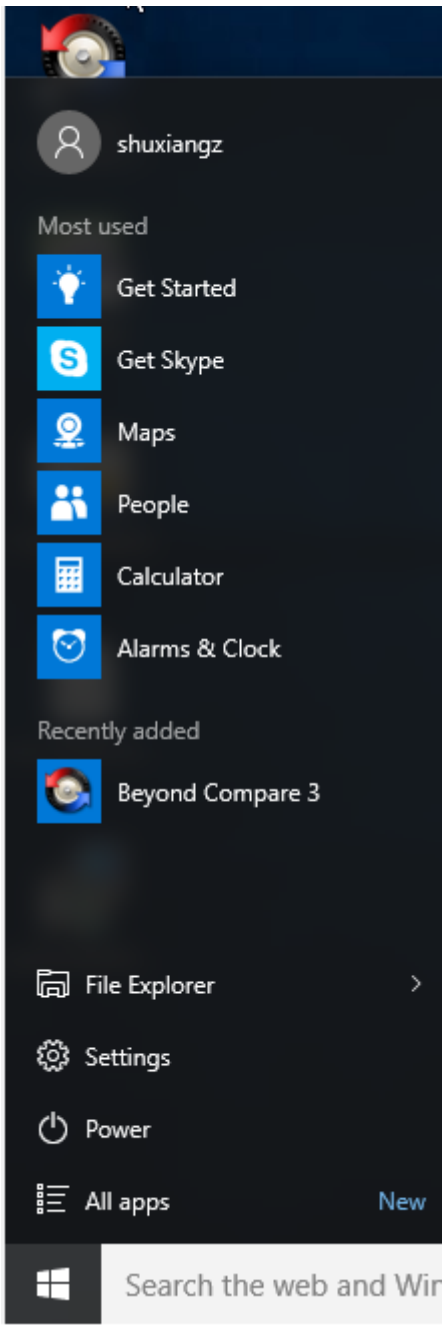
新しい AppDisk が作成され、アプリがすべてのユーザーから利用可能になると、ディスクはデスクトップにアタッチされ、アプリのショートカットが［スタート］メニューに表示されます。AppDisk が現在のユーザーに対してのみ作成およびインストールされ、ディスクがデスクトップにアタッチされた場合、アプリのショートカットは［スタート］メニューに表示されません。

新しいアプリを作成して、それをすべてのユーザーが利用できるようにするには

1. AppDisk にアプリをインストールします（たとえば、*Beyond Compare* が選択されたアプリだとします）:

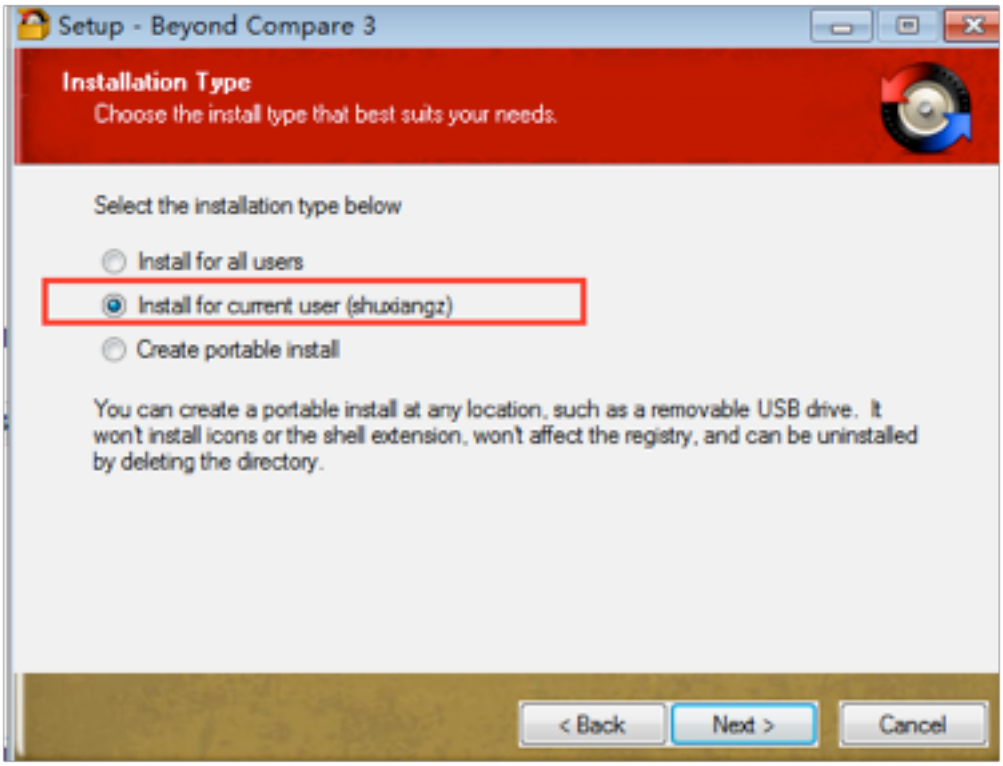


2. デスクトップにディスクをアタッチします。新しくインストールされたアプリ（*Beyond Compare*）のショートカットが、次のように［スタート］メニューに表示されます：

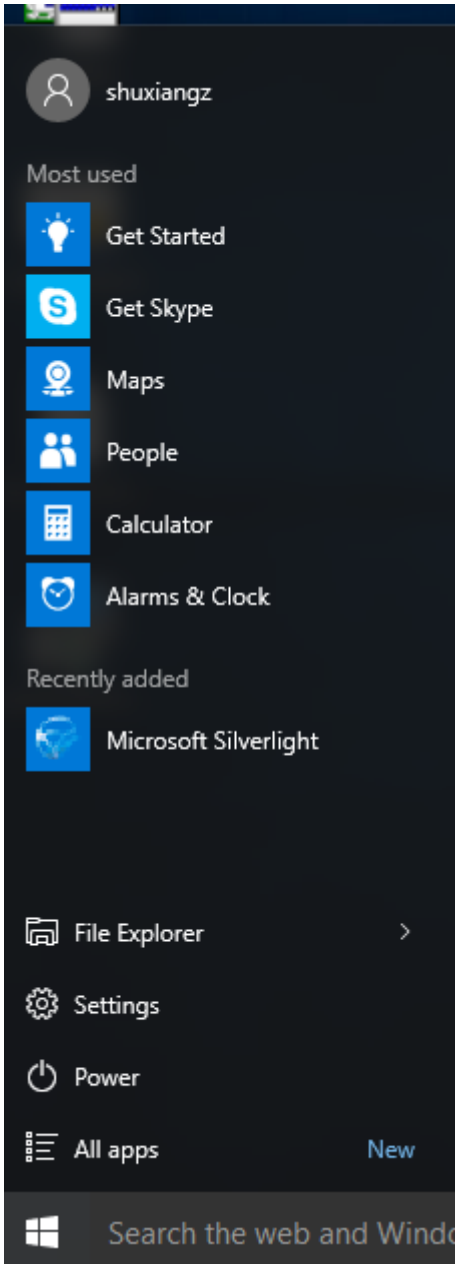


現在のユーザー用にのみアプリケーションをインストールするには

1. AppDisk にアプリをインストールし、現在のユーザーが利用できるようにします:



2. デスクトップにディスクをアタッチします。ショートカットが［スタート］メニューに表示されないことに注意してください：



AppDisk ログの更新

このリリースで AppDisk のログとサポートのパラダイムが強化されました。このアップデートによって、AppDisk ユーザーは、診断情報を取得して、任意でCIS（Citrix Insight Services）の Web サイトにアップロードできるようになりました。

どのように動作するのですか**?**

この新機能で使用されるスクリプトベースの PowerShell ツールによって、AppDisk や PVD が作成するログファイルをすべて洗い出し、システム（およびプロセス）に関する情報を含む PowerShell コマンドの出力を収集して、すべての情報を整理された単一のファイルに圧縮し、最終的に圧縮されたフォルダーをローカルに保存するか、CIS にアップロードするかを選択できます。

> 注:
>
> CIS では匿名の診断情報を収集し、AppDisk や PVD の機能強化に役立てています。Citrix Insight Services（CIS）の Web サイトにアクセスして、手動で診断バンドルをアップロードしてください。このサイトへのアクセスには、お手持ちの Citrix 資格情報でログインする必要があります。

PowerShell スクリプトを使用して **AppDisk** や **PVD** のログファイルを収集する

AppDisk および PVD のインストーラーに診断データ収集のためのスクリプトが新たに 2 つ追加されました。

- **Upload-AppDDiags.ps1** – AppDisk の診断データ収集を実行します
- **Upload-PvDDiags.ps1** – PvD の診断データ収集を実行します

> 注:
>
> これらのスクリプトは、C:\Program Files\Citrix\personal vDisk\bin\scripts に追加されています。これらの PowerShell スクリプトは管理者として実行する必要があります。

Upload-AppDDiags.ps1 を使って AppDisk の診断データ収集を開始し、任意で手動により CIS の Web サイトにデータをアップロードします。

```
SYNTAX
     Upload-AppDDiags [[-OutputFile] <string>] [-help] [<
        CommonParameters>]
         -OutputFile
             Local path for zip file instead of uploading to CIS
 EXAMPLES
     Upload-AppDDiags
         Upload diagnostic data to Citrix CIS website using credentials
             entered by interactive user.
     Upload-AppDDiags -OutputFile C:\MyDiags.zip
         Save AppDisk diagnostic data to the specified zip file. You
            can access https://cis.citrix.com/ to upload it later.
```

> ヒント:
>
> **–OutputFile** 引数を指定しない場合、アップロードが実行されます。**–OutputFile** を指定した場合は、スクリプトによって zip ファイルが作成され、後から手動でアップロードできます。

Upload-PvDDiags.ps1 を使って PvD の診断データ収集を開始し、任意で手動により CIS の Web サイトにデータをアップロードします。


```
SYNTAX
 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
     -OutputFile
         Local path for zip file instead of uploading to CIS
 EXAMPLES
     Upload-PvDDiags
         Upload PvD diagnostic data to Citrix CIS website using
            credentials entered by interactive user.
     Upload-PvDDiags -OutputFile C:\MyDiags.zip
         Save PvD diagnostic data to the specified zip file. You can
            access https://cis.citrix.com/ to upload it later.
```

> ヒント:
>
> **–OutputFile** 引数を指定しない場合、アップロードが実行されます。**–OutputFile** を指定した場合は、スクリプトによって zip ファイルが作成され、後から手動でアップロードできます。

XenApp Secure Browser

August 24, 2021

アプリケーションの Web への移行が進むにつれて、Web ベースのアプリケーションに対応するために、ユーザーは複数のベンダーおよびバージョンのブラウザーを使用する必要があります。アプリケーションを社内でホストしていると、多くの場合、組織はリモートユーザーにアクセスを提供するために複雑な VPN ソリューションをインストールして構成する必要があります。一般的な VPN ソリューションには、クライアント側のエージェントが必要ですが、このエージェントもさまざまなオペレーティングシステムで維持する必要があります。

XenApp Secure Browser を使用すると、ユーザーに Web ベースのアプリケーションのエクスペリエンスをシームレスに提供することができます。ホストしている Web ベースのアプリケーションは、ユーザーが希望するローカルブラウザーに表示されます。たとえば、ユーザーがブラウザーに Mozilla Firefox を希望しても、アプリケーションが対応しているのは Microsoft Internet Explorer のみという場合があります。XenApp Secure Browser を使用すると、Internet Explorer に対応するアプリケーションが、Firefox ブラウザーのタブに表示されます。

XenApp Secure Browser Edition の展開

XenApp Secure Browser の展開には、次の手順が含まれます:

- 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

XenApp Secure Browser のインストール

1. Citrix のダウンロードサイトから、Citrix XenApp Secure Browser Edition ISO をダウンロードします。(ダウンロードページ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. さまざまな XenApp コンポーネントのインストール手順に従います。
3. 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。

      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`を実行し、Citrix 固有の PowerShell モジュールをロードします。`Asnp`は Add-PSSnapin を意味します。
   c) 現在のサイト設定とライセンスモードを確認するには、`Get-ConfigSite`を実行します。
   d) ライセンスモードを XenApp Secure Browser エディションに設定するには、`Set-ConfigSite -ProductCode XDT -ProductEdition BAS`を実行します。
   e) 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するには、`Get-BrokerSite`を実行します。

コンテンツの公開

August 24, 2021

Microsoft Word ドキュメントや Web リンクなどのリソースへの URL または UNC パスを、アプリケーションとして公開できます。この機能は、コンテンツの公開と呼ばれています。コンテンツの公開機能を使用することで、ユーザーへのコンテンツの配信をより柔軟に行うことができるようになります。既存のアプリケーションのアクセス制御と管理機能を使用できるというメリットもあります。さらに、コンテンツを開くのにローカルアプリケーションと公開アプリケーションのどちらを使用するかも指定できます。

公開コンテンツは、StoreFront や Citrix Receiver の他のアプリケーションと同じように表示されます。アクセス方法はアプリケーションへアクセスするときと同じです。クライアントでは、リソースは通常どおりに開かれます。

- ローカルにインストールされているアプリケーションが適している場合は、こうしたアプリケーションが起動されリソースが開かれます。
- ファイルタイプの関連付けが定義されている場合は、公開アプリケーションが起動されリソースが開かれます。

コンテンツの公開には PowerShell SDK を使用します。(Studio を使用してコンテンツを公開することはできませんが、アプリケーションの公開後に Studio を使用してそのプロパティを編集することはできます)。

構成の概要と準備

コンテンツの公開では、New-BrokerApplication コマンドレットに以下のキープロパティを指定して使用します（すべてのコマンドレットプロパティの説明についてはこのコマンドレットのヘルプを参照してください）。

```
New-BrokerApplication  -ApplicationType PublishedContent
\-CommandLineExecutable \<*location*> -Name \<*app-name*>
\-DesktopGroup \<*delivery-group-name*>
```

ApplicationType プロパティには PublishedContent を指定する必要があります。

CommandLineExecutable プロパティでは、公開するコンテンツの場所を指定します。以下の形式を使用でき、最大文字数は 255 文字です。

- HTML Web サイトアドレス（例: `https://www.citrix.com`）
- Web サーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTP サーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTP サーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt`）
- UNC ディレクトリパス（例: `file://myServer/myShare`または`\\myServer\myShare`）
- UNC ファイルパス（たとえば、`file://myServer/myShare/myFile.asf`または`\\myServer\myShare\myFile.asf`）

適切な SDK があることを確認します。

- 展開環境が XenApp および XenDesktop Service の場合は、XenApp と XenDesktop 用の Remote PowerShell SDK をダウンロードしてインストールします。
- 展開環境がオンプレミスの XenApp および XenDesktop の場合は、Delivery Controller とともにインストールされている PowerShell SDK を使用します。公開コンテンツアプリケーションの追加には Delivery Controller のバージョン 7.11 以上が必要です。

以下の手順ではサンプルを利用しています。このサンプルの詳細は次のとおりです。

- マシンカタログを作成しています。
- PublishedContentApps という名前のデリバリーグループを作成しています。このデリバリーグループでは、カタログのサーバー OS マシンを使用しています。このデリバリーグループには、ワードパッドアプリケーションが追加されています。
- デリバリーグループ名、CommandLineExecutable の場所、およびアプリケーション名用の変数を作成しています。

はじめに

PowerShell SDK をインストール済みのマシンで PowerShell を開きます。

次のコマンドレットにより、適切な PowerShell スナップインを追加し、返されたデリバリーグループレコードを変数に代入します。


```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

XenApp および XenDesktop Service を使用している場合は、Citrix Cloud 資格情報を入力して認証を行います。ユーザーが複数存在する場合は 1 人を選択します。

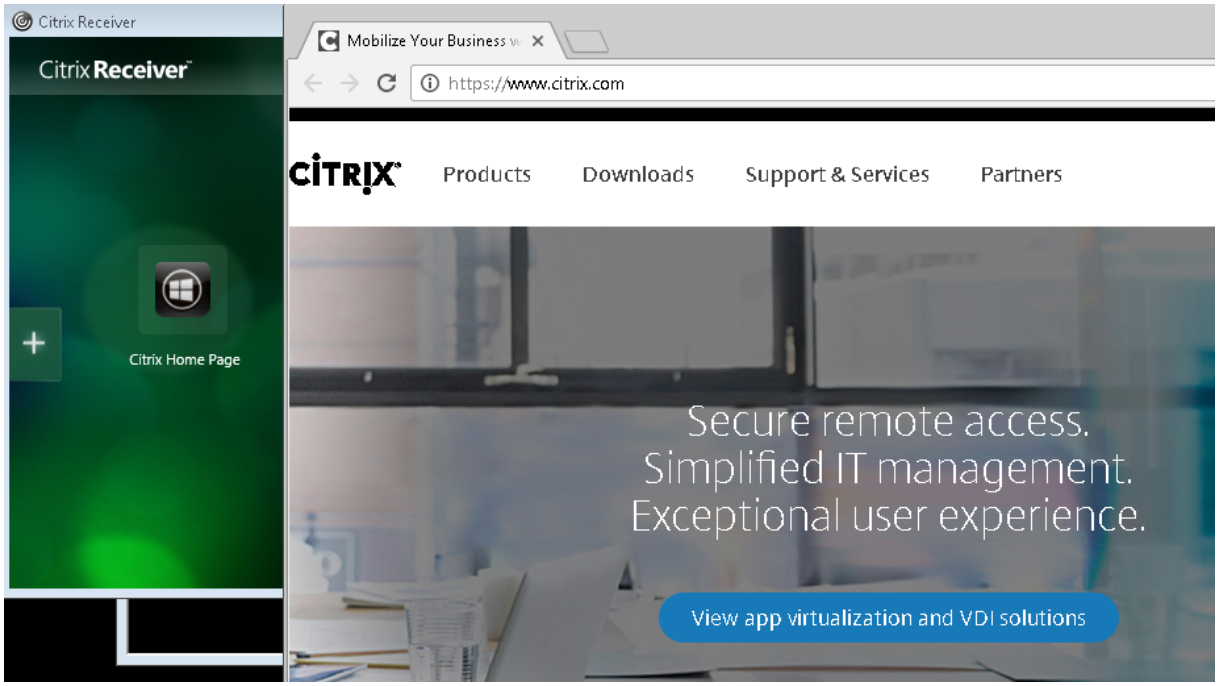
URL の公開

次のコマンドレットでは、場所とアプリケーション名を変数に代入してから Citrix ホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $citrixURL -Name $appName
 -DesktopGroup $dg.Uid
<!--NeedCopy-->
```

実行結果の確認

- StoreFront を開き、PublishedContentApps デリバリーグループのアプリケーションにアクセスできるユーザーとしてログオンします。新しく作成したアプリケーションが、デフォルトのアイコンで表示されます。アイコンのカスタマイズ方法については、https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/を参照してください。
- Citrix Home Page アプリケーションをクリックします。ローカルで実行されているデフォルトブラウザーのインスタンスの新しいタブで、指定した URL が開かれます。



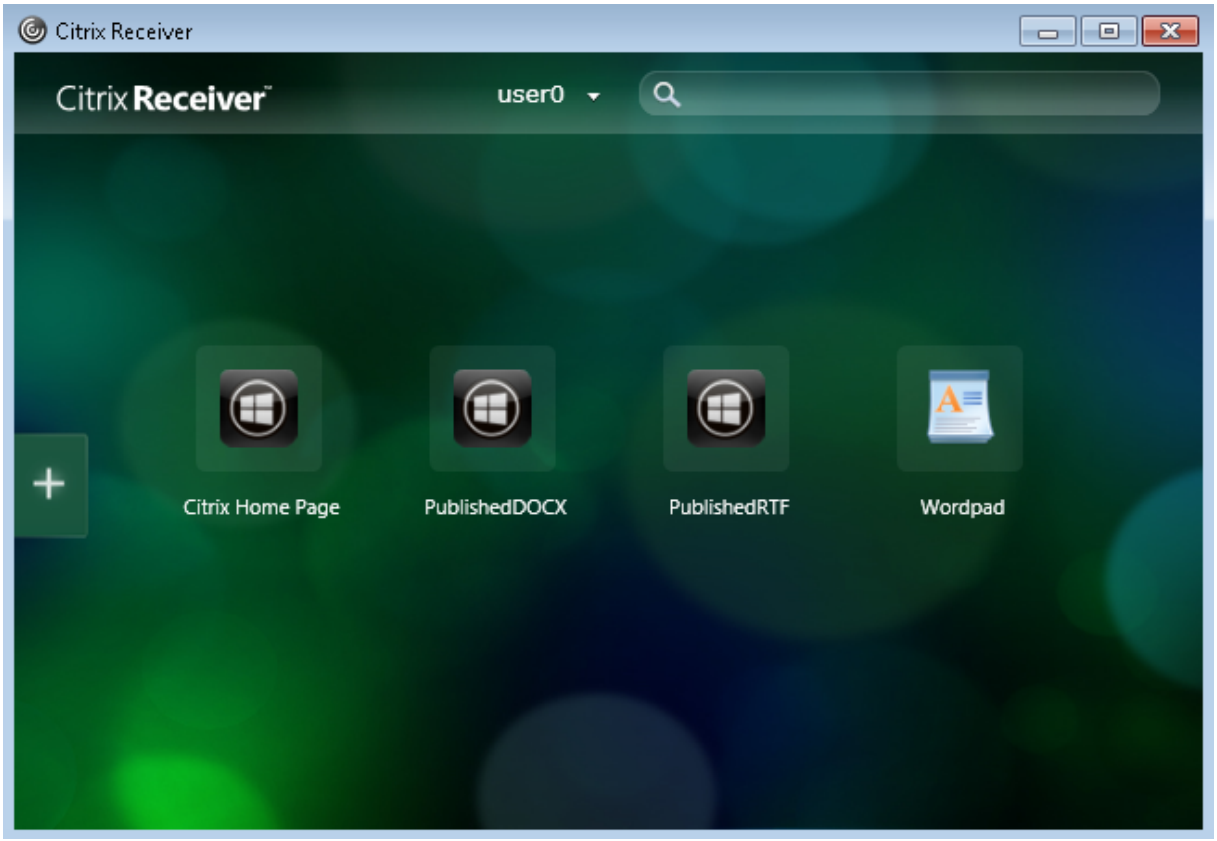
UNC パスに配置されているリソースの公開

この例では、管理者が共有名 PublishedResources をすでに作成しています。次のコマンドレットで、場所とアプリケーション名を変数に代入してから、この共有に含まれる RTF ファイルと DOCX ファイルをリソースとして公開します。

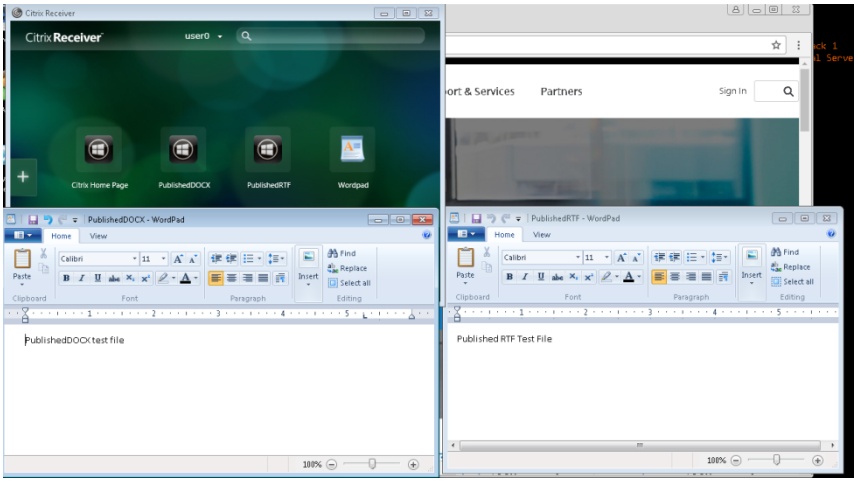
```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

実行結果の確認

- StoreFront ウィンドウを更新して、新しく公開したドキュメントが表示されることを確認します。

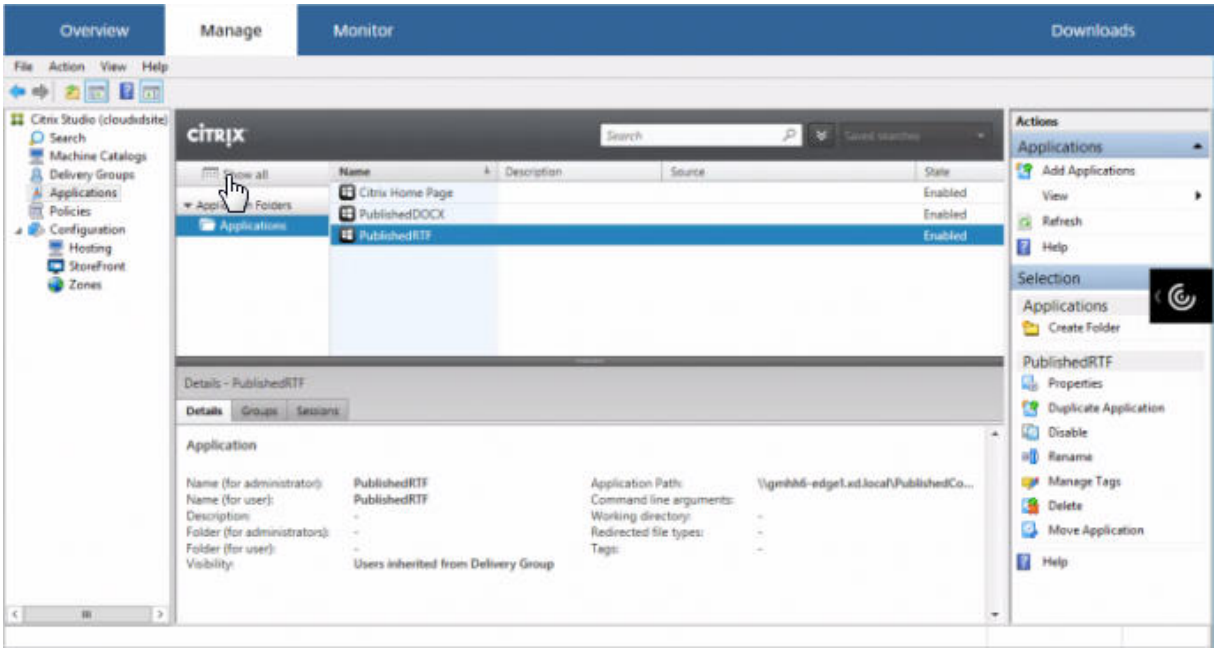


- PublishedRTF アプリケーションおよび PublishedDOCX アプリケーションをクリックします。各ドキュメントが、ローカルで実行されるワードパッドで開きます。

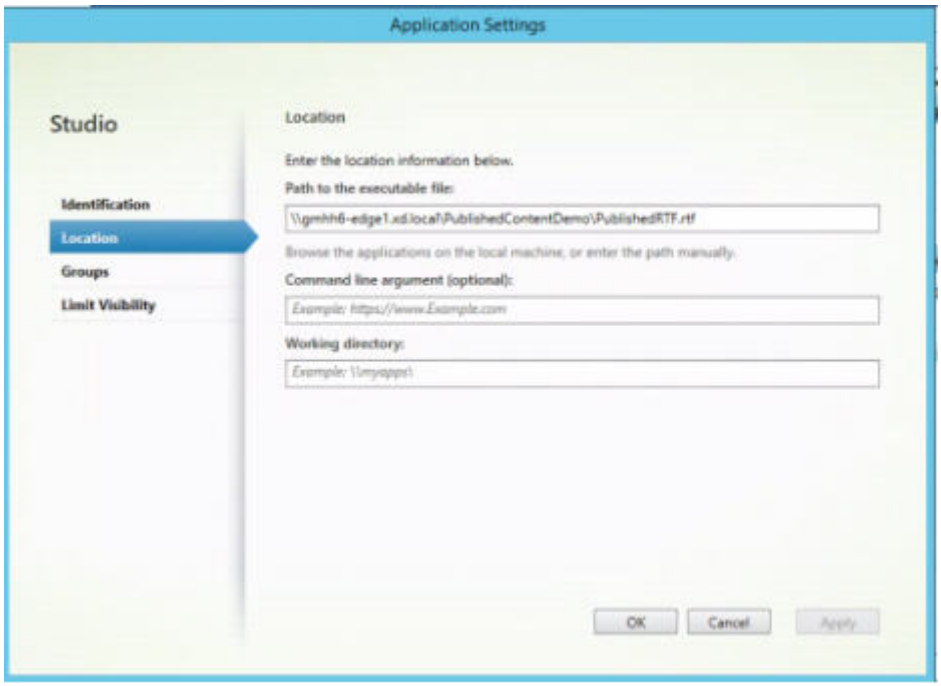


PublishedContent アプリケーションの確認と編集

公開コンテンツは、他の種類のアプリケーションと同じ方法で管理できます。公開されたコンテンツアイテムは Studio のアプリケーション一覧に表示され、Studio で編集できます

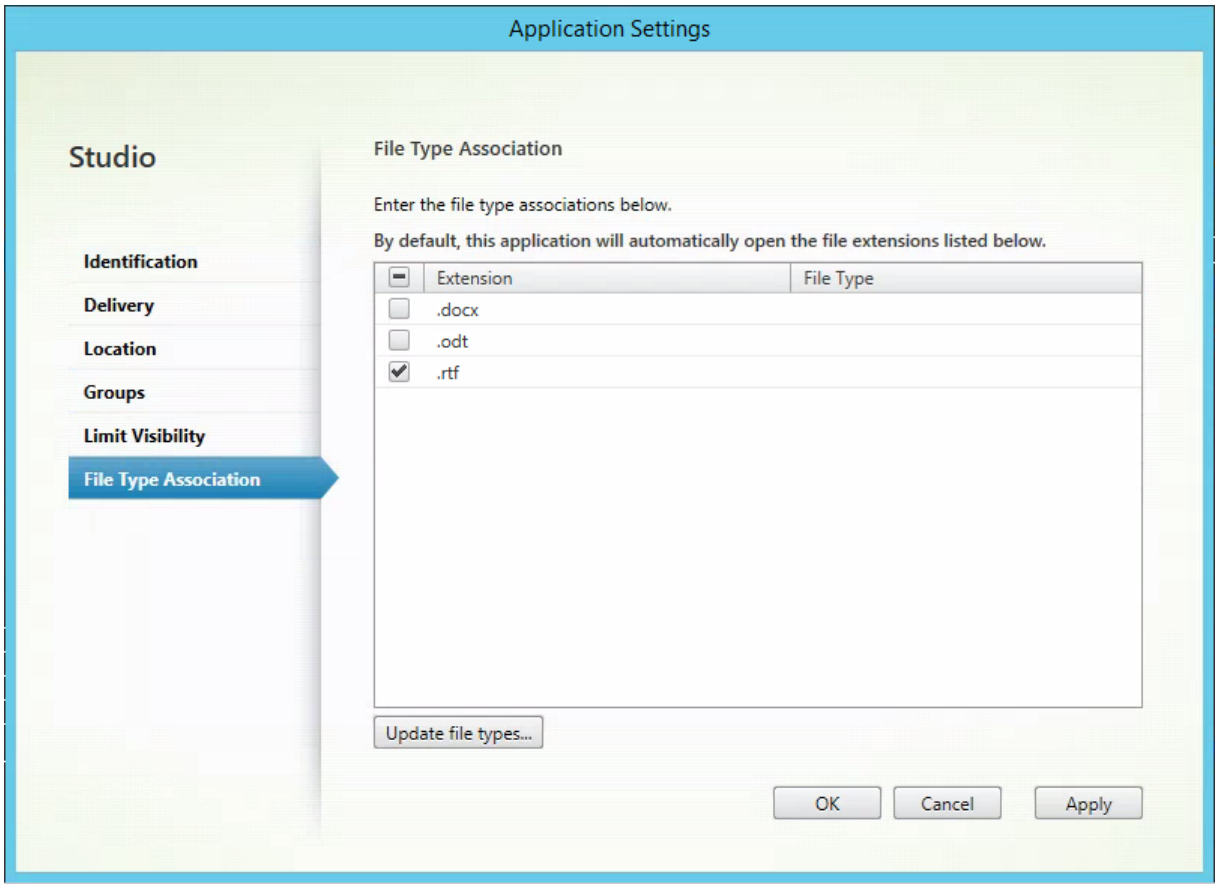


公開コンテンツには、アプリケーションのプロパティ（表示できるユーザー、グループ割り当て、ショートカットなど）が適用されます。ただし、［場所］ページでコマンドライン引数や作業ディレクトリプロパティを変更することはできません。リソースを変更するには、［場所］ページの［実行可能ファイルのパス］を変更します。

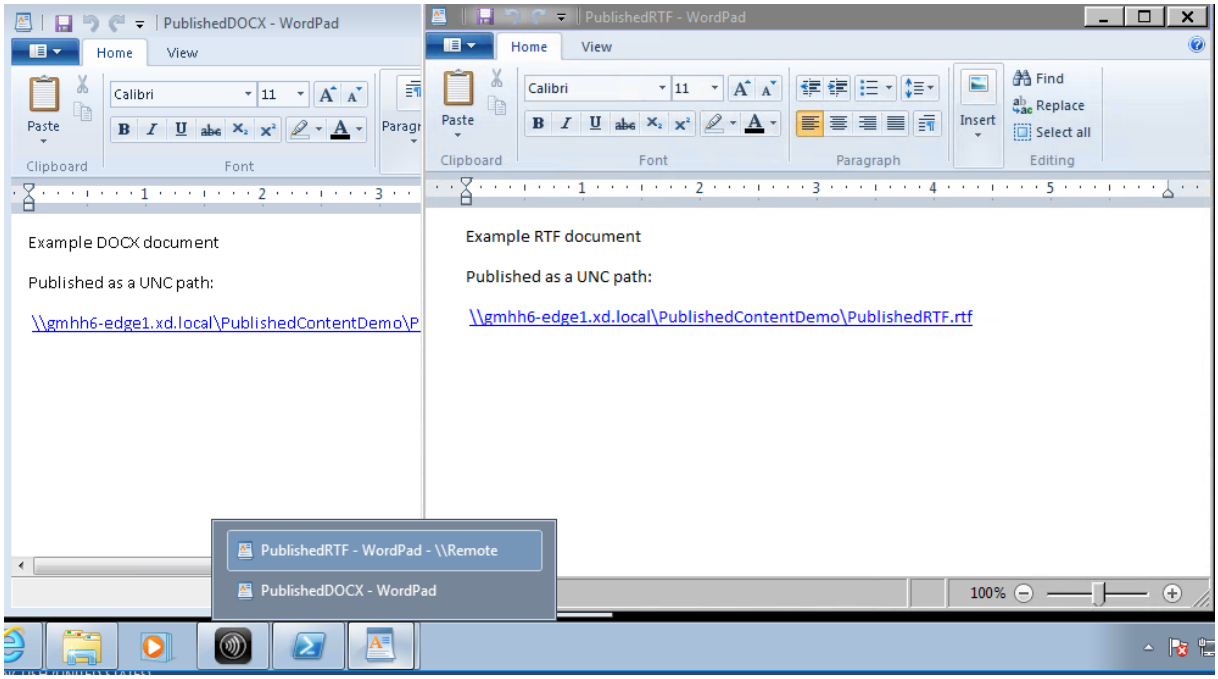


PublishedContent アプリケーションを開くのに（ローカルアプリではなく）公開アプリケーションを使用するには、該当する公開アプリケーションのファイルタイプの関連付けプロパティを編集します。この例では、公開済みのワードパッドアプリケーションを編集して、.rtf ファイルに対するファイルタイプの関連付けを作成しています。

> 重要:
>
> ファイルタイプの関連付けを編集する前にデリバリーグループのメンテナンスモードを有効にしてください。編集が完了したらメンテナンスモードはオフにしてください。



StoreFront を更新してファイルタイプの関連付けに対する変更を反映させ、PublishedRTF アプリケーションおよび PublishedDOCX アプリケーションをクリックします。違いに注目してください。PublishedDOCX は以前と同様にローカルのワードパッドで開かれますが、PublishedRTF は、ファイルタイプの関連付けにより公開済みのワードパッドアプリケーションで開かれるようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

Personal vDisk

February 3, 2020

Personal vDisk 機能を使用すると、プールされるデスクトップやストリーム配信されるデスクトップを単一のイメージで管理でき、しかもユーザーによるアプリケーションのインストールやデスクトップ設定の変更が可能になります。従来の仮想デスクトップインフラストラクチャ（VDI）では、仮想デスクトップでユーザーが設定を変更したりアプリケーションをインストールしたりしても、管理者がマスターイメージを更新するたびにそれらの変更が破棄されてしまいます。Personal vDisk を使用すると、ユーザーによる変更がそのまま保持されます。管理者は、ユーザーによるデスクトップのカスタマイズや個人設定を許可しながら、マスターイメージを容易に一元管理できます。

Personal vDisk では、ユーザーの仮想マシンに対するすべての変更をその仮想マシンに割り当てられた別ディスク（Personal vDisk）にリダイレクトすることにより、変更内容を保持します。Personal vDisk に保存された内容はデスクトップの実行時にマスターイメージの内容と統合され、ユーザーに一貫した操作環境が提供されます。この方法では、管理者がマスターイメージでプロビジョニングしたアプリケーションにもユーザーは引き続きアクセスできます。

Personal vDisk は、デフォルトで同じ容量の 2 つの領域で構成されます。

- ユーザープロファイル：ここには、ユーザーデータ、ドキュメント、およびユーザープロファイルが格納されます。デフォルトではドライブ文字「P」が割り当てられますが、マシンカタログを作成するときに別のドライブ文字を選択することもできます。使用されるドライブの設定は、レジストリキー EnableUserProfileRedirection にも依存します。
- 仮想ハードディスク（VHD）ファイル：ここには、そのほかのすべてのファイル（C:\Program Files にインストールされたアプリケーションなど）が格納されます。この部分は Windows Explorer には表示されず、Version 5.6.7 以降ではドライブ文字は必要ありません。

Personal vDisk では、個々のユーザーがダウンロードしてインストールするアプリケーションに加えて、部門レベルでプロビジョニングするアプリケーションがサポートされます。これにはドライバー（Phase 1 ドライバーを除く）やデータベースを必要とするアプリケーション、およびマシン管理ソフトウェアなどがあります。ユーザーによる変更と管理者による変更が競合する場合でも、Personal vDisk の機能を使って簡単かつ自動的に解決できます。

さらに、ローカルで管理されるアプリケーション（ローカルの IT 部門によりプロビジョニングされて管理されるアプリケーションなど）をユーザーの環境にプロビジョニングすることもできます。Personal vDisk を使用する場合でも、ユーザーの操作性は変更されません。ユーザーが変更した設定やインストールしたアプリケーションは、自動的に Personal vDisk 上に格納されます。Personal vDisk 上のアプリケーションがマスターイメージ上のものとまったく同じである場合、Personal vDisk 上のアプリケーションが破棄されます。これにより、そのアプリケーションは使用可能なまま Personal vDisk の容量が節約されます。

物理的には、Personal vDisk をハイパーバイザーに格納します。ただし、仮想デスクトップにアタッチされているほかのディスクと同じ場所に配置する必要はありません。これにより、Personal vDisk ストレージのコストを削減できます。

サイトの作成中、コネクションを作成するときに、仮想マシンで使用されるディスクのストレージを指定します。Personal vDisk は、オペレーティングシステム用のディスクとは異なるストレージに配置できます。各仮想マシンは、どちらのストレージにもアクセスできる必要があります。これらのディスクをローカルストレージに配置する場合は、同じハイパーバイザーからアクセスできる必要があります。このため、これらの条件を満たすストレージのみが表示されます。後で、Personal vDisk とそのストレージを既存のホストに追加することもできます（マシンカタログには追加できません）。これを行うには Studio で ［構成］**>**［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。

> 注：
>
> PvD のレポート、メッセージ、および既知の問題については、「トラブルシューティング」の記事を参照してください。

インストールとアップグレード

August 24, 2021

Personal vDisk 7.x は、XenDesktop Version 5.6 以降でサポートされています。XenDesktop の各バージョンの「システム要件」のトピックを参照して、サポートされる Virtual Delivery Agent（VDA）のオペレーティングシステム、ホスト（仮想化リソース）、および Provisioning Services について確認してください。Provisioning Services の操作について詳しくは、現行の Provisioning Services のドキュメントを参照してください。

Personal vDisk のインストールと有効化

マシン上に VDA for Desktop OS をインストールしたりアップグレードしたりするときに、Personal vDisk をインストールして有効化できます。これらの操作は、インストールウィザードの ［追加コンポーネント］と ［機能］ページでそれぞれ選択します。詳しくは、「Install Capture」を参照してください。

VDA のインストール後に Personal vDisk をアップデートする場合は、ここで提供されている Personal vDisk の MSI ファイルを XenApp または XenDesktop のインストールメディアで使用してください。

Personal vDisk は、以下の状況で有効になります。

- Machine Creation Services（MCS）を使用している場合、Personal vDisk 用のデスクトップ OS マシンカタログの作成時に Personal vDisk が自動的に有効になります。
- Provisioning Services（PVS）を使用している場合、マスター（基本）イメージ作成時に管理者がインベントリを実行したとき、および自動更新によるインベントリ実行時に Personal vDisk が自動的に有効になります。

そのため、VDA のインストール中に Personal vDisk コンポーネントをインストールしたのに有効化しなかったとしても、カタログ作成時に Personal vDisk が有効になるため、同じイメージを使用して Personal vDisk が有効なデスクトップおよび Personal vDisk が無効なデスクトップを作成できます。

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:

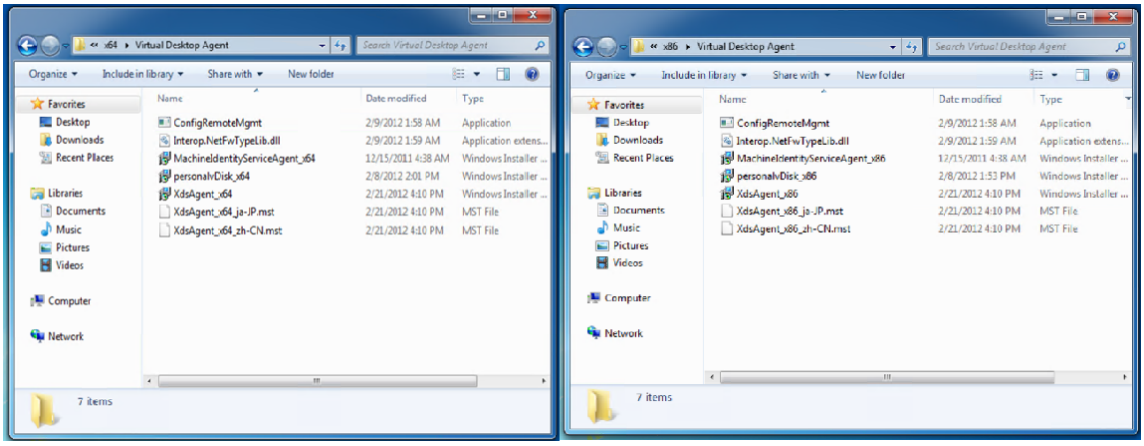
- VDA をアンインストールします。これにより、Personal vDisk ソフトウェアもアンインストールされます。
- Personal vDisk の MSI ファイルを使用して Personal vDisk をアップデートした場合は、コントロールパネルを使用してアンインストールできます。

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。

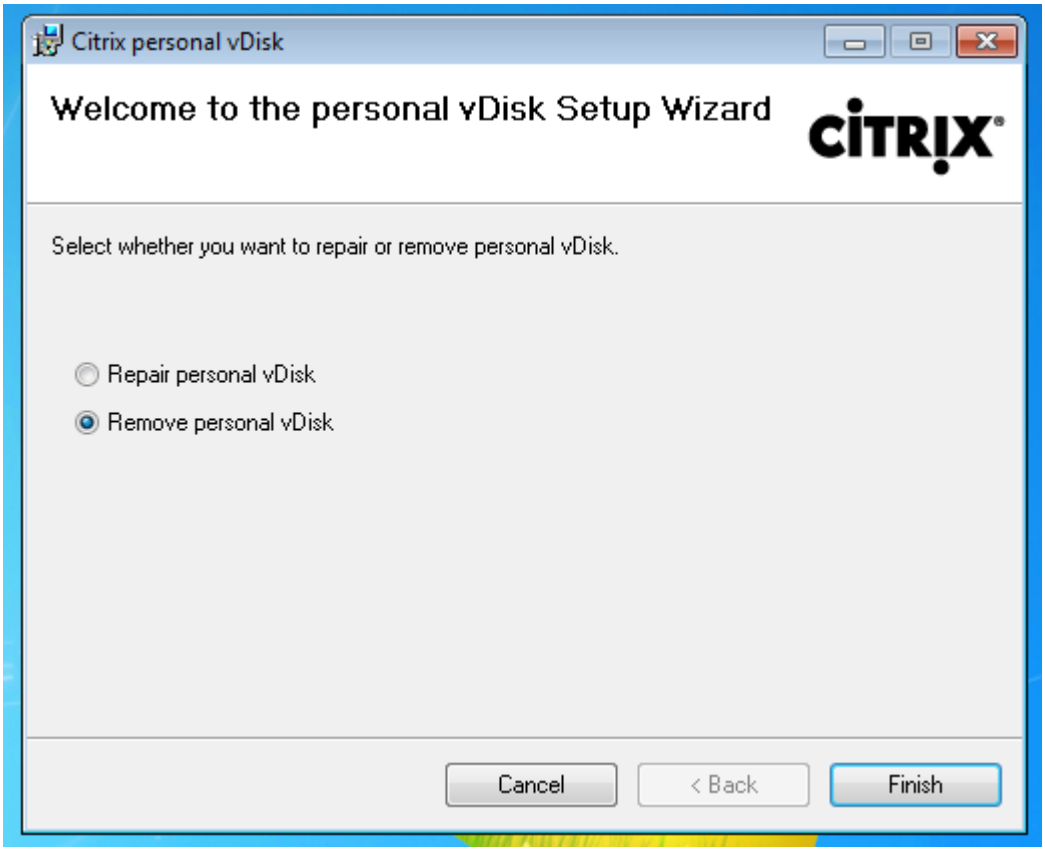
Personal vDisk をアンインストールする時の重要な考慮事項

Personal vDisk が Windows 7（64 ビット）で基本イメージにインストールされていると、アンインストールできないことがあります。この問題を解決するには、以下の手順で Personal vDisk を削除してからアップグレードしてください:

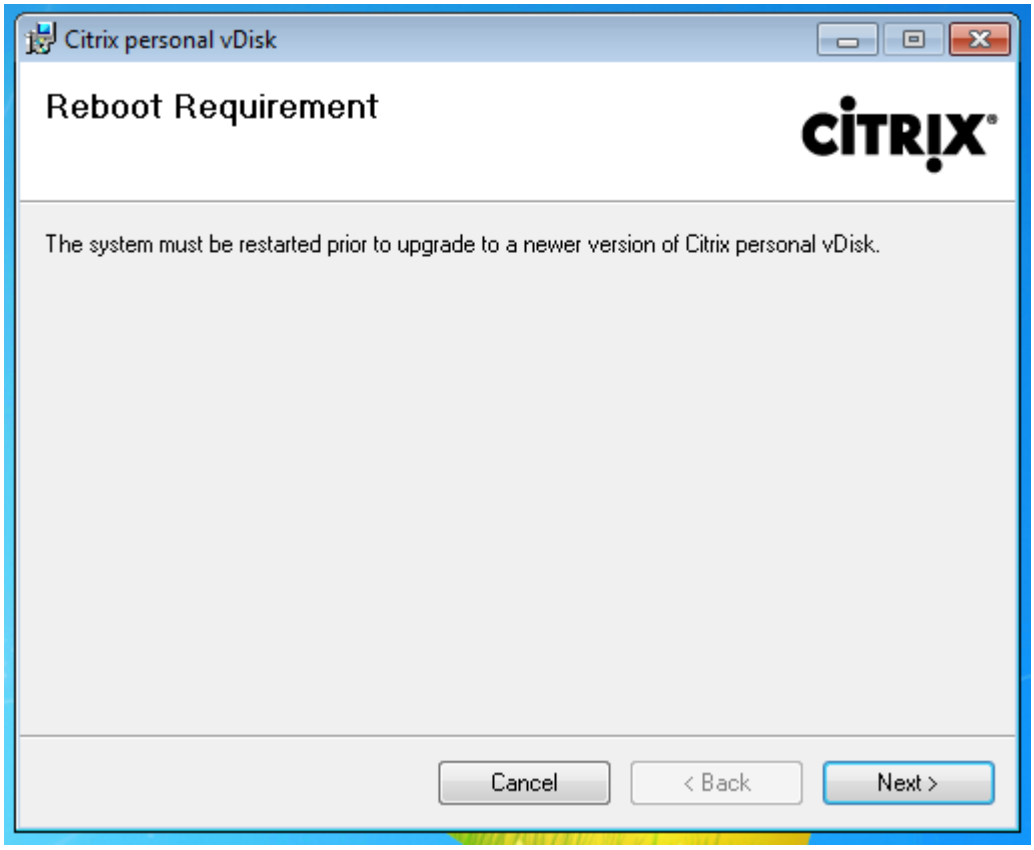
1. XenApp および XenDesktop メディアから vDisk インストーラーの適切なコピーを選択します。次のいずれかの場所（アップグレードされた仮想マシンが 32 ビットか 64 ビットかによる）の XenApp および XenDesktop ISO から最新の Personal vDisk の MSI インストーラーを見つけます。
   - 32 ビット: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
   - 64 ビット: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



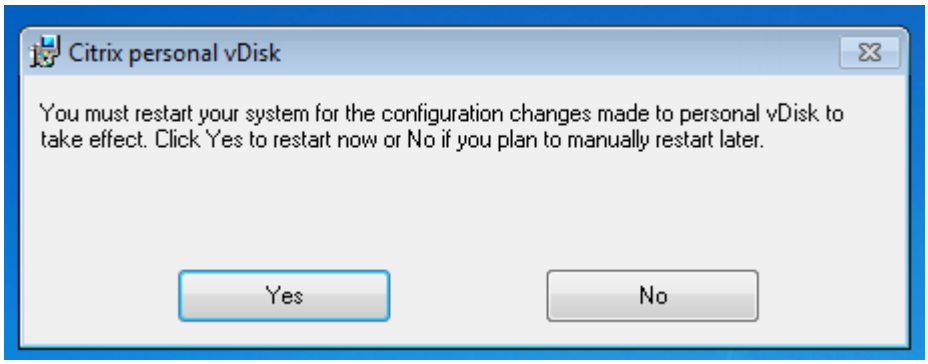
2. 既存の Personal vDisk インストールを削除します。手順 1 で見つけた Personal vDisk の MSI インストーラーパッケージを選択します。Personal vDisk のセットアップ画面が開きます。
3. [Remove personal vDisk] を選択します。
4. [完了] をクリックします。



5. ［再起動してください］ページが開きます。［次へ］をクリックします:



6. ［はい］をクリックしてシステムを再起動し、構成の変更を適用します：



構成と管理

August 24, 2021

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、シトリックス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。

  追加されるスペース＝（5.0 − 4.7）÷2 + 3.0÷2 ＝ 1.65GB

  アプリケーション領域に追加されるスペースのサイズは概算値です。これは、ログやオーバーヘッド用にわずかな余分スペースが追加されるためです。この計算およびサイズ調整は、各再起動時に行われます。

- ユーザープロファイルのサイズ（ほかのプロファイル管理ツールを使用しない場合）

  アプリケーションに必要な容量に加えて、ユーザープロファイルの格納に十分な容量が Personal vDisk 上にあることを確認してください。また、リダイレクトされないユーザーフォルダー（マイドキュメントやマイミュージックなど）の容量についても考慮する必要があります。既存のプロファイルのサイズを確認するには、コントロールパネルから［システムのプロパティ］（sysdm.cpl）を開きます。

  プロファイルをリダイレクトする一部のツールを使用すると、実際のプロファイルデータの代わりにスタブファイル（センチネルファイル）が格納されます。これらのプロファイル管理ツールでは初期状態でディスクが消費されていないように見えますが、各スタブファイルについて 1 ファイルディレクトリエントリがファイルシステム上に作成されます（通常、各ファイルについて 4KB 程度）。このようなプロファイル管理ツールを使用する場合は、スタブファイルではなく実際のプロファイルデータのサイズを考慮する必要があります。

  エンタープライズクラスのファイル共有アプリケーション（ShareFile、Dropbox など）により、Personal vDisk 上のユーザープロファイル領域がデータの同期に使用される場合があります。このようなアプリケーションを使用する場合は、同期データのサイズも考慮する必要があります。

- **Personal vDisk** インベントリを含んでいるテンプレート **VHD** で使用される容量

  テンプレート VHD には、Personal vDisk インベントリデータ（マスターイメージの内容に対応するセンチネルファイル）が含まれています。Personal vDisk のアプリケーション領域はこの VHD から作成されます。

各センチネルファイルやフォルダーによりファイルディレクトリエントリが構成されるため、ユーザーがアプリケーションをインストールしていなくても Personal vDisk のアプリケーション領域がテンプレート VHD の内容により消費されます。テンプレート VHD のサイズは、インベントリを実行した後でマスターイメージを参照すると確認できます。または、以下の式でおおよそのサイズを算出できます。

テンプレート VHD のサイズ＝マスターイメージ上のファイル数 ×4KB

マスターイメージ上のファイルおよびフォルダーの数を確認するには、そのイメージの C ドライブを右クリックして［プロパティ］を選択します。たとえば、イメージに 250,000 個のファイルがある場合、テンプレート VHD のサイズはおよそ 1,024,000,000 バイト（ちょうど 1GB）になります。つまり、Personal vDisk のアプリケーション領域のうち 1GB 弱のディスクスペースには、アプリケーションをインストールできません。

- **Personal vDisk** イメージの更新時に使用される容量

  Personal vDisk イメージを更新するときには、イメージの 2 つのバージョンの差分やユーザーによる Personal vDisk の変更内容を統合するために十分な空き領域が、Personal vDisk（デフォルトで P ドライブ）のルートに必要になります。通常、Personal vDisk の 200～300MB がこの目的で予約されます。ただし、P ドライブに追加されるデータの量によっては、イメージの更新に必要な容量を確保できなくなることがあります。Personal vDisk プール統計スクリプト（XenDesktop インストールメディアの Support/Tools/Scripts フォルダー）または Personal vDisk イメージ更新監視ツール（Support/Tools/Scripts\PvdTool フォルダー）を使用して、更新対象のカタログから空き領域が少ない Personal vDisk ディスクを特定できます。

  アンチウイルス製品をインストールすると、インベントリや更新に時間がかかる場合があります。CtxPvD.exe および CtxPvDSvc.exe をアンチウイルス製品の除外の一覧に追加すると、パフォーマンスを向上させることができます。これらのファイルは、C:\Program Files\Citrix\personal vDisk\bin にあります。ウイルスチェックの対象からこれらの実行可能ファイルを除外すると、インベントリおよびイメージ更新の処理パフォーマンスが最大で 10 倍に向上することがあります。

- 予定外の追加容量（計画外のアプリケーションのインストールなど）

  ユーザーが追加のアプリケーションをインストールできるように、（特定サイズまたは全体に対する割合で）追加領域を加算することを検討してください。

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ために、デフォルトのアルゴリズムで決定されるサイズでは足りなくなることがわかっている場合などには、この機能が役に立ちます。この場合、アプリケーションをインストールするための領域が足りなくならないように、アプリケーション領域の初期サイズを増やします。

可能な場合は、マスターイメージ上で VHD の初期サイズを調整します。または、仮想デスクトップ上で VHD のサイズを調整して、ユーザーのアプリケーションのインストールに必要な領域を確保することもできます。ただし、この方法では各仮想デスクトップ上で個別に調整する必要があります。作成済みのマシンカタログで VHD の初期サイズを調整することはできません。

VHD には、アンチウイルス定義ファイルを保存するのに十分なサイズを設定してください。通常、アンチウイルス定義ファイルのサイズは小さくありません。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config で、以下のレジストリキーを設定します。これ以外のレジストリキーは変更しないでください。MinimumVHDSizeInMB を除き、すべての値はマスターイメージ上で設定します（MinimumVHDSizeInMB はマシン単位で変更できます）。マスターイメージ上で設定された値は、次回イメージ更新時に適用されます。

- **MinimumVHDSizeMB**

  Personal vDisk のアプリケーション領域（C ドライブ）の最小サイズを MB 単位で指定します。新しいサイズは、既存のサイズよりも大きなものにする必要がありますが、ディスクのサイズから PvDReservedSpaceMB の値を差し引いた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、アプリケーション領域（AppContainer。表示上は C ドライブ）は空き領域が 10% 未満になった時点で動的に拡張されます。

  PercentOfPvDForApps の値を増やしても、AppContainer の拡張が許可される最大領域が増えるだけです。設定した値がすぐに適用されるわけではありません。また、この割り当て比率の設定はマスターイメージ内で構成する必要があります。これにより、次回イメージ更新時に設定が反映されます。

  EnableDynamicResizeOfAppContainer を 1 に設定したままマシンカタログを生成した場合は、マスターイメージ内でこの値を 0 に変更して、適切な割り当て比率を構成してください。構成する割り当て比率は、C ドライブの現在の割り当てサイズよりも大きな値である必要があります。

  この値を 0 に設定すると、管理者が割り当て比率を完全に制御できます。つまり、ユーザーが消費する領域サイズにかかわらず C ドライブのサイズを完全に制御でき、動的なサイズ調整は行われません。

  デフォルト値：50%（2 つの領域に同じサイズが割り当てられます）

- **PvDReservedSpaceMB**

  Personal vDisk ログおよびほかのデータ用に予約される Personal vDisk 上の領域を MB 単位で指定します。

  XenApp 6.5（またはそれ以前のバージョン）が動作する環境でアプリケーションのストリーム配信機能を使用する場合は、Rade Cache のサイズに応じてこの値を増やしてください。

デフォルト値 =512

- **PvDResetUserGroup**

  Citrix XenDesktop 5.6 にのみ適用され、Personal vDisk のリセットを許可するユーザーのグループを指定します。これ以降のバージョンの XenDesktop では、管理権限の委任機能を使用します。

そのほかの設定:

- **Windows Update** サービス - マスターイメージでは、Windows Update のオプションとして［更新プログラムを確認しない］を選択し、Windows Update サービスを［無効］に設定します。Windows Update サービスを実行する必要がある場合でも、［更新プログラムを確認しない］を選択することで更新プログラムがマシン上にインストールされることを防ぐことができます。

  たとえば、Windows ストアから Windows ストアアプリをインストールする場合は、このサービスを実行しておく必要があります。

- **Windows** の更新プログラム - Internet Explorer を含む Windows の更新プログラムをマスターイメージに適用しておきます。
- 再起動が必要な更新プログラム - Windows の更新プログラムの中には、インストールを完了するために何回かの再起動が必要になるものがあります。Personal vDisk インベントリを収集する前に、マスターイメージを正しく再起動して、適用した更新プログラムが完全にインストールされたことを確認してください。
- アプリケーションの更新プログラム - マスターイメージ上のアプリケーションに必要な更新プログラムを適用しておくと、ユーザーの vDisk に必要なディスク領域を節約できます。また、各ユーザーの vDisk 上のアプリケーションを個別に更新する手間も省けます。

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（ドングルを使用したり署名ベースのハードウェアを使用したりするもの）はサポートされません。

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大きくなくてはなりません。Personal vDisk が Provisioning Service の書き込みキャッシュより小さいと、Personal vDisk ディスクが書き込みキャッシュとして使用されてしまう場合があります。
- デリバリーグループを作成した後では、Personal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）またはサイズ変更とプール統計のスクリプト（personal-vdisk-poolstats.ps1）を使用して Personal vDisk を監視することができます。

書き込みキャッシュディスクのサイズを正しく設定してください。Personal vDisk がアクティブな場合、ユーザーによる多くの書き込み処理（変更内容）が Personal vDisk 上にリダイレクトされます。このため、Provisioning Services の書き込みキャッシュディスクのサイズを小さく設定できる場合があります。ただし、Personal vDisk が

アクティブでないとき（イメージ更新時など）に Provisioning Services 書き込みキャッシュディスクのサイズが足りなくなり、マシンがクラッシュすることがあります。

Provisioning Services のベストプラクティスに従って Provisioning Services 書き込みキャッシュディスクのサイズを設定し、さらにマスターイメージ上のテンプレート VHD の 2 倍のサイズを統合（マージ）処理用に追加することをお勧めします。マージ処理ですべての領域が使用されることはまれですが、可能性はあります。

Personal vDisk が有効なマシンのカタログを Provisioning Services で展開する場合は、以下の点に注意してください：

- Provisioning Servicesのドキュメントの手順に従います。
- Studio のホスト接続の設定を編集して、同時操作を制限することができます。方法については、後述の説明を参照してください。
- アプリケーションやほかのソフトウェアをインストールまたはアップデートして Provisioning Services vDisk を再起動した後でその vDisk を更新した場合は、Personal vDisk インベントリを実行して仮想マシンをシャットダウンしてください。その後で、新しいバージョンを実稼働モードに昇格させます。そのカタログ内の Personal vDisk デスクトップが自動的に準備中の状態になります。準備中にならない場合は、Soap Service アカウントに Controller のマシン管理者またはそれ以上の権限が付与されていることを確認してください。

Provisioning Services のテストモード機能を使用すると、更新済みのマスターイメージを使用するマシンのテストカタログを作成できます。このテストカタログで実用性をテストしてから、それを実稼働用に昇格させることができます。

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しなくなります。これにより Personal vDisk が機能しなくなります。

シャットダウンを中断した場合は、マシンを再起動してから再度シャットダウンし、メッセージが表示されたら［インベントリの更新］をもう一度クリックします。

4. インベントリ操作によりマシンがシャットダウンしたら、マスターイメージのスナップショットを作成します。

インベントリをネットワーク共有上にエクスポートして、それをマスターイメージ上にインポートできます。詳しくは、「Personal vDisk インベントリのエクスポートとインポート」を参照してください。

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更新 - 同時に実行可能な Personal vDisk の電源操作の上限値を指定します。この値は、絶対値および接続に対するパーセンテージで指定できます。2 つの設定値のうちより小さい値が適用されます。
     デフォルト値：絶対値 50、25%
     絶対値を計算するには、エンドユーザーのストレージでサポートされる合計 IOPS（1 秒あたりの読み取り/書き込み回数）を使用します。さらに、各仮想マシンの IOPS（IOPS/VM）を 350 として、ストレージで同時にアクティブにできる仮想マシン数を計算します。合計 IOPS 値を IOPS/VM 値で除算するとこの値が算出されます。
     たとえば、エンドユーザーのストレージの IOPS が 14000 の場合、同時にアクティブにできる仮想マシン数は 40（14000÷350 ＝ 40）になります。
   - **1** 分あたりの最大新規操作 - ハイパーバイザーに送信可能な新規電源操作の 1 分あたりの上限値を指定します。この値は、設定値で指定します。
     デフォルト値：10

これらの設定について最適な値を確認するには、以下の操作を行います。

1. デフォルトの値を使用して、テストカタログの単一イメージ更新にかかる合計応答時間を計測します。つまり、イメージ更新の開始時刻（T1）からカタログ内の最後のマシンでの VDA の Controller への登録時刻（T2）

までの時間を計測します（合計応答時間＝ T2 − T1）。

2. イメージ更新時のハイパーバイザーストレージの IOPS（1 秒あたりの読み取り/書き込み回数）を計測します。この値を最適化の基準値として使用します。通常はデフォルトの設定値を使用しますが、IOPS の限界まで達する場合はより小さい値を設定します。
3. 以下の手順に従って［Personal vDisk ストレージインベントリの同時更新］の値を変更します（ほかのすべての設定値はそのまま保持します）。
   a) 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。
   b) 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、ほかのマスターイメージアプリケーションと同じ方法でインストールできます。以下の説明は、System Center Configuration Manager 2007 にのみ適用されます。Configuration Manager 2007 より前のバージョンはサポートされません。

Personal vDisk 環境で Configuration Manager 2007 エージェントソフトウェアを使用するには、以下の操作を行います。

1. マスターイメージにクライアントエージェントをインストールします。
   a) マスターイメージに Configuration Manager クライアントをインストールします。
   b) ccmexec service（SMS Agent）を停止して、さらに無効に設定します。
   c) 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。
   d) C:\Windows\smscfg.ini を削除するか、名前を変更します。
2. クライアント固有の情報を削除します。
   a) C:\Windows\System32\CCM\Logs のログファイルを削除または移動します（オプション）。
   b) 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。
   c) マスターイメージをシャットダウンしてスナップショットを作成し、このスナップショットを使用してマシンカタログを作成します。

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

August 24, 2021

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。

- Personal vDisk 上のファイルの表示/非表示
- ファイルに対する変更内容のマージ方法
- ファイルの書き込みの許可/禁止

カスタムの規則ファイルおよびコピーオンライトについて詳しくは、各ファイル内に記述されているコメントを参照してください。これらのファイルは、Personal vDisk をインストールしたマシンの C:\ProgramData\Citrix\personal vDisk\Config にあります。「custom_*」という名前のファイルには、規則の説明と規則を有効にする方法が記述されています。

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。

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 **C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset** を実行します。
- Citrix Director でユーザーのデスクトップを選択します。［**Personal vDisk** をリセット］をクリックして［**OK**］をクリックします。

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ファイル共有に対して認証します。このとき、エクスポートまたはインポートで使用するすべてのファイル共有にユーザー環境からアクセスできることが必要です。

エクスポート

- 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、<path-to-export-location> 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。コマンド出力の一部を次に示します:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
    exportinventory
\share location\ExportedInventory
Current inventory source location C:\CitrixPvD\Settings\Inventory
    \VER-LAS
...
Exporting current inventory to location \ ... .
...
Deleting any pre-existing inventory folder at \ ... .
.Successfully exported current inventory to location \ ... .
    Error code = OPS
<!--NeedCopy-->
```

- 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。

インポート

マスターイメージ上で、管理者として次のインポートコマンドを実行します。

```
Ctxpvdsvc.exe importinventory "\<path-to-exported-inventory>"
```

<path to exported inventory> には、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。コマンド出力の一部を次に示します:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
    importinventory
\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \share location\ExportedInventory\
    ExportedPvdInventory
…
Successfully added inventory \share location\ExportedInventory\
    ExportedPvdInventory to the
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
<!--NeedCopy-->
```

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

表示、メッセージ、およびトラブルシューティング

August 24, 2021

レポートを介した **PvD** のモニター

Personal vDisk のユーザーデータ領域およびアプリケーション領域に対するユーザーによる変更は、Personal vDisk の診断ツールを使って監視できます。これらの変更には、ユーザーがインストールしたアプリケーションや修正したファイルが含まれます。変更内容はいくつかのレポートに保存されます。

1. 監視するマシン上で、**C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe** を実行します。
2. レポートとログを保存する場所を参照し、生成するレポートを選択して［**OK**］をクリックします。以下のレポートを利用できます。

SOFTWARE ハイブレポート：このレポートは次の 2 つのファイルを生成します：Software.Dat.Report.txt と Software.Dat.delta.txt です。

Software.Dat.Report.txt ファイルには、HKEY_LOCAL_MACHINE\Software ハイブに対してユーザーが行った変更が記録されます。以下のセクションがあります：

- List of Applications installed on the base - レイヤー 0 にインストールされたアプリケーション
- List of user installed software - Personal vDisk のアプリケーション領域にユーザーがインストールしたアプリケーション
- List of software uninstalled by user - レイヤー 0 からユーザーが削除したアプリケーション

Software.Dat.delta.txt に記録される情報については、この表の「ハイブデルタレポート」を参照してください。

SYSTM ハイブレポート：生成される SYSTEM.CurrentControlSet.DAT.Report.txt ファイルには、HKEY_LOCAL_MACHINE\System ハイブに対してユーザーが行った変更が記録されます。以下のセクシ

ョンがあります:

- List of user installed services - ユーザーがインストールしたサービスおよびドライバー。
- Startup of following services were changed - ユーザーが起動の種類を変更したサービスおよびドライバー。

SECURITY ハイブレポート:生成される SECURITY.DAT.Report.txt ファイルにより、HKEY_LOCAL_MACHINE\Security ハイブでユーザーが行ったすべての変更が監視されます。

SAM ハイブレポート: 生成される SAM.DAT.Report.txt ファイルにより、HKEY_LOCAL_MACHINE\SAM ハイブでユーザーが行ったすべての変更が監視されます。

ハイブデルタレポート: 生成される Software.Dat.delta.txt ファイルにより、追加または削除されたすべてのレジストリキーおよび値と、HKEY_LOCAL_MACHINE\Software ハイブでユーザーが変更したすべての値が記録されます。

Personal vDisk のログ: ログファイル Pud-IvmSupervisor.log、PvDActivation.log、PvDSvc.log、PvD-WMI.log、SysVol-IvmSupervisor.log、および vDeskService-[#].log は、デフォルトでは *P:\Users\<user account>\AppData\Local\Temp\PVDLOGS* に生成されますが、選択した場所に移動されます。

Windows オペレーティングシステムのログ:

- EvtLog_App.xml および EvtLog_System.xml は、Personal vDisk ボリュームから生成される XML 形式のアプリケーションおよびシステムイベントログです。
- Setupapi.app.log および setuperr.log には、Personal vDisk のインストールで msiexec.exe を実行したときからのログメッセージが記録されます。
- Setupapi.dev.log には、デバイスインストールログメッセージが記録されます。
- Msinfo.txt には、msinfo32.exe からの出力が記録されます。詳しくは、Microsoft 社のドキュメントを参照してください。

ファイルシステムレポート: 生成される FileSystemReport.txt ファイルにより、ユーザーがファイルシステムに対して行った変更が以下のセクションに記録されます。

- Files Relocated - ユーザーが Personal vDisk に移動したレイヤー 0 のファイル。レイヤー 0 のファイルは、Personal vDisk が接続されたマシンによりマスターイメージから継承されます。
- Files Removed - ユーザーの操作（アプリケーションの削除など）によって非表示になったレイヤー 0 のファイル。
- Files Added（MOF、INF、SYS）- Personal vDisk に追加された拡張子.mof、.inf、または.sys を持つファイル（Visual Studio 2010 などのアプリケーションのインストールにより登録された自動回復用の MOF ファイルなど）。
- Files Added Other - Personal vDisk に追加されたそのほかのファイル（アプリケーションのインストールにより追加されたファイルなど）。
- Base Files Modified But Not Relocated - 変更されたレイヤー 0 のファイルで、Personal vDisk カーネルモードドライバーにより移動されないもの。

イメージの更新

Personal vDisk が有効なマシンを Studio のマシンカタログで選択すると、［PvD］タブにイメージ更新時の監視状態や推定完了時間、および進行状況が表示されます。イメージ更新時には、準備完了、準備中、待機中、失敗、および要更新のいずれかの状態が表示されます。

イメージの更新は、ディスクの空き容量不足や Personal vDisk が見つからないなど、さまざまな要因で失敗することがあります。Studio でイメージ更新に失敗したことが示されると、トラブルシューティングに役立つエラーコードおよび説明が表示されます。Personal vDisk Image Update Monitoring Tool（イメージ更新監視ツール）または personal-vdisk-poolstats.ps1 スクリプトを使用すると、イメージの更新状況を監視して、問題が生じた場合はそのエラーコードを取得できます。

イメージ更新に失敗した場合は、以下のログファイルを参照してトラブルシューティングを行います。

- Personal vDisk サービスログ - C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Personal vDisk アクティブ化ログ - P:\PVDLOGS\PvDActivation.log.txt

最新の情報は、これらのログファイルの末尾に記録されます。

エラーメッセージ：**Version 7.6** 以降

Personal vDisk 7.6 以降では、以下のエラーメッセージが生成されます。

- 内部エラーが発生しました。詳しくは、**Personal vDisk** のログを参照してください。エラーコード**%d**（**%s**）

  このメッセージは未分類のエラーに対して生成され、特定のエラーコードは提供されません。インベントリ作成または Personal vDisk 更新時に予期されないエラーが発生すると、このメッセージが生成されます。

  - ログファイルを収集して Citrix のサポート担当者に問い合わせてください。
  - カタログ更新時にこのエラーが発生した場合は、カタログをロールバックして以前のマスターイメージの状態に戻してください。

- 規則ファイルに構文エラーがあります。詳しくは、ログを参照してください。

  エラーコードは、2 です。規則ファイルに構文エラーが含まれています。Personal vDisk のログファイルに、規則ファイルの名前と構文エラーの行番号が記録されます。規則ファイルの構文エラーを修正して再試行してください。

- 前のバージョンのマスターイメージに対応している **Personal vDisk** 上のインベントリが破損しているか、読み取ることができません。

  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\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損失防止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、データ損失防止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ーのインストールに失敗しました。

  エラーコードは、14 です。Personal vDisk をインストールした後の初回インベントリ更新時に、ドライバーがインストールされます。一部のアンチウイルス製品では、インストーラーコンテキスト外のドライバーのインストールがブロックされることがあります。初回インベントリ作成時にアンチウイルス製品のリアルタイムスキャン機能を一時的に無効にするか、例外規則を追加してください。

- システムボリュームのスナップショットを作成できません。**Volume Shadow Copy** サービスが有効になっていることを確認してください。

  エラーコードは、15 です。このエラーは、Volume Shadow Copy サービスが無効になっていると発生します。Volume Shadow Copy サービスを有効にしてからインベントリ操作を再試行してください。

- 変更ジャーナルのアクティブ化に失敗しました。数分待ってから再試行してください。

  エラーコードは、16 です。Personal vDisk では、マスターイメージに対する変更を追跡するために「変更ジャーナル」が使用されます。インベントリ更新時に変更ジャーナルが無効になっていることが検出されると、有効化が試行され、有効化に失敗するとこのエラーが発生します。しばらくしてから再試行してください。

- システムボリュームに十分な空き領域がありません。

  エラーコードは、17 です。デスクトップの C ドライブにイメージの更新操作に必要な空き領域がない場合にこのエラーが発生します。システムボリュームを拡張するか、不要なファイルを削除して空き領域を確保してください。十分な空き領域を確保すると、次回再起動時にイメージ更新が開始されます。

- **Personal vDisk** ストレージに十分な空き領域がありません。**Personal vDisk** ストレージを拡張して空き領域を増やしてください。

エラーコードは、18 です。イメージの更新時に Personal vDisk 用のドライブに十分な空き領域がない場合にこのエラーが発生します。Personal vDisk ストレージを拡張するか、不要なファイルを削除して空き領域を確保してください。十分な空き領域を確保すると、次回再起動時にイメージ更新が再開されます。

- **Personal vDisk** ストレージがオーバーコミットされました。**Personal vDisk** ストレージを拡張して空き領域を増やしてください。

  エラーコードは、19 です。シックプロビジョニングされた UserData.V2.vhd を格納するための空き領域が Personal vDisk 用のドライブにない場合にこのエラーが発生します。Personal vDisk ストレージを拡張するか、不要なファイルを削除して空き領域を確保してください。

- システムレジストリが破損しています。

  エラーコードは、20 です。システムレジストリが破損または欠落しているか、読み取り不能になっています。Personal vDisk をリセットするか、作成済みのバックアップから復元してください。

- **Personal vDisk** のリセット時に内部エラーが発生しました。詳しくは、**Personal vDisk** のログを参照してください。

  エラーコードは、21 です。このメッセージは、Personal vDisk のリセット時に発生したすべてのエラーに対して生成されます。ログファイルを収集して Citrix のサポート担当者に問い合わせてください。

- **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。

エラーコード	説明
0x20	イメージ更新用のアプリケーションコンテナーのマウントに失敗しました。Version 5.6.12 にアップグレードすることで解決できます。
0x70	ディスク上に十分な領域がありません。

- スタートアップに失敗しました。**Citrix Personal vDisk** を起動できませんでした。**[**または「**Personal vDisk** で内部エラーが発生しました。」**]** 詳細は **...** 状態コード：**20**、エラーコード **0x20000028**

  このメッセージは、Personal vDisk が見つかったにもかかわらず Personal vDisk セッションを作成できなかったことを示します。

  ログを収集して、SysVol-IvmSupervisor.log にセッションの作成の失敗が記録されていないかどうかを確認してください。

  1. 「IvmpNativeSessionCreate: failed to create native session, status <XXXXX>」というエントリを検索します。
  2. <XXXXX> 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。

  - 互換性のないウイルス対策ソフトウェア（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。

イベント ID	説明
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 コンテナーの作成に必要な領域がありません。

バージョンに依存しない既知の問題

次の PvD の問題が確認されています。

- Personal vDisk 上にインストールされたアプリケーションがマスターイメージ上にインストールされた同一バージョンのアプリケーションと関連付けられている場合、イメージの更新後に Personal vDisk 上のアプリケーションが動作しなくなることがあります。この問題は、マスターイメージ上のアプリケーションをアンインストールしたりアップグレードしたりしたために、Personal vDisk 上のアプリケーションで必要なファイルがマスターイメージから削除されると発生します。この問題を回避するには、マスターイメージ上のアプリケーションを保持しておきます。

  たとえば、マスターイメージ上に Office 2007 をインストールして、Personal vDisk 上に Visio 2007 をインストールします。その後で管理者がマスターイメージ上の Office 2007 を Office 2010 にアップグレードして、そのイメージを使用してマシンを更新すると、Visio 2007 が動作しなくなります。この問題を避けるには、Office 2007 をマスターイメージ上にインストールしたままにしておきます。[320915]

- Personal vDisk を使用するデスクトップに McAfee Virus Scan Enterprise（VSE）を展開する場合は、マスターイメージ上に Version 8.8 Patch 4 以降をインストールしてください。[303472]
- マスターイメージ内で作成されたファイルのショートカットが動作しなくなった場合（そのショートカットのリンク先の名前が Personal vDisk 内で変更された場合など）は、ショートカットを作成し直してください。[367602]
- マスターイメージ内で絶対/ハードリンクを使用しないでください。[368678]
- Windows 7 のバックアップと復元機能は、Personal vDisk ではサポートされていません。[360582]
- 更新したマスターイメージを適用した後で、ローカルユーザーおよびグループのコンソールがアクセス不能になったり不正なデータが表示されたりすることがあります。この問題を解決するには、仮想マシン上でユーザーアカウントをリセットします。これを行うには、セキュリティハイブのリセットが必要です。この問題は Version 7.1.2 で解決されており、Version 7.1.2 以降で作成された仮想マシンは正しく処理されます。ただし、アップグレード前に作成された仮想マシンでの問題は解決されません。[488044]
- ESX ハイパーバイザー環境でプールされた仮想マシンを使用する場合、SCSI コントローラーの種類として［VMware Paravirtual］を選択すると再起動を確認するメッセージがユーザーに表示されます。この問題を避けるには、SCSI コントローラーの種類として LSI を使用してください。[394039]
- Provisioning Services で作成されたデスクトップ上で Personal vDisk をリセットすると、ログオンしたユーザーに再起動を確認するメッセージが表示されることがあります。この問題が発生した場合は、デスクトップを再起動してください。[340186]
- Windows 8.1 のデスクトップを使用するユーザーが Personal vDisk にログオンできなくなることがあります。この問題が発生すると、「システムが正しくシャットダウンされなかったため Personal vDisk が無効になっています」というメッセージが管理者に表示され、PvDActivation.log に「Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]」というメッセージが記録されます。この問題は、ユーザーの仮想マシンを正しくシャットダウンできなかった場合に発生します。この問題を解決するには、Personal vDisk をリセットしてください。[474071]

コンポーネントの削除

August 24, 2021

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。

VDA を削除すると、削除後にデフォルトでマシンが自動的に再起動します。

プログラムの削除や変更を行う **Windows** の機能を使用してコンポーネントをアンインストールする

プログラムの削除や変更を行うための Windows 機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います:

- Controller、Studio、Director、ライセンスサーバー、または StoreFront をアンインストールするには、[Citrix XenApp <*version*>］または［Citrix XenDesktop <*version*>］を選択してから右クリックし、［アンインストール］を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。StoreFront は、［**Citrix StoreFront**］を右クリックしてから ［アンインストール］を選択して削除することもできます。
- VDA を削除するには、［**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。
- ユニバーサルプリントサーバーをアンインストールするには、［**Citrix** ユニバーサルプリントサーバー］を選択してから右クリックし、［アンインストール］を選択します。

コマンドラインを使ってコアコンポーネントをアンインストールする

インストールメディアの\x64\XenDesktop Setup ディレクトリから、**XenDesktopServerSetup.exe** コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、/remove および/components オプションを使用します。
- すべてのコンポーネントをアンインストールするには、/removeall オプションを使用します。

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。

```
1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
    studio
```


コマンドラインを使って **VDA** をアンインストールする

インストールメディアの\x64\XenDesktop Setup ディレクトリから、**XenDesktopVdaSetup.exe** コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、/remove および/components オプションを使用します。
- すべてのコンポーネントをアンインストールするには、/removeall オプションを使用します。

コマンドおよびパラメーターについて詳しくは、「コマンドラインを使ったインストール」を参照してください。

たとえば、VDA および Citrix Receiver をアンインストールするには次のコマンドを実行します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Active Directory のスクリプトを使用して VDA を削除するには、「スクリプトを使った Virtual Delivery Agent のインストールまたは削除」を参照してください。

アップグレードと移行

August 24, 2021

アップグレード

新しいバージョンのマシンやサイトをセットアップしなくても、既存の環境をアップグレードすることで最新バージョンのコンポーネントを使用できます。これをインプレースアップグレードと呼びます。次のバージョンから現在のバージョンにアップグレードできます。

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

*XenDesktop 5.6 からアップグレードするには、まず最新の CU を使用して 7.6 LTSR にアップグレードしてから、7.15 LTSR にアップグレードします。

XenApp 6.5 ワーカーのサーバーを最新の VDA for Windows Server OS にアップグレードすることもできます。これは、XenApp 6.5 からの移行時に補足的に行います。「XenApp 6.5 ワーカーの VDA for Windows Server OS へのアップグレード」を参照してください。

アップグレードするには

1. コアコンポーネントおよび VDA のインストール先のマシン上でインストーラーを実行します。アップグレードが可能かどうかが検出され、新しいバージョンのソフトウェアがインストールされます。
2. アップグレードした Studio を使用して、データベースとサイトをアップグレードします。

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、CTX205921を参照してください。

移行

以前のバージョンの環境から、より新しいバージョンの環境にデータを移行できます。XenApp 6.x の環境から XenApp 7.6 に移行できます。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。

7.x リリースで導入されたアーキテクチャ、コンポーネントおよび機能変更について詳しくは、「7.x での変更点」を参照してください。

移行について詳しくは、「XenApp 6.x からの移行」を参照してください。

7.x での変更点

August 24, 2021

7.x リリース以降で、XenApp および XenDesktop のアーキテクチャ、用語、および機能が変更されました。ここでは、旧（7.x より前の）バージョンしか詳しくないユーザーに必要な変更情報を提供します。

7.x バージョンに移行後のバージョンの変更点については、「新機能」で説明されています。

特記しない限り、*7.x* は XenApp バージョン 7.5 以降、および XenDesktop バージョン 7 以降を指します。

この記事に概要を示します。7.x より前のバージョンから最新バージョンへの移行の包括的な情報については、「XenApp 7 へのアップグレード」を参照してください。

XenApp 6 と現在のバージョンの **XenApp** との相違点

XenApp 6.5 以前のバージョンと XenApp/XenDesktop 7.x 以降との機能や用語の対応は次の表のとおりです。ただし、これらは単なる名前の置き換えではなく、機能的にも更新されていることに注意してください。アーキテクチ

ャ上の相違点の説明が続きます。

XenApp 6.x 以前の機能および用語	バージョン 7.x の機能および用語
Independent Management Architecture（IMA）	FlexCast Management Architecture（FMA）
ファーム	サイト
ワーカーグループ	マシンカタログ、デリバリーグループ
Worker	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、スコープ

アーキテクチャの相違

XenApp/XenDesktop 7.x 以降は、「FlexCast Management Architecture（FMA）」と呼ばれるアーキテクチャに基づいています。FMA は、Citrix テクノロジ間の相互運用性と管理モジュール性を可能にする、サービス指向のアーキテクチャです。FMA により、アプリケーション配信、モビリティ、サービス、フレキシブルなプロビジョニング、およびクラウド管理のためのプラットフォームが提供されます。

FMA は、XenApp 6.5 以前で使用されていた IMA（Independent Management Architecture）を置き換えるものです。

FMA の主要要素と XenApp 6.5 以前のバージョンとの違いは以下のとおりです。

- デリバリーサイト：XenApp 6.5 以前のバージョンでは、最上位レベルのオブジェクトが「ファーム」と呼ばれていました。XenApp/XenDesktop 7.x での最上位レベルは「サイト」です。デリバリーサイトでは、ユーザーのグループにアプリケーションやデスクトップが提供されます。FMA では、サイトを展開する管理者がドメインに属している必要があります。たとえばサーバーをインストールするには、アカウントにローカル管理者権限があり、Active Directory のドメインユーザーである必要があります。
- マシンカタログとデリバリーグループ：XenApp 6.5 以前のバージョンでは、アプリケーションやサーバーソフトウェアを効率的に管理するため、ホストマシンがワーカーグループとしてグループ化されました。管理者は、ワーカーグループ内のすべてのマシン上のアプリケーションや負荷分散を単一エンティティとして管理

できました。また、アプリケーションやマシンをフォルダーで分類することもできました。XenApp および XenDesktop 7.x では、マシンカタログ、デリバリーグループ、およびアプリケーショングループを使用して、マシン、負荷分散、およびホストされたアプリケーションやデスクトップを管理します。また、アプリケーションフォルダーを使用することもできます。

- **VDA**: XenApp 6.5 以前のバージョンでは、ワーカーグループ内のワーカーマシンがユーザーのアプリケーションをホストして、データコレクターと通信していました。XenApp/XenDesktop 7.x では、VDA が Delivery Controller と通信して、Delivery Controller がユーザー接続を管理します。
- **Delivery Controller**: XenApp 6.5 以前のバージョンでは、ユーザーからの接続要求とハイパーバイザーとの通信をゾーンマスターが担当していました。XenApp/XenDesktop 7.x では、接続要求はサイト内の各 Controller に分散されて処理されます。XenApp 6.5 以前のバージョンでは、ゾーンにより WAN 接続を介したサーバー集約およびデータ複製が提供されていました。XenApp/XenDesktop 7.x にはこのようなゾーンに正確に対応するものがありませんが、7.x でのゾーンとゾーン優先度機能を使用して、リモートのユーザーが WAN の大規模セグメントを経由する接続を必ずしも必要とせず、リソースに接続できるようにサポートできます。
- **Studio** と **Director**: Studio コンソールでは、環境を構成したり、ユーザーにアプリケーションやデスクトップへのアクセスを提供したり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（およびオプションでアプリケーショングループ）を選択します。Studio では、最初にサイトを構成し、マシンカタログを作成および指定してから、そのカタログのマシンを使用するデリバリーグループを作成します。デリバリーグループでは、アプリケーションへのアクセスを許可するユーザーを指定します。必要な場合は、複数のデリバリーグループを作成する代わりに、アプリケーショングループを作成することを選択できます。
- データベース: XenApp/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

展開全体を監視して、システム全体の問題を解決できます。

機能比較

FMA への移行により、XenApp 6.5 以前のバージョンで提供されていたいくつかの機能の実装が変更されたり、ほかの機能、コンポーネント、またはツールに置き換えられたりしています。

XenApp 6.5 以前の機能:	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。
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。
ローカルホストキャッシュにより、データストアに接続できない状態でもワーカーサーバーが正しく動作します。	ローカルホストキャッシュを使用すると、Controller とサイトデータベースの間の接続が失敗しても、接続仲介操作を続行できます。この実装は、より頑強で、必要なメンテナンスも少なくなります。「ローカルホストキャッシュ」を参照してください。
アプリケーションのストリーム配信	Citrix App-V によるアプリケーションのストリーム配信を Studio で管理できます。「App-V」を参照してください。
Web Interface	StoreFront への移行をお勧めします。
ユーザーセッションの画面上アクティビティを録画する SmartAuditor	7.6 Feature Pack 1 以降、この機能は Session Recording により提供されます。また、構成ログを使用して、すべてのセッションアクティビティを管理の視点から記録することもできます。

XenApp 6.5 以前の機能：	7.x の機能：
節電やサーバー能力の管理に役立つ電源能力管理。	Microsoft Configuration Manager を使用します。

機能のサポートと変更

以下の機能は、現在提供されていないか、もうサポートされていないか、7.x 以降の XenApp または XenDesktop で大幅に変更されました。

128 ビット未満の **SecureICA** 暗号化：7.x より前のリリースでは、SecureICA により基本レベル、40 ビット、56 ビット、および 128 ビットの暗号化でクライアント接続を保護できました。このリリースの SecureICA では、128 ビットの暗号化のみを使用できます。

従来の印刷機能：以下の印刷機能は、7.x でサポートされなくなりました：

- Dos クライアントと 16 ビットプリンターに対する後方互換性。
- 強化された拡張プリンタープロパティおよび Win32FavorRetainedSetting を含む、Windows 95 および Windows NT オペレーティングシステムに接続されたプリンターのサポート。
- 自動保持および自動復元プリンターを有効または無効にする機能
- 自動保持および自動復元プリンターを有効または無効にするサーバーのレジストリ設定である DefaultPrnFlag。サーバー上のユーザープロファイルに保存されます。

従来のクライアントプリンター名は使用できます。

Secure Gateway：7.x より前のリリースでは、Secure Gateway を使用してサーバーとユーザーデバイス間の接続を保護できました。このリリースでは、外部接続をセキュリティで保護するためのオプションとして、NetScaler Gateway を使用します。

ユーザーのシャドウ：7.x より前のリリースでは、管理者はポリシーを設定してユーザー間のシャドウを制御しました。このリリースでは、エンドユーザーのシャドウ機能が Director コンポーネントに統合されています。管理者は、Director から Windows リモートアシスタンスを使用してユーザーのアプリケーションや仮想デスクトップをシャドウして、問題のトラブルシューティングを行います。

第 **1** 世代の **Flash** リダイレクト：第 2 世代 Flash リダイレクトをサポートしないクライアントでは、従来の Flash リダイレクトが機能しないためにサーバー側でのレンダリングにフォールバックされます。このリリースに含まれる VDA は、第 2 世代の Flash リダイレクト機能をサポートします。

ローカルテキストエコー：この機能は、以前の形式の Windows アプリケーション上で入力文字列を高速に表示するために使用されました。このリリースでは HDX SuperCodec およびグラフィックサブシステムが改善されたため、この機能は削除されています。

Single Sign-on：パスワードセキュリティを提供するこの機能は、Windows 8、Windows Server 2012、および新しくサポートされた Windows オペレーティングシステムのバージョンではサポートされません。Windows 2008 R2 および Windows 7 環境ではサポートされますが、このリリースには含まれていません。ただし、Citrix のダウンロード Web サイト（https://citrix.com/downloads）から入手することができます。

Oracle データベースのサポート：このリリースでは、SQL データベースを使用します。

サーバーヘルスの監視および復元（**HMR**）：7.x より前のリリースでは、この機能を使用してサーバーファーム内のサーバーでテストを実行し、サーバーの状態を監視したり、サーバーヘルスのリスクを発見したりできました。このリリースでは、Director のコンソールを使用して、インフラストラクチャ全体のシステム状態を一元的に管理および監視できます。

カスタム **ICA** ファイル：7.x より前のリリースでは、カスタムの ICA ファイルを使用して、ユーザーデバイスから特定のマシンへの直接接続が可能でした。このリリースでは、この機能はデフォルトでは無効になっていますが、ローカルグループを使用する標準的な使用においては有効にできます。また、Controller が使用できなくなった場合に高可用性モードで使用することもできます。

Management Pack for System Center Operations Manager（**SCOM**）**2007**：このリリースでは、SCOM を使って XenApp ファームのアクティビティを監視する管理パックはサポートされていません。最新のCitrix SCOM Management Pack for XenApp and XenDesktopを参照してください。

CNAME 機能：7.x より前のリリースでは、CNAME 機能はデフォルトで有効になっていました。このため、CNAME レコードに依存する FQDN の再ルーティングや NetBIOS 名の使用に失敗することがありました。このリリースでは、Controller の自動更新機能により Controller の一覧が動的に更新され、サイトの Controller が追加または削除されると VDA に自動的に通知されます。この自動更新機能は Citrix ポリシーのデフォルトで有効になっていますが、無効にできます。または、レジストリで CNAME 機能を有効にして、従来の FQDN の再ルーティングや NetBIOS 名の使用を許可することもできます。詳しくは、CTX137960を参照してください。

簡易展開ウィザード：7.x より前のリリースの XenDesktop では、この Studio オプションを選択してすべてが構成済みの XenDesktop 展開をすばやく作成することができました。このリリースではインストールおよび構成のワークフローが簡素化されたため、簡易展開ウィザードが不要になりました。

自動管理用のリモート **PC** サービス構成ファイルおよび **PowerShell** スクリプト：リモート PC アクセスは、Studio および Controller に統合されました。

Workflow Studio：7.x より前のリリースでは、XenDesktop のワークフロー構成用のグラフィカルインターフェイスとして Workflow Studio を使用しました。このリリースでは、この機能はサポートされません。

クライアント接続での非公開アプリケーションの起動：7.x よりも前のリリースでは、この Citrix ポリシー設定は、サーバー上の ICA または RDP を介して開始アプリケーションまたは公開アプリケーションを起動するかどうかを指定しました。7.x リリースでは、サーバー上の RDP を介して開始アプリケーションまたは公開アプリケーションを起動するかどうかのみを指定します。

デスクトップの起動：7.x よりも前のリリースでは、この Citrix ポリシー設定は非管理者ユーザーがデスクトップセッションに接続できるかどうかを指定しました。7.x リリースでは、VDA 上のセッションに接続するため、非管理者ユーザーが VDA マシンの Direct Access Users グループのメンバーである必要があります。デスクトップの起動設定により、VDA の Direct Access Users グループの非管理者ユーザーは、ICA コネクションを使って VDA に接続できます。デスクトップの起動設定は、RDP 接続には影響を与えません。VDA の Direct Access Users グループのユーザーは、この設定が有効であるかどうかにかかわらず、RDP 接続を使って VDA に接続できます。

色数：リリース 7.6 以前の Studio では、デリバリーグループのユーザー設定で色数を指定していました。バー

ジョン 7.6 以降、デリバリーグループの色数は New-BrokerDesktopGroup または Set-BrokerDesktopGroup PowerShell コマンドレットを使って設定できます。

タッチパネルでの操作に最適化されたデスクトップ：この設定は無効になっており、Windows 10 および Windows Server 2016 マシンでは使用できません。詳しくは、「モバイルデバイスでの動作のポリシー設定」を参照してください。

Citrix Workspace アプリ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：ユーザーデバイス上の COM ポートへのアクセスを許可または禁止します。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 ポートへの従来のアプリケーションのアクセスを制御します。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）。

詳しくは、使用しているバージョンの Citrix Workspace アプリのドキュメントを参照してください。

環境のアップグレード

October 22, 2021

はじめに

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。このプロセスはインプレースアップグレードと呼ばれます。アップグレード可能なバージョンの一覧は、「アップグレード」を参照してください。

最新の XenApp インストーラーでは、XenApp 6.5 ワーカーサーバーを最新の VDA for Windows Server OS にアップグレードすることもできます。これは、XenApp 6.5 からの移行時に補足的に行います。「XenApp 6.5 ワーカーの VDA for Windows Server OS へのアップグレード」を参照してください。

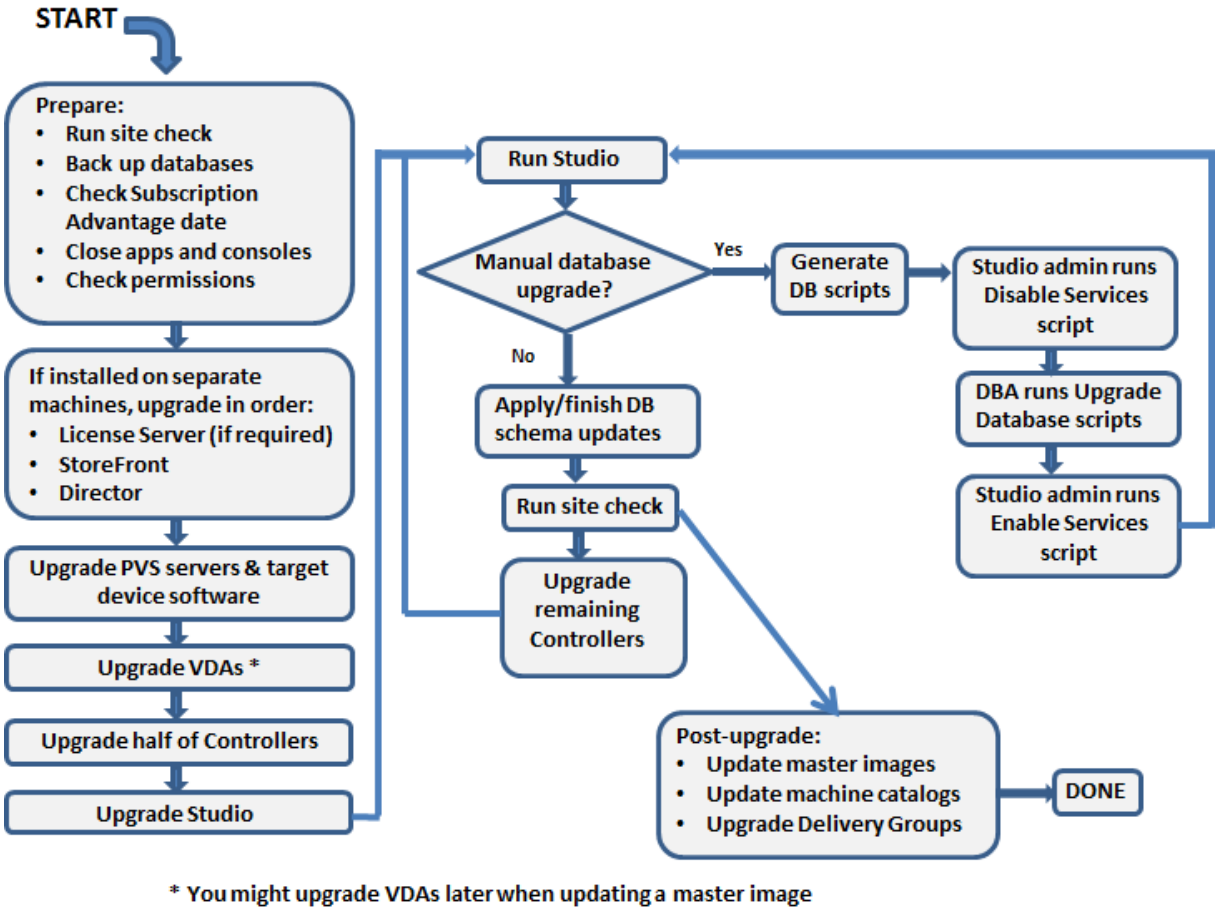
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、既存のコアコンポーネント（Delivery Controller、Citrix Studio、Citrix Director、Citrix ライセンスサーバー）と VDA をアップグレードします。その後、データベースとサイトをアップグレードします。

アップグレードを開始する前に、この記事の情報をすべて確認するようにしてください。

（7.16 以降のリリースにアップグレードする場合は、「環境のアップグレード」のガイダンスを参照してください）。

アップグレードの順序

次の図に、アップグレードの順序の概要を示します。詳細については、下記「アップグレード手順」で説明します。サーバーに複数のコアコンポーネントがインストールされている場合、このサーバーマシンでインストーラーを実行すると、新しいバージョンが存在するすべてのコンポーネントがアップグレードされます。マスターイメージで使用されている VDA をアップグレードしてから、このマスターイメージを更新することもできます。その後、このマスターイメージを使用するカタログと、このカタログを使用するデリバリーグループを更新します。手順の詳細では、サイトデータベースとサイトを自動または手動でアップグレードする方法についても説明します。



アップグレードできる製品コンポーネントのバージョン

製品のインストーラーを使って、以下のコンポーネントをアップグレードできます。

- Citrix ライセンスサーバー、Studio、StoreFront
- Delivery Controllers 7.0 以降
- VDA 5.6 以降
  - 以前の VDA リリースとは異なり、VDA をアップグレードするには製品のインストーラーを使用する必要があります。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 5.6～VDA 7.8：マシンで Receiver for Windows Enterprise（CitrixReceiverEnterprise.exe）が検出された場合は、Receiver for Windows Enterprise 3.4 にアップグレードされます。
- Director 1 以降
- データベース：スキーマがアップグレードされ、サイトデータベースのデータが移行されます（Version 7.x からのアップグレードでは、構成ログデータベースと監視データベースのデータも移行されます）
- Personal vDisk

注：XenDesktop 5.6 からアップグレードするには、まず最新の CU を使用して 7.6 LTSR にアップグレードしてから、このリリースにアップグレードします。

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。ターゲットデバイスのアップグレード前にサーバーのアップグレードをお勧めします。詳しくは、「Provisioning サーバーのアップグレード」を参照してください。
  - Provisioning Services 7.x は XenDesktop 5 でのデスクトップの作成をサポートしていません。既存のデスクトップは引き続き使用できますが、XenDesktop をアップグレードするまでは Provisioning Services 7.x で新しいデスクトップを作成することはできません。このため、XenDesktop 7.x と XenDesktop 5.6 のサイトを同時に運用する場合は、Provisioning Services 7 にアップグレードしないでください。
- ホストハイパーバイザーのバージョン。
- StoreFront。
- Profile Management。
- フェデレーション認証サービス

制限事項

アップグレードには以下の制限があります。

- コンポーネント選択インストール：コンポーネントを新しいバージョンをインストールまたはアップグレードしていて、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択している場合、Studio によって確認メッセージが表示されます。たとえば、アップグレードに Controller と Studio の新しいバージョンが含まれるとします。Controller をアップグレードしますが、Studio がインストールされているマシン上でインストーラーを実行しません。Studio をアップグレードするまではサイトを管理できません。

VDA をアップグレードする必要はありませんが、利用できる機能をすべて使用できるようにするために、すべての VDA をアップグレードすることを Citrix ではお勧めします。

- バージョン **7.5** より前の **XenApp**：バージョン 7.5 より前の XenApp からアップグレードすることはできません。XenApp 6.x の環境を移行することはできます。「XenApp 6.x からの移行」を参照してください。XenApp 6.5 ファームはアップグレードできませんが、Windows Server 2008 R2 マシン上の XenApp 6.5 ソフトウェアを、最新の VDA for Server OS に交換できます。「XenApp 6.5 ワーカーから新しい VDA へのアップグレード」を参照してください。
- バージョン **5.6** より前の **XenDesktop**：バージョン 5.6 より前の XenDesktop からアップグレードすることはできません。
- **XenDesktop Express Edition**： XenDesktop Express Edition をアップグレードすることはできません。現在サポートされているエディションのライセンスを入手してインストールしてからアップグレードしてください。
- **Early Release** または **Technology Preview** バージョン： Early Release バージョン、および Technology Preview バージョンからアップグレードすることはできません。
- **Windows XP** および **Windows Vista**： VDA が Windows XP または Windows Vista のマシンにインストールされている場合は、「Windows XP または Windows Vista を実行しているマシンの VDA」を参照してください。
- 製品選択：以前の 7.x バージョンからアップグレードする場合、最初のインストール時に設定されていた製品（XenApp または XenDesktop）を選択または指定しないでください。
- 混在環境またはサイト：以前のバージョンのサイトと現行バージョンのサイトの実行を継続する必要がある場合は、「混在環境での考慮事項」を参照してください。

準備

アップグレードを始める前に：

- 使用するインストーラーとインターフェイスを決定する： XenApp または XenDesktop ISO で提供される全製品インストーラーを使用して、コアコンポーネントをアップグレードできます。全製品インストーラーまたはスタンドアロンの VDA インストーラーを使用して、VDA をアップグレードできます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。詳しくは、「インストーラー」を参照してください。

  アップグレードできるバージョンからデータをインポートまたは移行することによってアップグレードすることはできません（注：非常に古いバージョンは、アップグレードするのではなく移行する必要があります。ど

のバージョンをアップグレードできるかは、「アップグレードと移行」を参照してください)。

デスクトップ VDA の最初のインストールに VDAWorkstationCoreSetup.exe インストーラーを使用した場合は、アップグレードするときもそのインストーラーを使用することを推奨しています。全製品 VDA インストーラーまたは VDAWorkstationSetup.exe インストーラーを使用して VDA をアップグレードする場合、明示的にアップグレードを省略または除外していない限り、元は除外されていたコンポーネントがインストールされることがあります。

たとえば、VDAWorkstationCoreSetup.exe を使って VDA バージョン 7.13 をインストールし、全製品インストーラーを使って VDA をバージョン 7.14 にアップグレードするときにデフォルト設定をそのまま使用するか、/exclude コマンドラインオプションを使用しない場合、最初のインストールから除外されたコンポーネント（Profile Management や Personal vDisk など）が、このアップグレードでインストールされることがあります。

- サイトの正常性を確認する：アップグレードを開始する前に、サイトが安定して機能している状態であることを確認してください。サイトに問題がある場合、アップグレードでは解決されず、サイトが複雑で修復が困難な状態になる可能性があります。サイトをテストするには、Studio のナビゲーションペインの ［サイト］ エントリをクリックします。中央ペインのサイト構成の部分で、［サイトのテスト］ をクリックします。
- サイトデータベース、監視データベース、構成ログデータベースをバックアップする： CTX135207の手順に従います。アップグレード後に問題を検出した場合は、バックアップを回復できます。

  必要な場合は、テンプレートをバックアップしてハイパーバイザーをアップグレードします。

  他の準備タスクが事業継続計画に記載されていれば、それも完了します。
- **Citrix** ライセンスが最新であることを確認する：アップグレードする前に、Customer Success Services、Software Maintenance、および Subscription Advantage の日付が新しい製品バージョンで有効であることを確認してください。製品の Version 7.x からのアップグレードでは、この日付が 2017.0801 以降である必要があります。(この日付は 7.15 LTSR リリースに適用され、以降の累積更新プログラム（CU）には適用されません。)
- 使用中の **Citrix** ライセンスサーバーと互換性があることを確認する： Citrix ライセンスサーバーが新しいバージョンと互換性があることを確認します。次のいずれかの方法を使用します：
  - 他のシトリックスコンポーネントをアップグレードする前に、ライセンスサーバーがあるマシンでインストーラーを実行します。アップグレードが必要な場合は、インストーラーが開始されます。
  - インストールメディアの XenDesktop Setup ディレクトリから、次のコマンドを実行します： `.\LicServVerify.exe -h \<License-Server-fqdn> -p 27000 -v`。ライセンスサーバーに互換性があるかどうかが表示されます。ライセンスサーバーに互換性がない場合、対象のマシンでインストーラーを実行してアップグレードを実行します。
- **StoreFront** の変更のバックアップを作成する： *default.ica* や *usernamepassword.tfrm* など、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`のファイルを変更した場合は、ストアごとにバックアップを作成します。アップグレード後はそれらを復元して、変更内容を元に戻すことができます。

- アプリケーションとコンソールを終了する：アップグレードを開始する前に、ファイルロックが発生する可能性があるすべてのプログラム（管理コンソールや PowerShell のセッションなど）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。）

  アップグレードの開始前に、サードパーティの監視エージェントサービスを停止し、無効にしてください。

- 適切な権限を持っていることを確認する：ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンのローカル管理者である必要があります。

サイトデータベースとサイトは、自動でも手動でもアップグレードできます。データベースの自動アップグレードでは、SQL Server データベーススキーマを更新できる権限（db_securityadmin または db_owner データベースロールなど）が Studio ユーザーに必要です。詳しくは、「データベース」を参照してください。Studio ユーザーにこれらの権限がない場合は、データベースの手動アップグレードで生成されるスクリプトを使用します。生成されるスクリプトの一部を Studio ユーザーが Studio から実行して、ほかスクリプトをデータベース管理者が SQL Server Management Studio などのツールを使って実行します。

混在環境に関する考慮事項

環境内に異なる製品バージョンの Sites/farms がある場合（混在環境）、StoreFront を使って異なる製品バージョンのアプリケーションやデスクトップ（XenDesktop 7.13 サイトと XenDesktop 7.14 サイトがある場合など）を集約することをお勧めします。詳しくは、StoreFront のドキュメントを参照してください。

- 混在環境では、異なるバージョンの Studio や Director を同一マシン上にインストールすることはできません。
- Provisioning Services を使用する XenDesktop 7.x および XenDesktop 5.6 のサイトを同時に運用する場合は、XenDesktop 7.x サイト用に新しい Provisioning Services を展開するか、Provisioning Services を最新バージョンにアップグレードし、XenDesktop 5.6 サイトでのワークロードのプロビジョニングを無効にしてください。

各サイト内ですべてのコンポーネントをアップグレードすることをお勧めします。コンポーネントによっては以前のバージョンを使用できますが、最新バージョンの機能を一部使用できない場合があります。たとえば、以前のバージョンの Controller を含む環境で最新の VDA を使用できますが、最新リリースの新機能を使用できない場合があります。最新でないバージョンを使用すると、VDA 登録で問題が発生する可能性もあります。

- Version 5.x の Controller と Version 7.x の VDA との混在環境は、アップグレードに伴う一時的な構成としてのみ運用してください。可能な限り、環境内のすべてのコンポーネントのアップグレードを早急に完了してください。
- スタンドアロンの Studio は、新しいバージョンを使用する準備ができるまでアップグレードしないでください。

Windows XP または Windows Vista 上の VDA

Windows XP または Windows Vista が動作するマシンにインストールされている VDA を Version 7.x にアップグレードすることはできません。特定の Hotfix が適用された VDA 5.6 FP1 を使用する必要があります。手順について

は、CTX140941を参照してください。以前のバージョンの VDA を Version 7.x のサイトで実行することは可能ですが、次のような多くの機能を使用できません。

- 新しいバージョンの VDA を必要とする Studio の機能。
- Studio を使った App-V アプリケーションの構成。
- Studio を使った StoreFront のアドレスの構成。
- Machine Creation Services を使用する場合の Microsoft Windows KMS ライセンスの自動サポート。CTX128580を参照してください。
- Director での情報の表示:
  - [ダッシュボード]、[傾向]、および [ユーザーの詳細] ビューでログオン処理時間を算出するためのログオン時間およびログオン終了イベント。
  - HDX 接続時間および認証時間のログオン処理時間ブレークダウンの詳細と、プロファイルロード、GPO ロード、ログオンスクリプト、および対話型セッション確立の期間の詳細。
  - マシンおよび接続の障害率のいくつかのカテゴリ。
  - [ヘルプデスク] ビューおよび [ユーザーの詳細] ビューのアクティビティマネージャー。

Windows XP と Windows Vista のマシンは、サポートされているオペレーティングシステムで再イメージ化して最新の VDA をインストールすることをお勧めします。

Windows 8.x および Windows 7 上の VDA

Windows 8.x または Window 7 を実行しているマシン上にインストールされた VDA を Windows 10 にアップグレードするには、Windows 7 および Windows 8.x マシンを Windows 10 に再イメージ化して、Windows 10 用にサポートされている VDA をインストールすることをお勧めします。再イメージ化がオプションではない場合は、オペレーティングシステムをアップグレードする前に VDA をアンインストールします。これを実行しない場合、VDA は未サポート状態となります。

VDA の混在環境のサポート

製品バージョンをアップグレードするときには、すべてのコアコンポーネントおよび VDA をアップグレードすることをお勧めします。これにより、そのエディションで追加されたり強化されたりした機能をすべて使用できるようになります。

環境のすべての VDA を同時にアップグレードできない場合は、マシンカタログを作成するときに、マシンにインストールされている VDA のバージョンを指定できます。デフォルトでは、推奨される最新バージョンが指定されます。したがって、ここで変更が必要になるのは、以前のバージョンの VDA がインストールされているマシンがマシンカタログに含まれている場合だけです。ただし、マシンカタログで複数のバージョンの VDA を混在させることは推奨されていません。

マシンカタログを作成するときに VDA のバージョンとして推奨バージョンを指定する場合、そのカタログに以前のバージョンの VDA が含まれていると、それらのマシンは Controller に登録されず、機能しなくなります。

詳しくは、「VDA バージョンと機能レベル」を参照してください。

以前の **OS** の **Controller**

サイト内のすべての Delivery Controller で OS を同じにすることをお勧めします。次のアップグレードシーケンスでは、複数の Controller の OS が異なる間隔を最小限に抑えています。

1. サイト内のすべての Delivery Controller のスナップショットを作成し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しい Delivery Controller をインストールします。
3. 新しい Controller をサイトに追加します。
4. 最新リリースで有効でないオペレーティングシステムを実行している Controller を取り外します。

Controller の追加と削除については、「Delivery Controller」を参照してください。

アップグレード手順

製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、インストールメディアまたは ISO ファイルの **AutoSelect** をダブルクリックします。コマンドラインインターフェイスを使用する場合は、「コマンドラインを使ったインストール」を参照してください。

1. アップグレード可能な複数のコアコンポーネント（Controller、Studio、ライセンスサーバーなど）が同じサーバーにインストールされている場合、インストーラーによりそれらがすべてアップグレードされます。

   コアコンポーネントが Controller 以外のマシンにインストールされている場合は、各マシン上でインストーラーを実行します。推奨される順番は次のとおりです：License Server、StoreFront、Director。

   新しいバージョンでライセンスサーバーに互換性があるか確認できない場合（「準備」を参照）、他のコアコンポーネントをアップグレードする前にライセンスサーバーでインストーラーを実行する必要があります。

   StoreFront ストアへの手動での変更を保持する場合は、StoreFront をアップグレードする前にストアファイルをバックアップしてください（「準備」を参照）。

2. Provisioning Services を使用する場合、Provisioning Servicesのドキュメントの手順に従って、PVS サーバーとクライアントをアップグレードします。

3. アップグレードする VDA のマシン上で製品インストーラーを実行します。（マスターイメージおよび Machine Creation Services を使用する場合は、手順 12 を参照してください）。

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. 既にアップグレードした Controller とは別のマシンに Studio がインストールされている場合は、そのマシン上でインストーラーを実行します。
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. 残りの Controller でのアップグレードが完了したら、Studio をいったん閉じてから再度開きます。Studio に、Controller のサービスをサイトに登録するため、またはゾーン ID がまだ存在しない場合は作成するために、追加のサイトアップグレードを要求するメッセージが表示されることがあります。
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 の利用統計情報プログラムに登録するかどうかを選択できるページが表示されます。このプログラムでは、使用環境に関する情報が収集されます。収集された情報は、弊社製品の品質、信頼性、およびパフォーマンスの向上のために使用させていただきます。
11. コンポーネント、データベース、およびサイトのアップグレードが完了したら、新しくアップグレードされたサイトをテストします。Studio の [ナビゲーション] ペインで、**Citrix Studio** のサイト名を選択します。[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。

    Controller を Windows Server 2016 にインストールして、サイトデータベースにローカルの SQL Server Express を使用している場合、SQL Server Browser が開始されてないと、サイトのテスト機能でエラーが発生する可能性があります。これを回避するには、以下のタスクを行います。

    a)（必要に応じて）SQL Server Browser サービスを有効にして開始します。

    b) SQL Server（SQLEXPRESS）サービスを再開始します。
12. Machine Creation Services を使用しておりアップグレード後の VDA を使用する必要がある場合：アップグレードと環境のテスト後に、マスターイメージで使用する VDA を更新します（まだ更新していない場合）。これらの VDA を使用するマスターイメージを更新します。「マスターイメージの更新または新しいマスターイメージの作成」を参照してください。次に、これらのマスターイメージを使用するマシンカタログを更新し、さらにこれらのカタログを使用するデリバリーグループをアップグレードします。

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。

そのほかの注意事項：権限要件に関して上記の「準備」セクションを確認してください。

- データベースの自動アップグレードでは、SQL Server データベーススキーマを更新できる権限が Studio ユーザーに必要です。
- 手動アップグレードの場合、Studio ユーザーは Studio が生成したスクリプトをいくつか実行します。データベース管理者は、SQLCMD ユーティリティ、または SQL Server Management Studio を SQLCMD モードで使用し、そのほかのスクリプトを実行します。このようにしないと、エラーが発生することがあります。

アップグレードする前にデータベースをバックアップしておくことを Citrix では強くお勧めします。CTX135207を参照してください。データベースのアップグレード中は製品サービスが無効になります。その間は、Controller がサイトへの接続要求を仲介できなくなるため、慎重に計画しておく必要があります。

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。サイトのアップグレードを自動的に開始することを選択して、準備ができていることを確認すると、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:

1. アップグレードした Studio を起動します。サイトを手動でアップグレードすることを選択します。ウィザードでライセンスサーバーの互換性がチェックされ、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。
    - **DisableServices.ps1**: 製品サービスを無効にするために、Controller 上の Studio ユーザーが実行する PowerShell スクリプト。
    - **UpgradeSiteDatabase.sql**: サイトデータベースがあるサーバー上でデータベース管理者が実行する SQL スクリプト。
    - **UpgradeMonitorDatabase.sql**: 監視データベースがあるサーバー上でデータベース管理者が実行する SQL スクリプト。
    - **UpgradeLoggingDatabase.sql**: 構成ログデータベースがあるサーバー上でデータベース管理者が実行する SQL スクリプト。このスクリプトは、このデータベースが変更された場合にのみ実行します (Hotfix の適用後など)。
    - **EnableServices.ps1**: 製品サービスを有効にするために、Controller 上の Studio ユーザーが実行する PowerShell スクリプト。
3. チェックリストのタスクを完了したら、[アップグレードを完了する] を選択します。

Dbschema のアップグレード

環境を新しい CU に更新すると、一部のデータベーススキーマがアップグレードされます。このプロセスでアップグレードされるデータベーススキーマについては、次の表を参照してください:

7.15 DBschema upgrade	7.15 CU1	7.15 CU2	7.15 CU3	7.15 CU4	7.15 CU5	7.15 CU6	7.15 CU7	7.15 CU8
7.15 RTM	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU1		Config	Site; Config	Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU2			Site; Config	Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU3				Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU4					Monitor, Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU5						Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
7.15 CU6							Site; Monitor; Config	Site; Monitor; Config
7.15 CU7								Site; Config

用語の定義:

- サイト＝サイトデータストア。サイトデータストアに対して Dbschema の更新が行われます。
- モニター＝モニターデータストア。モニターデータストアに対して Dbschema の更新が行われます。
- 構成＝構成テーブル。Desktop Studio のバージョン、ライセンスサーバーのバージョン、またはその両方が構成テーブルで更新されます。
- ログ＝ログデータストア。ログデータストアに対して Dbschema の更新が行われます。

XenApp 6.5 ワーカーから新しい VDA へのアップグレード

August 24, 2021

XenAppp6.5 ファームに移行した後は、以前のソフトウェアを削除し、新しい VDA for Server OS をインストールすることで、セッションホスト専用モード（セッションホストモードまたはワーカーとも呼ばれます）で構成された XenApp6.5 サーバーを使用できます。

注: XenApp 6.5 ワーカーサーバーはアップグレードできますが、クリーンなマシンに最新の VDA ソフトウェアをインストールする方が、セキュリティは優れています。

XenApp 6.5 ワーカーから新しい VDA にアップグレードするには、以下の操作を行います。

1. hotfix readme の説明に従って、XenApp 6.5 の Hotfix Rollup Pack 7 を削除します。CTX202095を参照してください。
2. 「役割やコンポーネントを削除する」の説明に従って、XenApp 6.5 をアンインストールします。このプロセスでは再起動が数回必要です。アンインストール時にエラーが発生した場合は、エラーメッセージに従ってアンインストールエラーログを参照してください。ログファイルは、%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\フォルダーに生成されます。
3. このリリースで提供されるインストーラーを使って、VDA for Server OS をインストールします。「VDA のインストール」または「コマンドラインを使ったインストール」を参照してください。

新しい VDA をインストールした後、新しい XenApp サイトの Studio を使用して、アップグレードされたワーカーのマシンカタログを作成（または既存のマシンカタログを編集）します。

トラブルシューティング

問題：XenApp 6.5 ソフトウェアのアンインストールに失敗し、アンインストールログにメッセージ「Error 25703. XML の Internet Information Server への関連付け中にエラーが発生しました。IIS の Scripts ディレクトリにファイルをコピーできません。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。

解決方法：

1. Windows のサーバーの役割の削除ウィザードを使用して［Web サーバー（IIS）の役割］を削除します。Web サーバー（IIS）の役割は必要に応じて後で再インストールできます。
2. サーバーを再起動します：
3. ［プログラムの追加と削除］を使って、Citrix XenApp 6.5 と Microsoft Visual C++ 2005 Redistributable（x64）バージョン 8.0.56336 をアンインストールします。
4. サーバーを再起動します：
5. VDA for Windows Server OS をインストールします。

XenApp 6.x からの移行

October 22, 2021

注： Citrix Smart Migrate 製品をこのバージョンの XenApp および XenDesktop とともに使用することはできません。移行ツールは使用できます。

この記事で説明する移行ツールを使用して、XenApp 6.x から XenApp 7.6 へ移行することができます。その後、XenApp 7.6 からサポート対象の LTSR や Citrix Virtual Apps and Desktops の現行リリースにアップグレードできます。

XenApp 6.x 移行ツール

XenApp 6.x の移行ツールでは、いくつかの PowerShell スクリプトが実行されます。これらのスクリプトにより、XenApp 6.x（6.0 または 6.5）のポリシーおよびファームデータを移行するためのコマンドレットが実行されます。XenApp 6.x Controller の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 Controller 上で、以下の操作を行います。
2. PowerShell のエクスポートモジュールをインポートします。

3. 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。
4. 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。
5. XenApp 7.6 の Controller 上で、以下の操作を行います。
6. PowerShell のインポートモジュールをインポートします。
7. 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。
8. 移行後のタスクを完了します。

実際に移行を実行する前に、XenApp 6.x の設定をエクスポートしてから XenApp 7.6 サイトでプレビューインポートを実行できます。これにより、問題が発生する可能性がある箇所を特定して、実際にインポートを実行する前に問題を修正できます。たとえば、新しい XenApp 7.6 サイトに同じ名前のアプリケーションが既に存在していることが検出される場合があります。プレビューによって生成されるログファイルを実際の移行を実行するためのガイドとして使用することもできます。

特に明記されている場合を除き、6.x は XenApp 6.0 または 6.5 を指します。

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（https://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、ReadIMA.zip と ImportFMA.zip 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、ReadIMA.zip のみが必要です。XenApp 7.6 サーバーへのインポートでは、ImportFMA.zip のみが必要です。
- Export-XAFarm コマンドレットに EmbedIconData パラメーターが追加されました。これを使用すると、アイコンデータを別個のファイルとしてコピーする必要がなくなります。
- Import-XAFarm コマンドレットに以下の 3 つのパラメーターが追加されました。
- MatchServer - 条件に一致する名前のサーバーからアプリケーションをインポートします。
- NotMatchServer - 条件に一致しない名前のサーバーからアプリケーションをインポートします。
- IncludeDisabledApps - 無効に設定されたアプリケーションをインポートします。
- 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、シトリックスのダウンロードサイトから入手できます。XAMigration.zip ファイルには、以下の 2 つのパッケージが含まれています：

- ReadIMA.zip - XenApp 6.x ファームからデータをエクスポートするためのファイルと、共有モジュールが含まれています。

モジュールまたはファイル	説明
ExportPolicy.psm1	XenApp 6.x のポリシーを XML ファイルにエクスポートする PowerShell スクリプトモジュール。
ExportXAFarm.psm1	XenApp 6.x のファーム設定を XML ファイルにエクスポートする PowerShell スクリプトモジュール。
ExportPolicy.psd1	スクリプトモジュール ExportPolicy.psm1 の PowerShell マニフェストファイル。
ExportXAFarm.psd1	スクリプトモジュール ExportXAFarm.psm1 の PowerShell マニフェストファイル。
LogUtilities.psm1	ログ機能を含んでいる共有 PowerShell スクリプトモジュール。
XmlUtilities.psd1	スクリプトモジュール XmlUtilities.psm1 の PowerShell マニフェストファイル。
XmlUtilities.psm1	XML 機能を含んでいる共有 PowerShell スクリプトモジュール。

- ImportFMA.zip - XenApp 7.6 ファームにデータをインポートするためのファイルと、共有モジュールが含まれています。

モジュールまたはファイル	説明
ImportPolicy.psm1	ポリシーを XenApp 7.6 サイトにインポートする PowerShell スクリプトモジュール。
ImportXAFarm.psm1	アプリケーションを XenApp 7.6 サイトにインポートする PowerShell スクリプトモジュール。
ImportPolicy.psd1	スクリプトモジュール ImportPolicy.psm1 の PowerShell マニフェストファイル。
ImportXAFarm.psd1	スクリプトモジュール ImportXAFarm.psm1 の PowerShell マニフェストファイル。
PolicyData.xsd	ポリシーデータの XML スキーマ。
XAFarmData.xsd	XenApp ファームデータの XML スキーマ。
LogUtilities.psm1	ログ機能を含んでいる共有 PowerShell スクリプトモジュール。

モジュールまたはファイル	説明
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が XenApp 7.6 サイトにインポートされます。つまり、公開アプリケーション、公開コンテンツ、および多くのストリーム配信アプリケーション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、各ポリシーのオブジェクト割り当てをよく調べて、インポートに起因するセキュリティ上

の脆弱性がないことを確認してください。インポートしたポリシーに別のユーザー、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。

Citrix ではエクスポートおよびインポートのコマンドレットを実行するときは、常に個別のログファイルを指定することをお勧めします。

ログファイルの名前を指定しない場合、実行ユーザーの既存のホームフォルダー（PowerShell $HOME 変数で指定される）にログファイルが格納されます。ホームフォルダーが存在しない場合は、スクリプトの現在の実行フォルダーに格納されます。デフォルトでは、「XFarm<YYYYMMDDHHmmSS-xxxxxx>」というログファイルが生成されます。ここで、「xxxxxx」はランダムな数字で構成されます。

デフォルトでは、すべての進捗情報が表示されます。表示されないようにするには、エクスポートコマンドレットとインポートコマンドレットで NoDetails パラメーターを指定します。

通常、スクリプトでエラーが発生すると処理がそこで停止します。エラー状態を解決した後で、コマンドレットを再実行できます。

エラーとしてみなされない状態も多くは警告としてログに記録され、スクリプトの実行は続行されます。たとえば、アプリケーションの種類がサポートされない場合は警告として記録され、インポートから除外されます。XenApp 7.6 サイトに既に存在するアプリケーションはインポートされません。XenApp 7.6 でサポートされなくなったポリシー設定はインポートされません。

移行スクリプトでは多くの PowerShell コマンドレットが使用され、一部のエラーがログに記録されない場合があります。ログに記録される情報を追加するには、PowerShell のログ機能を使用してください。たとえば、PowerShell で画面上に出力されるすべての情報をログに記録できます。詳しくは、Start-Transcript および Stop-Transcript コマンドレットのヘルプを参照してください。

要件、準備、およびベストプラクティス

移行には、Citrix XenApp 6.5 SDK を使用する必要があります。https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.htmlからこの SDK をダウンロードしてください。

重要：移行を開始する前に、このトピック全体をよくお読みください。

PowerShell の実行ポリシー、モジュール、スクリプトなどについての基本的な理解が必要です。スクリプトを作成するための専門知識は必要ありませんが、実行するコマンドレットについて理解しておく必要があります。事前に Get-Help コマンドレットを使用して、各移行コマンドレットのヘルプを確認しておいてください。例：

```
Get-Help -full Import-XAFarm
```

コマンドラインでログファイルを指定して、コマンドレットの実行後にそのログファイルを確認してください。スクリプトの処理に失敗した場合は、ログファイルを参照してエラーを解決し、コマンドレットを再実行してください。

ヒント：

- 2 つの環境（XenApp 6.x ファームと新しい XenApp 7.6 サイト）を実行している間のアプリケーション配信を容易にするには、StoreFront または Web Interface で両方の環境を集約します。eDocs で、使用する StoreFront または Web Interface のドキュメント（「管理」>「ストアの作成」）を参照してください。
- アプリケーションのアイコンデータは、以下のいずれかの方法で処理されます。
- EmbedIconData パラメーターを指定して Export-XAFarm コマンドレットを実行すると、アプリケーションのアイコンデータが埋め込まれた XML ファイルがエクスポートされます。
- EmbedIconData パラメーターを指定せずに Export-XAFarm コマンドレットを実行すると、エクスポートされた XML ファイルのベース名に「-icons」を追加した名前のフォルダーにアプリケーションのアイコンデータが格納されます。たとえば、XmlOutputFile パラメーターで「FarmData.xml」を指定した場合は、「FarmData-icons」というフォルダーが作成され、そこにアプリケーションアイコンが格納されます。

  このフォルダーに格納されるアイコンデータファイルは、その公開アプリケーションの表示名に基づく名前の TXT ファイルです。これらのファイルにはエンコードされたバイナリアイコンデータが記述されており、インポートスクリプトがこれを読み込んでアプリケーションアイコンを再作成します。インポート時に XML ファイルと同じフォルダー内にアイコンフォルダーが見つからない場合、インポートした各アプリケーションで標準的なアイコンが使用されます。
- スクリプトモジュール、マニフェストファイル、共有モジュール、およびコマンドレットには類似した名前が付けられています。Tab キーによる補完機能を使用して、入力エラーを避けることができます。たとえば、Export-XAFarm はコマンドレット名です。ExportXAFarm.psd1 および ExportXAFarm.psm1 には似たファイル名が付いていますが、コマンドレットとは異なり実行不能です。
- 後述の手順説明で、<string> パラメーターの値は二重引用符で囲んであります。値にスペースが含まれない場合、二重引用符で囲まなくても正しく処理されます。

XenApp 6.x サーバーからのエクスポート：

- エクスポートは、コントローラーモードとセッションホストモード（通常コントローラーと呼ばれます）で構成された XenApp 6.x サーバー上で実行する必要があります。
- エクスポートコマンドレットを実行するには、オブジェクトの読み取り権限を持つ XenApp 管理者である必要があります。また、PowerShell スクリプトを実行するための Windows 権限も必要です。設定方法は、後述の手順説明に記載されています。

- エクスポートを開始する前に、XenApp 6.x ファームのヘルス状態が良好であることを確認します。ファームデータベースをバックアップします。Citrix IMA Helper ツール（CTX137461）を使用してファームの整合性を確認します。[IMA Datastore] タブで Master Check を実行します（実行後、DSCheck オプションを使用して無効なエントリを解決します）。移行前に問題を解決しておくと、エクスポートエラーを避けることができます。たとえば、ファームから不適切に削除されたサーバーがあると、データベースにそのサーバーのデータが残ってしまい、エクスポートスクリプトのコマンドレット（Get-XAServer-ZoneName など）の処理が失敗することがあります。コマンドレットの処理が失敗すると、スクリプトの処理も失敗します。
- ファームにユーザーが接続している状態でもエクスポートコマンドレットを実行できます。エクスポートスクリプトでは、静的なファーム構成とポリシーデータのみが読み取られます。

XenApp 7.6 サーバーへのインポート：

- XenApp 7.6 環境（およびそれ以降の移行可能なバージョン）にデータをインポートできます。XenApp 6.x ファームからエクスポートしたデータをインポートする前に、XenApp 7.6 の Controller と Studio をインストールしてサイトを作成しておく必要があります。設定をインポートするために VDA をインストールしておく必要はありませんが、インストールしておくとアプリケーションのファ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 Controller から XML ファイルにデータをエクスポートするには、次の手順に従います。

1. Citrix のダウンロードサイトから、移行ツールのパッケージ XAMigration.zip をダウンロードします。XenApp 6.x ファームおよび XenApp 7.6 サイトの両方からアクセスできるネットワーク上の共有フォルダーにパッケージをダウンロードすると便利です。ネットワーク上の共有フォルダーで XAMigration.zip を展開します。ReadIMA.zip および ImportFMA.zip の 2 つの ZIP ファイルが展開されます。
2. ファームに対する読み取り以上の権限と、PowerShell スクリプトを実行できる Windows 権限を持つ XenApp 管理者として XenApp 6.x Controller にログオンします。

3. 共有フォルダーの ReadIMA.zip を XenApp 6.x Contorller にコピーします。Controller 上の ReadIMA.zip を展開し、新規フォルダー（C:\XAMigration など）にスクリプトを展開します。
4. PowerShell コンソールを開き、カレントディレクトリをスクリプトの場所に移動します。例:

   ```
   cd C:\XAMigration
   ```

5. Get-ExecutionPolicy を実行して、スクリプトの実行ポリシーを確認します。
6. スクリプトを実行するには、実行ポリシーを RemoteSigned またはそれ以上に設定する必要があります。例:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

7. 以下のコマンドを実行して、モジュール定義ファイル ExportPolicy.psd1 および ExportXAFarm.psd1 をインポートします。

   ```
   Import-Module .\ExportPolicy.psd1
   ```

   ```
   Import-Module .\ExportXAFarm.psd1
   ```

   ヒント:

   - 移行するデータがポリシーデータのみの場合は、モジュール定義ファイル ExportPolicy.psd1 のみをインポートできます。同様に、移行するデータがファームデータのみの場合は、ExportXAFarm.psd1 のみをインポートできます。
   - モジュール定義ファイルをインポートすると、必要な PowerShell スナップインも追加されます。
   - スクリプトモジュールファイル（*.psm1）をインポートしないでください。

8. Export-Policy コマンドレットを実行して、ポリシーデータをエクスポートします。

パラメーター	説明
-XmlOutputFile “<string>.xml”	出力する XML ファイルの名前です。このファイルにエクスポートされたデータが記述されます。拡張子として「.xml」を指定する必要があります。既存のファイル名を指定しないでください。ただし、パスを指定する場合は既存のパスを指定してください。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

パラメーター	説明
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFile パラメーターが無視されます。デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFile パラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。デフォルト：False。上記のメッセージがコンソールに表示されます。

例：次のコマンドレットを実行すると、MyPolicies.xml という名前の XML ファイルにポリシー情報がエクスポートされます。この処理は、MyPolicies.log という名前のログファイルに記録されます。

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
<!--NeedCopy-->
```

1. 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。

パラメーター	説明
-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なため、このパラメーターを指定することは推奨されません。デフォルト：False。上記のメッセージがコンソールに表示されます。
-IgnoreAdmins	管理者情報をエクスポートから除外します。使用方法については、「高度な使用方法」を参照してください。デフォルト：False。管理者情報がエクスポートされます。
-IgnoreApps	アプリケーション情報をエクスポートから除外します。使用方法については、「高度な使用方法」を参照してください。デフォルト：False。アプリケーション情報がエクスポートされます。
-IgnoreServers	サーバー情報をエクスポートから除外します。デフォルト：False。サーバー情報がエクスポートされます。

パラメーター	説明
-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（前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	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	エクスポートを省略するアプリケーションの数を指定します。使用方法については、「高度な使用方法」を参照してください。デフォルト：アプリケーションは省略されません。

例：次のコマンドレットを実行すると、MyFarm.xml という名前の XML ファイルにファーム情報がエクスポートされます。この処理は、MyFarm.log という名前のログファイルに記録されます。MyFarm.XML と同じフォルダー内に「MyFarm-icons」という名前のフォルダーが作成され、そこにアプリケーションのアイコンデータが格納されます。

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

エクスポートスクリプトの処理が完了すると、コマンドラインで指定した XML ファイルにポリシーと XenApp ファームのデータが含まれています。アプリケーションアイコンファイルにはアイコンデータが含まれ、ログファイルにはエクスポート処理の内容が記述されます。

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 Controller でエクスポートされた XML ファイルを、XenApp 7.6 Controller の ImportFMA.zip の展開先フォルダー（つまり C:\XAMigration など）にコピーします。

   Export-XAFarm コマンドレット実行時にアプリケーションのアイコンデータを XML ファイルに埋め込まなかった場合は、アイコンデータのフォルダーおよびファイルを XML ファイルのコピー先フォルダー（つまり C:\XAMigration など）にコピーします。
4. PowerShell コンソールを開き、カレントディレクトリをスクリプトの場所に移動します。

   ```
   cd C:\XAMigration
   ```
5. Get-ExecutionPolicy を実行して、スクリプトの実行ポリシーを確認します。
6. スクリプトを実行するには、実行ポリシーを RemoteSigned またはそれ以上に設定する必要があります。例:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```
7. 以下のコマンドを実行して、PowerShell モジュール定義ファイル ImportPolicy.psd1 および ImportXAFarm.psd1 をインポートします。

   ```
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1
   ```

   ヒント

   - 移行するデータがポリシーデータのみの場合は、モジュール定義ファイル ImportPolicy.psd1 のみをインポートできます。同様に、移行するデータがファームデータのみの場合は、ImportXAFarm.psd1 のみをインポートできます。
   - モジュール定義ファイルをインポートすると、必要な PowerShell スナップインも追加されます。
   - スクリプトモジュールファイル（*.psm1）をインポートしないでください。
8. Import-Policy コマンドレットを実行して、ポリシーデータをインポートします。

パラメーター	説明
-XmlInputFile “<string>.xml”	入力する XML ファイルの名前です。Export-Policy コマンドレットで収集されたデータが記述されています。拡張子として「.xml」を指定する必要があります。デフォルト：なし。必須パラメーターです。
-XsdFile “<string>”	XSD ファイルの名前です。インポートスクリプトでは、このファイルにより入力 XML ファイルの構文が検証されます。使用方法については、「高度な使用方法」を参照してください。デフォルト：PolicyData.XSD。
-LogFile “<string>”	ログファイルの名前です。エクスポート時に生成されたログファイルも Controller 上にコピーしてある場合は、異なるログファイル名を指定してください。デフォルト：「ログとエラー処理」を参照
-NoLog	ログファイルを生成しません。このパラメーターを指定すると、-LogFile パラメーターが無視されます。デフォルト：False。ログファイルが生成されます。
-NoClobber	-LogFile パラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。デフォルト：False。上記のメッセージがコンソールに表示されます。

パラメーター	説明
-Preview	プレビューインポートを実行します。この処理では、入力 XML ファイルからデータが読み込まれますが、サイトへのオブジェクトのインポートは実行されません。プレビューインポートにより、実際のインポートで実行される処理内容がログファイルおよびコンソールに出力されます。これにより、管理者はインポートの問題を事前に解決できます。デフォルト：False。実際のインポートが実行されます。

例：次のコマンドレットを実行すると、MyPolicies.xml という名前の XML ファイルからポリシーデータがインポートされます。この処理は、MyPolicies.log という名前のログファイルに記録されます。

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
<!--NeedCopy-->
```

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。

パラメーター	説明
-NoClobber	-LogFile パラメーターで指定した既存のログファイルの上書きを禁止します。指定したログファイルが存在しない場合、このパラメーターは無視されます。デフォルト：False。既存のファイルが上書きされます。
-NoDetails	スクリプト実行の詳細なレポートをコンソールに表示しません。デフォルト：False。詳細なレポートがコンソールに表示されます。
-SuppressLogo	メッセージ「XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#」をコンソールに表示しません。トラブルシューティング時にスクリプトのバージョンを確認する場合に便利なため、このパラメーターを指定することは推奨されません。デフォルト：False。上記のメッセージがコンソールに表示されます。
-Preview	プレビューインポートを実行します。この処理では、入力 XML ファイルからデータが読み込まれますが、サイトへのオ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：”- デリバリーグループ”
-MatchFolder “<string>”	<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：<string> の指定なし。
-NotMatchFolder “<string>”	<string> にマッチしない名前のフォルダー内のアプリケーションのみをインポートします。使用方法については、「高度な使用方法」を参照してください。デフォルト：<string> の指定なし。

パラメーター	説明
-MatchServer “<string>”	<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>”	<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：<string> の指定なし。
-MatchWorkerGroup “<string>”	<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：<string> の指定なし。
-NotMatchWorkerGroup “<string>”	<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：<string> の指定なし。
-MatchAccount “<string>”	<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：<string> の指定なし。
-NotMatchAccount “<string>”	<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：<string> 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。（他のストリーミング配信されるアプリケーションはインポートされません）。デフォルト：ストリーミング配信される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、MyFarm.log という名前のログファイルに記録されます。

```
1 Import-XAFarm -XmlInputFile ".\MyFarm.XML"
```



```
-LogFile ".\MyFarm.Log"

<!--NeedCopy-->
```

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、本質的に移行前後の比較になります。

1. ログファイルには、インポートされたり無視されたりしたすべてのポリシーおよび設定項目が記録されます。まず、ログファイルを参照してインポートされなかったポリシーおよび設定項目を確認します。
2. XenApp 6.x のポリシーと XenApp 7.6 にインポートされたポリシーを比較します。同じ設定値が保持されていることを確認します（次の手順で説明する廃止予定の設定項目を除く）。
    - 移行したポリシーの数が多くない場合は、XenApp 6.x の AppCenter と XenApp 7.6 の Studio の両方でポリシーを並べて表示して視覚的に比較できます。
    - ポリシーの数が多い場合、視覚的に比較することは困難です。この場合、ポリシーのエクスポートコマンドレット（Export-Policy）を使用して XenApp 7.6 のポリシーを別名の XML ファイルにエクスポートして、テキストファイルの比較ツール（windiff など）を使用して XenApp 6.x からエクスポートしたファイルと比較します。
3. 「インポートされないポリシー設定」セクションを参照して、インポート時に変更された可能性のある設定項目を確認します。XenApp 6.x のポリシーに廃止予定の設定項目のみが含まれる場合、そのポリシーはインポートされません。たとえば、XenApp 6.x で［サーバーヘルス監視テスト］設定のみが構成されたポリシーがある場合、対応する設定項目が XenApp 7.6 にないため、そのポリシーは無視されます。

    一部の XenApp 6.x ポリシー設定はサポートされなくなりましたが、同等の機能が XenApp 7.6 に実装されています。たとえば、XenApp 7.6 では、デリバリーグループを編集してサーバー OS マシンの再起動スケジュールを構成できます。この機能は、以前はポリシー設定で実装されていました。
4. XenApp 7.6 サイトと XenApp 6.x ファームでのポリシーの適用フィルターの動作について確認します。XenApp 6.x ファームと XenApp 7.6 サイトとのフィルターの違いについては、次のセクションを参照してください。

- フィルター

各ポリシーに適用されるフィルター（割り当て先）を慎重に確認してください。XenApp 6.x での元のフィルター設定が XenApp 7.6 でも正しく適用するようにするには、設定の変更が必要になる場合があります。

フィルター	注意事項
アクセス制御	XenApp 6.x からインポートしたアクセス制御フィルターには元の設定と同じ値が適用されており、変更は不要です。
Citrix CloudBridge	単純なブール値なので変更は不要です。（この製品は現在 NetScaler SD-WAN と呼ばれています。）
クライアント 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。

フィルター	注意事項
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"
<!--NeedCopy-->
```

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

- エクスポートから除外するオブジェクトの指定 - インポートされないオブジェクトなど、一部のオブジェクトはエクスポート時に無視されます。これらのオブジェクトについては、「インポートされないポリシー設定」および「アプリケーションプロパティの対応」を参照してください。以下のパラメーターを使用すると、特定の種類のオブジェクトをエクスポートから除外できます:
- IgnoreAdmins - 管理者オブジェクトをエクスポートから除外します。
- IgnoreServers - サーバーオブジェクトをエクスポートから除外します。
- IgnoreZones - ゾーンオブジェクトをエクスポートから除外します。
- IgnoreOthers - そのほかのオブジェクト（構成ログ、負荷評価基準、負荷分散ポリシー、プリンタードライバー、ワーカーグループ）をエクスポートから除外します。
- IgnoreApps - アプリケーションオブジェクトをエクスポートから除外します。アプリケーション以外のデータとアプリケーションを別の XML ファイルにエクスポートする場合に使用します。

これらのパラメーターは、エクスポート時の問題を回避するときに使用することもできます。たとえば、ゾーン内に不適切なサーバーがあるとエクスポートが失敗する場合があります。この場合は、IgnoreZones パラメーターを使用してほかのオブジェクトをエクスポートできます。

- デリバリーグループ名 - インポートするアプリケーションを複数のデリバリーグループ内に分けて追加する場合（異なるユーザーグループに提供する場合や異なるサーバーグループで公開する場合など)、Import-XAFarm コマンドレットを複数に分けて実行し、異なるアプリケーションとデリバリーグループを指定します。移行後に PowerShell コマンドレットを使ってアプリケーションをほかのデリバリーグループに移動することもできますが、インポート時にデリバリーグループを指定しておくと、後でアプリケーションを移動する手間が省けます。

1. DeliveryGroupName パラメーターを指定して Import-XAFarm コマンドレットを実行します。これにより、指定されたデリバリーグループが存在しない場合は作成されます。
2. 以下のパラメーターで正規表現を使用して、アプリケーションを特定のフォルダー、ワーカーグループ、ユーザーアカウント、サーバー名に基づいて特定のデリバリーグループにインポートします。正規表現の部分を引用符または二重引用符で囲むことをお勧めします。正規表現について詳しくは、https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expressionsを参照してください。
    - MatchWorkerGroup および NotMatchWorkerGroup - たとえば、ワーカーグループに公開されたアプリケーションに対して次のコマンドレットを実行すると、ワーカーグループ「Productivity Apps」内のアプリケーションが XenApp 7.6 の同じ名前のデリバリーグループにインポートされます。

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
-MatchWorkerGroup 'Productivity Apps' -DeliveryGroupName '
   Productivity Apps'
<!--NeedCopy-->
```

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

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/.\*"
<!--NeedCopy-->
```


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

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

- カスタマイズ - PowerShell のプログラミング知識がある場合は、カスタムのツールを作成できます。たとえば、エクスポートスクリプトをインベントリツールとして使用して、XenApp 6.x ファームの変更履歴を追跡できます。また、XSD ファイルを編集したり新しく作成したりして、XML ファイルに記述されるデータを追加したり、記述形式を変更したりできます。各インポートコマンドレットに非デフォルトの XSD ファイルを指定できます。

注：特定の移行要件に応じてスクリプトファイルを編集することができますが、その場合はサポート対象外になります。Citrix のテクニカルサポートは、スクリプトを元の状態に戻したうえで正しい動作を確認することを推奨し、必要な場合サポートを提供します。

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 プロバイダースナップインまたは Citrix Common Commands スナップインを追加した場合、エクスポートまたはインポートコマンドレットの実行時に「オブジェクト参照がオブジェクトインスタンスに設定されていません」というエラーメッセージが表示されることがあります。このエラーメッセージはスクリプトの実行に影響せず、無視して構いません。
- Citrix Group Policy PowerShell プロバイダースナップインはエクスポートおよびインポートのスクリプトモジュールにより自動的に追加されるため、これらのスクリプトモジュールを使用するコンソールセッション上にこのスナップインを追加したり削除したりすることは避けてください。このスナップインを事前に追加したり削除したりすると、以下のエラーメッセージが表示されることがあります。
- 「名前 'LocalGpo' のドライブは既に存在しています。」このエラーメッセージは、スナップインを 2 回追加すると表示されます。スナップインのロード時にドライブ「LocalGpo」のマウントが試行されるため、このメッセージが表示されます。

- 「パラメーター名 'Controller' に一致するパラメーターが見つかりません。」このエラーメッセージは、スナップインが追加されていないにもかかわらずドライブのマウントが試行されると表示されます。この問題は、スナップインが事前に削除されていると発生します。コンソールを閉じて新しいセッションを起動してください。新しいセッションでスクリプトモジュールをインポートします。事前にスナップインを追加したり削除したりしないでください。
- モジュールをインポートする場合、.psd1 ファイルを右クリックして［開く］または［PowerShell で開く］を選択するとすぐに PowerShell コンソールウィンドウが開き、プロセスを停止する場合に閉じることができます。この問題を避けるには、PowerShell コンソールのウィンドウに PowerShell スクリプトモジュールの名前を直接入力してください（「Import-Module .\ExportPolicy.psd1」など）。
- エクスポートまたはインポートの実行時にアクセス権に関するエラーが発生した場合は、オブジェクトの読み取り権限（エクスポート時）または読み取りおよび作成権限（インポート）を持つ XenApp 管理者アカウントを使用していることを確認してください。また、PowerShell スクリプトを実行するための Windows 権限も必要です。
- エクスポートに失敗した場合は、XenApp 6.x ファームのヘルス状態が良好であることを確認してください。これを行うには、XenApp 6.x Controller のサーバー上で DSMAINT および DSCHECK コマンドを使用します。
- プレビューインポートを実行した後で実際のインポートを実行しても何もインポートされない場合は、インポートコマンドレットから-Preview パラメーターを削除したことを確認してください。

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やコンポーネントに置き換えられたか、アーキテクチャやプラットフォームの変更によって適用されなくなりました。

インポートされないコンピューターポリシー設定

- 接続のアクセス制御
- サーバーの CPU 最適化レベル
- DNS アドレス解決
- ファーム名
- アイコンの完全キャッシュ
- サーバーヘルス監視、サーバーヘルス監視テスト
- ライセンスサーバーのホスト名、ライセンスサーバーポート
- ユーザーセッションの制限、管理者アカウントの接続も制限する
- 負荷評価基準名
- ログオン数制限のログ
- ログオン制御できる最大サーバー数（%）

- メモリの最適化、メモリ最適化のアプリケーション除外一覧、メモリの最適化の間隔、メモリの最適化のスケジュール：月間、メモリの最適化のスケジュール：週間、メモリの最適化のスケジュール：時間
- オフラインアプリケーションへの再認証なしでの再接続、オフラインアプリケーションのログ、オフラインライセンスの有効期間、オフラインアプリケーションユーザー
- パスワードを要求する
- 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
- 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

FMA のプロパティ	値
CommandLineArguments	XenApp 6.x のコマンドライン引数で初期化されます。
IconFromClient	初期化されずにデフォルト値の false になります。
IconUid	XenApp 6.x アイコンデータで作成されたアイコンオブジェクトに初期化されます。
SecureCmdLineArgumentsEnabled	初期化されずにデフォルト値の true になります。
UserFilterEnabled	初期化されずにデフォルト値の false になります。
UUID	読み取り専用で Controller により割り当てられます。
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。
アカウント	アプリケーションのユーザーアカウントはデリバリーグループとアプリケーションのユーザー一覧に分類されます。指定ユーザーのアカウントはアプリケーションのユーザー一覧を初期化するために使用されます。さらに、ユーザーアカウントが属するドメインの Domain Users アカウントがデリバリーグループのユーザー一覧に追加されます。

以下の XenApp 6.x プロパティはインポートされません。

IMA のプロパティ	コメント
ApplicationType	無視されます。
HideWhenDisabled	無視されます。
AccessSessionConditions	デリバリーグループのアクセスポリシーに置き換えられます。
AccessSessionConditionsEnabled	デリバリーグループのアクセスポリシーに置き換えられます。
ConnectionsThroughAccessGatewayAllowed	デリバリーグループのアクセスポリシーに置き換えられます。
OtherConnectionsAllowed	デリバリーグループのアクセスポリシーに置き換えられます。
AlternateProfiles	FMA はストリーム配信アプリケーションをサポートしません。
OfflineAccessAllowed	FMA はストリーム配信アプリケーションをサポートしません。
ProfileLocation	FMA はストリーム配信アプリケーションをサポートしません。
ProfileProgramArguments	FMA はストリーム配信アプリケーションをサポートしません。
ProfileProgramName	FMA はストリーム配信アプリケーションをサポートしません。
RunAsLeastPrivilegedUser	FMA はストリーム配信アプリケーションをサポートしません。
AnonymousConnectionsAllowed	認証が不要なユーザー（匿名ユーザー）の接続は、FMA では別の方法でサポートされています。
ApplicationId、SequenceNumber	IMA 固有のデータです。
AudioType	FMA はクライアント接続の詳細オプションをサポートしません。
EncryptionLevel	SecureICA の有効/無効はデリバリーグループで設定します。
EncryptionRequired	SecureICA の有効/無効はデリバリーグループで設定します。
SslConnectionEnabled	FMA では別の方法で TLS が実装されています。
ContentAddress	FMA は公開コンテンツをサポートしません。

IMA のプロパティ	コメント
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。

セキュリティ

July 3, 2019

XenApp および XenDesktop では、セキュリティニーズに合わせて環境をカスタマイズできる、セキュアバイデザイン（セキュリティに配慮した設計）ソリューションが提供されます。

モバイルワーカーへの対応で IT 部門が直面するセキュリティ上の問題に、データの紛失や盗難があります。XenApp および XenDesktop では、アプリケーションとデスクトップがホストされ、すべてのデータがデータセンターに保持されるため、機密データや知的財産がエンドポイントデバイスから安全に分離されます。データ転送を許可するポリシーを有効にしている場合でも、すべてのデータが暗号化されます。

また、XenDesktop および XenApp のデータセンターでは、一元的な監視と管理サービスを利用できるため、インシデント対応が容易になります。Director では、ネットワーク経由でアクセスされたデータを監視して分析できま

す。また、Studio ではデータセンターにパッチを適用して多くの脆弱性を解決できるため、エンドユーザーデバイスごとにローカルで問題を解決する必要がありません。

XenApp および XenDesktop では、一元化された監査記録を使用して、どのアプリケーションやデータにどのユーザーがアクセスしたかを判別できるため、監査と法規制順守も簡素化されます。Director では、構成ログと OData API にアクセスして、システムに適用された更新とユーザーのデータ使用状況に関する履歴データが収集されます。

委任管理によって、管理者の役割を設定して、XenDesktop および XenApp へのアクセスを詳細に制御できます。これにより、ほかの管理者のアクセス権は制限したままで、特定の管理者に対してタスク、操作、およびスコープへの完全なアクセス権を組織内で柔軟に付与できます。

XenApp および XenDesktop では、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用してユーザーを制御できます。このポリシー制御によって、ユーザー、デバイス、またはユーザーやデバイスのグループが実行できる操作（接続、印刷、コピーと貼り付け、ローカルドライブのマップ）を指定できるため、社外作業者に対するセキュリティ上の問題を最小限に抑えることができます。Desktop Lock 機能を使用すると、エンドユーザーデバイスのローカルのオペレーティングシステムにアクセスできないようにして、エンドユーザーによる使用を仮想デスクトップのみに制限することも可能です。

管理者は、Controller で、またはエンドユーザーと VDA（Virtual Delivery Agent）間で TLS（Transport Layer Security）プロトコルが使用されるように構成して、XenApp または XenDesktop のセキュリティを強化できます。このプロトコルを有効にして、TCP/IP 接続に対してサーバー認証、データストリームの暗号化、およびメッセージの整合性チェックが行われるようにすることもできます。

さらに、XenApp および XenDesktop では、Windows や特定のアプリケーションでの複数要素認証がサポートされています。複数要素認証を使用して、XenApp および XenDesktop で配信されるすべてのリソースを管理することもできます。以下の認証方法を使用できます：

- トークン
- スマートカード
- RADIUS
- kerberos
- 生体認証

XenDesktop は、ID 管理からウイルス対策ソフトウェアまで、さまざまなサードパーティセキュリティソリューションを統合できます。サポートされている製品の一覧については、https://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、https://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

August 24, 2021

> 注:
>
> 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。セキュリティ標準と Citrix 製品に関する最新情報については、「https://www.citrix.com/security/」を参考にしてください。

セキュリティに関する推奨事項

セキュリティパッチを適用して、環境内にあるすべてのマシンを最新の状態にします。この製品の利点の 1 つは、シンクライアントをターミナルとして使用することによってこの作業を簡略化できることです。

環境内にあるすべてのマシンを、アンチウイルスソフトウェアで保護します。

Windows マシン向けの 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ブ境界を含む）で保護します。

従来の環境を新しいバージョンに移行する場合は、既存の境界ファイアウォールを移動するか、新しい境界ファイアウォールを追加する必要があります。たとえば、従来のクライアントとデータセンター内のデータベースサーバーとの間に境界ファイアウォールがあるとします。このリリースを使用するときは、仮想デスクトップおよびユーザーデバイスと、データセンター内のデータベースサーバーおよび Delivery Controller との間に境界ファイアウォールを設定する必要があります。したがって、データベースサーバーと Controller を含むエンクレーブをデータセンター内に作成することを検討します。また、ユーザーデバイスと仮想デスクトップ間のセキュリティについても考慮する必要があります。

環境内にあるすべてのマシンは、パーソナルファイアウォールで保護する必要があります。コアコンポーネントと VDA をインストールするときに Windows Firewall サービスが検出された場合は（ファイアウォールが無効であったとしても）、コンポーネントと機能の通信に必要なポートが自動的に開放されるように設定できます。また、それらのファイアウォールポートを手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、Citrix ではこれらの 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（https://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。

> 注:
>
> Citrix SecureICA は、ICA/HDX プロトコルの一部ですが、Transport Layer Security（TLS）のような標準に準拠したネットワークセキュリティプロトコルではありません。TLS を使用して、ユーザーデバイスとデスクトップ間のネットワーク通信を保護することもできます。TLS を構成する方法については、「Transport Layer Security（TLS）」を参照してください。

Windows ベストプラクティスをアカウント管理に適用します。Machine Creation Services または Provisioning Services によって複製される前に、アカウントをテンプレートやイメージに作成しないでください。保存された、権限が付与されているドメインアカウントを使用して、タスクをスケジュールしないでください。共有 Active Directory マシンアカウントを手動で作成しないでください。こうすることにより、ローカルの永続アカウントのパスワードがマシンへの攻撃によって取得され、他者所有の MCS/PVS 共有イメージへのログオンに使用されるのを阻止することができます。

アプリケーションのセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐために、VDA ホストとローカル Windows クライアントで、インストーラー、アプリケーション、実行可能ファイル、スクリプトに対して Windows AppLocker の規則を構成することをお勧めします。

ユーザー権限の管理

ユーザーには、必要な権限だけを付与します。デスクトップのユーザーには、Microsoft Windows での権限（グループポリシーの［ユーザー権利の割り当て］およびグループメンバーシップ）がそのまま適用されます。このリリースの利点の 1 つは、仮想デスクトップが格納されているコンピューターに対する物理的な制御を許可せずに、デスクトップに対するユーザーの管理権限を付与できることです。

デスクトップに対する管理権限を計画するときは、以下の点に注意してください。

- デフォルトでは、権限を持たないユーザーがデスクトップに接続すると、ユーザーデバイスのタイムゾーンではなく、そのデスクトップを実行しているシステムのタイムゾーンが表示されます。デスクトップの使用時にローカルの時刻が表示されるようにする方法については、「基本設定の変更」を参照してください。
- デスクトップの管理者権限を持つユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールデスクトップの場合、管理者権限を持つユーザーはそのデスクトップのすべてのユーザー（将来のユーザーを含む）に信頼されている必要があります。このため、プールデスクトップのすべてのユーザーは、この状況によってデータのセキュリティに永続的な危険性が存在することを認識する必要があります。これは、1 人のユーザーに対してのみ割り当てられるデスクトップには当てはまりません。つまり、このユーザーはほかのデスクトップの管理者になることはできません。

- 通常、デスクトップの管理者であるユーザーはそのデスクトップにソフトウェアをインストールできます。インストールできるソフトウェアには悪意のあるものも含まれます。またユーザーが、そのデスクトップに接続しているすべてのネットワーク上のトラフィックを監視または制御することも可能です。

一部のアプリケーションでは、管理者ではなくユーザー向けであってもデスクトップ権限が必要です。こうしたユーザーはセキュリティリスクを認識していない可能性があります。

これらのアプリケーションは、たとえデータに機密性がない場合でも、機密性の高いアプリケーションとして扱います。セキュリティリスクを軽減するために、以下のアプローチを検討してください。

- 二要素認証を適用し、すべてのアプリケーションのシングルサインオンメカニズムを無効にする
- コンテキストアクセスポリシーを適用する
- 専用のデスクトップにアプリケーションを公開する。ホストされた共有デスクトップにアプリケーションを公開する必要がある場合は、その共有デスクトップに他のアプリケーションを公開しない
- デスクトップ権限がそのデスクトップにのみ適用され、他のコンピューターには適用されないようにする
- アプリケーションのセッションの録画を有効にする。また、アプリケーション内および Windows 内の他のセキュリティ記録機能も有効にする
- XenApp および XenDesktop を構成して、アプリケーションで使用される機能（クリップボード、プリンター、クライアントドライブ、USB リダイレクトなど）を制限する
- アプリケーションのセキュリティ機能を有効にする。厳密にユーザーの要件のみに一致するように制限する
- Windows のセキュリティ機能を厳密にユーザーの要件に合わせて構成する。これは単一のアプリケーションだけがデスクトップに公開されている場合、より簡単な構成を意味する。例：制限のある AppLocker 構成の使用。ファイルシステムへのアクセスを制御する
- 将来のデスクトップ権限が不要になるように、アプリケーションの再構成、アップグレード、または置き換えを計画する

これらのアプローチは、デスクトップ権限を必要とするアプリケーションからすべてのセキュリティリスクを排除するわけではありません。

ログオン権限の管理

ユーザーアカウントとコンピューターアカウントの両方にログオン権限が必要です。Microsoft Windows の権限では、ログオン権限は引き続き、［ユーザー権限の割り当て］で権限を設定し［グループポリシー］でグループメンバーシップを設定するという通常の方法で、デスクトップに適用されます。

Windows のログオン権限には次の種類があります。ローカルログオン、リモートデスクトップサービスを使ったログオン、ネットワーク経由でのログオン（ネットワーク経由でコンピューターへアクセス）、バッチジョブとしてログオン、サービスとしてログオン。

コンピューターアカウントでは、必要なログオン権限だけをコンピューターに付与します。次のアカウントに、ログオン権限「ネットワーク経由でコンピューターへアクセス」が必要です。

- VDA で、Delivery Controller のコンピューターアカウント

- Delivery Controller で、VDA のコンピューターアカウント。「Active Directory OU ベースの Controller 検出」を参照してください。
- StoreFront サーバーで、同じ StoreFront サーバーグループ内の他のサーバーのコンピューターアカウント

ユーザーアカウントでは、必要なログオン権限だけをユーザーに付与します。

Microsoft によると、デフォルトで Remote Desktop Users グループに［リモートデスクトップサービスを使ったログオンを許可］でログオン権限が付与されています（ドメインコントローラを除く）。

組織のセキュリティポリシーによっては、このグループがこのログオン権限から除外されることを明示的に設定している場合もあります。次の方法を検討してください。

- Virtual Delivery Agent（VDA）for Server OS は Microsoft リモートデスクトップサービスを使用します。Remote Desktop Users グループを制限されたグループとして構成し、Active Directory グループポリシー経由でグループのメンバーシップを制御できます。詳しくは、Microsoft 社のドキュメントを参照してください。
- VDA for Desktop OS を含む XenApp および XenDesktop の他のコンポーネントでは、Remote Desktop Users グループは必要ありません。このため、これらのコンポーネントでは Remote Desktop Users グループにログオン権限［リモートデスクトップサービスを使ったログオンを許可］の必要はなく、削除できます。さらに、以下を確認します。
  - リモートデスクトップサービスでこれらのコンピューターを管理する場合、すべての必要な管理者が既に Administrators グループのメンバーであることを確認してください。
  - リモートデスクトップサービスでこれらのコンピューターを管理しない場合、コンピューター上でリモートデスクトップサービスを無効にすることを検討してください。

ユーザーとグループをログオン権限［リモートデスクトップサービスによるログオンを拒否］に追加することは可能ですが、ログオン権限の拒否の使用は、通常推奨されません。詳しくは、Microsoft 社のドキュメントを参照してください。

ユーザー権利の構成

Delivery Controller をインストールすると、次の Windows サービスが作成されます。

- Citrix AD Identity Service（NT SERVICE\CitrixADIdentityService）：仮想マシンの Microsoft Active Directory コンピューターアカウントを管理します。
- Citrix Analytics（NT SERVICE\CitrixAnalytics）：Citrix が使用するサイト構成の使用状況情報の収集がサイト管理者によって承認されている場合、この情報を収集します。その後、製品の改善に役立てるために、この情報を Citrix に送信します。
- Citrix App Library（NT SERVICE\CitrixAppLibrary）：AppDisk の管理とプロビジョニング、AppDNA 統合、および App-V の管理をサポートします。
- Citrix Broker Service（NT SERVICE\CitrixBrokerService）：ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。
- Citrix Configuration Logging Service（NT SERVICE\CitrixConfigurationLogging）：すべての構成の変更と、管理者がサイトに対して行ったそのほかの状態の変更を記録します。

- Citrix Configuration Service（NT SERVICE\CitrixConfigurationService）：共有される構成のサイト全体のリポジトリです。
- Citrix Delegated Administration Service（NT SERVICE\CitrixDelegatedAdmin）：管理者に与えられた権限を管理します。
- Citrix Environment Test Service（NT SERVICE\CitrixEnvTest）：そのほかの Delivery Controller サービスのセルフテストを管理します。
- Citrix Host Service（NT SERVICE\CitrixHostService）：XenApp または XenDesktop 環境で使用されているハイパーバイザーインフラストラクチャに関する情報を保存します。また、コンソールで使用される、ハイパーバイザープールのリソース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）。
- Citrix Configuration Logging Service（NT SERVICE\CitrixConfigSyncService）：メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service（NT SERVICE\CitrixHighAvailabilityService）：メインサイトデータベースが使用できない場合に、ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これらは、そのほかの Citrix コンポーネントをインストールしたときにも作成されます。

- Citrix Diagnostic Facility COM Server（NT SERVICE\CdfSvc）：Citrix サポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service（NT SERVICE\CitrixTelemetryService）：Citrix が分析するための診断情報を収集することで、管理者が分析結果と推奨事項を確認してサイトの問題解決に役立てることができるようにします。

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これは現在使用されていません。有効だった場合、無効にしてください。

- Citrix Remote Broker Provider（NT SERVICE\XaXdCloudProxy）

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーションサービス（NT SERVICE\CitrixOrchestration）
- Citrix 信頼サービス（NT SERVICE\CitrixTrust）

Citrix Storefront Privileged Administration Service を除く、これらのサービスには、[サービスとしてログオ

ン］のログオン権限と［プロセスのメモリクォータの増加］、［セキュリティ監査の生成］、［プロセスレベルトークンの置き換え］の権限が付与されます。通常、これらのユーザー権利を変更する必要はありません。これらの権限は Delivery Controller では使用されないため、自動的に無効にされています。

サービス設定の構成

Citrix Storefront Privileged Administration Service と Citrix Telemetry Service を除く、上述の「ユーザー権利の構成」セクションに示す Delivery Controller Windows サービスは、ネットワークサービス ID でログオンするように構成されます。このサービス設定は変更しないでください。

Citrix Storefront Privileged Administration Service は、ローカルシステム（NT AUTHORITY\SYSTEM）にログオンするように構成されます。これは、通常はサービスで実行できない Delivery Controller StoreFront 操作（Microsoft IIS サイトの作成など）に必要な構成です。このサービス設定は変更しないでください。

Citrix Telemetry Service は、このサービス自体のサービス固有の ID でログオンするように構成されます。

Citrix Telemetry Service は、無効にすることができます。このサービスと、既に無効にされているサービス以外のそのほかの Delivery Controller Windows サービスは、無効にしないでください。

レジストリ設定の構成

VDA ファイルシステムで 8.3 ファイル名およびフォルダーの作成を有効にする必要はなくなりました。レジストリキー **NtfsDisable8dot3NameCreation** は、8.3 ファイル名およびフォルダーの作成が無効になるように構成できます。これは、「**fsutil.exe behavior set disable8dot3**」コマンドを使用しても構成できます。

展開シナリオのセキュリティ

ユーザー環境は、組織に管理されずにユーザーにより完全に制御されるユーザーデバイス、または組織により管理されたユーザーデバイスで構成できます。通常、これら 2 つの環境に対するセキュリティ上の考慮事項は異なります。

管理されるユーザーデバイス

「管理されるユーザーデバイス」とは、管理者または信頼されたほかの組織によって管理されるユーザーデバイスを指します。この場合、ユーザーデバイスを管理者が構成してユーザーに直接提供したり、全画面のみを実行するモードで単一のデスクトップを実行する端末を提供したりできます。管理されるユーザーデバイスに対しては、前述の一般的なセキュリティ構成を実装します。この製品の長所は、ユーザーデバイス上に最低限のソフトウェアしか必要としないという点です。

管理されるユーザーデバイスでは、仮想デスクトップの実行モードとして、全画面のみを実行するモードまたはウィンドウモードを構成できます。

- 全画面のみを実行するモード：ユーザーは通常の［Windows へのログオン］画面からユーザーデバイスにログオンします。すると、同じユーザー資格情報で自動的にこのリリースへのログオンが実行されます。

- 一方、ウィンドウモードを使用する場合、ユーザーは最初にユーザーデバイスにログオンし、次にこのリリースで提供された Web サイトを介してこの製品にログオンします。

管理されていないユーザーデバイス

「管理されていないユーザーデバイス」とは、管理者または信頼された組織によって管理されていないユーザーデバイスを指します。たとえば、ユーザーが自分のデバイスを使用する場合、上記のセキュリティ上の推奨事項にユーザーが従わないことがあります。このリリースでは、このような管理されていないユーザーデバイスにも、デスクトップを安全に配信できます。ただし、これらのユーザーデバイスでも、キーロガーやそれに類似した入力攻撃を阻止するための基本的なウイルス対策が施されている必要があります。

データストレージの考慮事項

このリリースを使用しているときに、ユーザーが自分のユーザーデバイスにデータを保存できないように構成できます。ただし、ユーザーが仮想デスクトップにデータを保存することを許可するかどうかも考慮する必要があります。ユーザーによるデスクトップ上へのデータ保存は推奨されません。データはファイルサーバー、データベースサーバー、またはデータが適切に保護されるそのほかのリポジトリに保存する必要があります。

デスクトップ環境は、プールデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールデスクトップなど、複数のユーザーで共有されるデスクトップ上にデータを保存するべきではありません。また、専用デスクトップでも、そのデスクトップをほかのユーザーが使用することになった場合に、保存されているデータを削除する必要があります。

バージョン混在環境

アップグレード処理のある時点においては、バージョンが混在する環境は不可避なものです。ベストプラクティスに従い、異なるバージョンの Citrix コンポーネントが同時に存在する時間を最短化させます。たとえばバージョン混在環境ではセキュリティポリシーが一律には適用されない可能性があります。

注：これは、ほかのソフトウェア製品では一般的な問題です。Active Directory の以前のバージョンを使用すると、最近のバージョンの Windows にはグループポリシーが部分的にしか適用されません。

次のシナリオでは、特定のバージョン混在 Citrix 環境で発生する可能性があるセキュリティ問題について説明します。XenApp および XenDesktop 7.6 Feature Pack 2 の Virtual Delivery Agent を実行している仮想デスクトップへの接続に Citrix Receiver 1.7 が使用されている場合、ポリシー設定 ［デスクトップとクライアント間におけるファイル転送の許可］はサイトでは有効ですが、XenApp および XenDesktop 7.1 を実行している Delivery Controller によっては無効にできません。製品のより新しいバージョンでリリースされたポリシーの設定は認識されません。このポリシーにより、ユーザーはファイルを自分の仮想デスクトップにアップロードしてダウンロードできます – セキュリティ問題。この問題を回避するには、Delivery Controller あるいは Studio のスタンドアロンインスタンスをバージョン 7.6 Feature Pack 2 にアップグレードし、その後でグループポリシーを使ってポリシーを無効にします。または、すべての該当する仮想デスクトップでローカルポリシーを使用します。

リモート **PC** アクセスのセキュリティに関する考慮事項

リモート PC アクセスでは、次のセキュリティ機能がサポートされます。

- スマートカードの使用がサポートされます。
- リモートセッションの間、社内の PC のモニターは非表示になります。
- リモート PC アクセスでは、すべてのキーボードおよびマウスの入力がリモートセッションにリダイレクトされます（Ctrl+Alt+Del キー入力、および USB 対応スマートカードや生体認証デバイスを除く）。
- SmoothRoaming は 1 人の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、シトリックス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 1 人の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

Name: AllowMultipleRemotePCAssignments

Type: REG\_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
   multiple user assignment.
```

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。

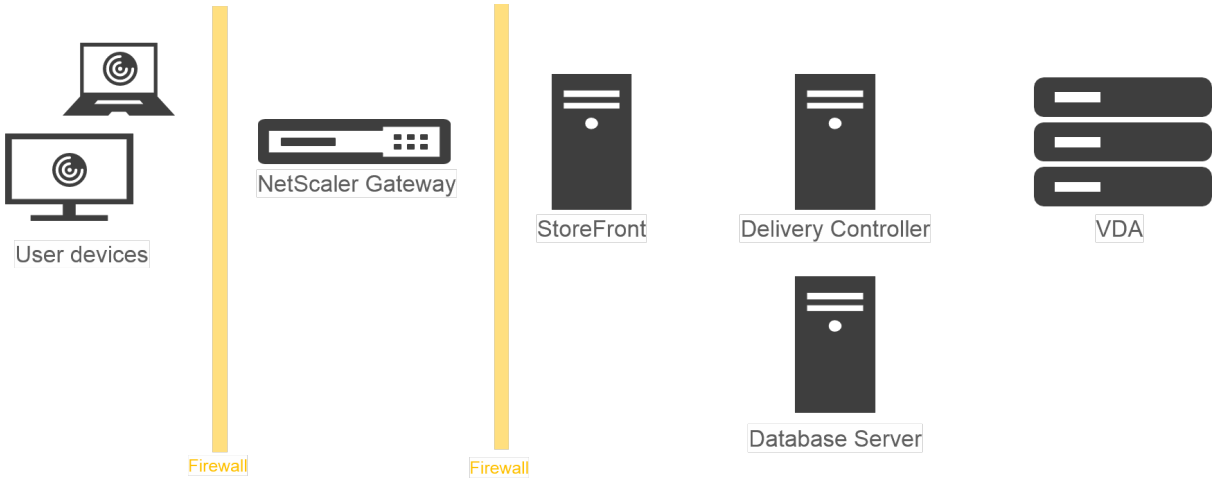
XenApp および XenDesktop の NetScaler Gateway との統合

August 28, 2019

公開リソースおよびデータへのアクセスを管理するには、StoreFront サーバーを展開および構成します。リモートアクセスの場合は、NetScaler Gateway を StoreFront の前に追加することをお勧めします。

> 注:
>
> XenApp および XenDesktop を NetScaler Gateway と統合する構成手順については、StoreFront のドキュメントを参照してください。

次の図は、NetScaler Gateway を含む簡略化された Citrix の展開例を示しています。NetScaler Gateway は StoreFront と通信して、XenApp および XenDesktop が配信するアプリやデータを保護します。ユーザーデバイスは Citrix Receiver を実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。



ユーザーは、NetScaler Gateway を使用してログオンおよび認証を行います。NetScaler Gateway は、DMZ で展開およびセキュリティ保護されます。2 要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します(図には表示されていません)。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

委任管理

August 24, 2021

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	すべてのタスクおよび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	全体的な情報および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、そのセッションや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。

役割	権限
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
ドメイン/fred	すべての管理権限を実行できる管理者	すべて（[すべての管理権限を実行できる管理者］の役割は、常に［すべて］スコープとペアになります）
ドメイン/rob	読み取り専用管理者	すべて
ドメイン/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業担当者
ドメイン/warehouseadmin	ヘルプデスク管理者	倉庫
ドメイン/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fred は「すべての管理権限を実行できる管理者」で、システム内のすべてのオブジェクトを表示、編集、および削除できます。
- Rob はサイト内のすべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidi はすべてのオブジェクトを表示でき、［営業］スコープのデリバリーグループでヘルプデスクタスクを実行できます。これにより、［営業］スコープのデリバリーグループに割り当てられているセッションとマシンを管理できます。ただし、これらのデリバリーグループに（マシンの追加や削除などの）変更を加えることはできません。
- Active Directory セキュリティグループ warehouseadmin のすべてのメンバーは、［倉庫］スコープのマシンに対するヘルプデスクタスクを表示および実行できます。
- Peter は Windows 7 の専門家で、すべての Windows 7 マシンカタログを管理でき、所属している部署のスコープに関係なく Windows 7 アプリケーション、デスクトップ、およびマシンを配信できます。当初、管理者は Peter を［Win7］スコープの「すべての管理権限を実行できる管理者」にしようとしましたが、考え直しました。これは、「すべての管理権限を実行できる管理者」には、そのスコープに含まれていないオブジェクト（「サイト」や「管理者」など）に対する全権限が付与されるためです。

委任管理の使用方法

一般的に、管理者数およびその権限の細分性は展開のサイズおよびその複雑度に応じて異なります。

- 小規模または検証用の展開サイトでは、1 人または少数の管理者ですべてを管理し、委任管理者は存在しません。この場合、組み込みの［すべての管理権限を実行できる管理者］役割（および［すべて］スコープ）の管理者を作成します。
- より多くのマシン、アプリケーション、およびデスクトップがあるサイトでは、委任管理者の配置が必要になります。何人かの管理者に、より専門的な管理責任（役割）を付与できます。たとえば、2 人の「すべての管理権限を実行できる管理者」を設定して、残りをヘルプデスク管理者にします。さらに、マシンカタログなど、特定グループ（スコープ）のオブジェクトの管理を 1 人の管理者に委任することもできます。この場合、新しいスコープを作成して、組み込みの役割とそのスコープをペアにした管理者を作成します。

- 大規模サイトにおいても、より多くの（またはより詳細な）スコープと、特殊な役割を持つさまざまな管理者が必要になることがあります。この場合は、追加のスコープを作成または編集して、カスタムの役割を作成し、組み込みまたはカスタムの役割と既存または新しいスコープを持つ各管理者を作成します。

新しいスコープは、管理者を作成するときに作成できます。また、マシンカタログやホスト接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカルの管理者アカウントを使用してサイトを作成するときは、すべてのオブジェクトに対する完全な管理権限を持つ管理者としてそのアカウントが設定されます。ただし、サイトを作成した後では、ローカル管理者には特別な特権は与えられません。

すべての管理タスクの実行権限を持つ管理者には、常に［すべて］のスコープが割り当てられます。これを変更することはできません。

デフォルトでは、管理者は有効になります。新しい管理者を作成するときに、その管理者が実際に作業を始めるまで管理者を無効にしておく必要が生じる場合があります。また、オブジェクトやスコープを再構成するときに、既存の管理者を一時的に無効にすることもできます。完全な管理権限を持つ管理者が 1 人しかいない環境では、その管理者を無効にすることはできません。管理者の有効/無効は、管理者を作成、コピー、または編集するときの［管理者を有効にする］チェックボックスで設定できます。

管理者を編集したりコピーしたりするときのダイアログボックスでスコープ/役割ペアを削除すると、その管理者とスコープ/役割ペアとの関連付けが削除され、個々のスコープや役割は削除されません。また、同じスコープ/役割ペアが割り当てられている管理者がいる場合でも、その関連付けは削除されません。

管理者を管理するには、
Studio
のナビゲーションペインで［構成］>［ 管理者］の順にクリックし、中央ペインの上部の［管理者］タブをクリックします。

- 管理者を作成するには、［操作］ペインの［管理者の作成］をクリックします。ユーザーアカウント名を入力するか参照し、スコープを選択または作成して、役割を選択します。新しい管理者はデフォルトで有効になりますが、無効にすることもできます。
- 管理者をコピーするには、中央ペインで管理者を選択し、［操作］ペインの［管理者のコピー］をクリックします。ユーザーアカウント名を入力するか参照します。必要に応じて、スコープ/役割ペアを編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になりますが、無効にすることもできます。
- 管理者を編集するには、中央ペインで管理者を選択し、［操作］ペインの［管理者の編集］をクリックします。必要に応じて、スコープ/役割ペアを編集または削除したり、新しいペアを追加したりできます。
- 管理者を削除するには、中央ペインで管理者を選択し、［操作］ペインの［管理者の削除］をクリックします。完全な管理権限を持つ管理者が 1 人しかいない環境では、その管理者を削除することはできません。

役割の作成と管理

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ます。

スコープには、64 文字までの Unicode 文字で名前を付けることができます。ただし、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らないかどうかを確認してください。

スコープを管理するには、Studio のナビゲーションペインで［構成］>［管理者］の順にクリックし、中央ペインの上部の［スコープ］タブをクリックします。

- スコープを作成するには、［操作］ペインの［スコープの作成］をクリックします。名前と説明を入力します。オブジェクトの種類（[デリバリーグループ］チェックボックスなど）を選択すると、その種類のすべてのオブジェクトがスコープに追加されます。特定のオブジェクトを追加するには、オブジェクトの種類を開き、個々のオブジェクトを選択します（営業部で使用される特定のデリバリーグループを選択する場合など)。
- スコープをコピーするには、中央ペインでスコープを選択し、［操作］ペインの［スコープのコピー］をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- スコープを編集するには、中央ペインでスコープを選択し、［操作］ペインの［スコープの編集］をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- スコープを削除するには、中央ペインでスコープを選択し、［操作］ペインの［スコープの削除］をクリックします。確認のメッセージが表示されたら、［削除］をクリックします。

レポートの作成

次の 2 種類の委任管理レポートを作成できます。

- 管理者に関連付けられているスコープ/役割ペアと各種類のオブジェクト（デリバリーグループ、マシンカタログなど）に対する個々の権限の一覧についての HTML レポート。Studio で生成できます。

  このレポートを作成するには、ナビゲーションペインで［構成］>［管理者］の順に選択します。中央ペインで管理者を選択し、操作ペインで［レポートの作成］をクリックします。

  このレポートは、管理者の作成、コピー、および編集時に作成することもできます。

- 組み込みおよびカスタムの役割とそれらに関連付けられた権限を一覧表示する HTML または CSV レポート。このレポートは、PowerShell スクリプト OutputPermissionMapping.ps1 を実行して生成します。

  このスクリプトを実行するには、すべての管理権限を実行できる管理者、読み取り専用管理者、または役割の読み取り権限を持つ管理者である必要があります。このスクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\にインストールされています。

  構文:

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

パラメーター	説明
-Help	スクリプトのヘルプを表示します。
-Csv	CSV レポートを作成します。デフォルト値：HTML
-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 ブラウザーなど）で表示されます。
<CommonParameters>	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 ブラウザーで表示されます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  - Show
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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


スマートカード

August 24, 2021

スマートカードおよび同等のテクノロジは、このアーティクルに記載されているガイドライン内でサポートされています。XenApp または XenDesktop でスマートカードを使用するには、以下を行う必要があります:

- 所属する組織における、スマートカードの使用に関するセキュリティポリシーを理解します。たとえば、スマートカードがどのように発行され、ユーザーがそれをどのように保護するかについてこれらのポリシーで規定してあることがあります。XenApp および XenDesktop の環境では、これらのポリシーの一部の変更が必要になる場合があります。
- どのユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションがスマートカードとともに使用されるかを決定します。
- スマートカードテクノロジ全般および選択したスマートカードベンダーのハードウェアとソフトウェアについて理解します。
- 分散環境でのデジタル証明書の展開管理方法について理解します。

スマートカードの種類

エンタープライズ向けとコンシューマー向けのスマートカードは、寸法も電気コネクタも同じで、同じスマートカードリーダーを使用できます。

エンタープライズ向けのスマートカードにはデジタル証明書が含まれています。これらのスマートカードは Windows ログオンをサポートしていて、ドキュメントや電子メールのデジタル署名と暗号化のためのアプリケーションと連携して使用できます。XenApp および XenDesktop は、これらの用途をサポートしています。

コンシューマー向けのスマートカードにはデジタル証明書は含まれていませんが、共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名、チップと PIN クレジットカードなど）をサポートできます。これらのスマートカードは、Windows ログインや一般的な Windows アプリケーションをサポートしていません。これらのスマートカードと合わせて使用するには、特別な Windows アプリケーションと、適切なソフトウェアインフラストラクチャ（支払いカードネットワークへの接続など）が必要です。XenApp または XenDesktop でのこのような特別なアプリケーションのサポートについて詳しくは、Citrix 担当者にお問い合わせください。

エンタープライズ向けスマートカードには、互換性のある同等のものが存在し、類似した方法で使用できます。

- スマートカードと同等の USB トークンは USB ポートに直接接続します。これらの USB トークンは通常 USB フラッシュドライブのサイズですが、携帯電話で使用される SIM カードと同じくらい小さいものもあります。それらは、スマートカードと USB スマートカードリーダーの組み合わせとして表示されます。
- Windows トラステッドプラットフォームモジュール（TPM：Trusted Platform Module）を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Receiver 4.3 以上を使用して、Windows 8 および Windows 10 でサポートされます。
  - XenApp および XenDesktop の 7.6 FP3 よりも前のバージョンは、仮想スマートカードをサポートしていません。

- 仮想スマートカードについて詳しくは、「Virtual Smart Card Overview」を参照してください。

注:「仮想スマートカード」という用語は、単にユーザーコンピューターに保存されたデジタル証明書についても使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

XenApp および XenDesktop のスマートカードのサポートは、Microsoft の PC/SC（Personal Computer/Smart Card）標準仕様に基づいています。スマートカードおよびスマートカードデバイスは、使用する Windows オペレーティングシステムでサポートされており、Microsoft WHQL（Windows Hardware Quality Lab）により承認されている必要があります。PC/SC に準拠しているハードウェアについては、Microsoft 社のドキュメントを参照してください。その他のタイプのユーザーデバイスは、PS/SC 標準に準拠していることがあります。詳しくは、Citrix Ready プログラム（https://www.citrix.com/ready/）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をユーザーデバイスと Virtual Delivery Agent（VDA）の両方にインストールする必要があります。多くの場合、デバイスドライバーは Citrix パートナーから入手可能なスマートカードミドルウェアパッケージの一部として提供されます。スマートカードミドルウェアパッケージにより、高度な機能が提供されます。デバイスドライバーは、暗号化サービスプロバイダー（CSP：Cryptographic Service Provider）、キーストレージプロバイダー（KSP：Key Storage Provider）、ミニドライバーとして説明されることもあります。

Windows システムでは、以下のスマートカードとミドルウェアでの Citrix 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、https://www.citrix.com/readyを参照してください。

ミドルウェア	スマートカード
ActivClient 7.0（DoD モード有効）	DoD CAC カード
PIV モードの ActivClient 7.0	NIST PIV カード
Microsoft ミニドライバー	NIST PIV カード
GemAlto Mini Driver for .NET カード	GemAlto .NET v2+
Microsoft ネイティブドライバー	仮想スマートカード（TPM）

他の種類のデバイスでのスマートカード使用法について詳しくは、そのデバイスに関する Citrix Receiver のドキュメントを参照してください。

他の種類のデバイスでのスマートカード使用法について詳しくは、そのデバイスに関する Citrix Receiver のドキュメントを参照してください。

リモート **PC** アクセス

オフィスで動作する、物理的な Window 10、Windows 8、または Windows 7 マシンにリモートアクセスする場合は、スマートカードがサポートされます。Windows XP マシンへのリモートアクセスでは、スマートカードはサポートされません。

以下のスマートカードが、リモート PC アクセス機能でテストされています。

ミドルウェア	スマートカード
Gemalto .NET ミニドライバー	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoft ミニドライバー	NIST PIV
Microsoft ネイティブドライバー	仮想スマートカード

スマートカードリーダーの種類

スマートカードリーダーはユーザーデバイス内に作成されることもありますし、別にユーザーデバイスに（通常は USB または Bluetooth で）接続することもあります。USB Chip/Smart Card Interface Devices（CCID）仕様に準拠する接触カードリーダーがサポートされます。これらのカードリーダーでは、ユーザーがスマートカードをスロットに挿入したりスワイプしたりします。Deutsche Kreditwirtschaft（DK）標準は、接触カードリーダーの 4 つのクラスを定義しています。

- Class 1 スマートカードリーダーは最も一般的で、通常 1 つのみのスロットを備えています。Class 1 スマートカードリーダーは通常、オペレーティングシステム付属の標準 CCID デバイスドライバーでサポートされます。
- Class 2 スマートカードリーダーには、ユーザーデバイスがアクセスできない安全なキーパッドも含まれています。Class 2 スマートカードリーダーは、内蔵の安全なキーパッドがあるキーボードに搭載される場合があります。Class 2 スマートカードリーダーについては、Citrix の担当者に連絡してください。安全なキーパッドの機能を有効化するには、リーダー固有のデバイスドライバーが必要になる場合があります。
- Class 3 スマートカードリーダーには、安全なディスプレイも含まれます。Class 3 スマートカードリーダーはサポートされません。
- Class 4 スマートカードリーダーには、安全なトランザクションモジュールも含まれます。Class 4 スマートカードリーダーはサポートされません。

注：スマートカードリーダーのクラスは、USB デバイスのクラスには無関係です。

スマートカードリーダーは、対応するデバイスドライバーとともにユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用している Citrix Receiver のマニュアルを参照してく

ださい。サポートされているバージョンは、通常、Citrix Receiver のドキュメントでスマートカードの記事でまたはシステム要件に関する記事に掲載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、デフォルトで有効な特定の ICA/HDX スマートカード仮想チャネルを使用して、XenApp および XenDesktop に統合されています。

重要：スマートカードリーダーでは汎用 USB リダイレクト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、https://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。

> 重要
>
> XenApp または XenDesktop セッションでは、Microsoft リモートデスクトップ接続アプリケーションでのスマートカードの使用はサポートされません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前の確認事項

- スマートカードリーダーのデバイスドライバーを入手して、ユーザーデバイスにインストールする必要があります。Microsoft により提供される CCID デバイスドライバーは、多くのスマートカードリーダーで使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手して、ユーザーデバイスと仮想デスクトップの両方にインストールします。このドライバーと CSP ソフトウェアは、XenApp や XenDesktop と互換性がある必要があります。詳しくは、ベンダーのドキュメントを参照してください。ミニドライバーモデルのスマートカードを使用する仮想デスクトップでは、スマートカードミニドライバーが自動的にダウンロードされます。また、https://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

August 24, 2021

この製品バージョンおよびこのバージョンと以前のバージョンとの混在環境では、以下の種類のスマートカード展開がサポートされます。そのほかの構成でも使用できる場合がありますが、サポートの対象外です。

種類	**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	何もしない。
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。

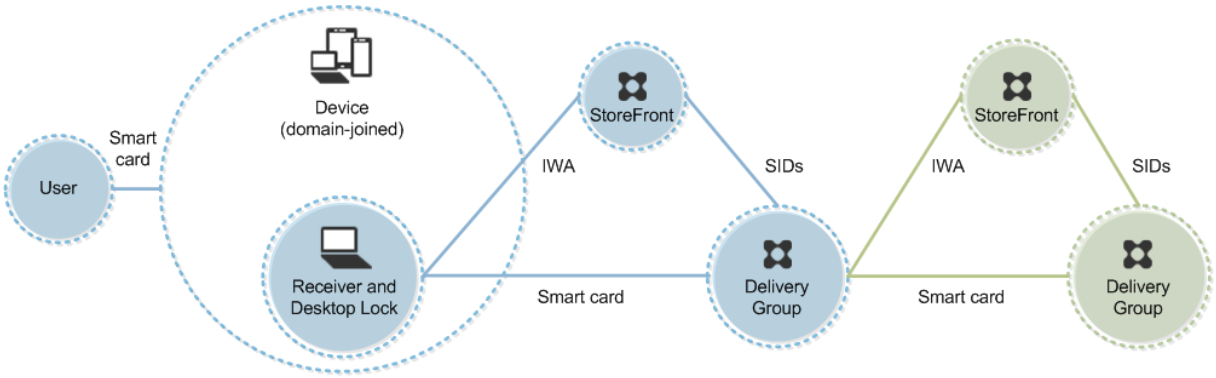
ポリシー設定	デスクトップの動作
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

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上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。

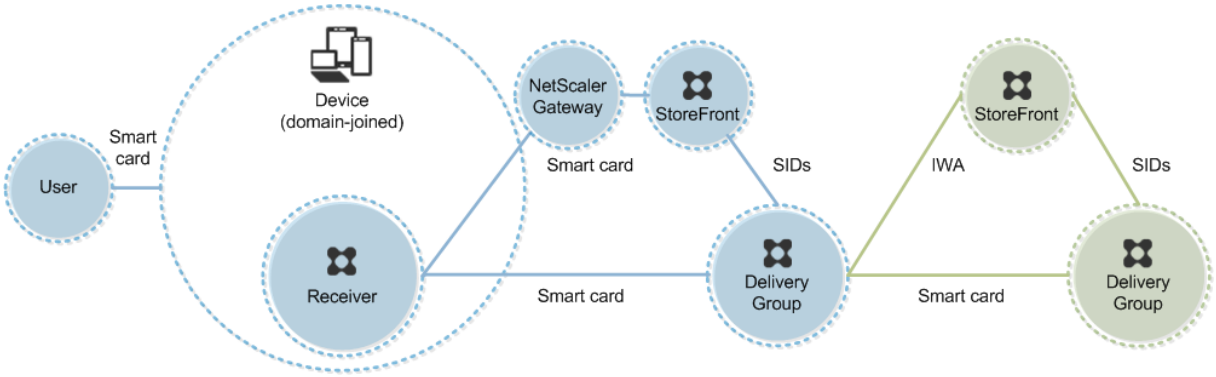


ユーザーは、スマートカードと PIN を使ってデバイスにログオンします。Receiver は、StoreFront サーバーにアクセスするユーザーを統合 Windows 認証（IWA）で認証します。StoreFront により、ユーザーのセキュリティ識別子（SID）が XenApp または XenDesktop に渡されます。Receiver でシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要はありません。

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。



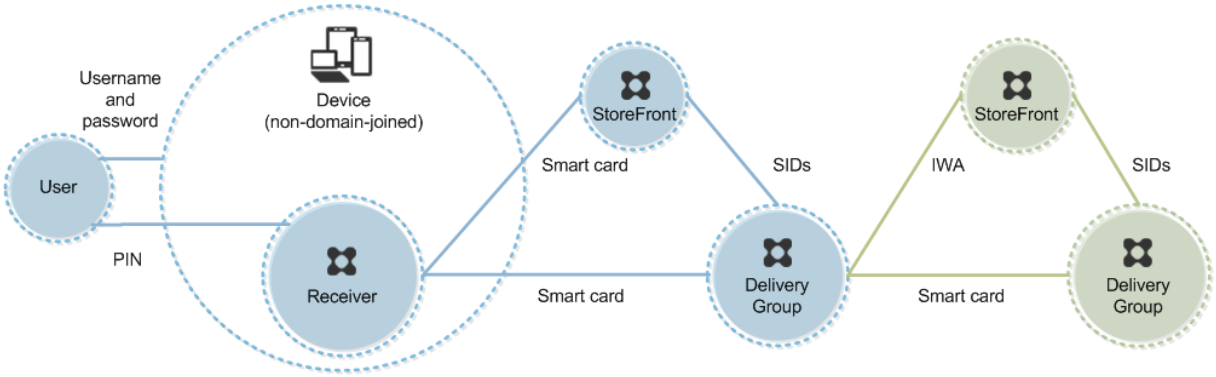
ユーザーはスマートカードと PIN を使ってデバイスにログオンし、次に NetScaler Gateway/Access Gateway にもう一度ログオンします。この展開では Receiver で 2 モード認証を使用できるため、この 2 つ目のログオンではスマートカードと PIN を使用したりユーザー名とパスワードを入力したりできます。

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。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン不参加コンピューター

この展開には、Desktop Viewer を実行し、StoreFront に直接接続する、ドメイン不参加のユーザーデバイスが含まれています。



ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。この展開では 2 モード認証を使用できるため、Receiver ではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。その後、Receiver が Storefront への認証を実行します。

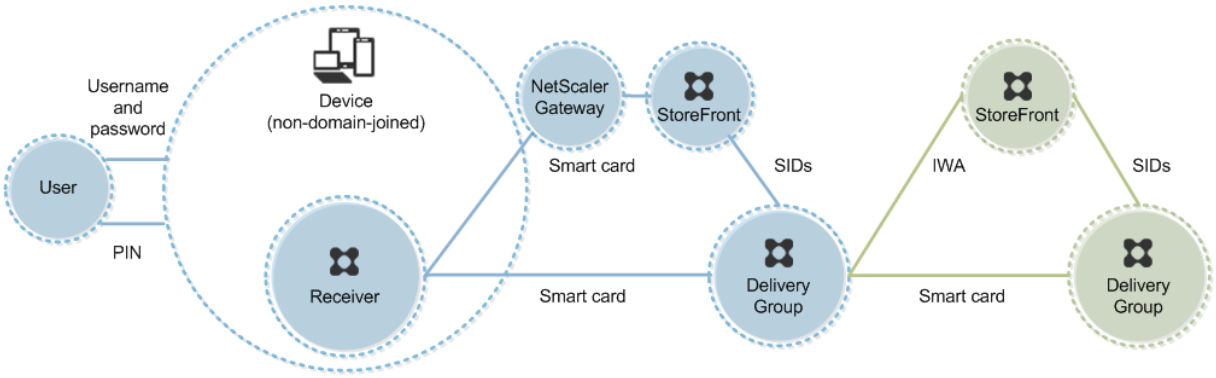
StoreFront により、ユーザーのセキュリティ識別子（SID）が XenApp または XenDesktop に渡されます。この

展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要があります。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン不参加コンピューターからのリモートアクセス

この展開には、Desktop Viewer を実行し、StoreFront に直接接続する、ドメイン不参加のユーザーデバイスが含まれています。



ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。この展開では 2 モード認証を使用できるため、Receiver ではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。その後、Receiver が Storefront への認証を実行します。

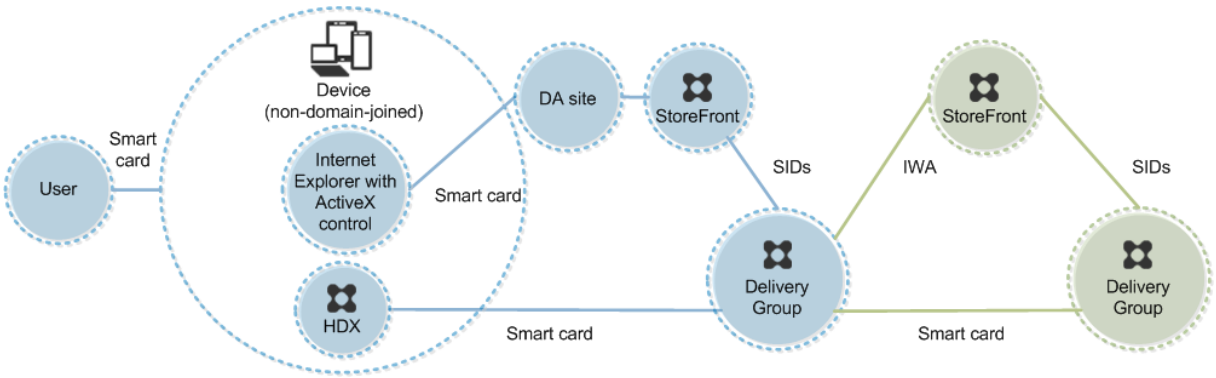
StoreFront により、ユーザーのセキュリティ識別子（SID）が XenApp または XenDesktop に渡されます。この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要があります。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：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。



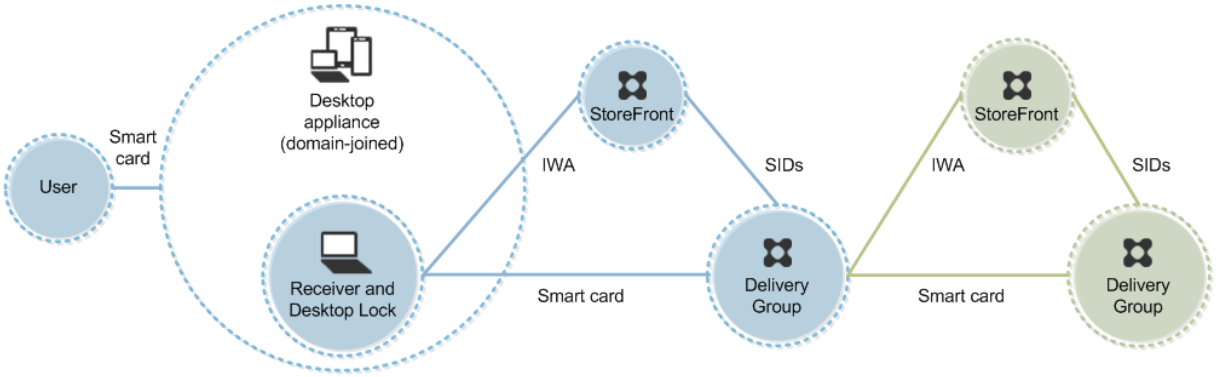
ユーザーは、スマートカードを使ってデバイスにログオンします。Desktop Lock を実行するデバイスは、キオスクモードで動作する Internet Explorer を介してデスクトップアプライアンスサイトを起動するように構成されます。サイトの ActiveX コントロールにより PIN の入力が求められ、それが StoreFront に送信されます。StoreFront により、ユーザーのセキュリティ識別子（SID）が XenApp または XenDesktop に渡されます。割り当てられたデスクトップグループ一覧で使用可能な（アルファベット順で）最初のデスクトップが起動します。

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。

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

March 25, 2020

パススルー認証

仮想デスクトップへのスマートカードによるパススルー認証は、Windows 10、Windows 8、Windows 7 Service Pack 1 Enterprise エディション、および Professional エディションが動作するユーザーデバイスでサポートされます。

ホストされるアプリケーションへのスマートカードによるパススルー認証は、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 SP1 が動作するサーバーでサポートされます。

サーバーでホストされるアプリケーションへのスマートカードパススルー認証を使用するには、サイトの認証方法としてスマートカードパススルーを構成するときに Kerberos を有効にする必要があります。

注：スマートカードによるパススルー認証を使用できるかどうかは、次の例のようなさまざまな要因により決定されます：

- パススルー認証に関する組織のセキュリティポリシー。

- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアの PIN キャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFront 上で構成します。詳しくは、StoreFront のドキュメントを参照してください。

シングルサインオン

「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。この画面ではシングルサインオンが機能しないため、ログオンを行うには、
[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）

October 22, 2021

XenApp または XenDesktop のサイトの TLS（Transport Layer Security）プロトコルを構成するには、以下の手順が必要です：

- サーバー証明書を入手して、すべての Delivery Controller 上にインストールして登録します。さらに、TLS 証明書のポート構成を行います。詳しくは、「TLS サーバー証明書の Controller へのインストール」を参照してください。

  必要な場合は、Controller で HTTP および HTTPS トラフィック用に使用されるポートを変更することもできます。

- ユーザーと Virtual Delivery Agent（VDA）間の TLS 接続を有効にします。これを行うには、以下のタスクが必要です:

  - VDA がインストールされたマシン上で TLS を構成します（便宜上、VDA がインストールされたマシンをここでは「VDA」と呼びます）。提供されている PowerShell スクリプトを使用したり、手作業で構成したりすることができます。全般的な情報については、「VDA 上の TLS 設定について」を参照してください。詳しくは、「VDA 上の TLS 構成：PowerShell スクリプトの使用」および「VDA 上の TLS 構成：手作業による構成」を参照してください。
  - VDA が追加されているデリバリーグループで TLS を構成します。これを行うには、Studio でいくつかの PowerShell コマンドレットを実行します。詳しくは、「デリバリーグループの TLS の構成」を参照してください。

  以下の要件および考慮事項があります:

  - ユーザーと VDA 間の TLS 接続を有効にするのは、XenApp 7.6 サイト、XenDesktop 7.6 サイト、およびこれ以降のリリースでのみ必要です。
  - デリバリーグループおよび VDA 上の TLS は、コンポーネントのインストール、サイトの作成、およびマシンカタログとデリバリーグループの作成を行った後で構成します。
  - デリバリーグループで TLS を構成するには、Controller のアクセス規則を変更するための権限が必要です。すべての管理権限を実行できる管理者には必要な権限が付与されています。
  - VDA 上の TLS を構成するには、そのマシン上の Windows 管理者権限が必要です。
  - VDA を以前のバージョンからアップグレードして TLS を構成する場合は、アップグレード前にすべての SSL リレーソフトウェアをアンインストールしておく必要があります。
  - PowerShell スクリプトでは、静的に割り当てられる VDA 上の TLS を構成できます。Machine Creation Services または Provisioning Services でプロビジョニングされてプールされる VDA は再起動時にマシンイメージがリセットされるため、PowerShell スクリプトで TLS を構成することはできません。

> 警告:
>
> Windows レジストリの編集を含むタスクの場合：レジストリの編集を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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。

> 注:
>
> TLS と UDT が両方とも VDA で有効な場合:
>
> - Citrix Director は、VDA への直接アクセスに常に TLS over TCP（UDP や UDT ではなく）を使用します。
> - NetScaler Gateway を使用して VDA に間接的にアクセスする場合、Citrix Receiver は、NetScaler Gateway との通信に DTLS over UDP を使用します。NetScaler Gateway と VDA 間の通信には、DTLS なしの UDP が使用されます。UDT が使用されます。

TLS サーバー証明書の **Controller** へのインストール

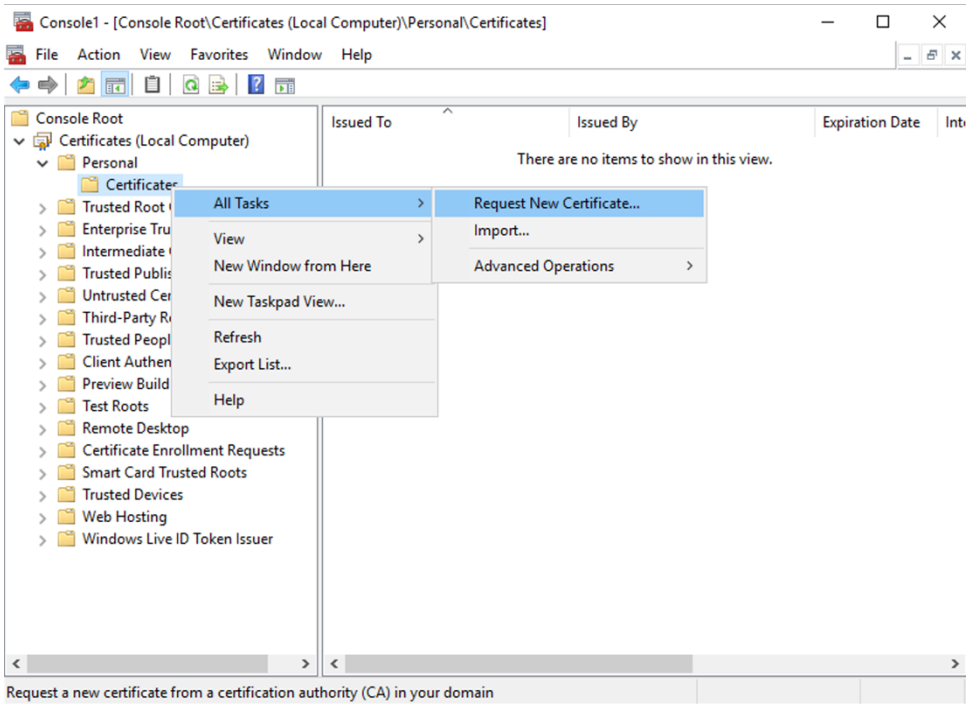
HTTPS 接続を使用する場合、XML Service はサーバー証明書を使用することで TLS 機能をサポートしますが、クライアント証明書はサポートしません。このセクションでは、Delivery Controller での TLS 証明書の取得とインストールについて説明します。同じ手順を Cloud Connector に適用して、STA および XML トラフィックを暗号化できます。

証明機関にはさまざまな種類があり、そこに証明書を要求する方法もさまざまですが、この資料では Microsoft 証明機関について説明します。Microsoft 証明機関は、サーバー認証の目的で発行された証明書テンプレートを保有している必要があります。

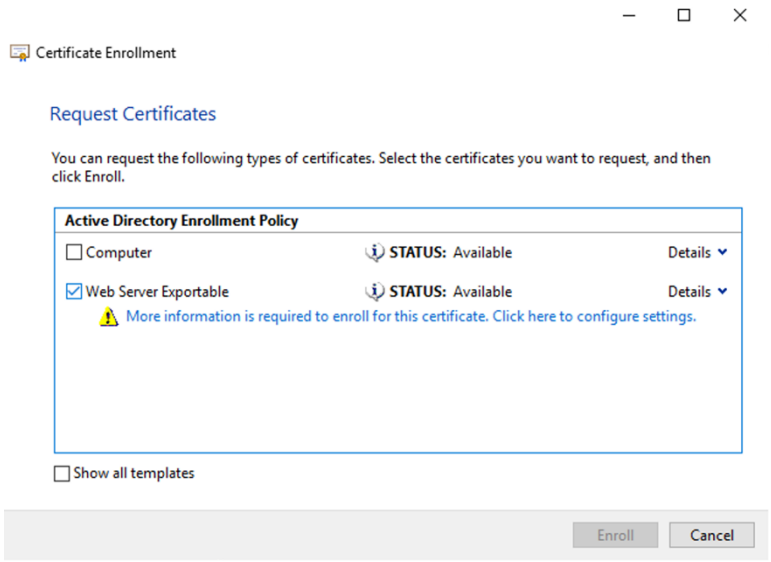
Microsoft 証明機関が、Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合は、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。

証明書の要求とインストール

1. Delivery Controller で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、［コンピューターアカウント］を選択します。
2. ［個人］**>**［証明書］を展開し、［すべてのタスク］**>**［新しい証明書の要求］コンテキストメニューコマンドを使用します。



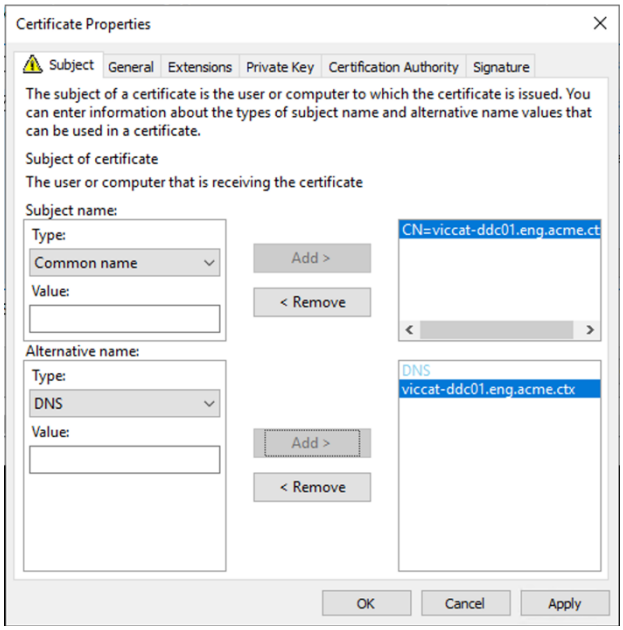
3. ［次へ］をクリックして開始し、［次へ］をクリックして、Active Directory の登録から証明書を取得していることを確認します。
4. サーバー認証証明書のテンプレートを選択します。［件名］の値が自動的に入力されるようにテンプレートが設定されている場合は、詳細を指定せずに ［登録］をクリックできます。



5. 証明書テンプレートの詳細情報を入力するには、［詳細］矢印ボタンをクリックし、次の項目を構成します：

   サブジェクト名：共通名を選択し、Delivery Controller の完全修飾ドメイン名を追加します。

   代替名： DNS を選択し、Delivery Controller の完全修飾ドメイン名を追加します。



SSL/TLS リスナーポートの構成

1. マシンの管理者として PowerShell コマンドウィンドウを開きます。
2. ブローカーサービスアプリケーション GUID を取得するには、次のコマンドを実行します:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $\_; $\_.GetValueNames() | ForEach-Object {
  $key.GetValue($\_)  }
  | Where-Object {
  $\_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
```



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

3. 同じ PowerShell ウィンドウで次のコマンドを実行して、以前にインストールした証明書の拇印を取得します:

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

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
<!--NeedCopy-->
```

4. 同じ PowerShell ウィンドウで次のコマンドを実行して、ブローカーサービスの SSL/TLS ポートを構成し、暗号化用の証明書を使用します:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

$SSLxml | netsh

. netsh http show sslcert
<!--NeedCopy-->
```

正しく構成された場合、最後のコマンド`.netsh http show sslcert`の出力に、リスナーが正しい`IP:port`を使用していること、および`Application ID`がブローカーサービスアプリケーション GUID と一致していることが示されます。

サーバーが Delivery Controller にインストールされた証明書を信頼している場合、StoreFront Delivery Controller および Citrix Gateway STA バインディングで、HTTP ではなく HTTPS を使用するように構成できます。

> 注:
>
> この構成の変更は、他のバージョンの Windows Server の組み合わせの Controller と StoreFront では必要ありません。

暗号の組み合わせの順序一覧には、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384またはTLS_ECDHE_RSA_WITH_AES の暗号の組み合わせ（またはこの両方）を含める必要があります。これらの暗号の組み合わせは、TLS_DHE_の暗号の組み合わせより前に配置する必要があります。

> 注:
>
> Windows Server 2012 では、GCM の暗号の組み合わせTLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384およびTLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256はサポートされません。

1. Microsoft のグループポリシーエディターを使用して、［コンピューターの構成］**>**［管理用テンプレート］**>**［ネットワーク］**>**［**SSL** 構成設定］の順に参照します。
2. ［**SSL** 暗号の順位］ポリシーを編集します。デフォルトでは、このポリシーは ［未構成］に設定されています。このポリシーを ［有効］に設定します。
3. 暗号の組み合わせを適切な順序に並び替え、使用しない暗号の組み合わせを削除します。

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384またはTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256のどちらかがすべてのTLS_DHE_暗号の組み合わせより前に配置されていることを確認します。

Microsoft MSDN の「Prioritizing Schannel Cipher Suites」も参照してください。

HTTP または **HTTPS** ポートの変更

デフォルトでは、XML Service は HTTP トラフィックにはポート 80 を、HTTPS トラフィックにはポート 443 を使用します。これらのポート番号を変更することもできますが、信頼されないネットワークに Controller を露出させる場合のセキュリティ上のリスクについて考慮してください。デフォルト構成を変更する場合は、スタンドアロンの StoreFront サーバーを使用することをお勧めします。

Controller で使用されるデフォルトの HTTP または HTTPS ポートを変更するには、Studio で次のコマンドを実行します:

```
BrokerService.exe -WIPORT http-port -WISSLPORT https-port
```

ここで、*http-port* は HTTP トラフィックのポート番号で、*https-port* は HTTPS トラフィックのポート番号です。

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-C |

> onfigServiceInstance

HTTPS トラフィックのみに制限する

HTTP トラフィックが XML Service で無視されるように構成するには、Controller 上の HKLM\Software\Citrix\DesktopServer
以下のレジストリ設定を作成してから Broker Service を再起動します。

HTTP トラフィックを無視するには、DWORD XmlServicesEnableNonSsl を作成して 0 に設定します。

同様に、HTTPS トラフィックを無視するために作成できるレジストリの DWORD 値も存在します：DWORD XmlServicesEnableSsl これは 0 に設定しないでください。

VDA 上の TLS 設定

TLS を構成した VDA と構成していない VDA を同一デリバリーグループ内で混在させることはできません。デリバリーグループの TLS を構成する前に、そのグループに属しているすべての VDA 上で TLS 構成を完了しておく必要があります。

VDA 上に TLS を構成すると、インストールされている TLS 証明書の権限が変更され、その証明書の秘密キーに対する読み取り権限が ICA Service に付与されます。ICA Service には、以下の情報が提供されます：

- **TLS** で使用される証明書ストア内の証明書。
- 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。

> 重要
>
> SSLv3 の使用状況を確認し、必要に応じ、それらの展開を再構成して SSLv3 のサポートを削除することを Citrix ではお勧めします。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次の通りです：（低いものから）SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2。許可する最低バージョンを指定すると、それ以上のバージョンを使用するすべてのプロトコル接続が許可されます。

たとえば、最低バージョンとして TLS 1.1 を指定すると、TLS 1.1 および TLS 1.2 のプロトコルを使用した接続が許可されます。最低バージョンとして SSL 3.0 を指定すると、サポートされる SSL プロトコルのすべてのバージョンが許可されます。最低バージョンとして TLS 1.2 を指定すると、TLS 1.2 の接続のみが許可されます。

- どの **TLS** 暗号の組み合わせが許可されるのか。

暗号スイートが、この接続において使用する暗号化を選択します。クライアントと VDA は、暗号スイートの異なる組み合わせをサポートできます。クライアント（Citrix Receiver または StoreFront）が VDA に接続するときは、そのクライアントがサポートする TLS 暗号スイートの一覧を VDA に送信します。VDA 側では、構成済みの暗号スイー

トの独自の一覧内にクライアントのいずれかの暗号スイートと一致するものがあるかどうかがチェックされ、あった場合にのみ接続が確立されます。一致する暗号スイートがない場合、その接続は VDA により拒否されます。

VDA がサポートしている暗号スイート（コンプライアンスモードとも呼ばれます）は、GOV（ernment）、COM（mercial）、および ALL の 3 つです。確立できる暗号スイートは、Windows の FIPS モードによっても異なります。Windows の FIPS モードについては、https://support.microsoft.com/kb/811833を参照してください。次の表は、各セットの暗号の組み合わせを示しています:

TLS 暗号の組み合わせ	GOV	COM	ALL	GOV	COM	ALL
FIPS モード	無効	無効	無効	有効	有効	有効
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_ECDHE_	x		x	x		x
TLS_RSA_WITH_AES_256_GCM_SHA384			x	x		x
TLS_RSA_WI	x	x	x	x	x	x
TLS_RSA_WITH_AES_256_CBC_SHA256			x	x		x
TLS_RSA_WI	x		x	x		x
TLS_RSA_WITH_AES_128_CBC_SHA			x		x	x
TLS_RSA_WI		x	x			
TLS_RSA_WITH_RC4_128_MD5			x			
TLS_RSA_WI	x		x	x		x

> 重要:
>
> VDA が、Windows Server 2012 R2、Windows Server 2016、Windows 10 Anniversary Edition、または以降のサポートリリースにインストールされている場合は、追加の手順が必要になります。これは、Citrix Receiver for Windows（バージョン 4.6～4.9）、Citrix Receiver for HTML5、および Citrix Receiver for Chrome からの接続に影響します。これには、NetScaler Gateway を介した接続も含まれます。
>
> この手順は、NetScaler Gateway と VDA 間の TLS が設定されている場合、すべての VDA バージョンで NetScaler Gateway を使用するすべての接続にも必要です。これは Citrix Receiver のすべてのバージョンに影響します。

グループポリシーエディターを使用する VDA（Windows Server 2016 または Windows 10 Anniversary Edition 以降）上で、［コンピューターの構成］**>**［管理用テンプレート］**>**［ネットワーク］**>**［**SSL** 構成設定］**>**［**SSL** 暗号の順位］と移動します。以下の順に選択します:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> 注:
>
> 最初の 4 つの項目は、楕円曲線、P384、または P256 も指定します。[curve25519] が選択されていないことを確認します。FIPS モードは、「curve25519」の使用を妨げません。

このグループポリシー設定が構成されると、VDA は、暗号の組み合わせを、グループポリシーの一覧と選択されたコンプライアンスモード（COM、GOV または ALL）の一覧の両方に表示されている場合のみ選択します。また、暗号スイートは、クライアント（Citrix Receiver または StoreFront）が送信する一覧にも記載されている必要があります。

このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、このグループポリシーの一覧に追加する必要がある場合があります。

> 重要:
>
> グループポリシーの変更が適用されたときに表示されても、TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。したがって、プールデスクトップの場合、TLS 構成のグループポリシーの変更は基本イメージに適用してください。

VDA 上の TLS 構成：PowerShell スクリプトの使用

VDA 上で Enable-VdaSSL.ps1 スクリプトを実行すると、その VDA での TLS リスナーを有効または無効にできます。このスクリプトは、インストールメディアの Support > Tools > SslSupport フォルダーに収録されています。

スクリプトで TLS を有効にする場合、指定した TLS TCP ポートについての既存の Windows ファイアウォール規則がすべて無効になります。その後で、ICA Service がそのポートで着信接続を受け入れるための新しい規則が追加されます。また、スクリプトにより以下の Windows ファイアウォール規則が無効になります:

- Citrix ICA（デフォルトで 1494）
- Citrix CGP（デフォルトで 2598）
- Citrix WebSocket（デフォルトで 8008）

この影響として、TLS を使用した場合のみ接続が可能になります。TLS を使用しないと、ICA/HDX、セッション画面を保持した ICA/HDX、WebSocket を介した HDX を使用することはできません。

「ネットワークポート」を参照してください。

> 注:
>
> PVS ターゲットや MCS クローンなどのステートレスマシンでは、デフォルトで FQDN 証明書が使用されます。

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。

> 重要:
>
> Enable または Disable パラメーターと CertificateThumbPrint パラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {
 -Enable | -Disable }
  -CertificateThumbPrint "<thumbprint>"
[ - SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-
    SSLCipherSuite"<suite>"]
<!--NeedCopy-->
```

パラメーター	説明
有効化	TLS リスナーを VDA 上にインストールして有効にします。このパラメーターまたは Disable パラメーターのいずれかを指定する必要があります。
無効化	VDA 上の TLS リスナーを無効にします。このパラメーターまたは Enable パラメーターのいずれかを指定する必要があります。このパラメーターを指定した場合、ほかのパラメーターは無視されます。
CertificateThumbPrint “<thumbprint>”	証明書ストア内の TLS 証明書の拇印を二重引用符で囲んで指定します。スクリプトは、指定された拇印によって使用する証明書を選択します。このパラメーターを省略すると、不正な証明書が選択されます。
SSLPort <port>	TLS ポート指定します。デフォルト: 443
SSLMinVersion “<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。使用できる値は、「SSL_3.0」、「TLS_1.0」(デフォルト)、「TLS_1.1」、および「TLS_1.2」です。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	説明
SSLCipherSuite “<suite>”	TLS 暗号スイートを二重引用符で囲んで指定します。使用できる値は、「GOV」、「COM」、および「ALL」（デフォルト）です。

例

次のスクリプトでは、TLS 1.2 プロトコルバージョン値をインストールして有効にします。拇印（この例の場合、「12345678987654321」）を指定して、使用する証明書を選択します。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトでは、TLS リスナーをインストールして有効化し、TLS ポートとして 400、暗号スイート GOV、および SSL プロトコルの最低バージョンとして TLS 1.2 を設定します。拇印（この例の場合、「12345678987654321」）を指定して、使用する証明書を選択します。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"-SSLPort 400
 -SSLMinVersion "TLS_1.2"-SSLCipherSuite "All"
```

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：

1. Microsoft 管理コンソール（MMC）を起動します：［スタート］**>**［ファイル名を指定して実行］**> mmc.exe**。
2. MMC に証明書スナップインを追加します。
   a) ［ファイル］**>**［スナップインの追加と削除］の順に選択します。
   b) ［証明書］を選択して ［追加］をクリックします。
   c) ［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。
   d) ［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。
3. コンソールツリーの ［証明書（ローカルコンピューター）］**>**［個人］**>**［証明書］で証明書を右クリックして、［すべてのタスク］**>**［秘密キーの管理］の順に選択します。

4. アクセス制御リストエディターで［(FriendlyName）プライベートキーのアクセス許可］ダイアログボックスが開きます。ここで（FriendlyName）は、TLS 証明書の名前です。以下のいずれかのサービスを追加して、［読み取り］アクセスを許可します:
   - VDA for Windows Desktop OS では「PORTICASERVICE」
   - VDA for Windows Server OS では「TERMSERVICE」
5. インストールした TLS 証明書をダブルクリックします。［証明書］ダイアログボックスの ［詳細］タブをクリックして、一番下までスクロールします。［拇印］をクリックします。
6. regedit を実行して、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd を開きます。
   a) SSL Thumbprint キーを編集して、TLS 証明書の拇印の値をバイナリ値にコピーします。［バイナリ値の編集］ダイアログボックスでは、不明な項目（「0000」や特殊文字など）は無視して構いません。
   b) 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)。
   c) 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)。
7. デフォルトの 443 以外の TLS TCP ポートを使用する場合は、そのポートが Windows ファイアウォールで開放されていることを確認します（Windows ファイアウォールで受信規則を作成するときは、［接続を許可する］および ［有効］が選択されていることを確認してください)。
8. ほかのアプリケーションやサービスなど（IIS など）がその TLS TCP ポートを使用していないことを確認します。
9. VDAs 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。

1. Studio から PowerShell コンソールを開きます。
2. `asnp Citrix.*`を実行して Citrix 製品のコマンドレットをロードします。
3. `Get-BrokerAccessPolicyRule -DesktopGroupName 'delivery-group-name'| Set-BrokerAccessPolicyRule -HdxSslEnabled $true`を実行します。
4. `Set-BrokerSite -DnsResolutionEnabled $true`を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDA のシステムイベントログを確認してください。

Citrix Receiver for Windows で TLS 関連の接続エラー（1030 など）が発生した場合は、Desktop Viewer を無効にしてから再試行してください。接続エラーは解決されませんが、TLS の問題についての情報が表示される場合があります。たとえば、証明機関に証明書を要求したときに正しくないテンプレートを使用したなどがあります。

Controller と **VDA** の間の通信

Controller と VDA 間の通信は、Windows Communication Framework（WCF）のメッセージレベルの保護によってセキュリティ保護されています。TLS を使用した追加の移送レベルの保護は必要ありません。WCF 構成では、Controller と VDA 間の相互認証に Kerberos が使用されます。暗号化には、CBC モードでの AES が 256 ビットキーで使用されます。メッセージの整合性には SHA-1 が使用されます。

Microsoft によると、WCF で使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2 を含む OASIS（Organization for the Advancement of Structured Information Standards）による標準に準拠しています。さらに、WCF は『Security Policy 1.2』に表記されているアルゴリズムスイートすべてをサポートしていることも明言されています。

Controller と VDA 間の通信には、上述のアルゴリズムによる basic256 アルゴリズムスイートが使用されます。

TLS および **HTML5** ビデオリダイレクション

HTML5 ビデオリダイレクションを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で動作する Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを達成するために、HTML5 ビデオリダイレクトサービスは VDA の証明書ストアで 2 つのカスタム証明書を生成します。このサービスを停止すると、証明書が削除されます。

HTML5 ビデオリダイレクションポリシーはデフォルトで無効になっています。

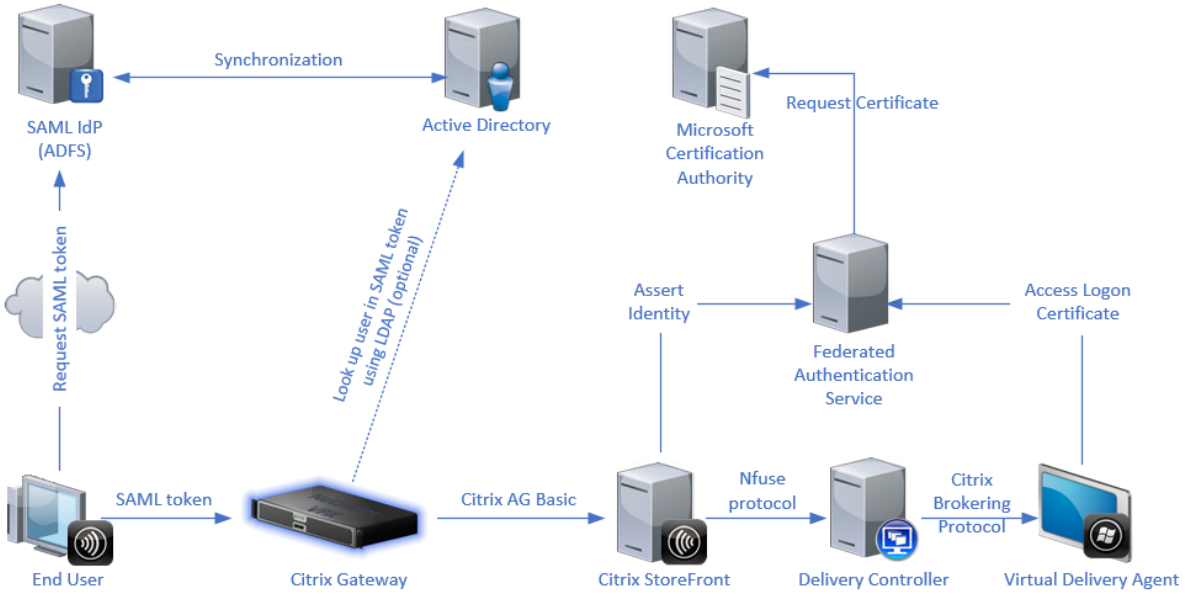
HTML5 ビデオリダイレクトについて詳しくは、「マルチメディアのポリシー設定」を参照してください。

フェデレーション認証サービス

August 24, 2021

Citrix フェデレーション認証サービスは、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フェデレーション認証サービスによる、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 サーバーがフェデレーション認証サービス（FAS）にアクセスします。FAS は、単一の XenApp または XenDesktop セッションがそのセッションの証明書で認証できるようにするチケットを付与します。VDA でユーザーを認証する必要がある場合、VDA は FAS にアクセスしてチケットを使用します。ユーザー証明書の秘密キーにアクセスできるのは FAS だけです。VDA は、証明書を使用して実行する必要のあるすべての署名処理および暗号化解除処理を、FAS に送信しなければなりません。

要件

フェデレーション認証サービスは Windows サーバー（Windows Server 2008 R2 以降）でサポートされます。

- FAS は、ほかの Citrix コンポーネントを含まないサーバーにインストールすることをお勧めします。
- Windows サーバーはセキュリティ保護されている必要があります。Windows サーバーには登録機関の証明書および秘密キーへのアクセス権限があり、ドメインユーザーに対して自動的に証明書を発行できます。また、これらのユーザー証明書および秘密キーへのアクセス権限もあります。
- FAS PowerShell SDKを使用するには、Windows PowerShell 64 ビットが FAS サーバーにインストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft エンタープライズ証明機関が必要です。

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 7.15 以上である必要があります。
- VDA のバージョンは 7.15 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、フェデレーション認証サービス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 3.12（XenApp および XenDesktop 7.15 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注意事項」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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)?redirectedfrom=MSDN

- 証明書ログオン用の Windows の構成

https://support.citrix.com/article/CTX206156

インストールとセットアップの順序

1. フェデレーション認証サービスのインストール
2. StoreFront サーバーでのフェデレーション認証サービスプラグインの有効化
3. グループポリシーの構成
4. フェデレーション認証サービス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、（c）フェデレーション認証サービスへの証明機関の使用権限の付与
5. ユーザールールの構成

フェデレーション認証サービスのインストール

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 ［フェデレーション認証サービス］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。

- フェデレーション認証サービス
- Federated Authentication Service をリモートで構成するPowerShell スナップインコマンドレット
- Federated Authentication Service の管理コンソール
- フェデレーション認証サービス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 ストアでのフェデレーション認証サービスプラグインの有効化

StoreFront ストアでフェデレーション認証サービス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。


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

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:

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

Delivery Controller の構成

フェデレーション認証サービスを使用するには、それに接続可能な 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。

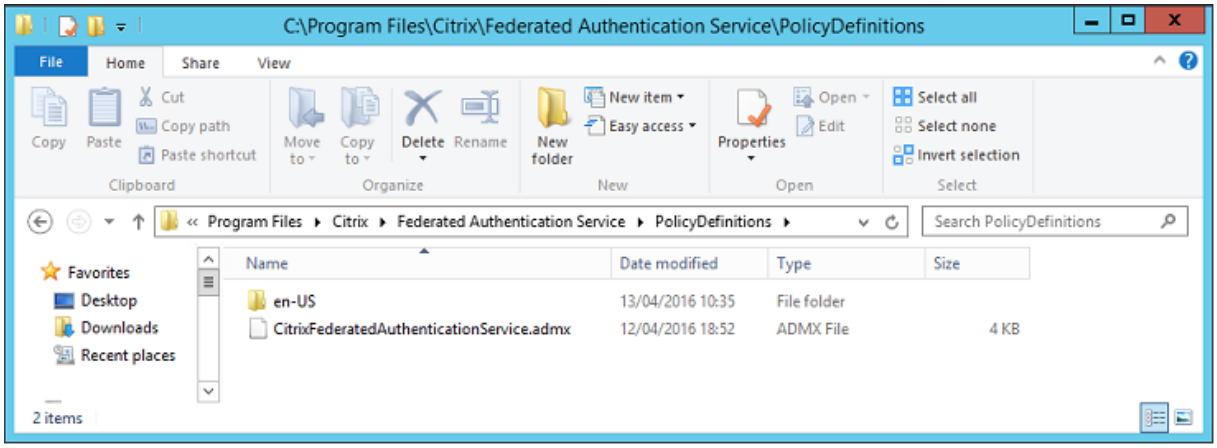
グループポリシーの構成

フェデレーション認証サービス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。

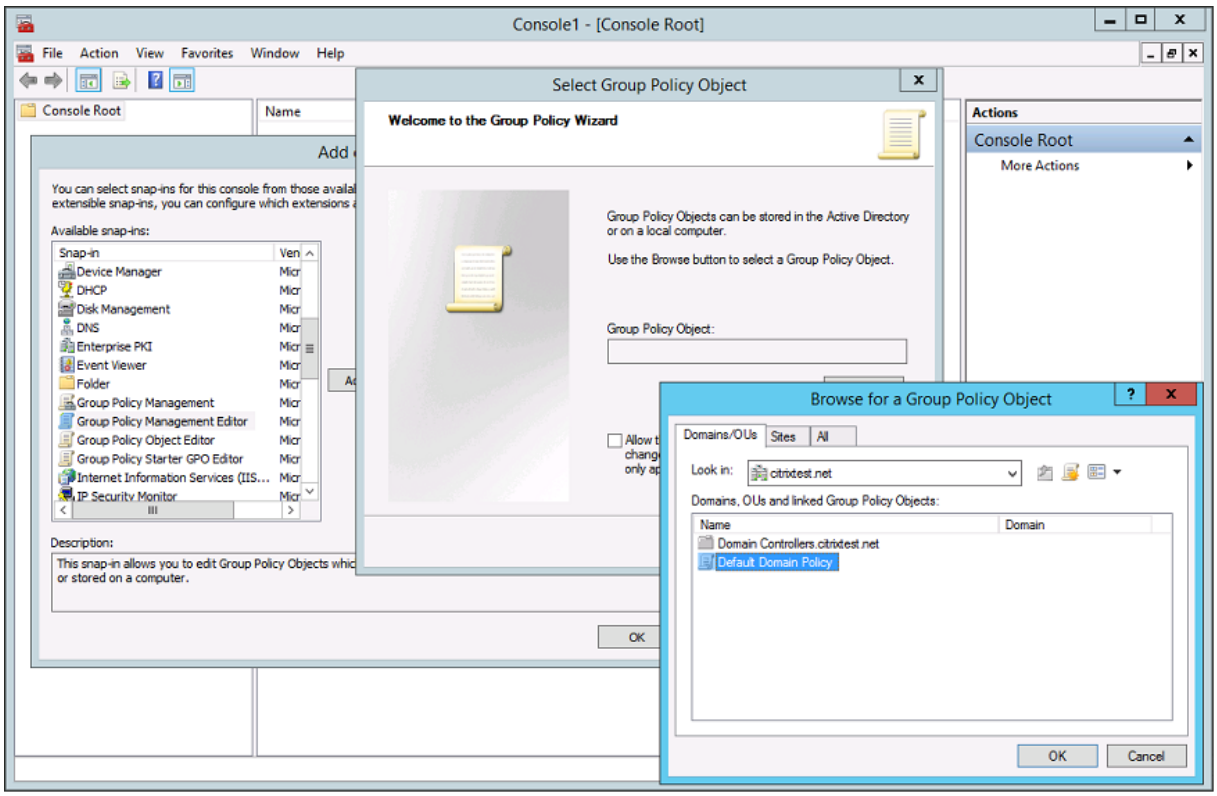
手順 **1**：FAS をインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx ファイルおよび en-US フォルダーを見つけます。



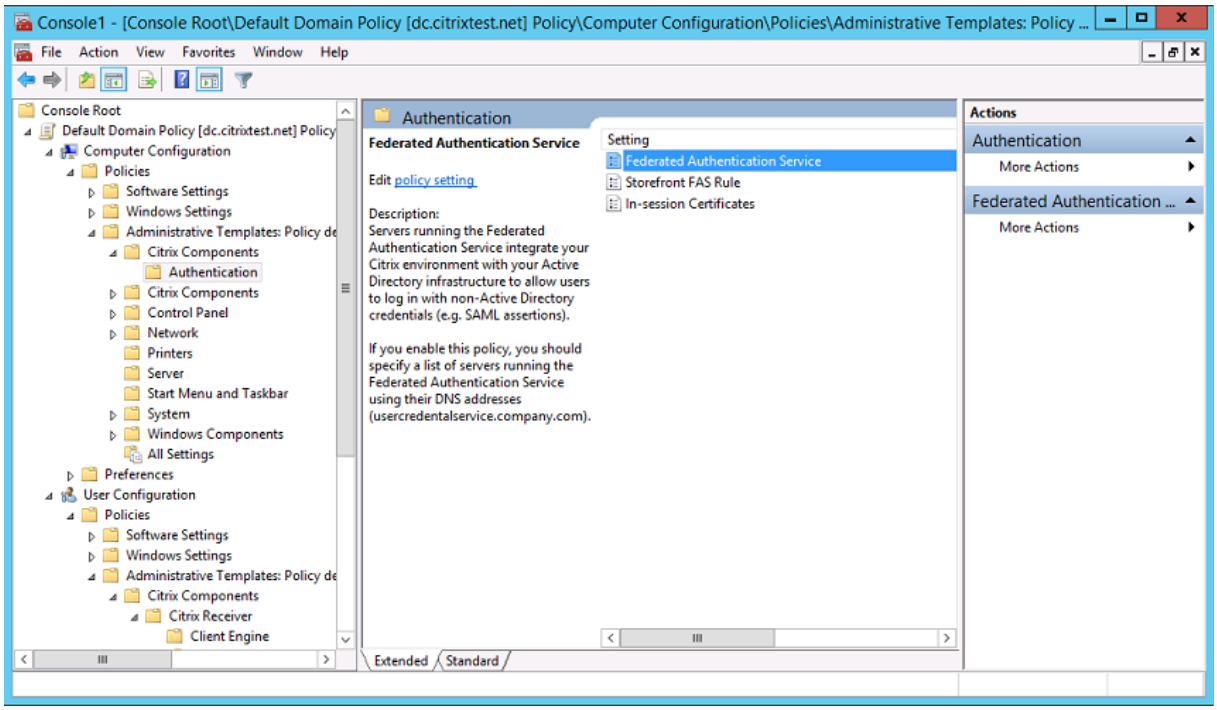
手順 **2**：これらをドメインコントローラーにコピーして、C:\Windows\PolicyDefinitions および en-US サブフォルダーに配置します。

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。

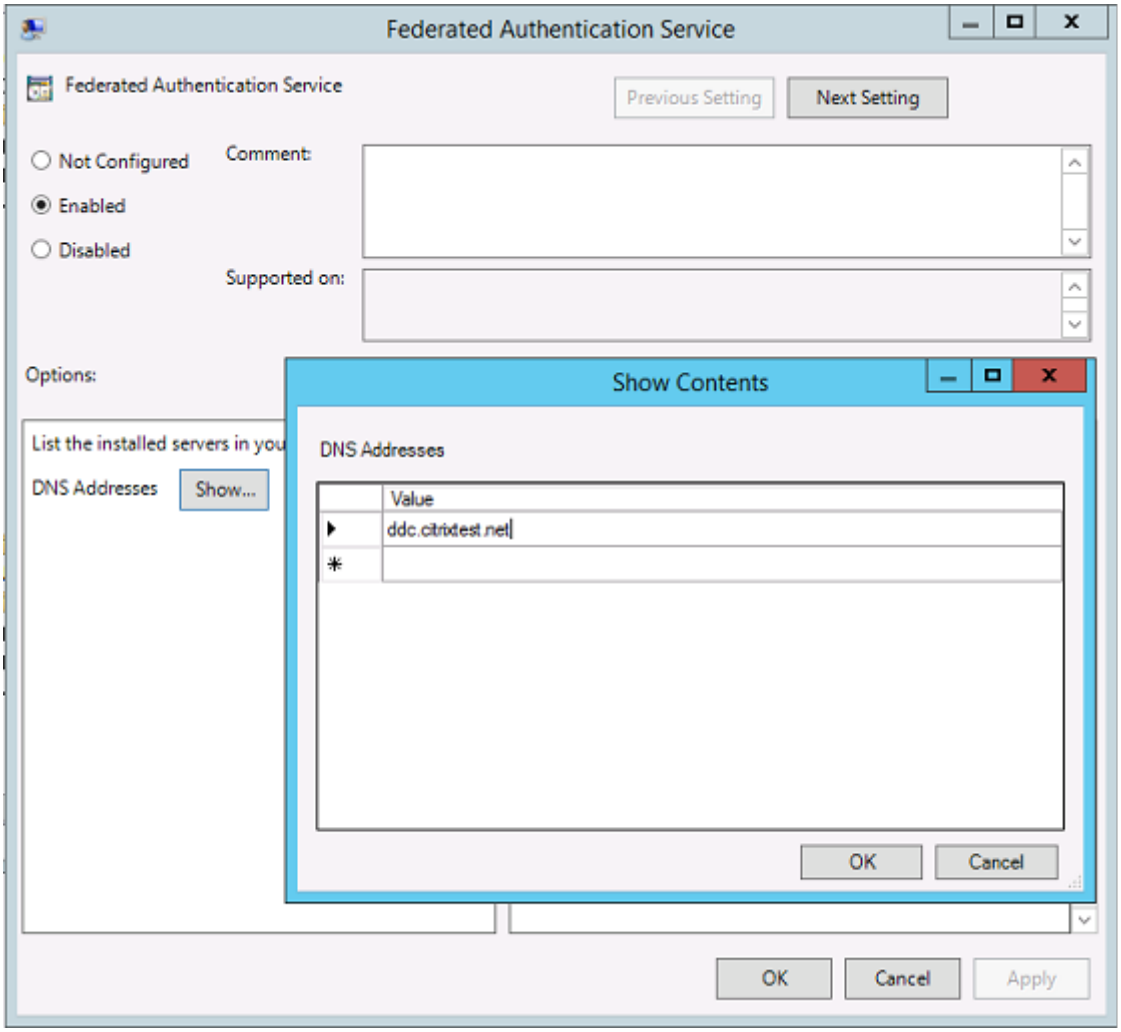
グループポリシーオブジェクトを入力するための画面が開いたら、［参照］を選択してから［既定のドメインポリシー］を選択します。または、任意のツールを使用して、環境に応じたポリシーオブジェクトを作成して選択することもできます。このポリシーは、影響を受ける Citrix ソフトウェア（VDA、StoreFront サーバー、管理ツール）を実行しているすべてのマシンに適用する必要があります。



手順 **4**: Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication にあるフェデレーション認証サービスポリシーに移動します。



手順 **5**: フェデレーション認証サービスポリシーを開き、［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。

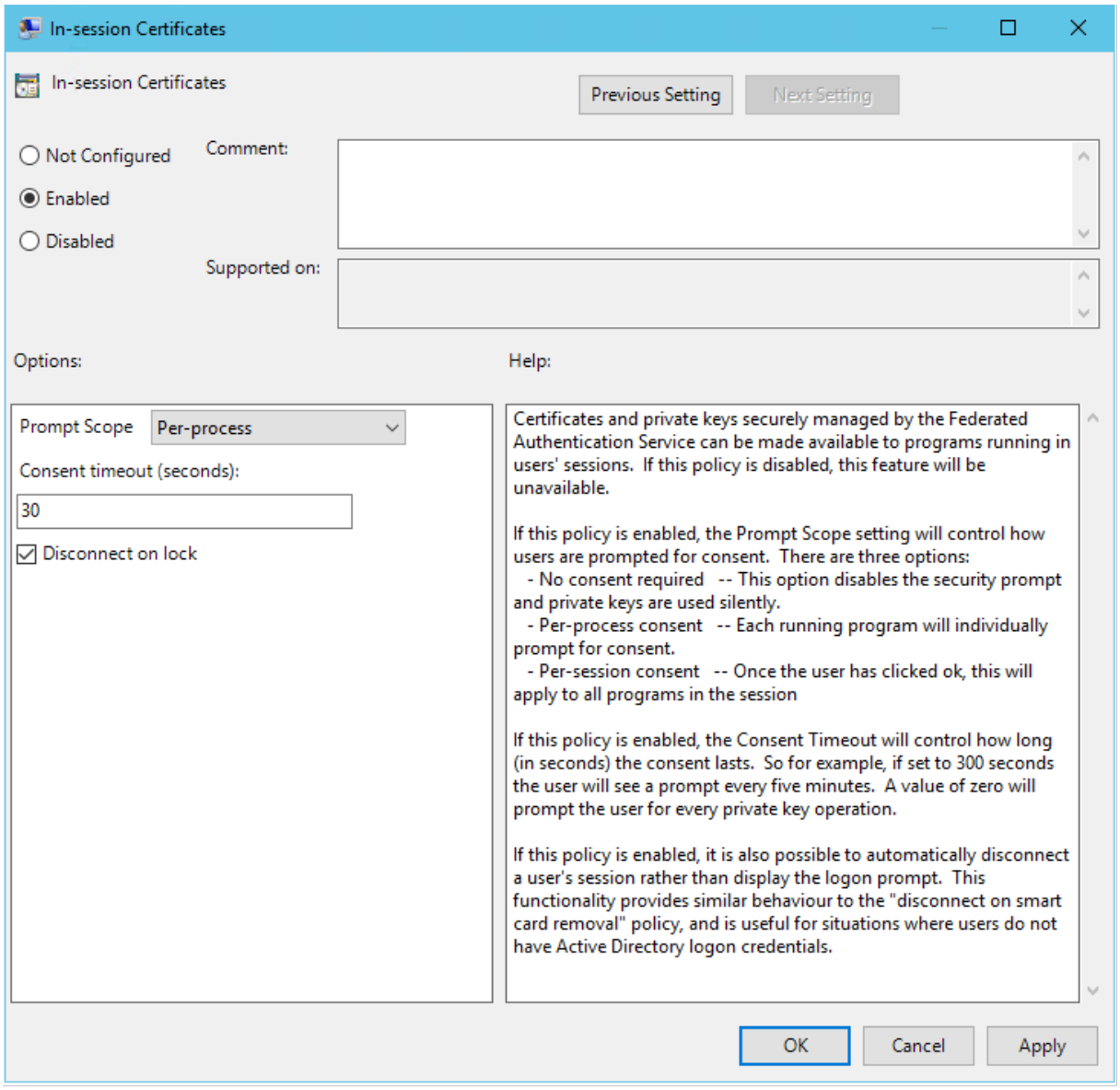


手順 **6**：フェデレーション認証サービスをホストしているサーバーの DNS アドレスを入力します。

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。

セッション内証明書サポートおよびロック時の切断を有効にする



セッション内証明書サポート

グループポリシーテンプレートには、セッション内証明書についてのシステムの構成のサポートが含まれます。これにより、ログオン後に、アプリケーションが使用できるようにユーザーの個人証明書ストアに証明書が配置されます。たとえば、VDA セッション内で Web サーバーへの TLS 認証が必要な場合、証明書は Internet Exploler によって使用されます。デフォルトで、VDA はログオン後の証明書へのアクセスを許可しません。

ロック時の切断

このポリシーを有効にすると、ユーザーが画面をロックしたときにセッションが自動的に切断されます。この機能で

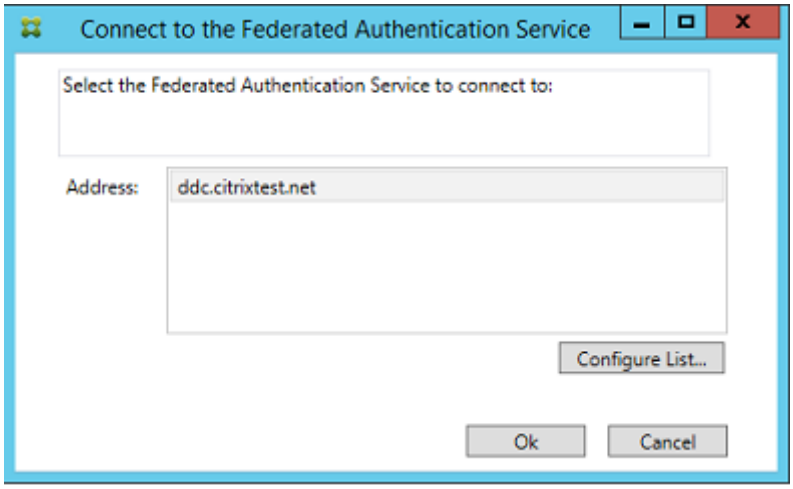
は「スマートカードの取り出し時の切断」ポリシーと同様の動作になるため、ユーザーが Active Directory ログオン資格情報を持っていない場合に便利です。

> 注:
>
> ロック時の切断ポリシーは、VDA 上のすべてのセッションに適用されます。

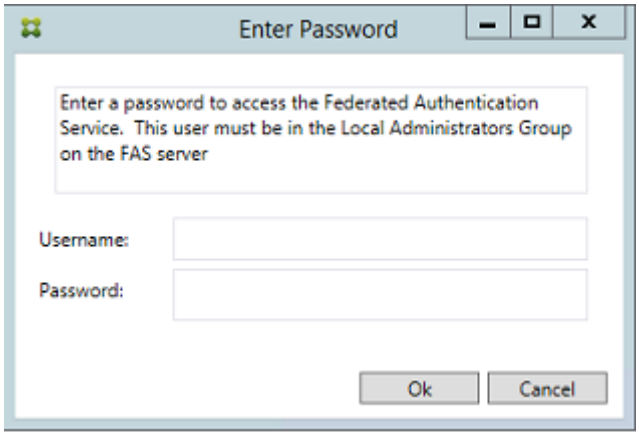
フェデレーション認証サービス管理コンソールの使用

フェデレーション認証サービス管理コンソールは、フェデレーション認証サービス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。

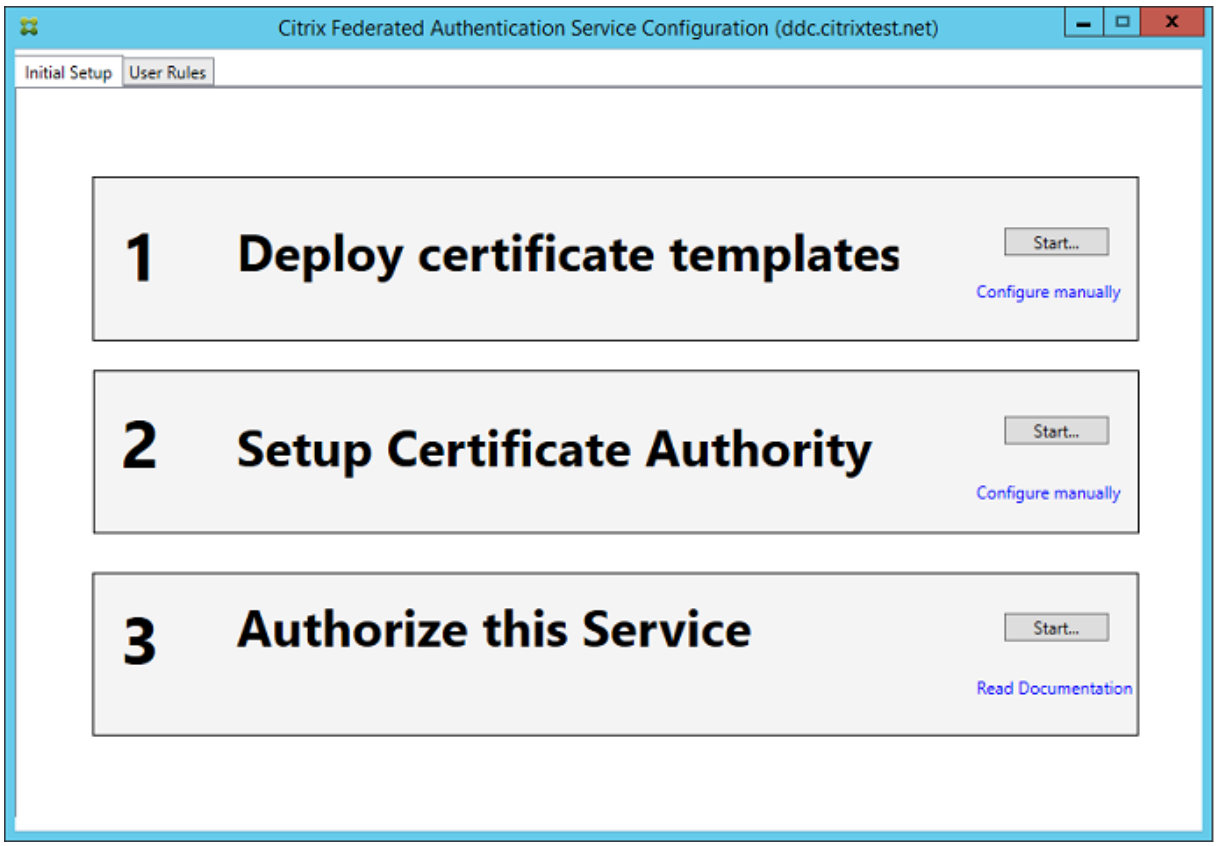
この管理コンソールは、グループポリシー構成を使用して、環境内の FAS サーバーを自動的に検出します。この検出に失敗した場合は、「グループポリシーの構成」セクションを参照してください。



ユーザーアカウントが、フェデレーション認証サービス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、およびフェデレーション認証サービス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。

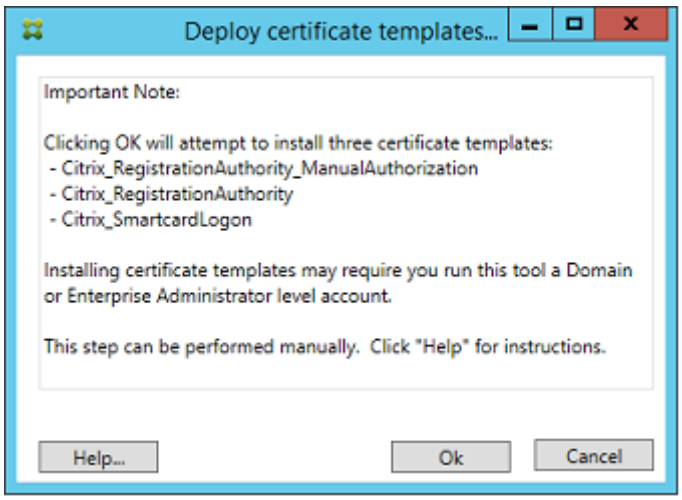


証明書テンプレートの展開

他のソフトウェアとの相互運用性の問題を避けるため、フェデレーション認証サービスでは、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フェデレーション認証サービス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。

```
```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

 $CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

 $CertEnrol.InitializeImport($template)

 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable

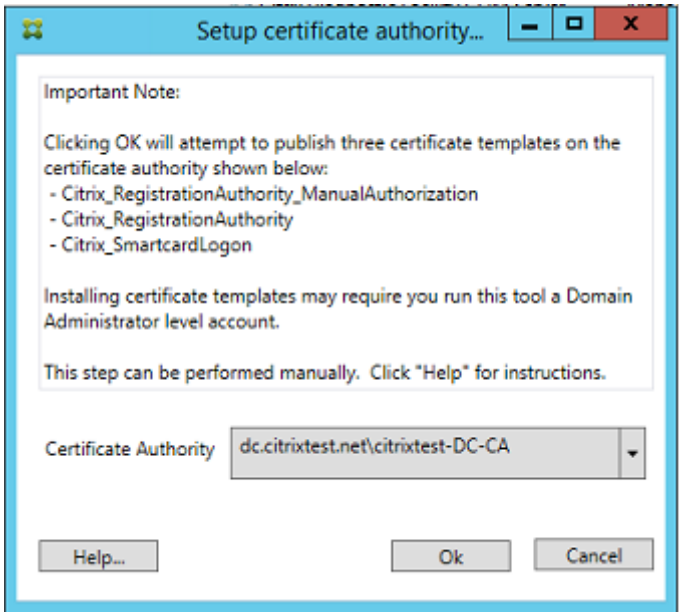
 $writabletemplate.Initialize($comtemplate)

 $writabletemplate.Commit(1, $NULL)
 <!--NeedCopy--> ```
```

### 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。

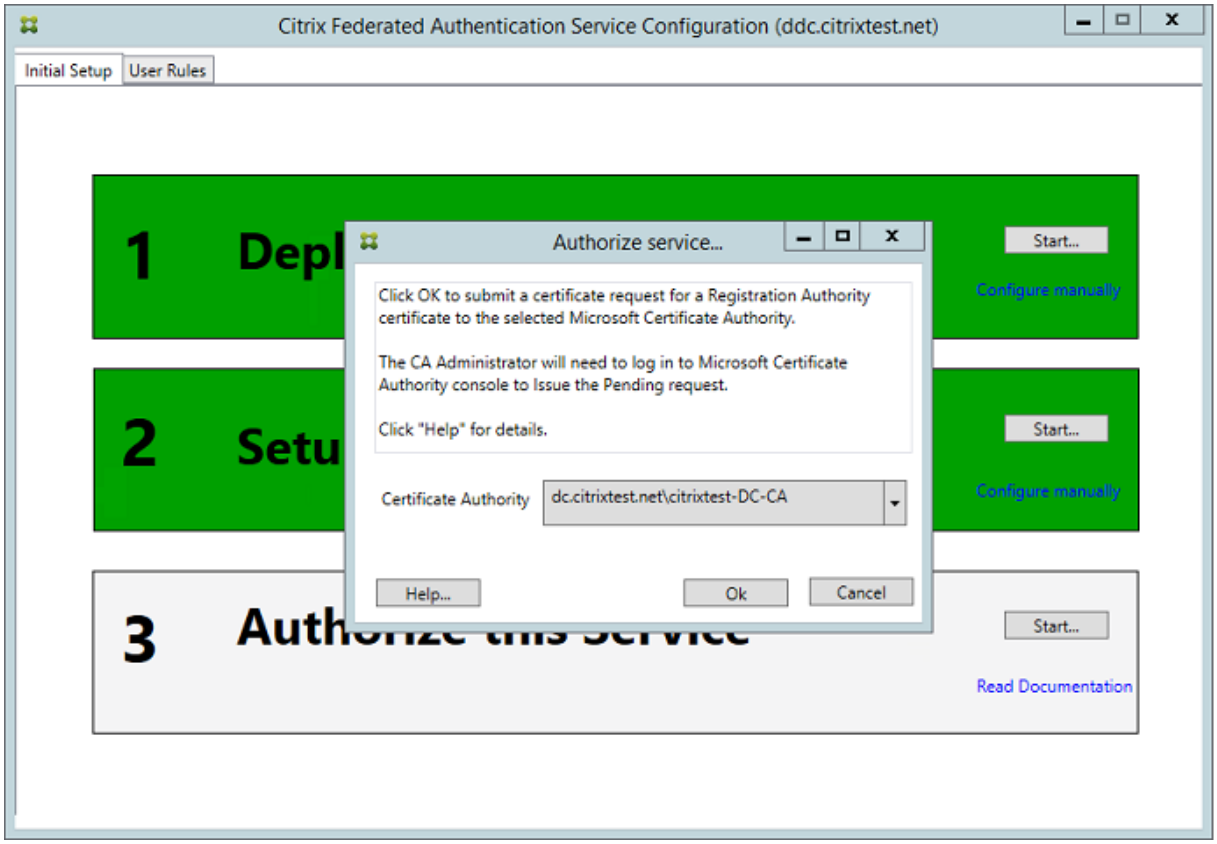
どのサーバーでもテンプレートが公開されていない場合は、証明書機関のセットアップツールによって公開できます。このツールは、証明機関の管理権限のあるユーザーとして実行する必要があります。

(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。)

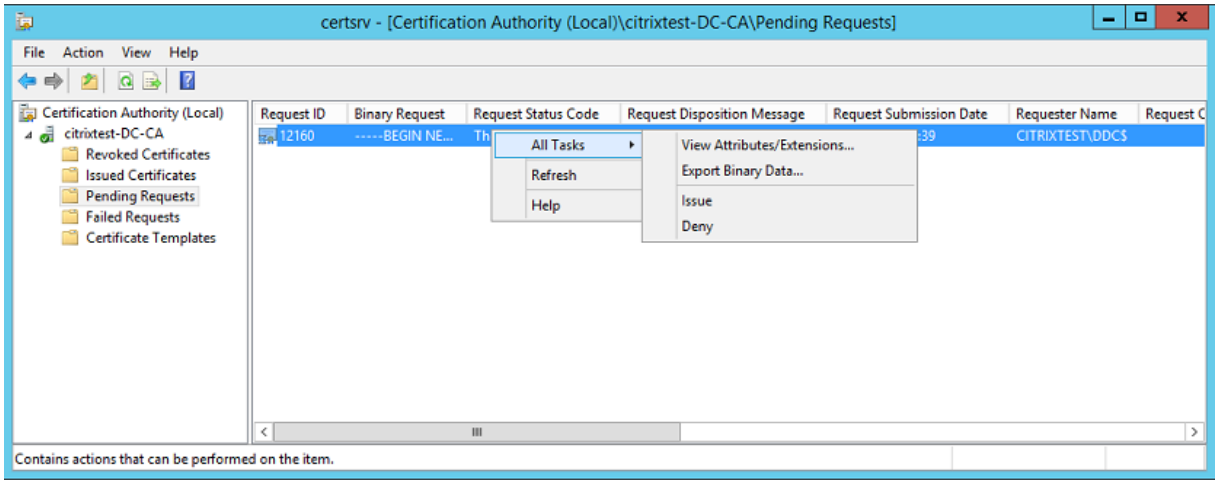


フェデレーション認証サービスへの権限付与

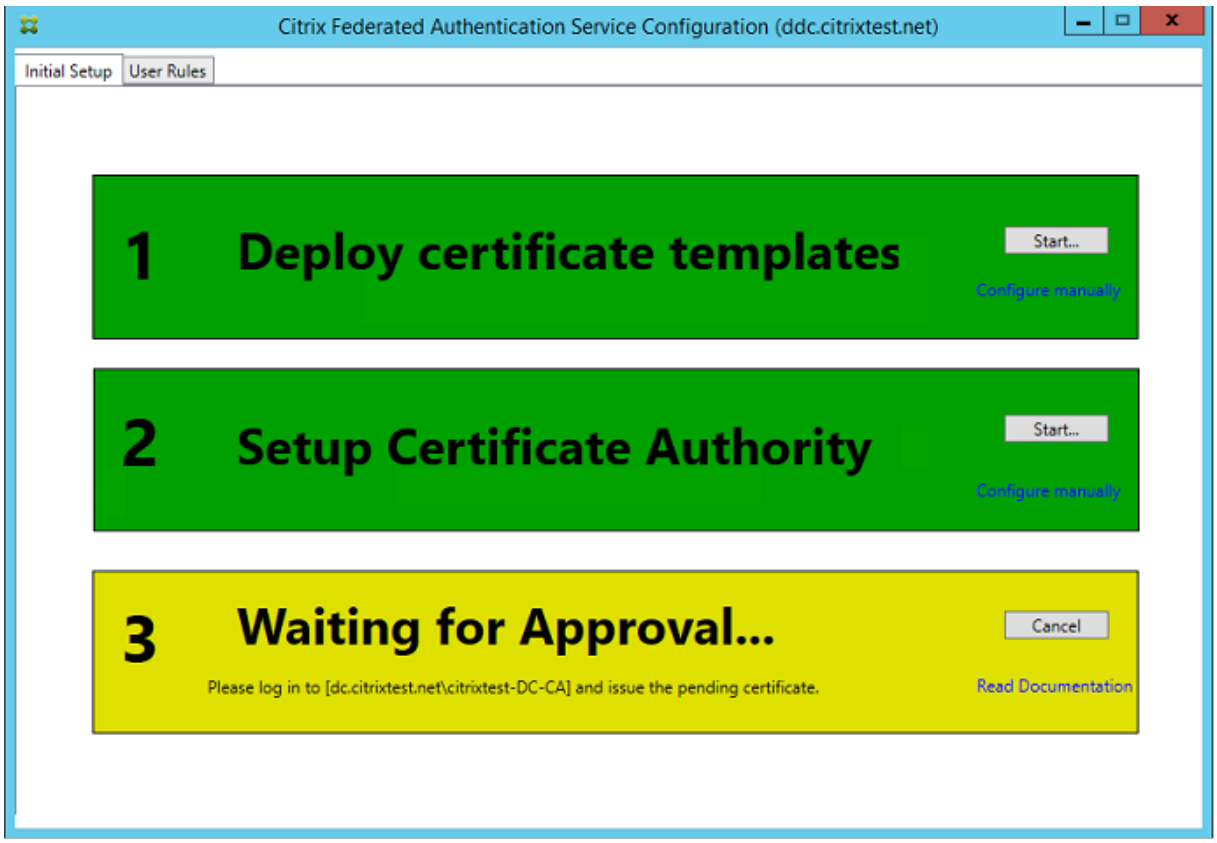
コンソールでの最終セットアップ手順では、フェデレーション認証サービスへの権限付与が開始されます。管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorization テンプレートを使用して証明書の要求生成し、この要求をテンプレートを公開する証明機関のいずれかに送信します。



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。フェデレーション認証サービス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。



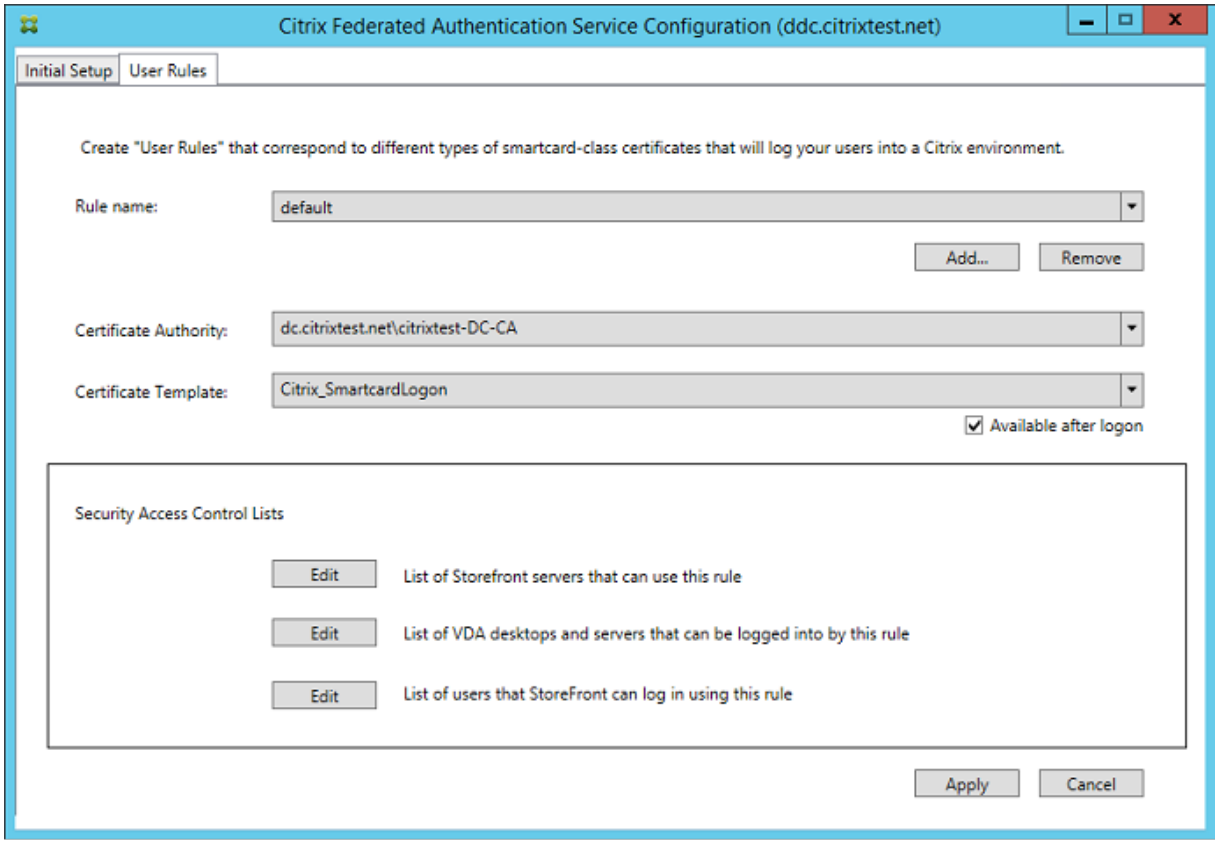
［すべてのタスク］を右クリックしてから、証明書要求に対して［発行］または［拒否］を選択します。フェデレーション認証サービス管理コンソールにより、このプロセスの完了が自動的に検出されます。この処理には数分かかることがあります。



ユーザールールの構成

ユーザールールにより、StoreFront の指示に従って、VDA ログオンおよびセッション中の使用に関する証明書発行の権限が付与されます。各ルールでは、証明書の要求を信頼する StoreFront サーバー、証明書を要求できる一連のユーザー、および証明書の使用を許可する一連の VDA マシンを指定します。

フェデレーション認証サービスのセットアップを完了するには、管理者が FAS 管理コンソールの［ユーザールール］タブに切り替え、Citrix_SmartcardLogon テンプレートの公開先となる証明機関を選択し、StoreFront サーバーの一覧を編集して、デフォルトのルールを定義する必要があります。デフォルトでは、VDA の一覧には各ドメインコンピューターが含まれ、ユーザーの一覧には各ドメインユーザーが含まれます。デフォルトが適切でない場合は、これらを変更できます。



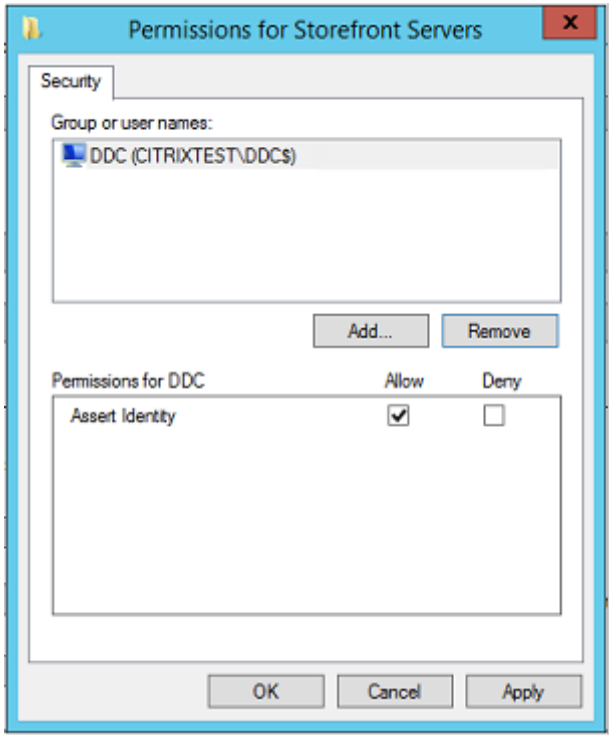
フィールド：

[証明機関および証明書テンプレート]：ユーザー証明書の発行に使用される証明書テンプレートおよび証明機関。これは、Citrix_SmartcardLogon テンプレートまたはこれのコピーを変更したものであり、いずれかの証明機関にはこのテンプレートが公開されている必要があります。

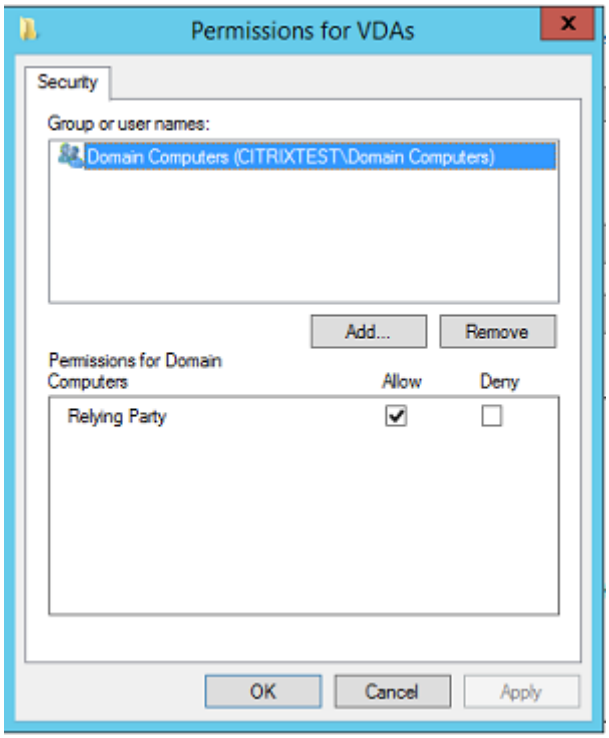
FAS では、フェールオーバーおよび負荷分散のために、PowerShell を使用して複数の証明機関の追加することができます。同様に、コマンドラインと構成ファイルを使用して、より詳細な証明書生成オプションを構成できます。詳しくは、「PowerShell」セクションおよび「ハードウェアセキュリティモジュール」セクションを参照してください。

[セッション内証明書]：[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内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。

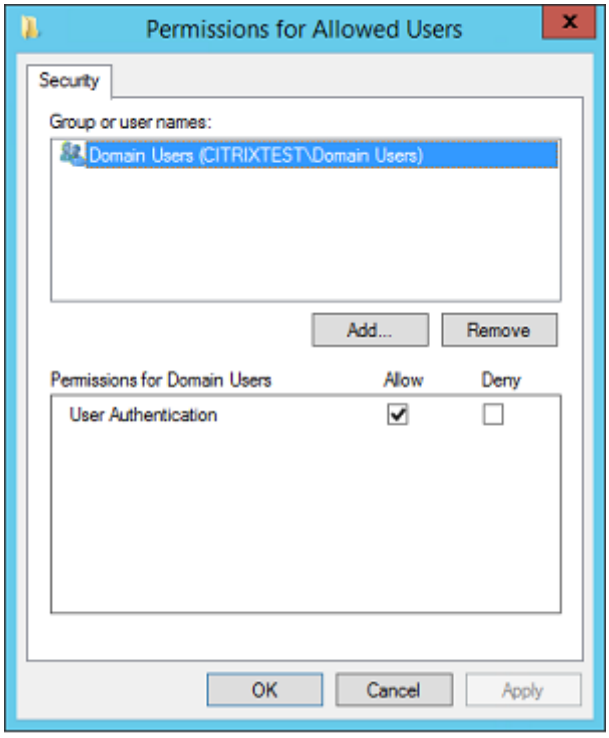
[このルールを使用できる **StoreFront** サーバーの一覧]：ユーザーのログオンまたは再接続用に証明書を要求する権限が付与された、信頼済み StoreFront サーバーの一覧。この設定はセキュリティ上非常に重要であり、慎重に管理する必要があります。



[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]：フェデレーション認証サービス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]：フェデレーション認証サービス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 はフェデレーション認証サービス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。

アップグレードに関する考慮事項

- インプレースアップグレードを行った場合、フェデレーション認証サービスサーバーの設定はすべて保持されます。
- フェデレーション認証サービスのアップグレードは、XenApp および XenDesktop の全製品インストーラーで行ってください。
- フェデレーション認証サービスを 7.15 LTSR から 7.15 LTSR CU2（またはそれ以降のサポート対象 CU）にアップグレードする前に、Delivery Controller と VDA（およびその他のコアコンポーネント）を所定のバージョンにアップグレードしてください。

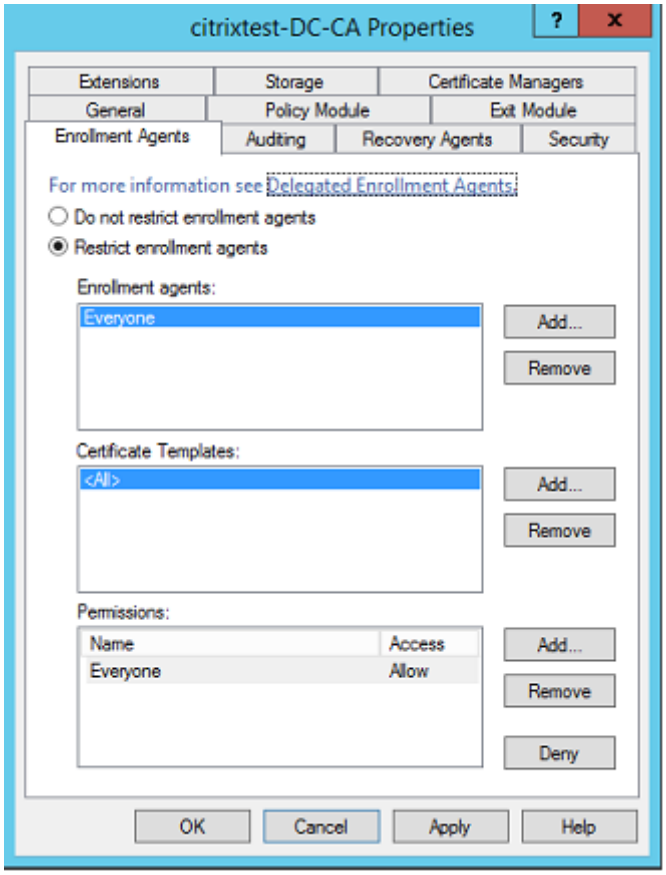
- フェデレーション認証サービスのアップグレード前に、フェデレーション認証サービスコンソールを必ず閉じてください。
- 1 台以上のフェデレーション認証サービスサーバーを常に利用可能な状態に維持してください。フェデレーション認証サービスに対応した StoreFront サーバーから到達可能なサーバーがない場合、ユーザーはログオンやアプリケーションの起動を行えなくなります。

セキュリティに関する注意事項

フェデレーション認証サービスには、フェデレーション認証サービス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

FAS は登録エージェントとして機能することによってユーザー証明書を発行します。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。



フェデレーション認証サービス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フェデ

レーション認証サービス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

「ユーザー規則の構成」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フェデレーション認証サービスに対するユーザー 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

フェデレーション認証サービスおよび 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

フェデレーション認証サービス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。フェデレーション認証サービスは、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。

パラメーター	説明
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フェデレーション認証サービス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、Citrix では PowerShell のみを使用して構成を行うことをお勧めします。

次のコマンドによって PowerShell コマンドレットが追加されます。

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Get-Help <*cmdlet name*> を使用すると、コマンドレットのヘルプが表示されます。次の表にいくつかのコマンドの一覧を示します。「*」は標準の PowerShell の動詞を表します（New、Get、Set、Remove など）。

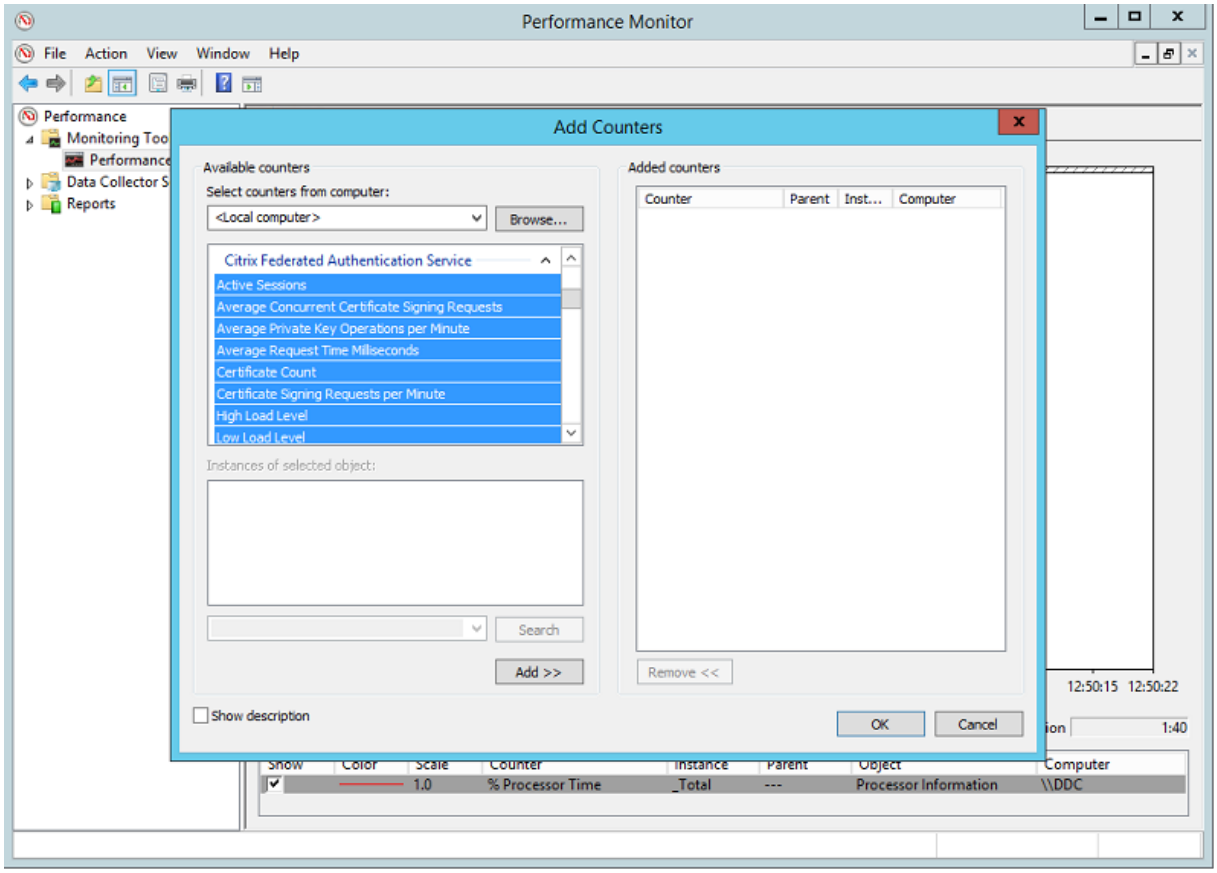
コマンド	概要
*-FasServer	現在の環境の FAS サーバーを一覧表示および再構成します。
*-FasAuthorizationCertificate	登録機関証明書を管理します。
*-FasCertificateDefinition	FAS が証明書の生成に使用するパラメーターを制御します。
*-FasRule	フェデレーション認証サービスで構成済みのユーザールールを管理します。
*-FasUserCertificate	フェデレーション認証サービスによってキャッシュされた証明書を一覧表示および管理します。

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

フェデレーション認証サービスには、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	フェデレーション認証サービス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。
Certificate Count	フェデレーション認証サービスでキャッシュされた証明書の数。

名前	説明
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」の観点からフェデレーション認証サービス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、フェデレーション認証サービス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、フェデレーション認証サービス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 フェデレーション認証サービスは 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［フェデレーション認証サービス］

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、ランタイム時にフェデレーション認証サービス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［フェデレーション認証サービス］

これらのイベントは、VDA にユーザーがログオンすると、ランタイム時にフェデレーション認証サービスサーバーに記録されます。

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}］

ログコード
[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 [フェデレーション認証サービス]

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、フェデレーション認証サービス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。認識できないフェデレーション認証サービス [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。フェデレーション認証サービス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

ログコード
[S107] ID アサーションログオンに失敗しました。[例外：{1}{2}]
[S108] ID アサーションサブシステム。ACCESS_DENIED [呼び出し元：{0}]

セッション内証明書 [**VDA**]

これらのイベントは、ユーザーがセッション内証明書を使用しようとすると、VDA に記録されます。

ログコード
[S201] 仮想スマートカードが認証されました [ユーザー：{0}] [PID：{1}、名前：{2}] [証明書 {3}]
[S202] 仮想スマートカードサブシステム。セッション {0} で使用可能なスマートカードはありません
[S203] 仮想スマートカードサブシステム。アクセスが拒否されました [呼び出し元：{0}、セッション：{1}、予測：{2}]
[S204] 仮想スマートカードサブシステム。スマートカードのサポートが無効化されました。

証明書要求および生成コード [フェデレーション認証サービス]

[イベントソース：Citrix.TrustFabric]

これらの低レベルイベントは、フェデレーション認証サービス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

ログコード
[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

ログコード
[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、「フェデレーション認証サービスのアーキテクチャの概要」を参照してください。
- 「フェデレーション認証サービスの構成と管理」では「方法」の記事を紹介しています。

フェデレーション認証サービスのアーキテクチャの概要

August 24, 2021

はじめに

フェデレーション認証サービス（FAS）は Active Directory 証明機関（CA）と統合して、Citrix 環境内でのシームレスなユーザー認証を実現する Citrix コンポーネントです。このドキュメントでは、環境に適した、さまざまな認証アーキテクチャについて説明します。

FAS が有効化されると、信頼された StoreFront サーバーにユーザー認証の判断が委任されます。StoreFront は最新の Web テクノロジを中心に構築されたビルトイン認証オプションの包括的なセットを搭載しており、StoreFront SDK やサードパーティの IIS プラグインを使用して容易に拡張できます。基本的な設計目標は、Web サイトへのユーザー認証が可能なすべての認証テクノロジを、Citrix XenApp または XenDesktop の展開へのログインに活用することです。

このドキュメントでは、複雑さを増す上位レベルの展開アーキテクチャについて、例をいくつか説明します。

- 内部展開
- NetScaler Gateway の展開
- ADFS SAML
- B2B アカウントのマッピング
- Windows 10 Azure AD への参加

FAS 関連記事にリンクしています。すべてのアーキテクチャにおける FAS のセットアップについては「Federated Authentication Service」を参照してください。

機能

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。

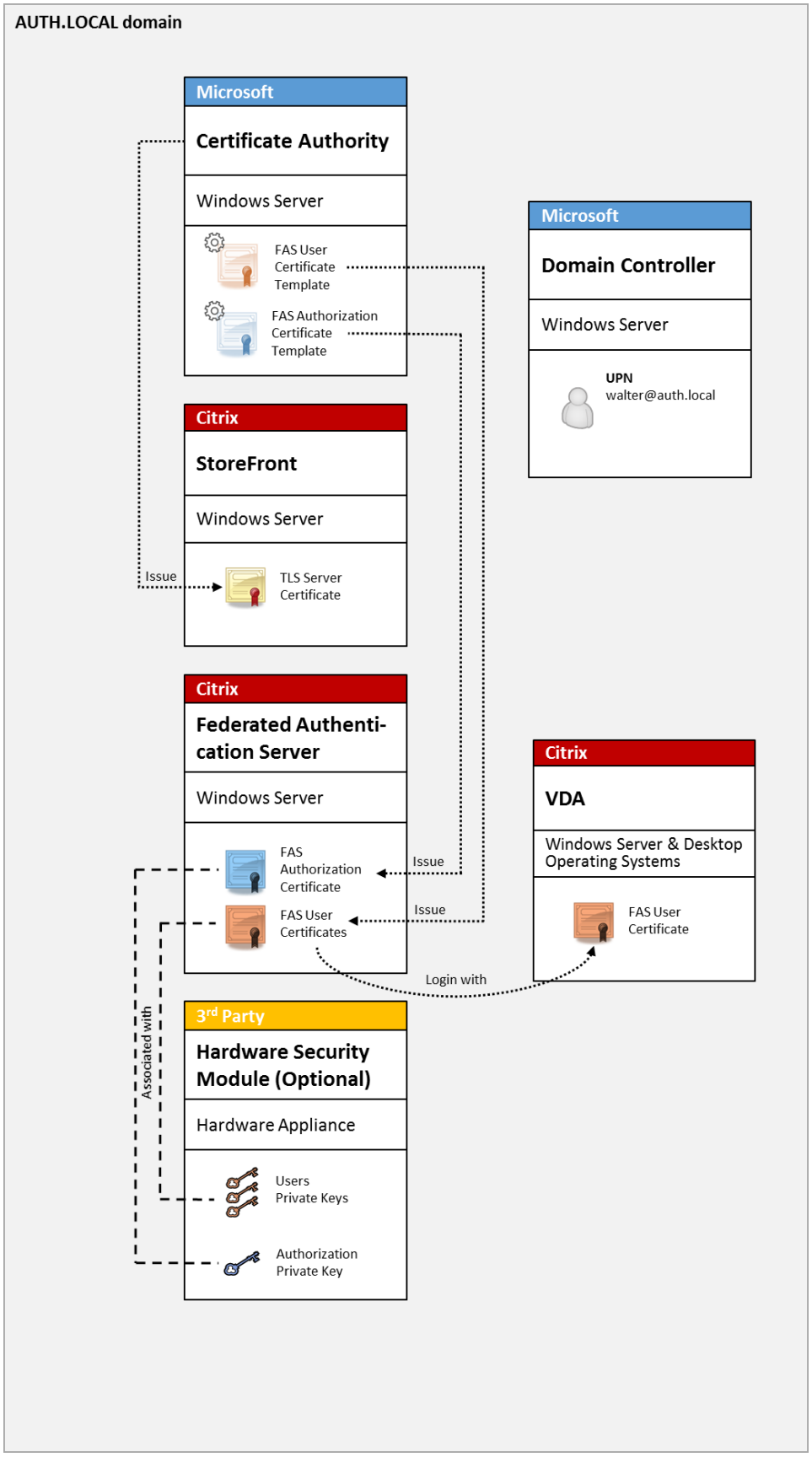
内部展開

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。）

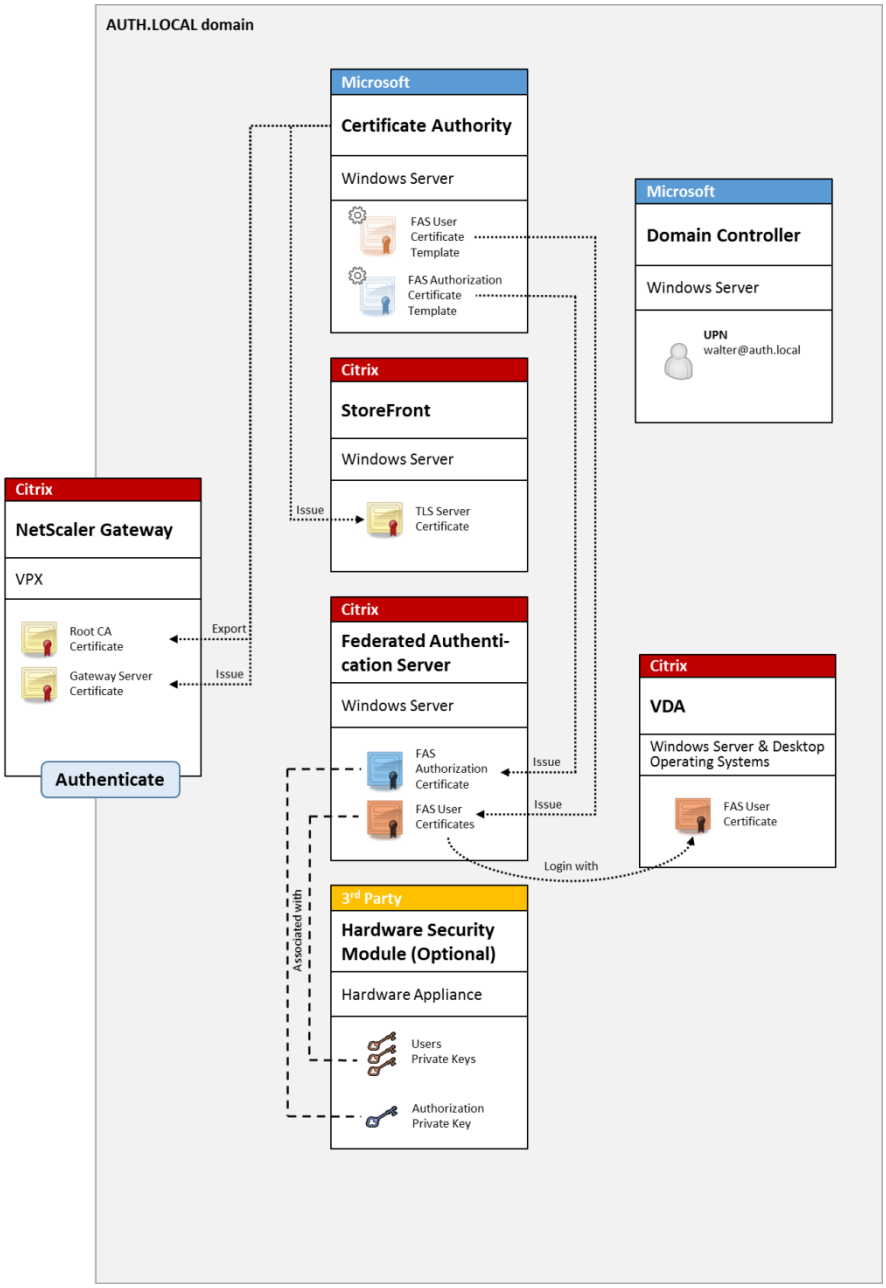
関連情報:

- 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、「フェデレーション認証サービスの秘密キー保護」を参照してください。
- 「Federated Authentication Service」では、FAS のインストールと構成の方法について説明します。

NetScaler Gateway の展開

NetScaler の展開は内部展開と似ていますが、StoreFront と組み合わせた Citrix NetScaler Gateway が追加されており、認証のプライマリポイントが NetScaler そのものに移動されています。Citrix NetScaler には、企業 Web サイトへのリモートアクセスの保護に使用できる、認証および承認の高度なオプションが含まれています。

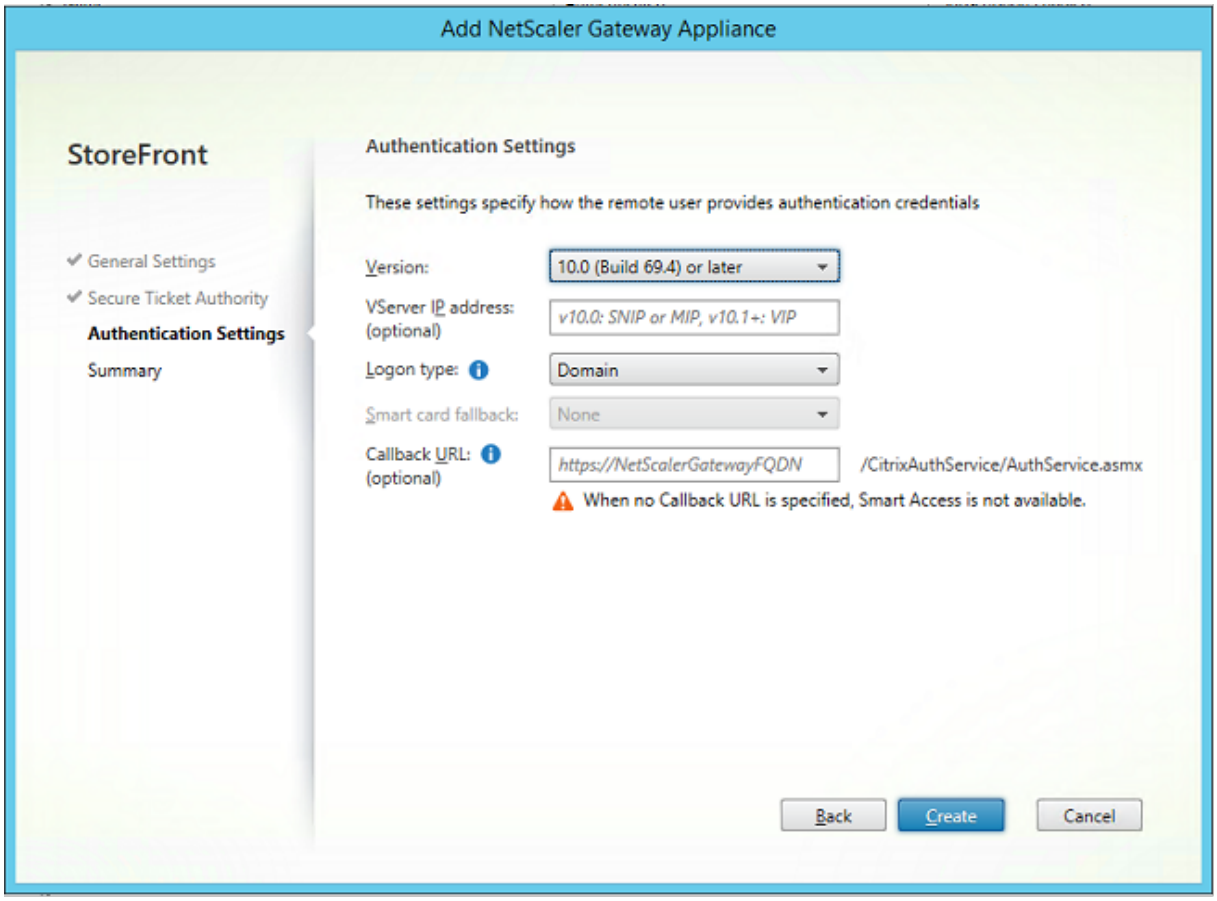
この展開を利用すれば、NetScaler への初回認証時およびユーザーセッションへのログイン時に、何度も PIN の入力が求められることはありません。また、AD パスワードやスマートカードを必要とせずに、高度な NetScaler 認証テクノロジを利用することができます。



XenApp または XenDesktop 環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加する Microsoft 証明機関（CA）を利用可能にし、ドメインコントローラーにドメインコントローラー証明書を割り当てるだけで済みます。（CTX206156 の「Issuing Domain Controller Certificates」セクションを参照してください）。

NetScaler をプライマリ認証システムとして構成する場合は、NetScaler と StoreFront 間のすべての接続を TLS で保護するようにします。特に、この展開では NetScaler サーバーの認証にコールバック URL が使用されるため、コールバック URL が NetScaler サーバーを指すよう正しく構成する必要があります。

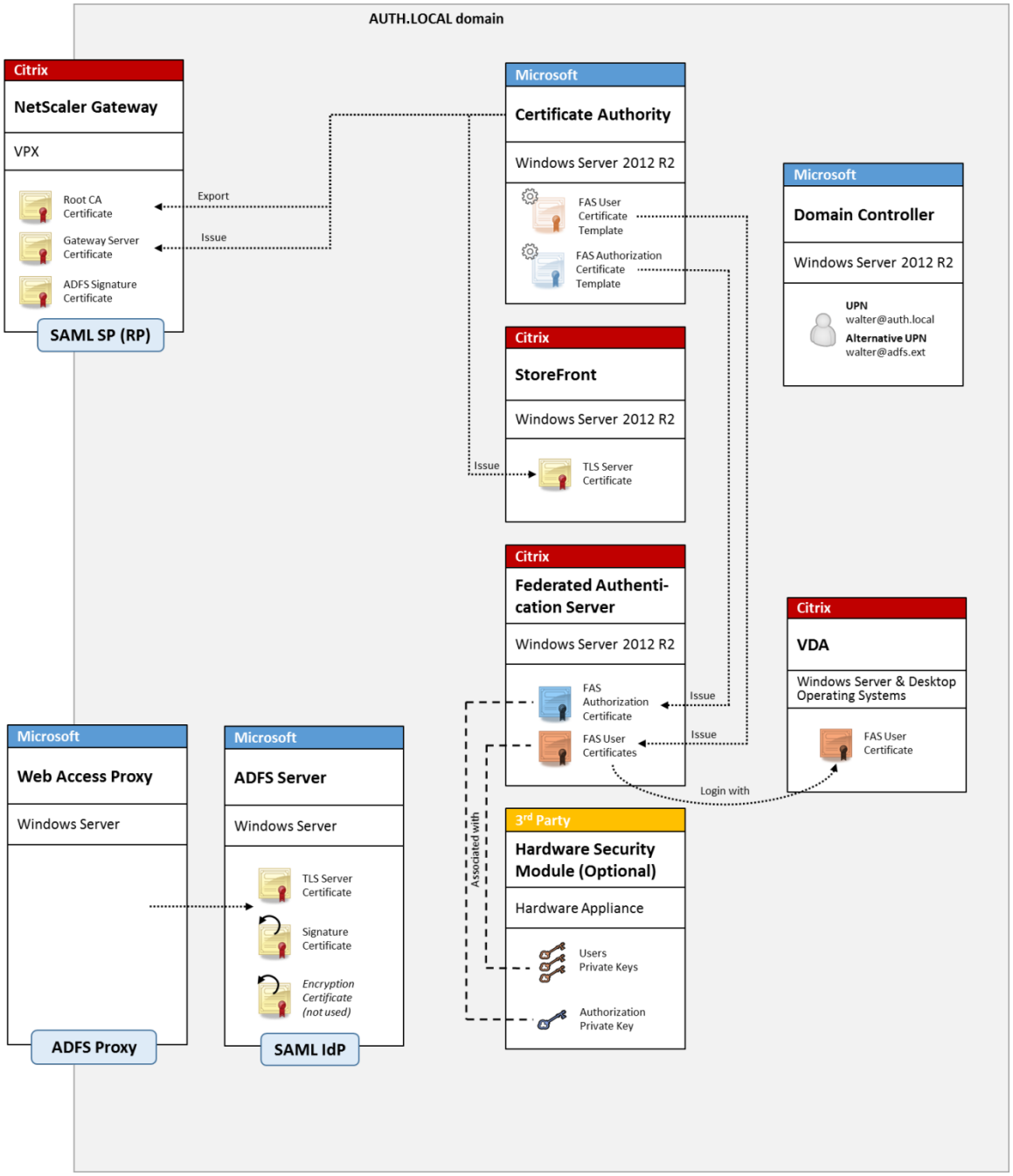


関連情報:

- NetScaler Gateway を構成するには、「How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6」を参照してください。
- 「フェデレーション認証サービス」では、FAS のインストールと構成の方法について説明します。

ADFS SAML の展開

NetScaler の主要な認証テクノロジにより、SAML ID プロバイダー（IdP）として機能できる、Microsoft ADFS との統合が実現します。SAML アサーションは暗号を使用して署名された XML ブロックであり、コンピューターシステムへのユーザーのログオンを承認する、信頼された IdP によって発行されます。つまり、FAS サーバーによって、Microsoft ADFS サーバー（またはほかの SAML 対応 IdP）へのユーザー認証の委任が許可されます。



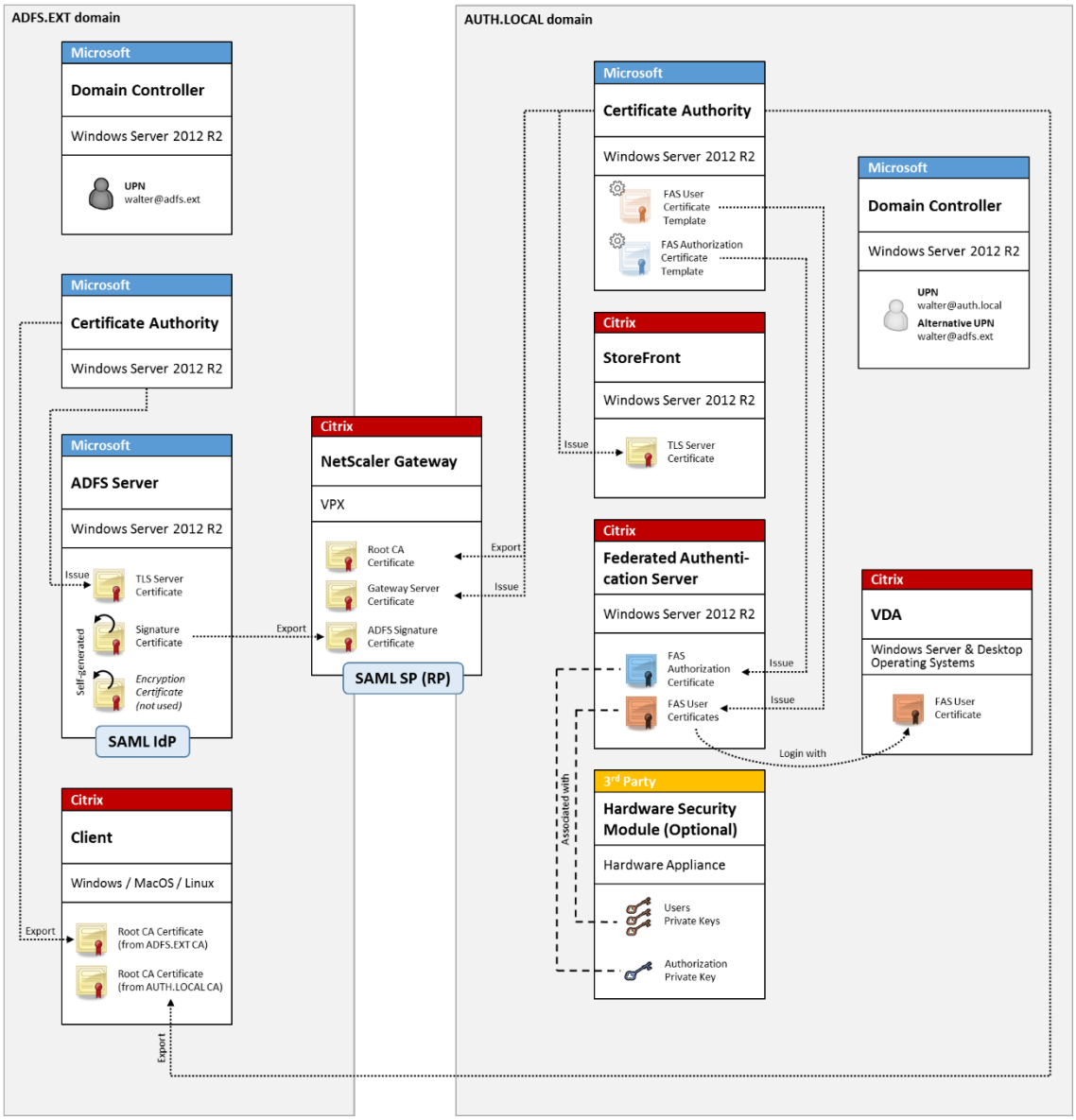
ADFS は、一般的にインターネットを利用して企業リソースにリモートでユーザーを安全に認証するために使用され、たとえば、Office 365 の統合に多く利用されます。

関連情報:

- 詳しくは、「フェデレーション認証サービスの ADFS の展開」を参照してください。
- FAS のインストールと構成の方法については、「フェデレーション認証サービス」で説明しています。
- 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。

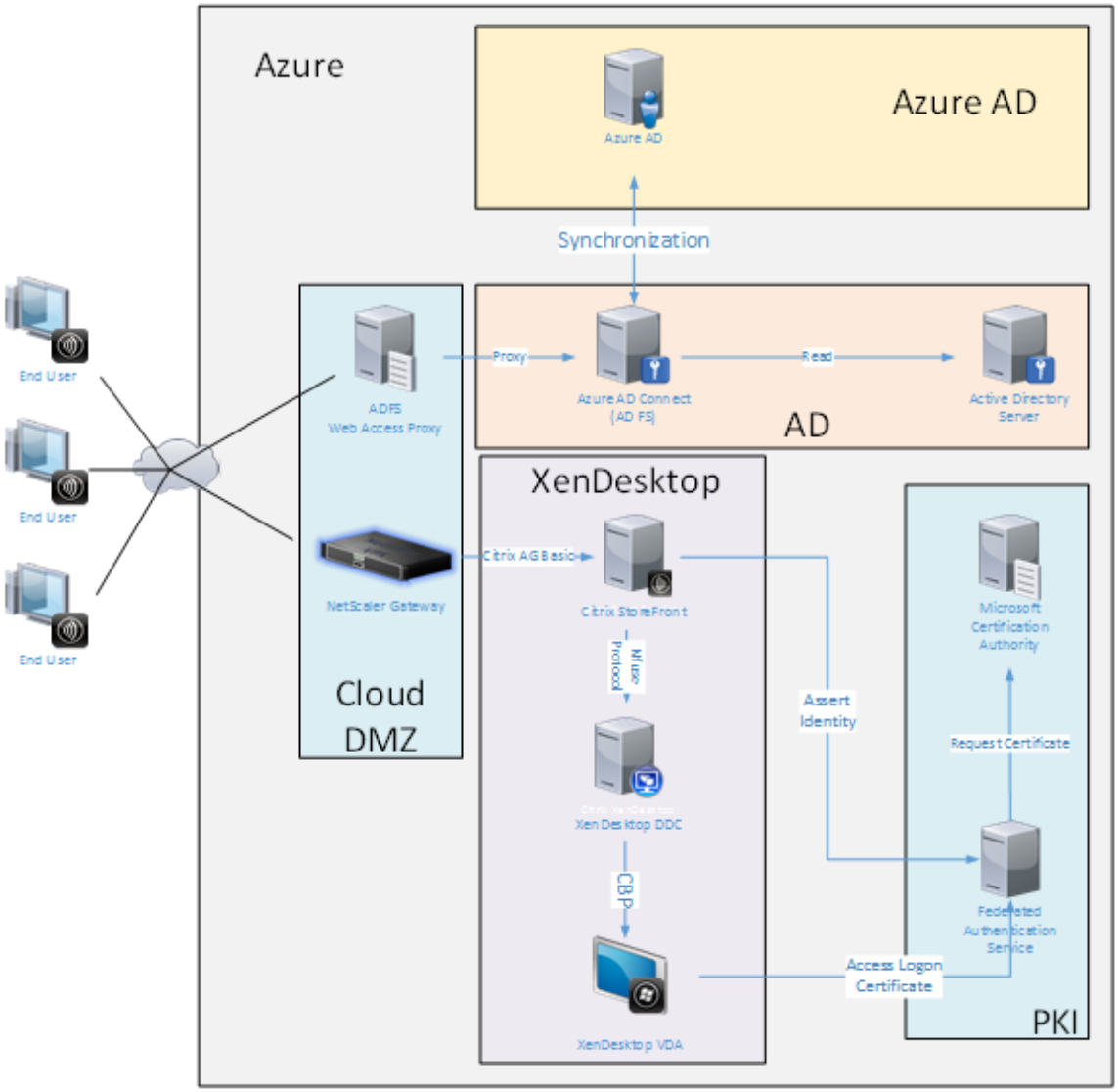


関連情報：

- FAS のインストールと構成の方法については、「フェデレーション認証サービス」で説明しています。

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、事実上「オフィスにいるエンドユーザー」の概念のない一例です。ラップトップコンピューターは最新の Azure AD 機能を使用して完全にインターネット経由で登録および認証されています。

この展開では、IP アドレスが使用可能なすべての場所、つまりオンプレミス、ホストされたプロバイダー、Azure、あるいはそのほかのクラウドプロバイダーで、インフラストラクチャが実行できる点に注意してください。Azure AD Connect の同期機能により、自動的に Azure AD に接続します。例として示した図では、簡単にするために Azure 仮想マシンを使用しています。

関連情報:

- FAS のインストールと構成の方法については、「フェデレーション認証サービス」で説明しています。
- 詳しくは、「Federated Authentication Service の Azure AD の統合」を参照してください。

フェデレーション認証サービスの **ADFS** の展開

August 24, 2021

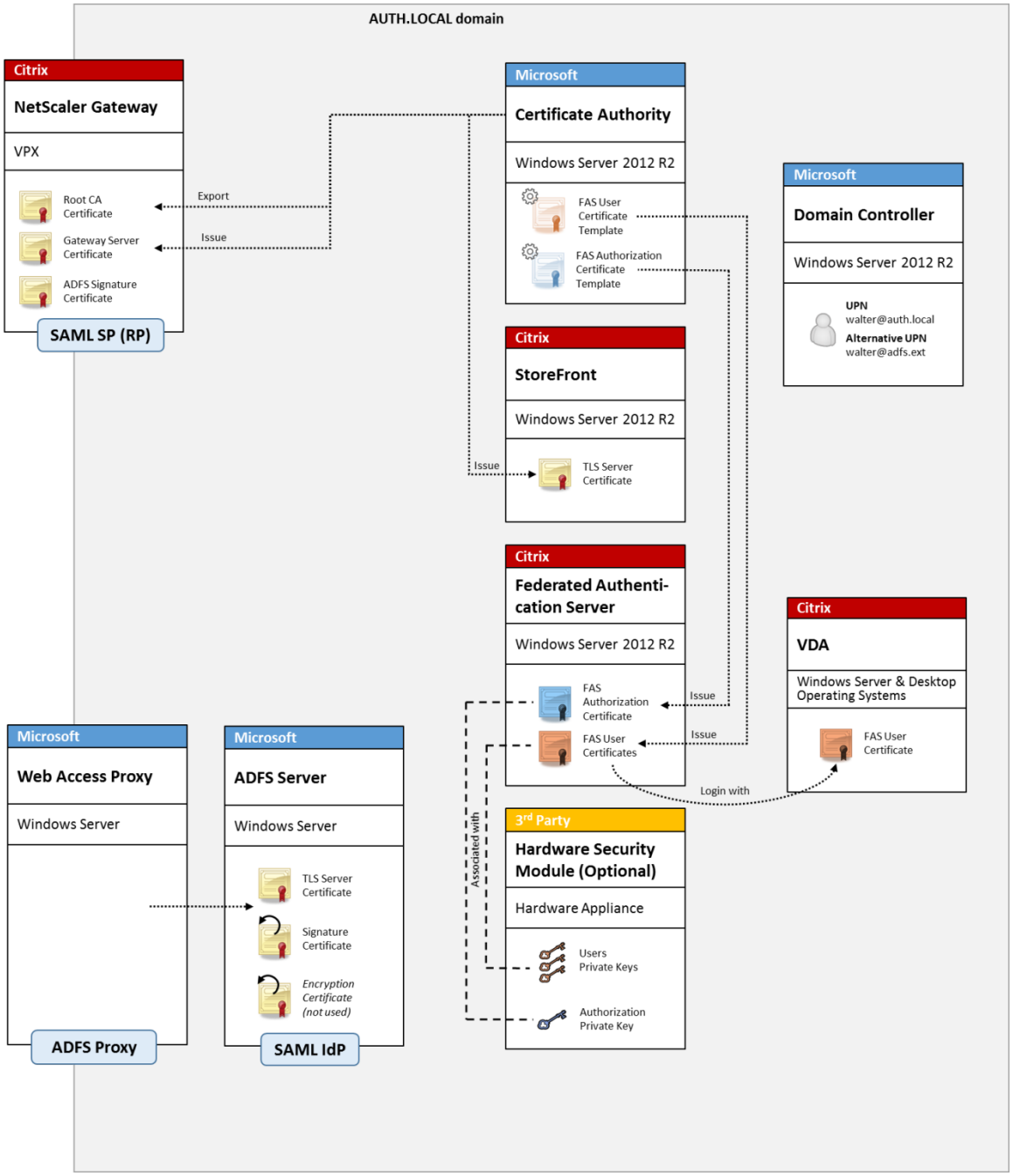
はじめに

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、フェデレーション認証サービス（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 ブラウザーのログオンシステムです。構成には次の項目が含まれます。

リダイレクト **URL**［シングルサインオンサービス **URL**］

ユーザー認証の必要があることを NetScaler が検出すると、NetScaler はユーザーが使用する Web ブラウザーに、ADFS サーバー上の SAML ログオン Web ページに HTTP POST を実行するよう指示します。この URL 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、NetScaler および ADFS から認められればどのような URL も使用できます（例：`https://ns.mycompany.com/application/logonpage`）。

リターンアドレス［応答 **URL**］

認証に成功すると、ADFS はユーザーの Web ブラウザーに、EntityID のために構成された応答 URL の 1 つに、SAML 認証 XML を POST し返すよう指示します。この URL は、通常は元の NetScaler サーバー上での次の形式の`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。

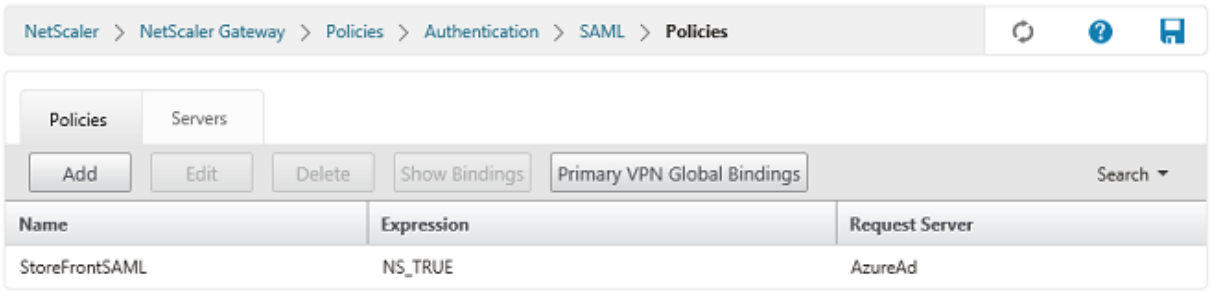
シングルサインアウト **URL**［シングルログアウト **URL**］

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。この URL 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。）

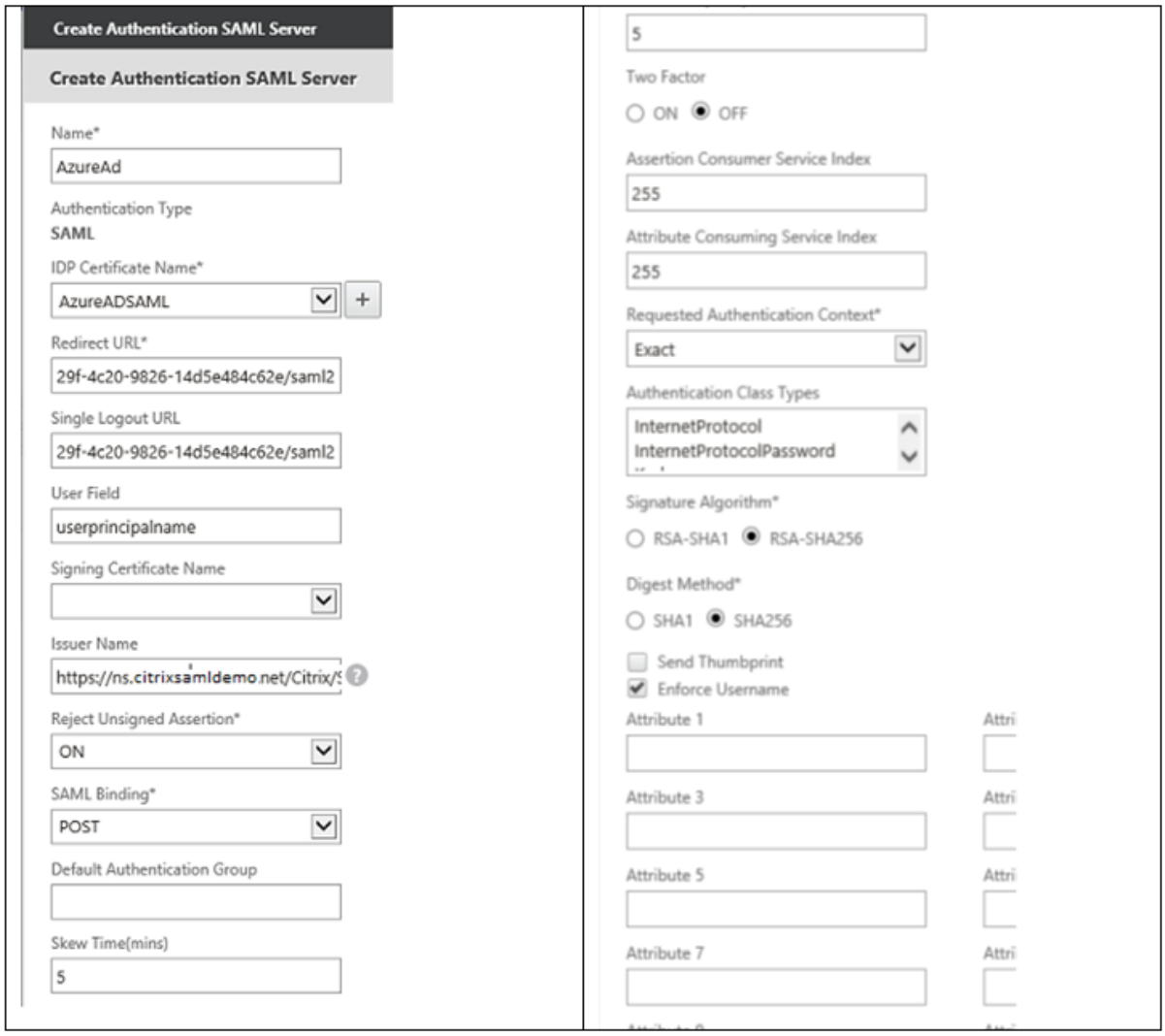
構成

「フェデレーション認証サービスアーキテクチャ」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。



SAML ポリシーの記入

ADFS 管理コンソールから前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。このポリシーが適用されると、NetScaler はログオンのためにユーザーを ADFS-signed にリダイレクトし、ADFS の署名した SAML 認証トークンを代わりに受け取ります。



関連情報

- FAS のインストールと構成については、「Federated Authentication Service」を参照してください。
- 一般的な FAS 環境については、「フェデレーション認証サービスのアーキテクチャの概要」を参照してください。
- 「フェデレーション認証サービスの構成と管理」では「方法」の記事を紹介しています。

フェデレーション認証サービスの **Azure AD** の統合

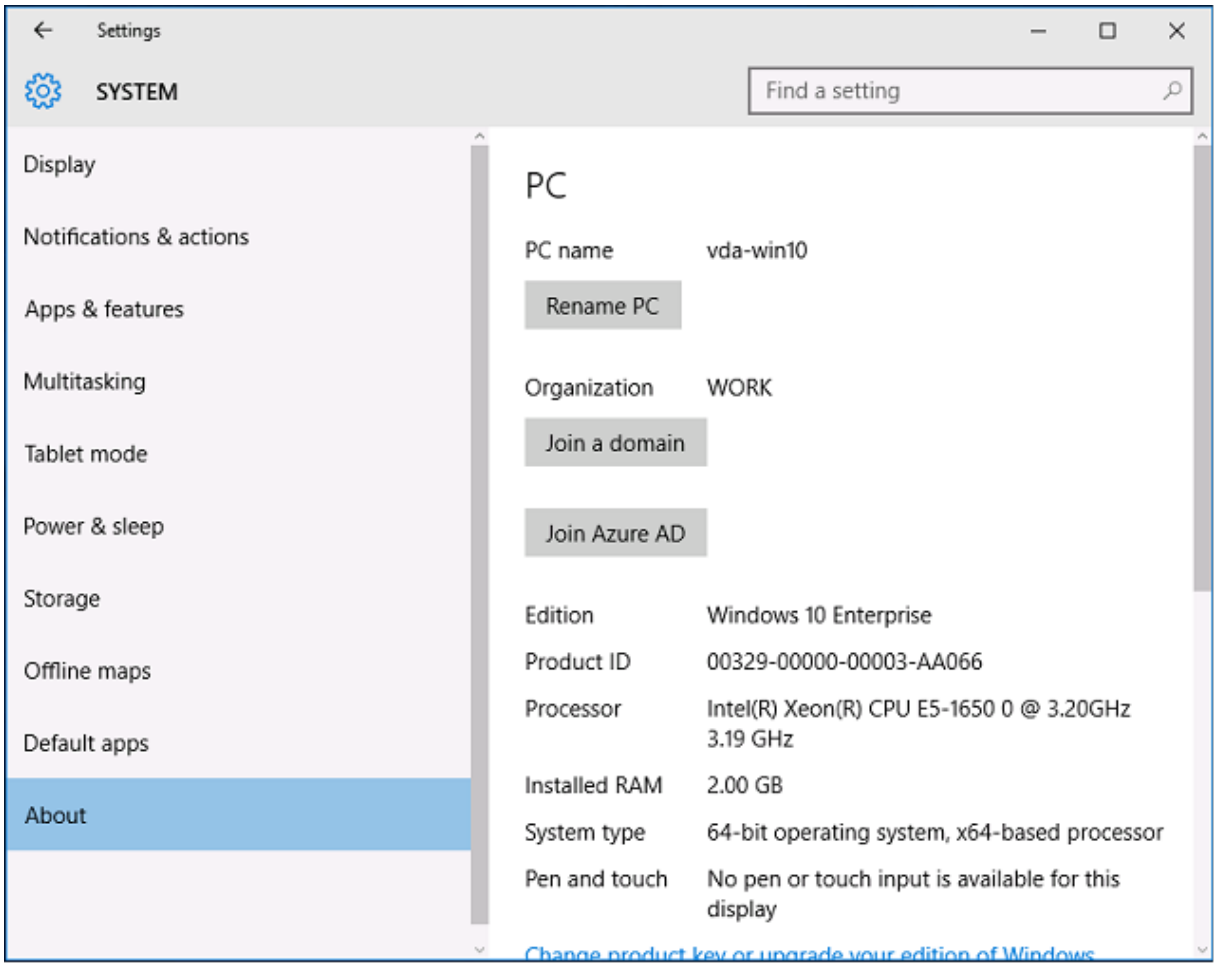
August 24, 2021

はじめに

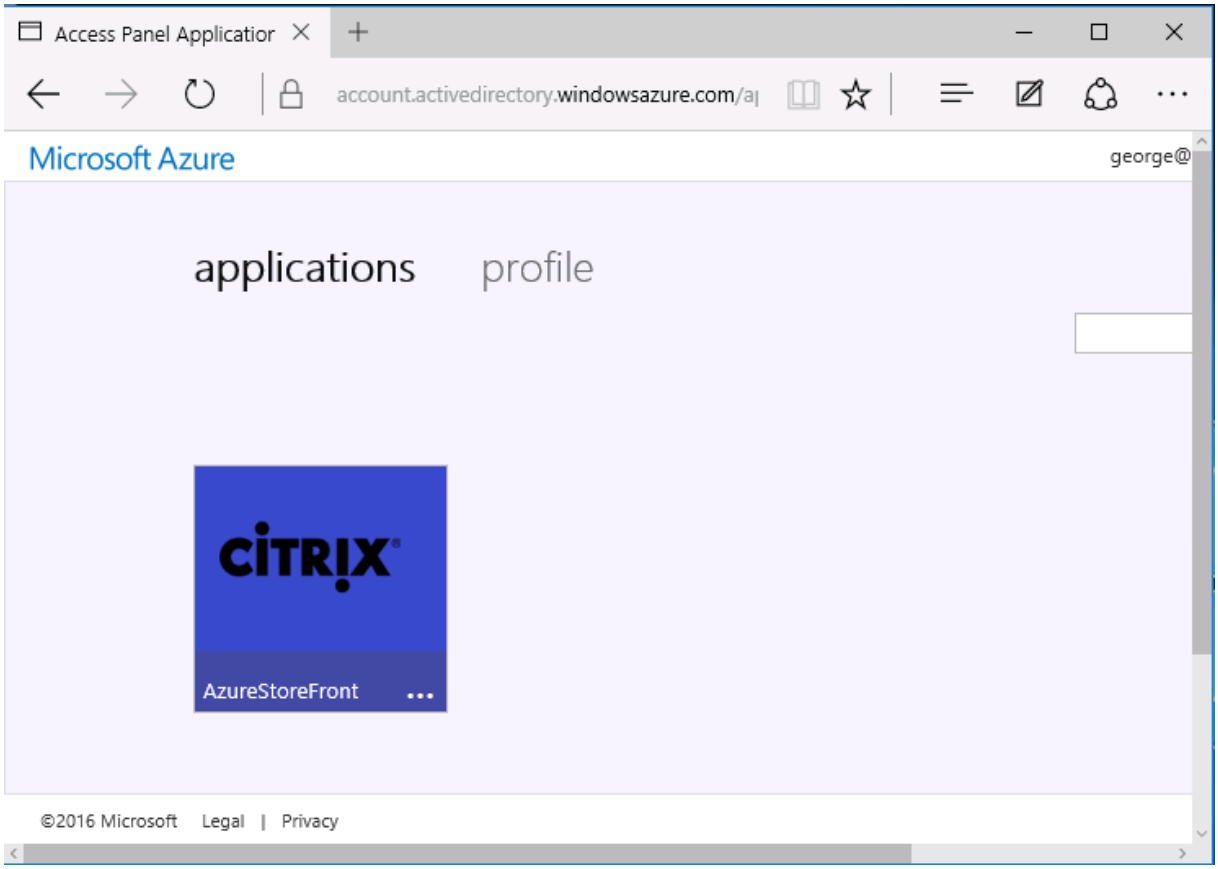
このドキュメントでは、Citrix 環境を Windows 10 Azure AD 機能と統合する方法について説明します。

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。



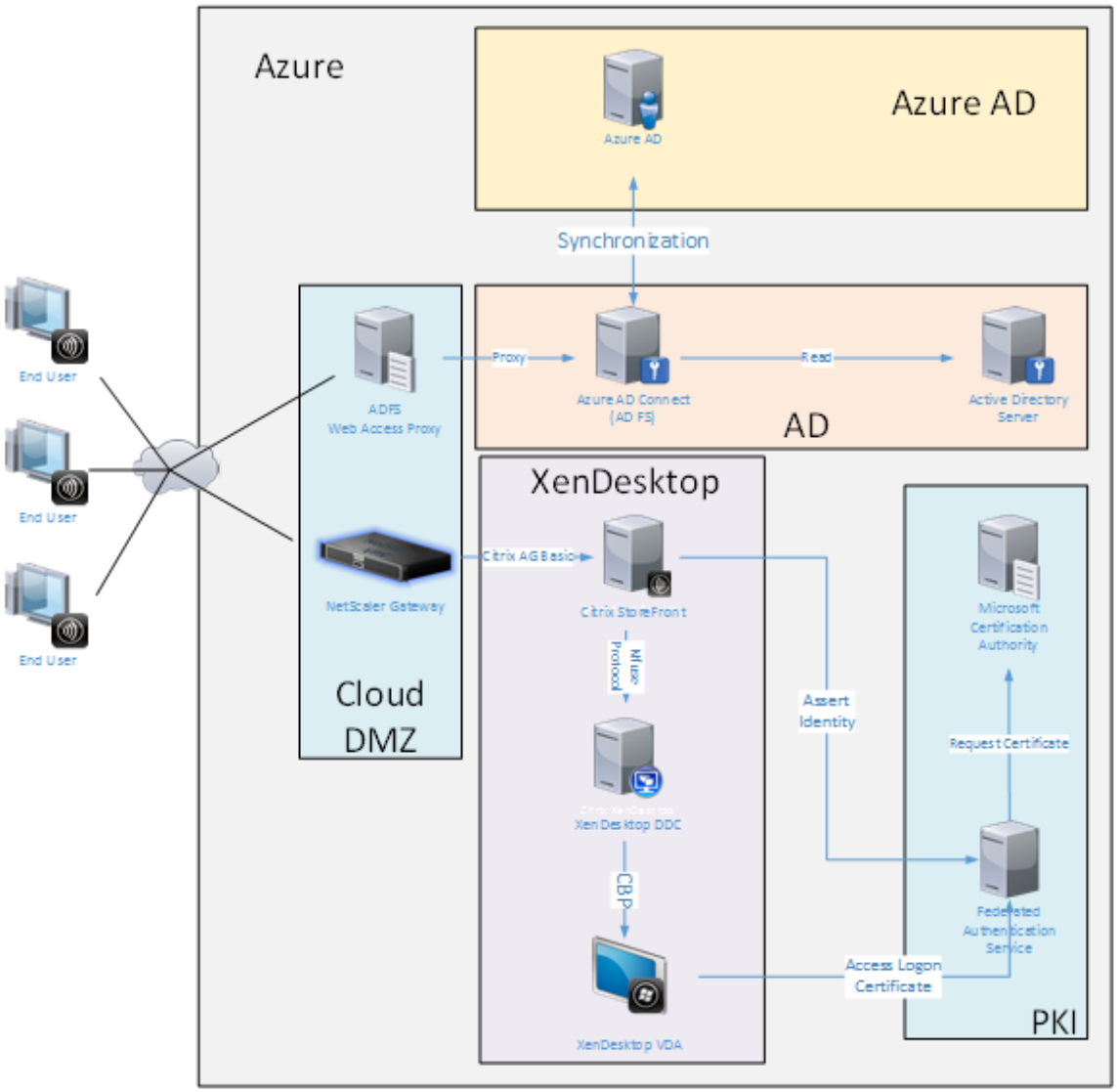
ラップトップが登録されると、Microsoft Edge の Web ブラウザーは、Azure SaaS アプリケーションの Web ページから、会社の Web サイトや Citrix の公開アプリケーション、および Office 365 などの Azure アプリケーションに自動的にサインオンします。



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。



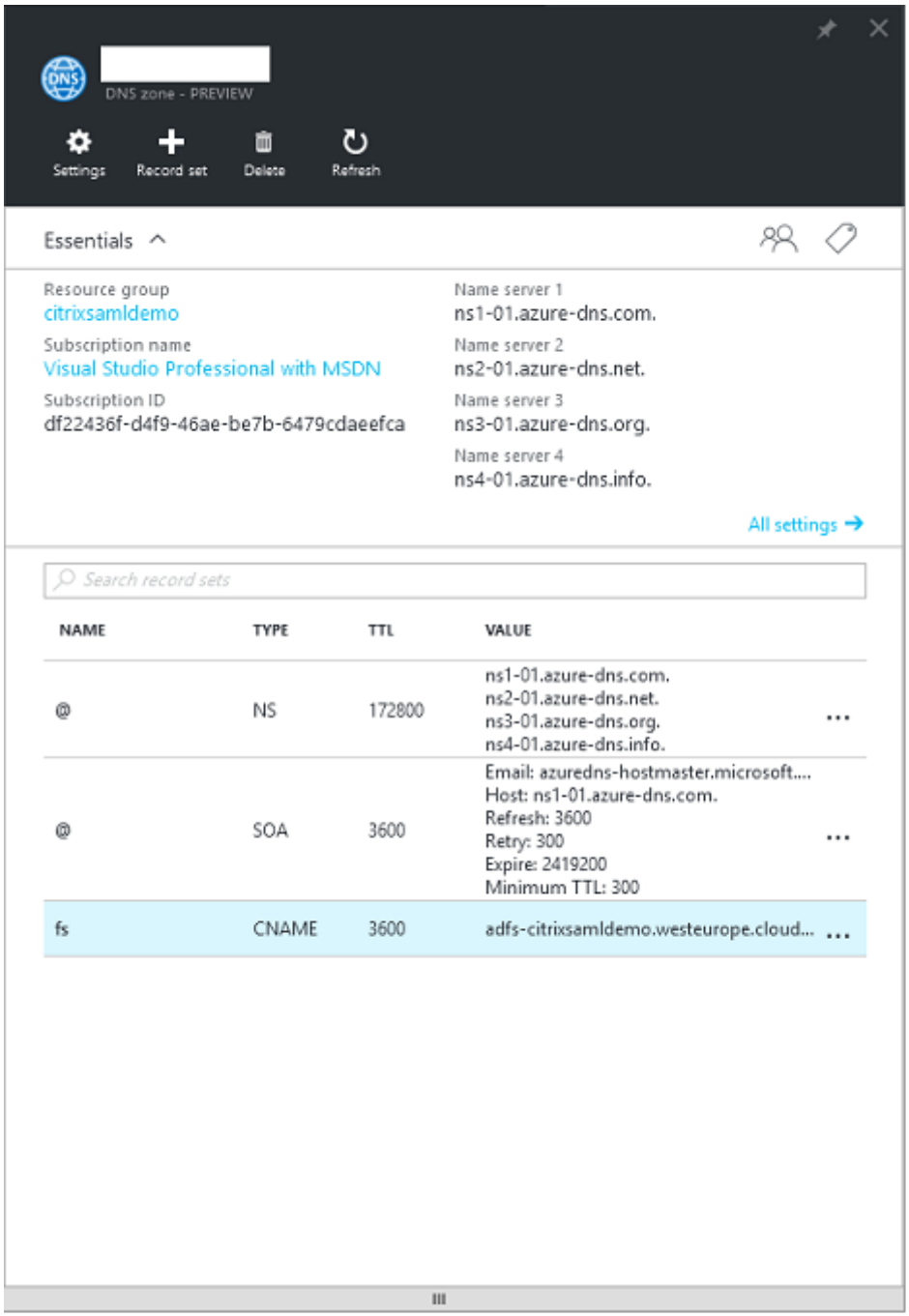
セキュアな接続やシングルサインオンといえば、従来はファイアウォールで保護された LAN や、Kerberos 認証および NTLM 認証でしたが、このアーキテクチャでは、Azure への TLS 接続および SAML がこれらに取って代わります。Azure アプリケーションの Azure AD への参加により、新しいサービスが生み出されています。Active Directory を必要とする既存のアプリケーション（SQL Server データベースなど）は、Azure クラウドサービスの IaaS 部分にある、標準的な Active Directory サーバーの仮想マシンを使用して実行できます。

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）。

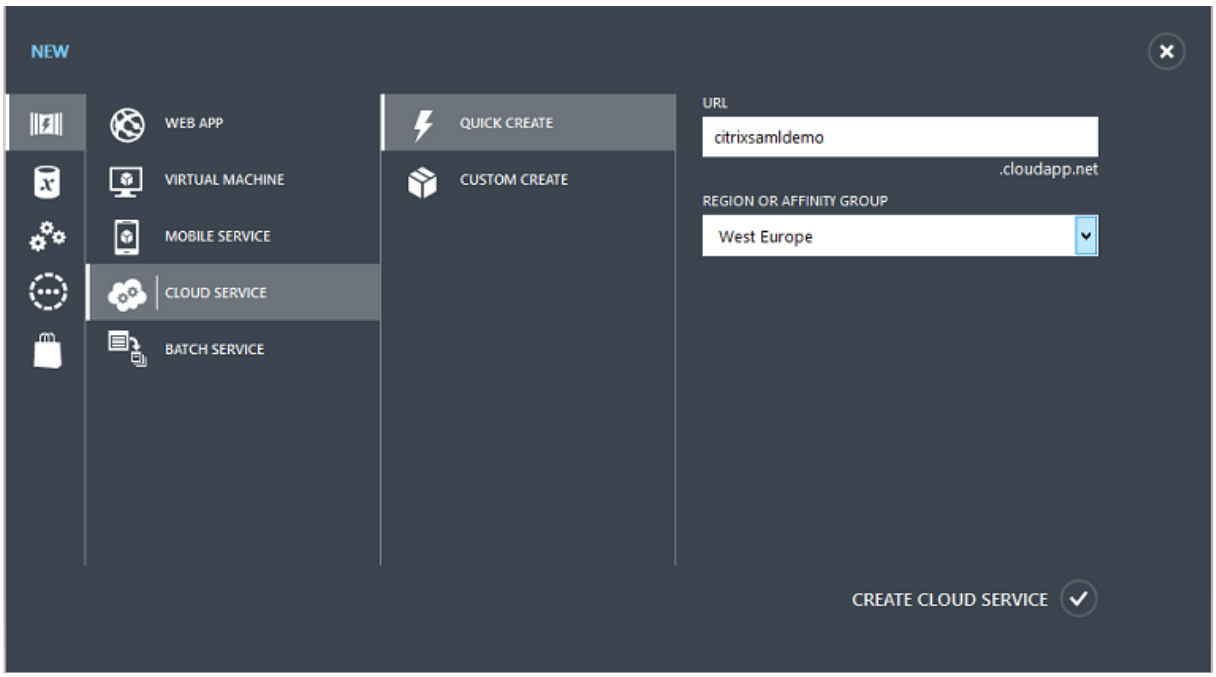
Azure で実行される仮想マシンへの参照を追加する場合は、CNAME ポインターを、Azure が管理する仮想マシンの DNS レコードに使用するのが最も簡単です。仮想マシンの IP アドレスが変更されている場合は、DNS ゾーンファイルを手動で更新する必要はありません。

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

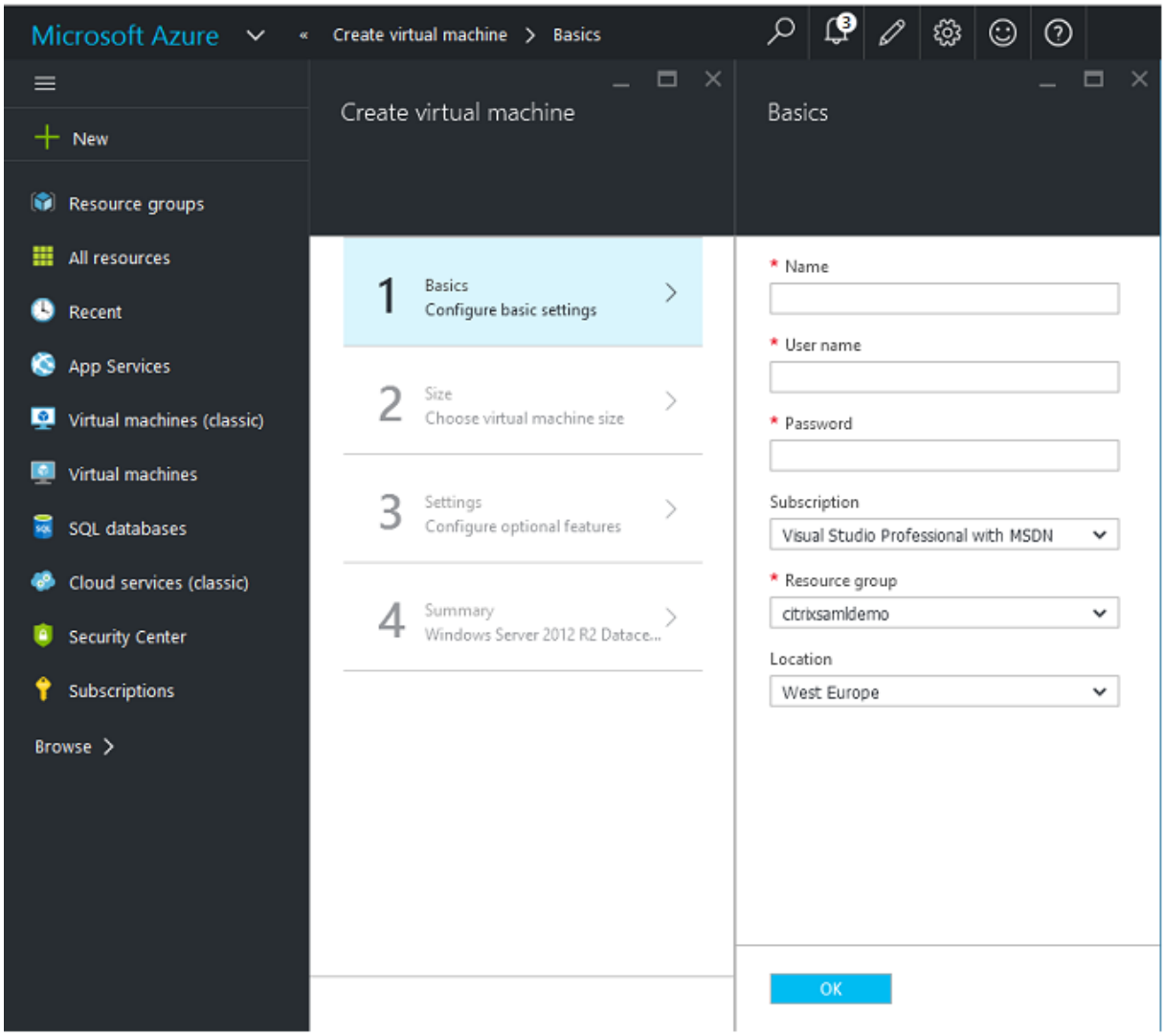
この例では、Azure で実行される ADFS サーバーが設置された AD 環境を含む、Citrix 環境を構成します。クラウドサービスを作成し、「citrixsamldemo」と名づけます。



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、citrixsamldemo.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@citrixsamldemo.net）。
- このサーバーでは内部 DNS が実行されるため、すべてのサーバーは DNS 解決にこのサーバーを参照する必要があります。これは、［**Azure DNS** 設定］ページで行います。（詳しくは、このドキュメントの付録を参照してください。）

ADFS コントローラーと **Web** アプリケーションプロキシサーバー

- ADFS サーバーを citrixsamldemo ドメインに参加させます。Web アプリケーションプロキシサーバーは、分離されたワークグループにとどまる必要があるため、AD DNS で DNS アドレスを手動で登録します。

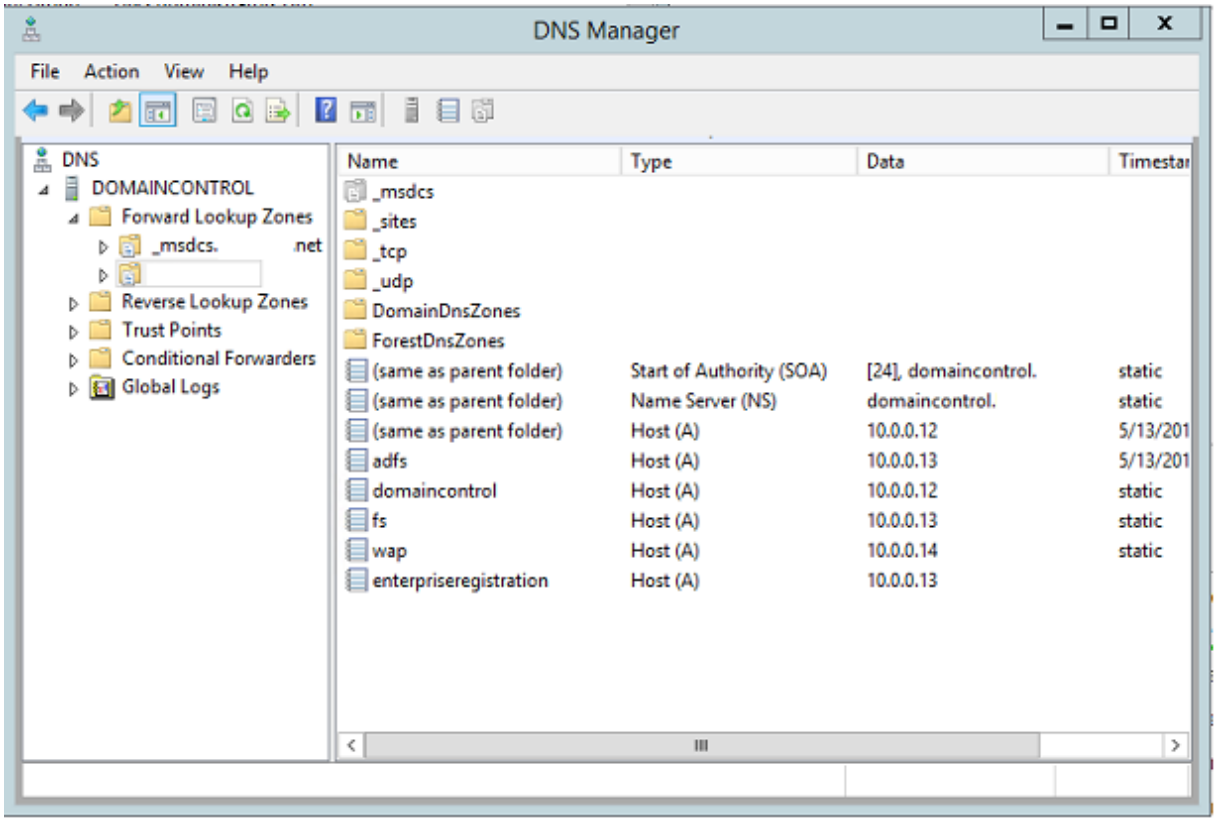
- これらのサーバーで **Enable-PSRemoting –Force** コマンドレットを実行して、Azure AD Connect ツールからファイアウォール経由の PS リモーティングを有効にします。

XenDesktop Delivery Controller と **VDA**

- XenApp または XenDesktop Delivery Controller、および VDA を、citrixsamldemo に参加した残り 2 台の Windows サーバーにインストールします。

内部 **DNS** の構成

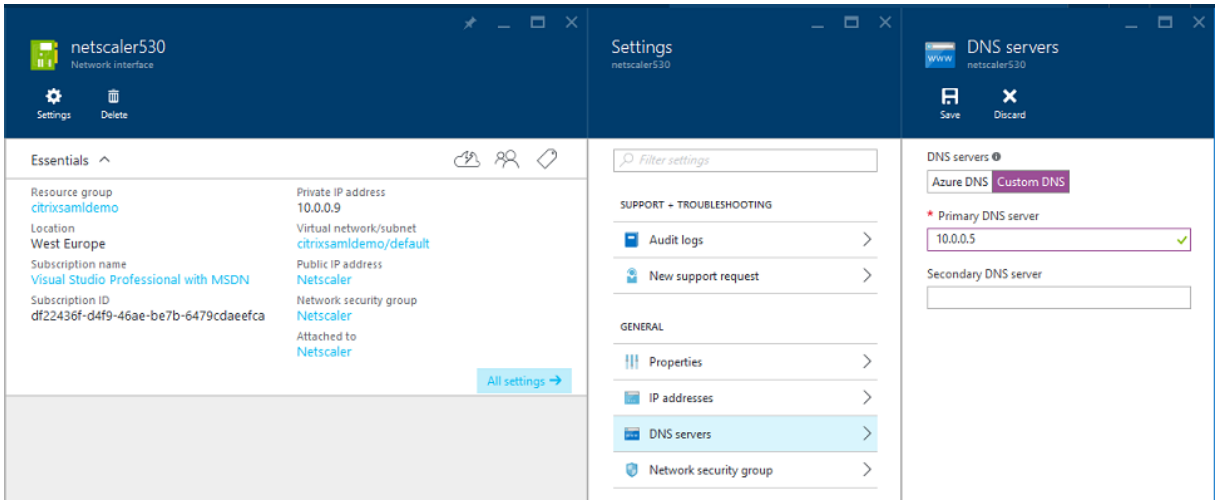
ドメインコントローラーのインストール後に DNS サーバーを構成し、citrixsamldemo.net の内部ビューを処理し、外部 DNS サーバーに対してフォワーダーとして機能するように設定します（例：8.8.8.8）。



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］

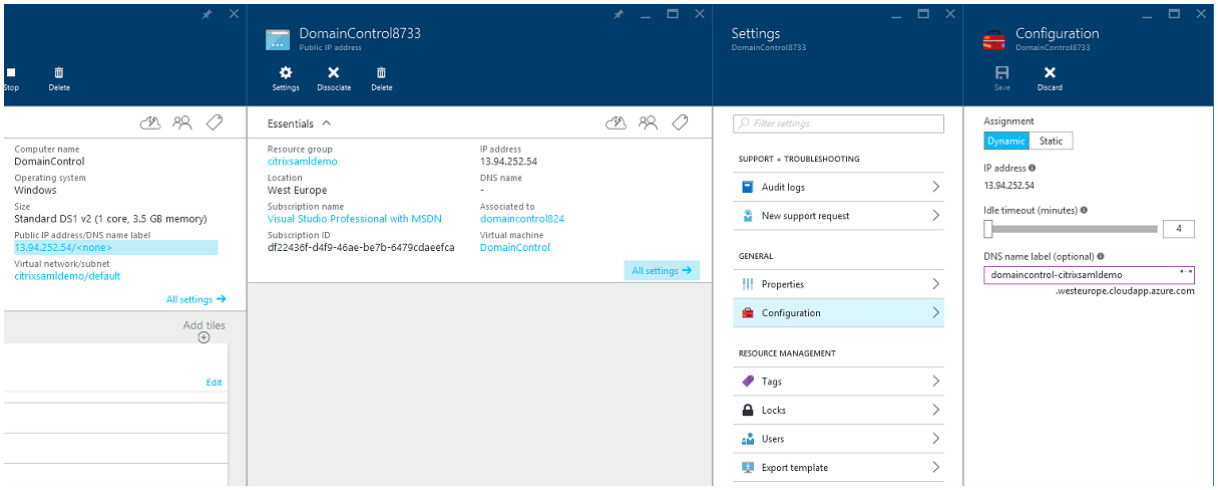
Azure で実行されるすべての仮想マシンは、この DNS サーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェイス GUI から実行できます。



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。

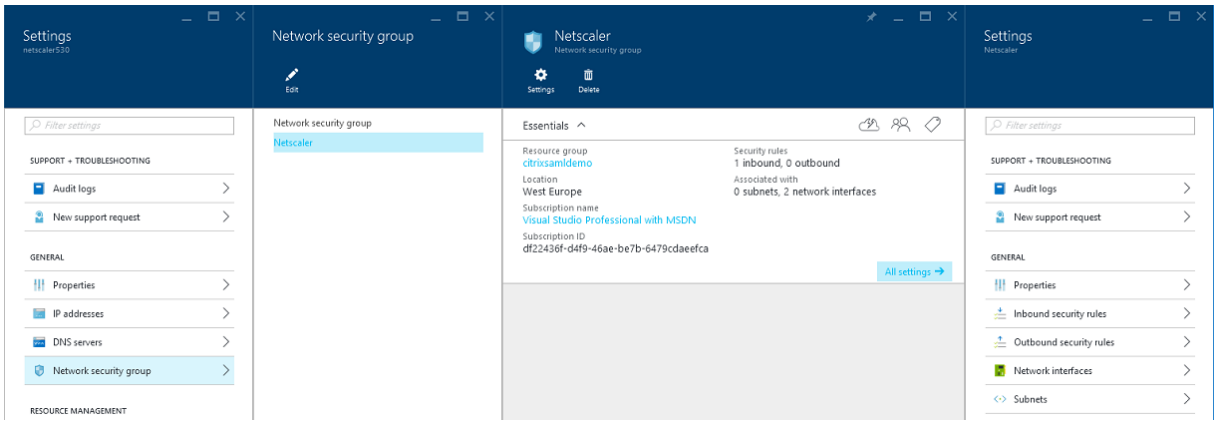


この例では、DNS アドレス domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com を、ドメインコントローラーに割り当てています。

リモート構成の完了時にパブリック IP アドレスを有効にする必要があるのは、Web アプリケーションプロキシと NetScaler 仮想マシンだけである点に注意してください。（構成では、環境への RDP アクセスにパブリック IP アドレスが使用されます）。

セキュリティグループの構成

Azure クラウドは、セキュリティグループを使用して、インターネットから仮想マシンへの TCP および UDP アクセスのファイアウォールルールを管理します。デフォルトでは、すべての仮想マシンで RDP アクセスが許可されます。また、NetScaler および Web アプリケーションプロキシサーバーでは、ポート 443 で TLS を許可する必要があります。

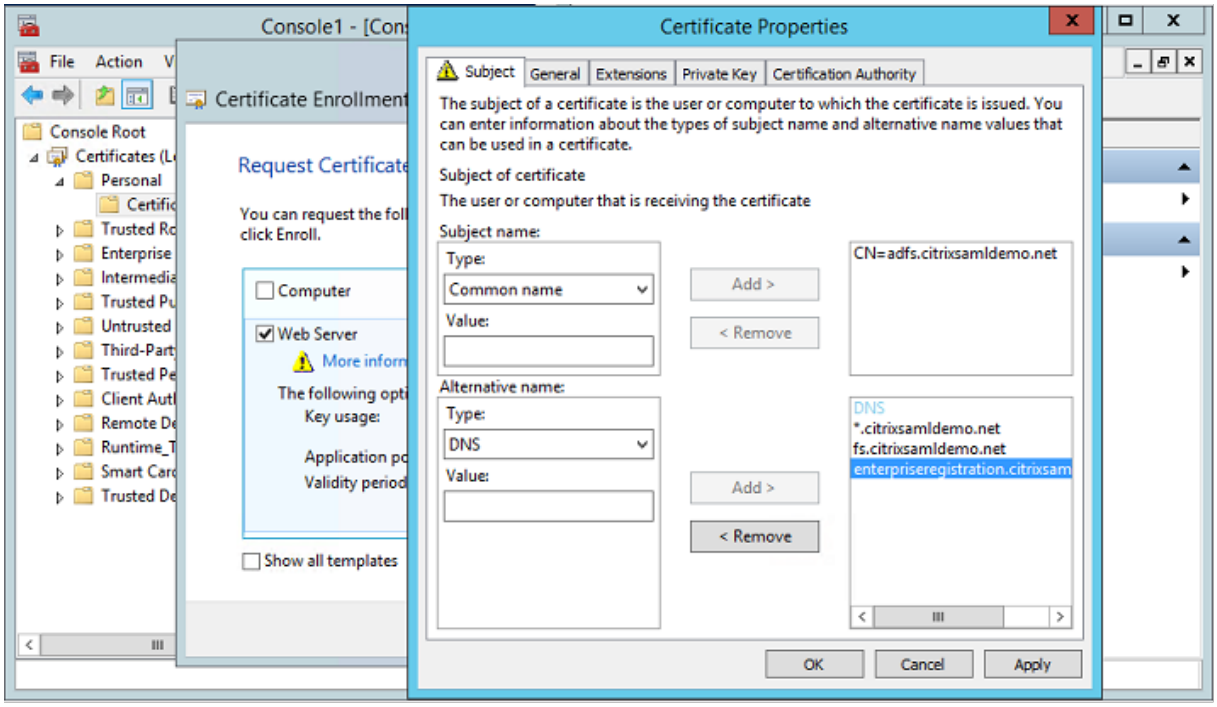


ADFS 証明書の作成

Microsoft 証明機関（CA）で **Web** サーバー証明書テンプレートを有効にします。これにより、PFX ファイルにエクスポート（秘密キーも含む）できる、カスタム DNS アドレスを持つ証明書を作成できます。PFX ファイルを優先オプションにするには、この証明書を ADFS と Web アプリケーションプロキシサーバーの両方にインストールする必要があります。

次のサブジェクト名を使用して、Web サーバー証明書を発行します。

- Commonname:
  - Adfs.citrixsamldemo.net［コンピューター名］
- SubjectAltname:
  - *.citrixsamldemo.net ［ゾーン名］
  - fs.citrixsamldemo. net ［DNS のエントリ］
  - enterpriseregistration.citrixsamldemo.net



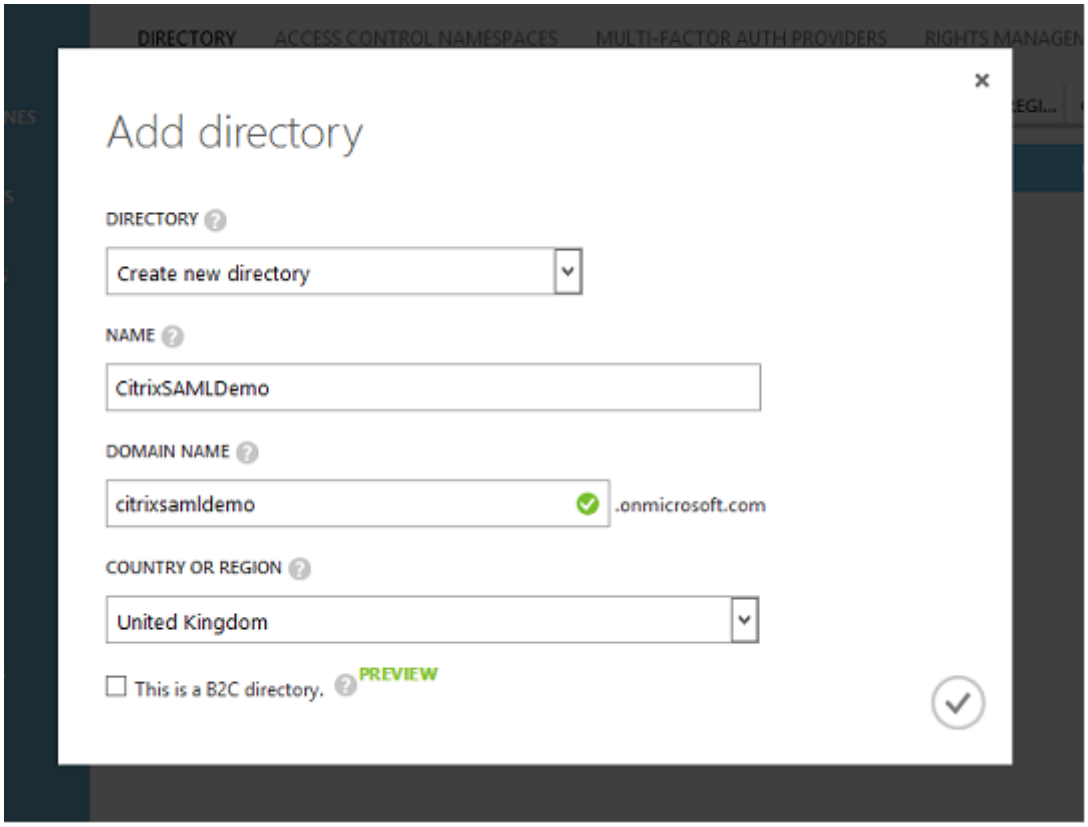
パスワードで保護された秘密キーを含め、証明書を PFX ファイルにエクスポートします。

Azure AD のセットアップ

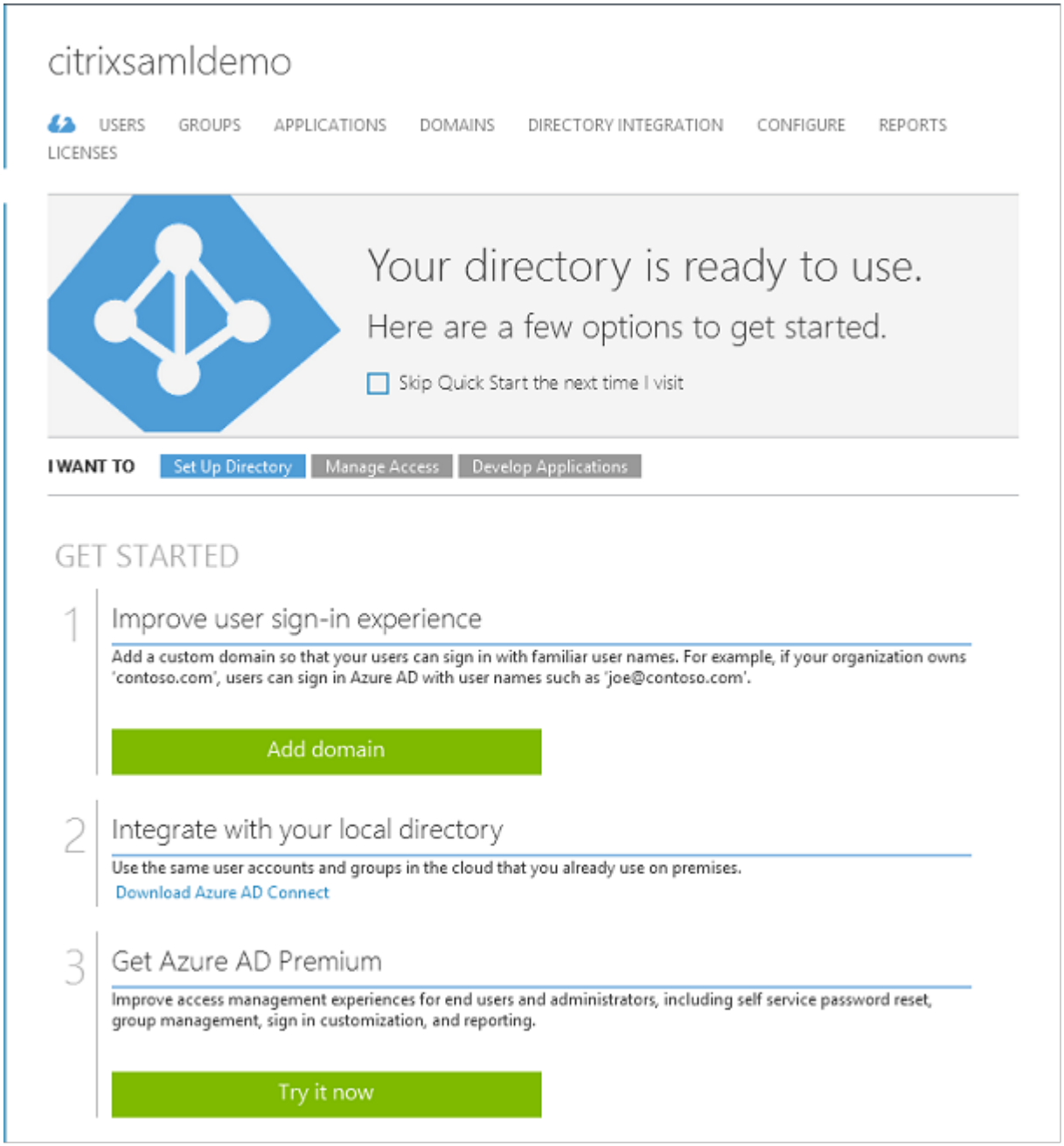
このセクションでは、新しい Azure AD インスタンスをセットアップして、Windows 10 を Azure AD に参加させるために使用できるユーザー ID を作成する方法について説明します。

新しいディレクトリの作成

Azure クラシックポータルにログオンして、新しいディレクトリを作成します。

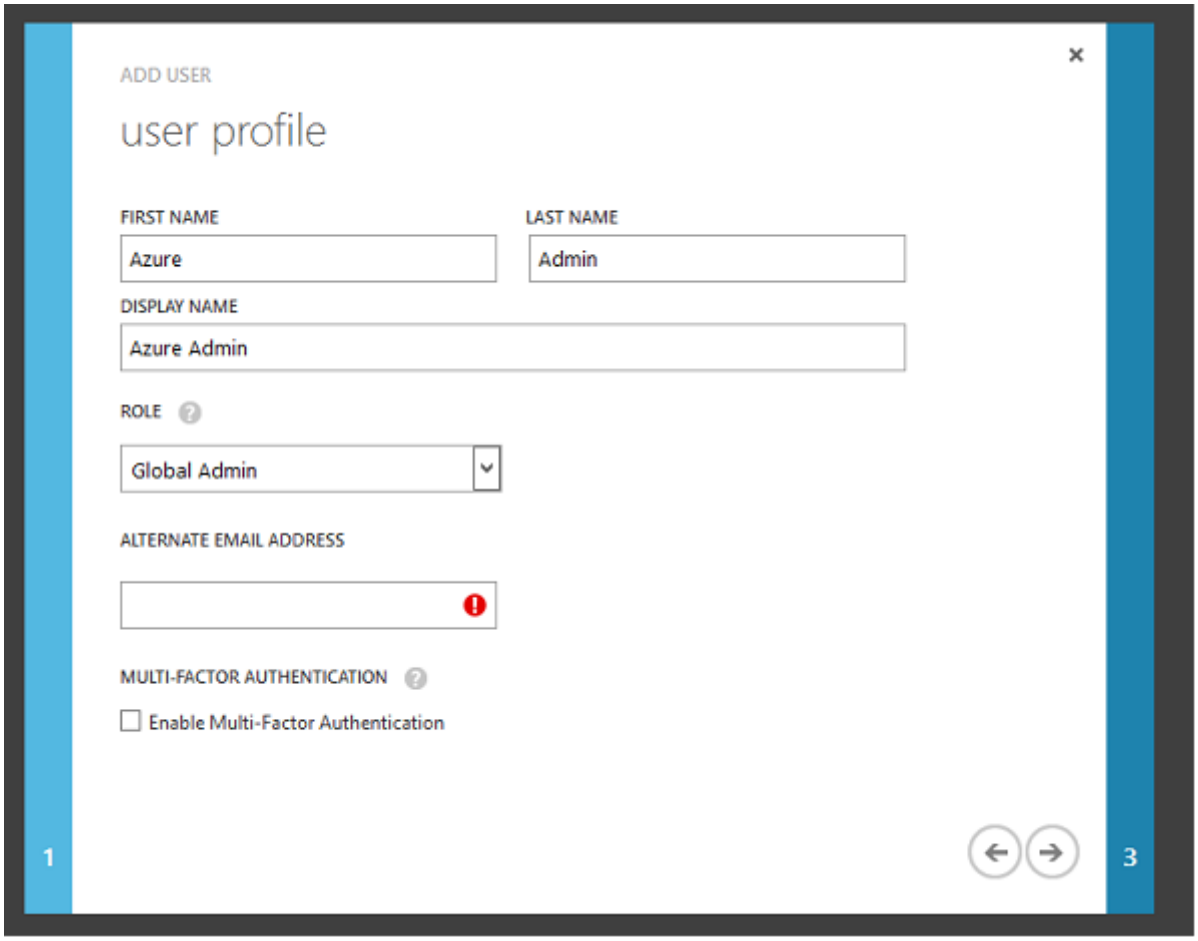


完了すると、概要ページが表示されます。



グローバル管理者ユーザー（**AzureAdmin**）の作成

Azure のグローバル管理者を作成し（この例では AzureAdmin@citrixsamldemo.onmicrosoft.com）、新しいアカウントでログオンしてパスワードをセットアップします。



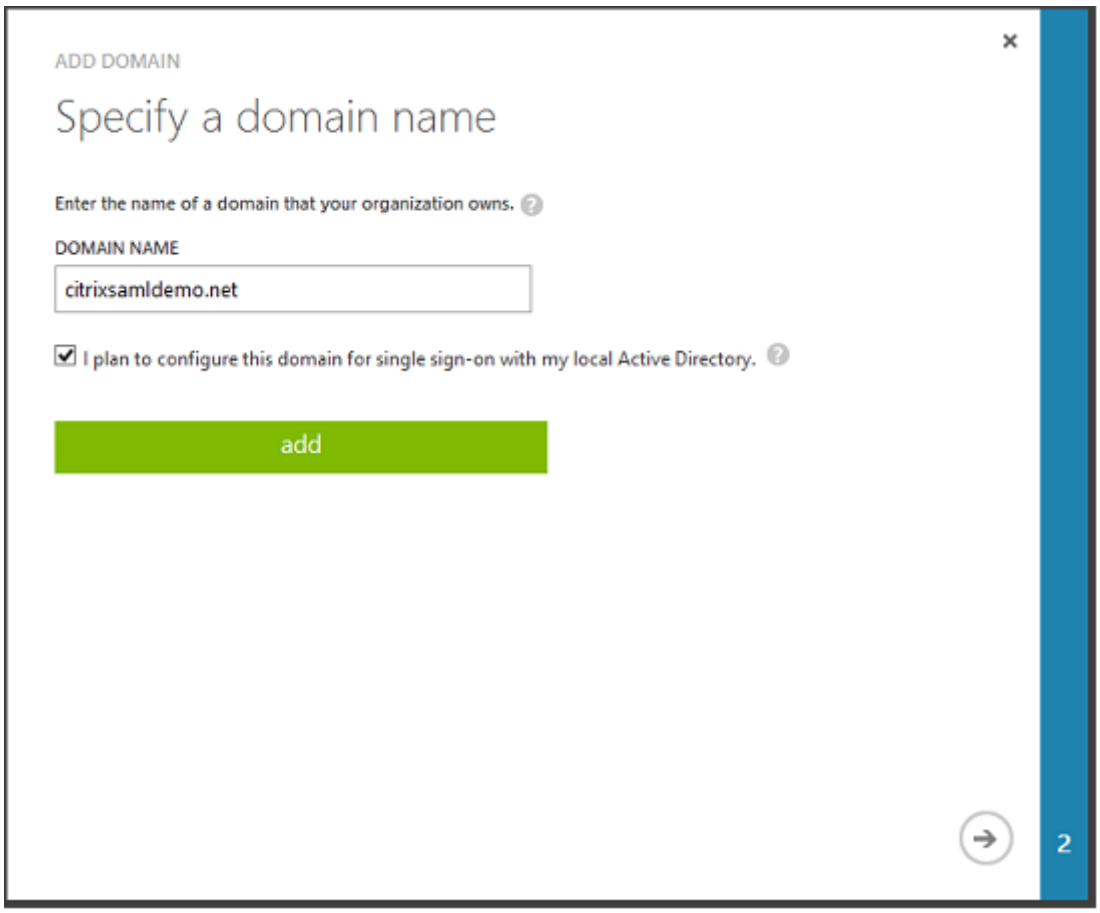
Azure AD を使用したドメインの登録

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： <user.name>@<company>.com

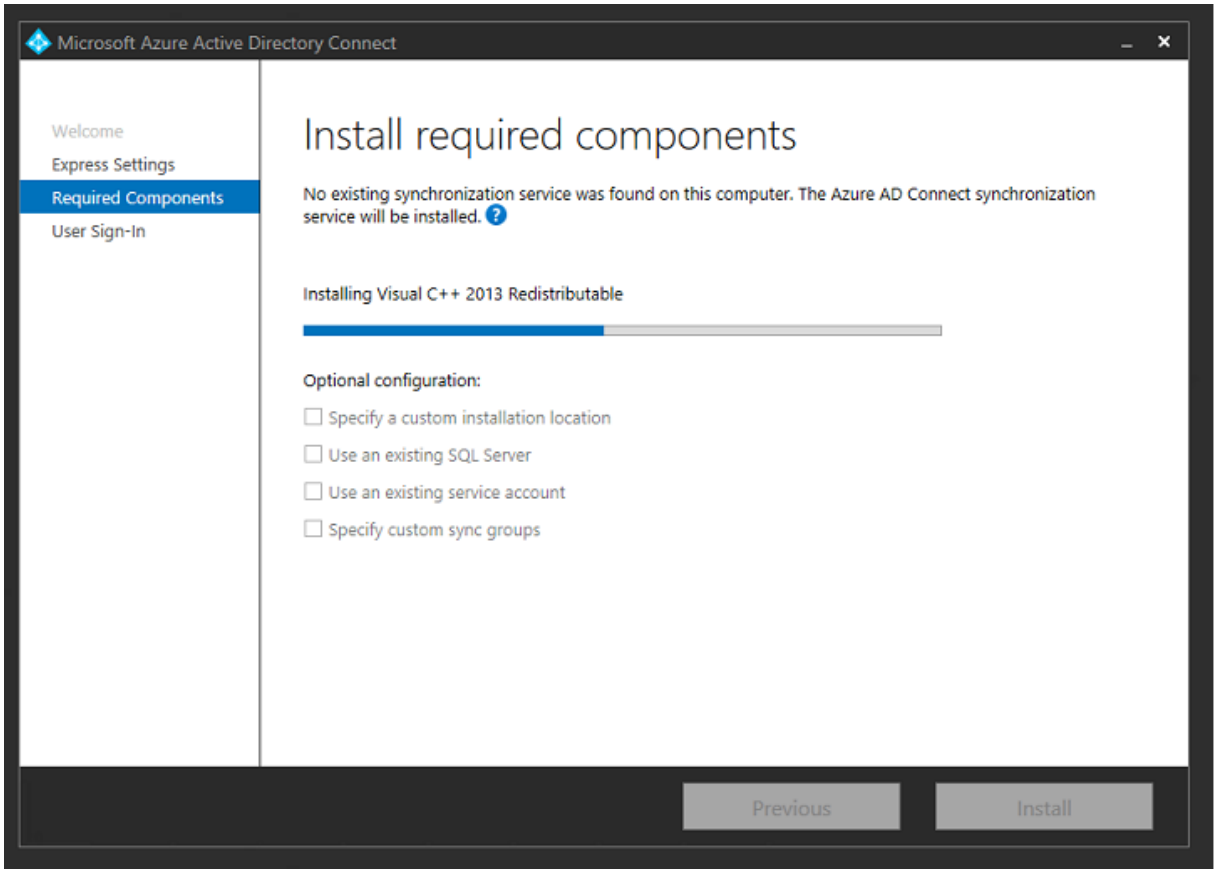
[ドメインの追加]で、ユーザーの会社のドメインからのリダイレクトを構成します。この例では citrixsamldemo.net を使用します。

ADFS をシングルサインオンにセットアップしている場合は、チェックボックスにチェックマークを入れます。

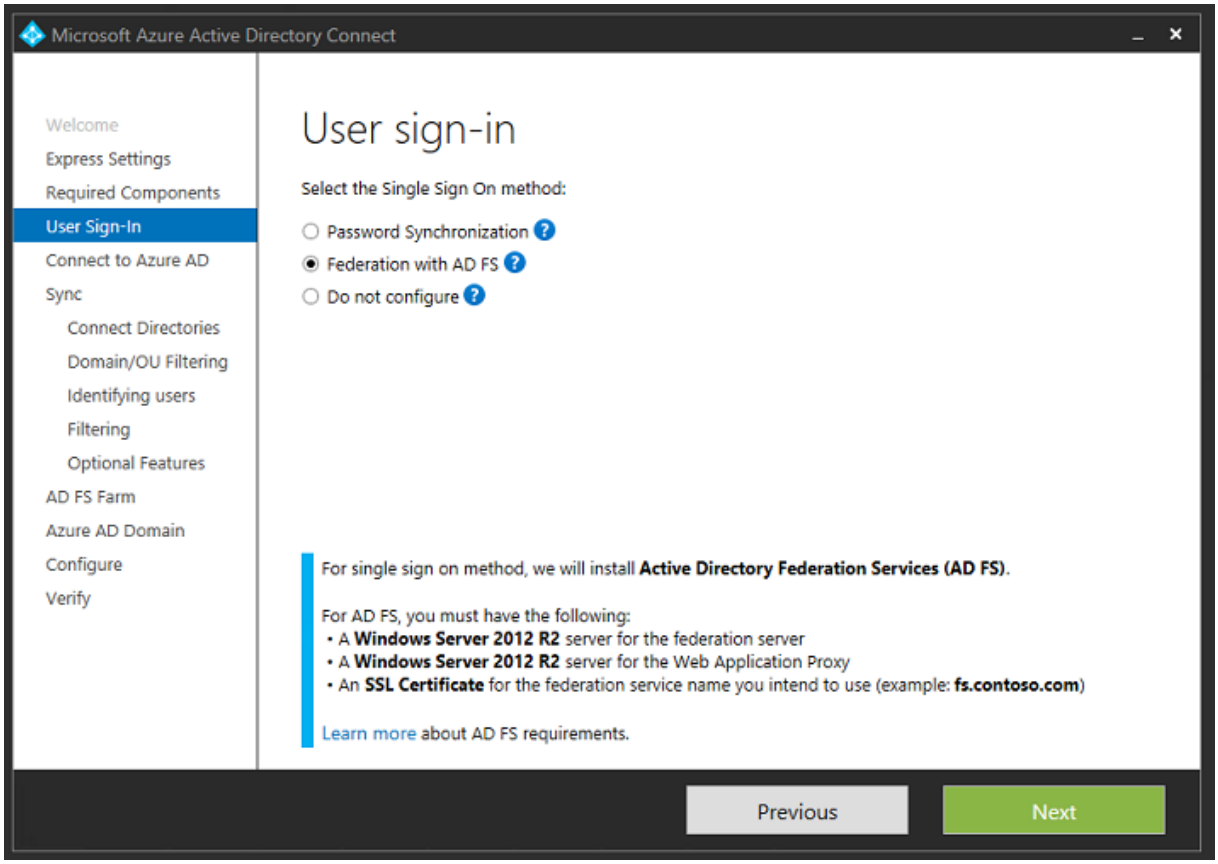


Azure AD Connect のインストール

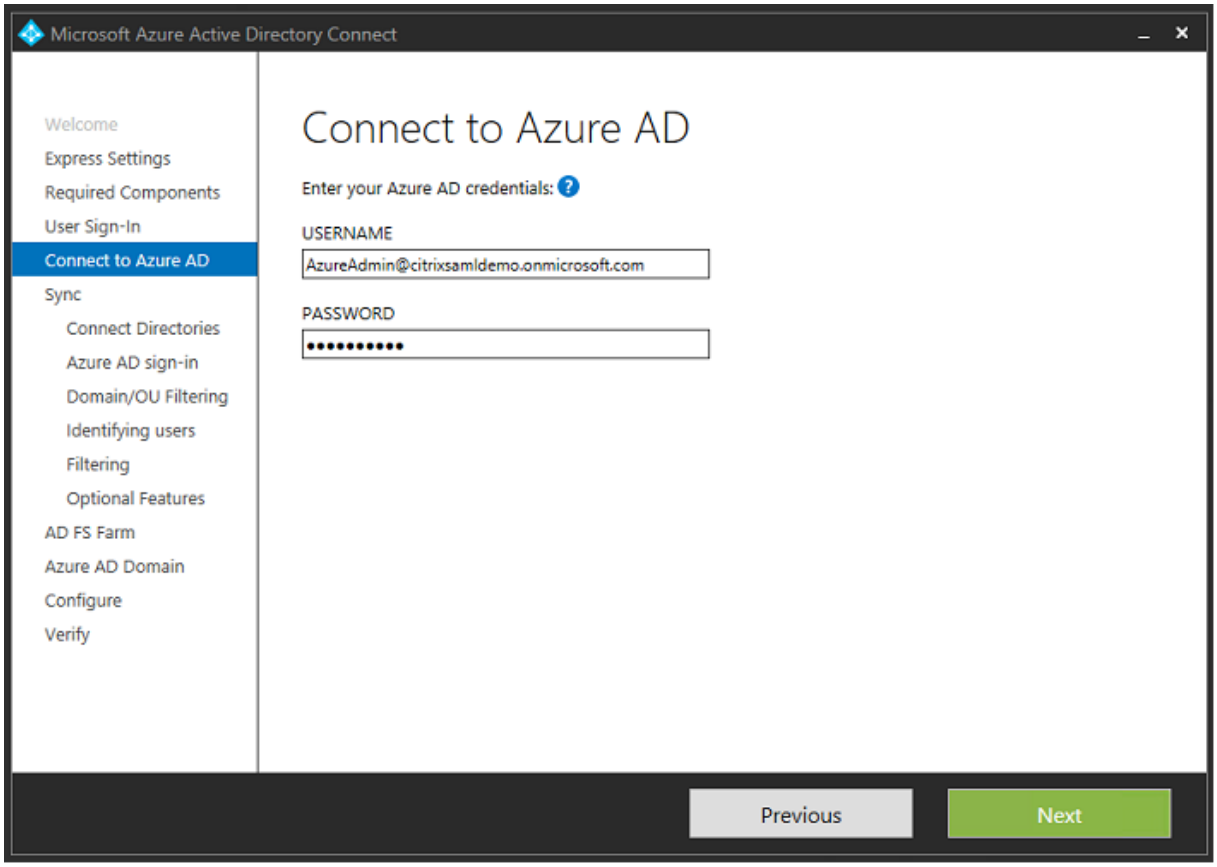
Azure AD 構成 GUI の手順 2 により、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS 仮想マシンにインストールします。［簡単設定］ではなく ［カスタムインストール］を使用し、ADFS のオプションが利用できるようにします。



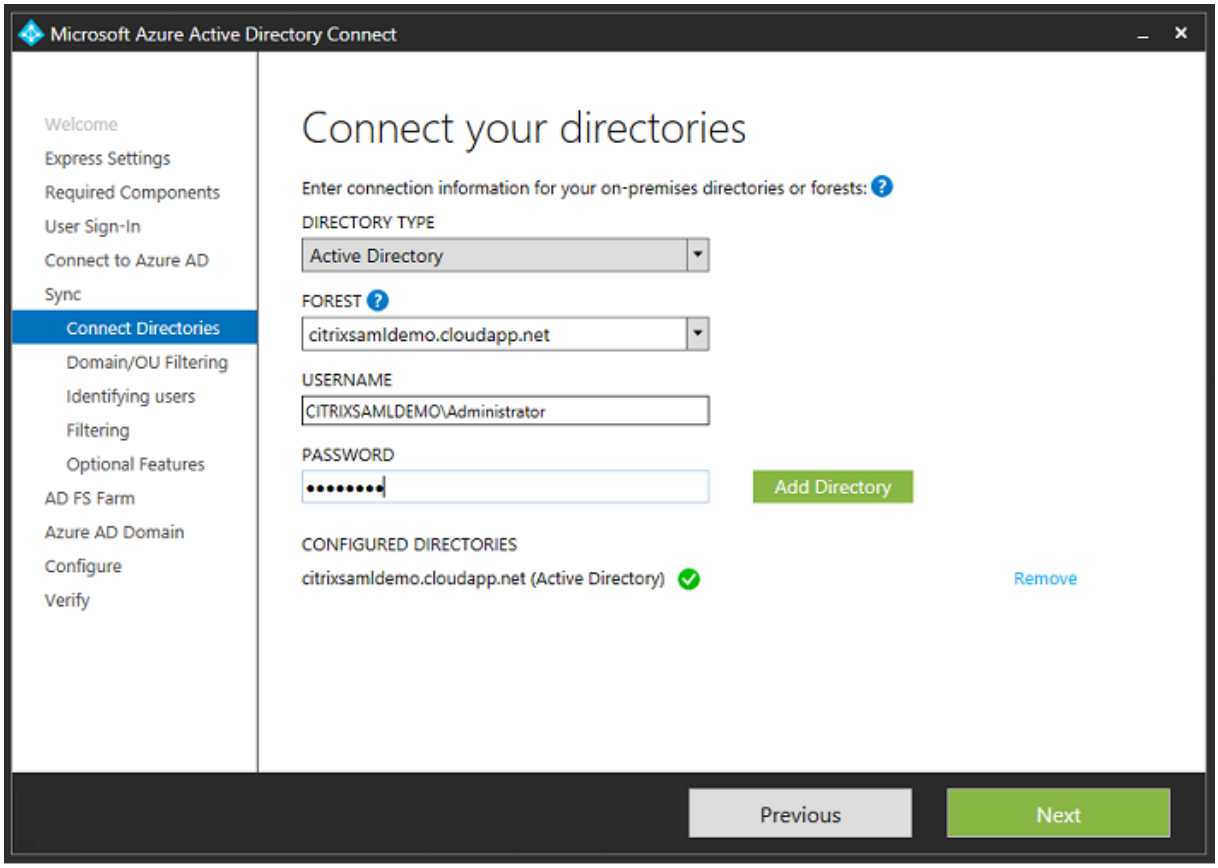
［**AD FS** とのフェデレーション］シングルサインオンオプションを選択します。



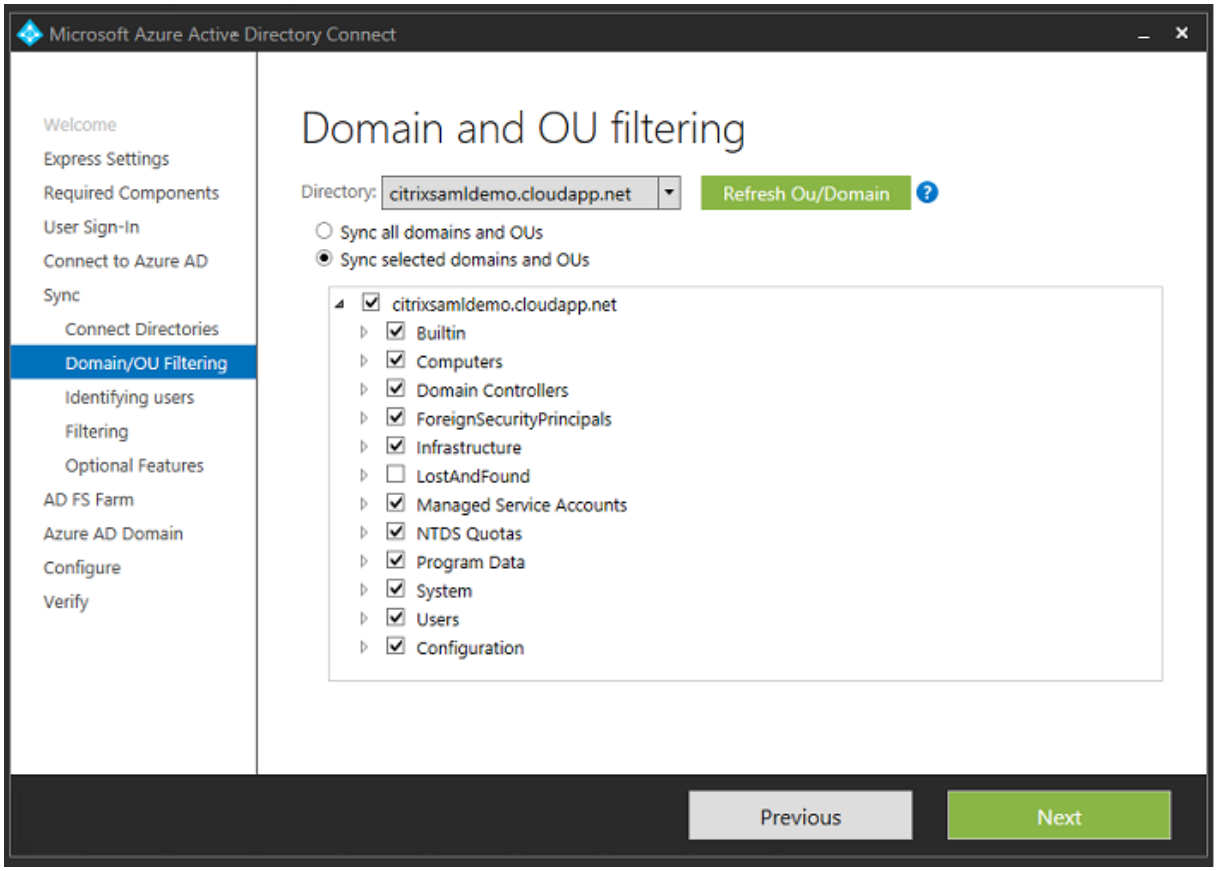
あらかじめ作成した管理アカウントで Azure に接続します。



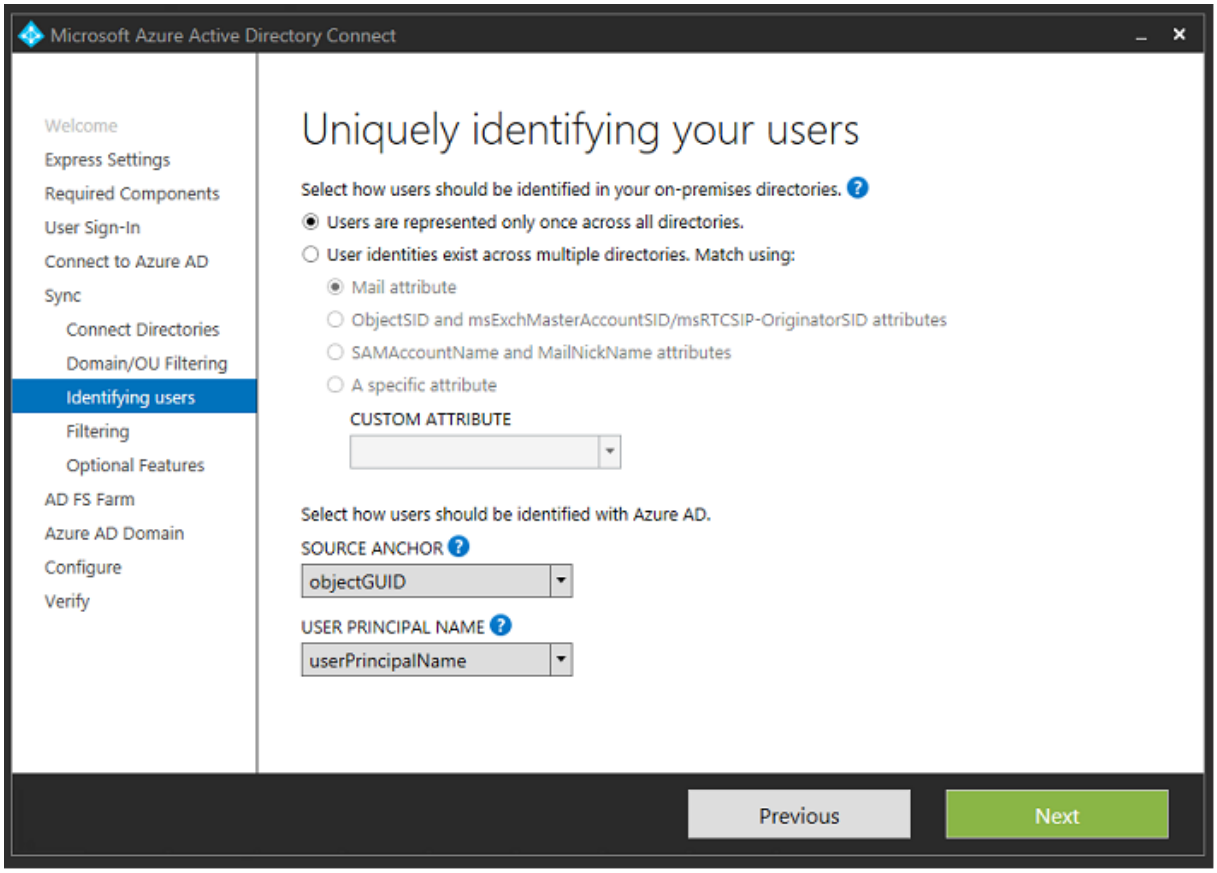
内部 AD フォレストを選択します。



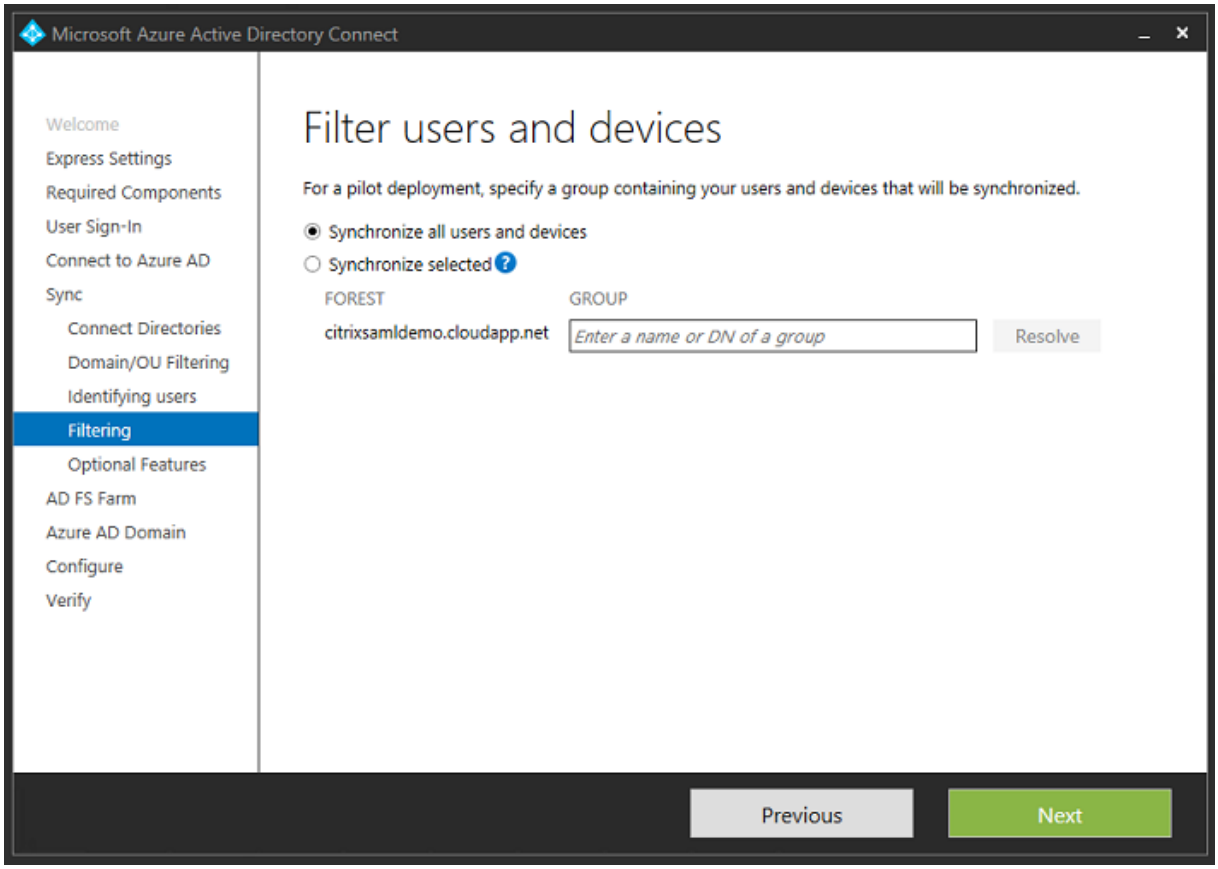
Active Directory の従来のオブジェクトをすべて Azure AD と同期します。



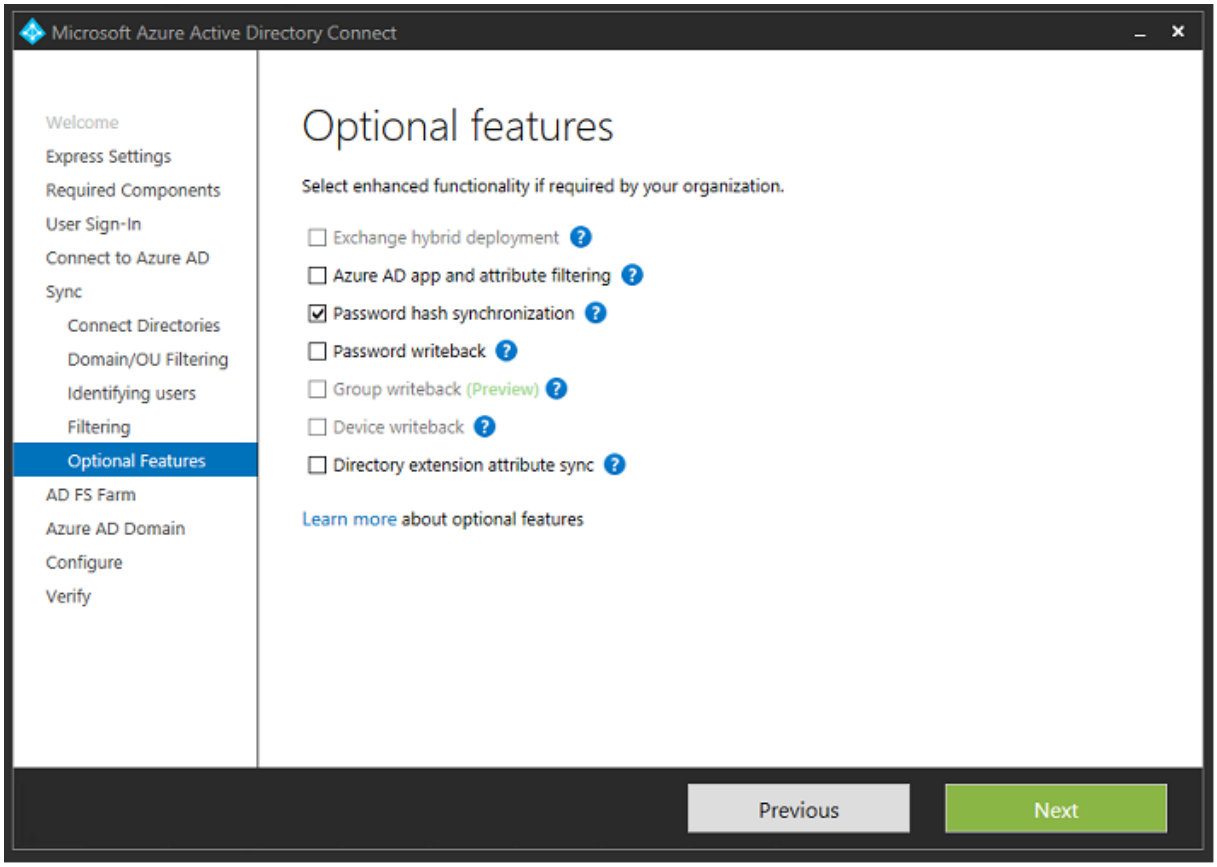
ディレクトリ構造がシンプルな場合は、ユーザー名の一意性に依存して、ログオンするユーザーを識別することができます。



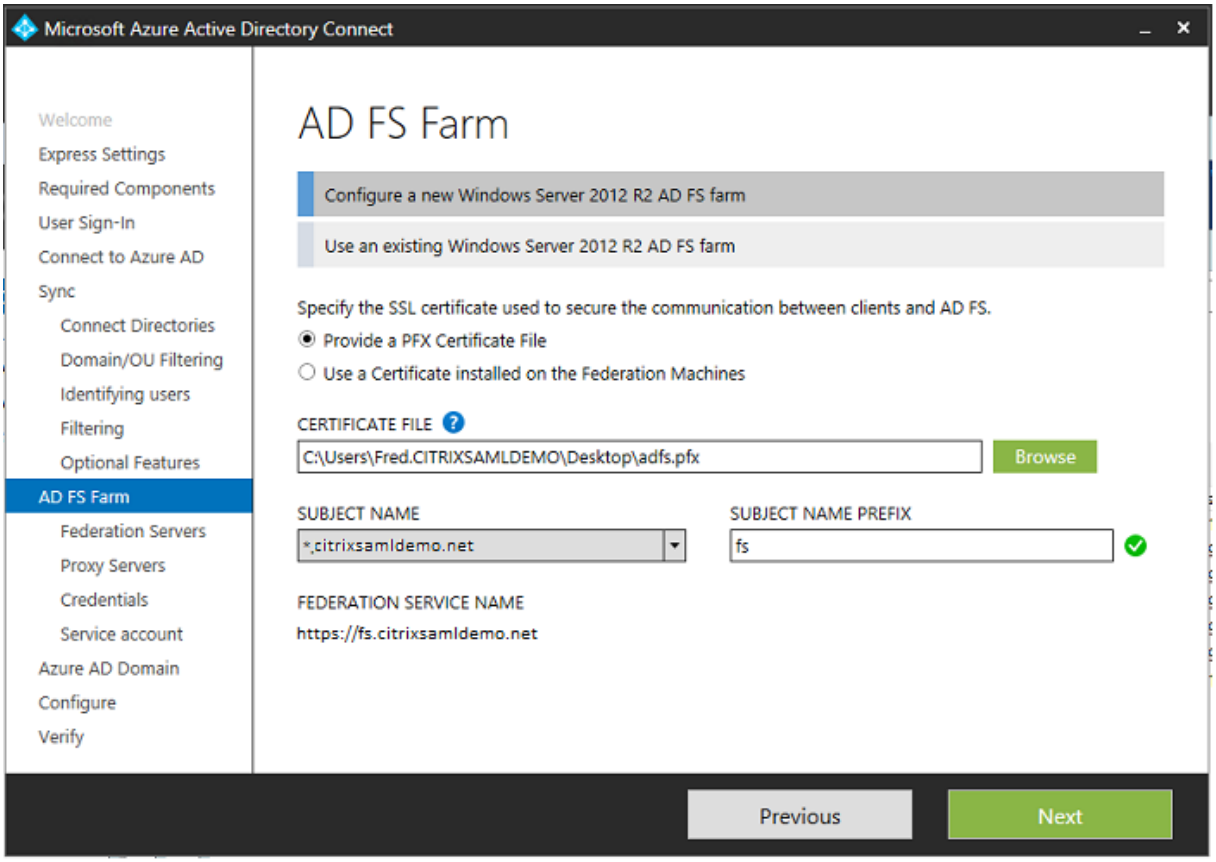
デフォルトのフィルタリングオプションを使用するか、あるいはユーザーとデバイスを特定のグループセットに制限します。



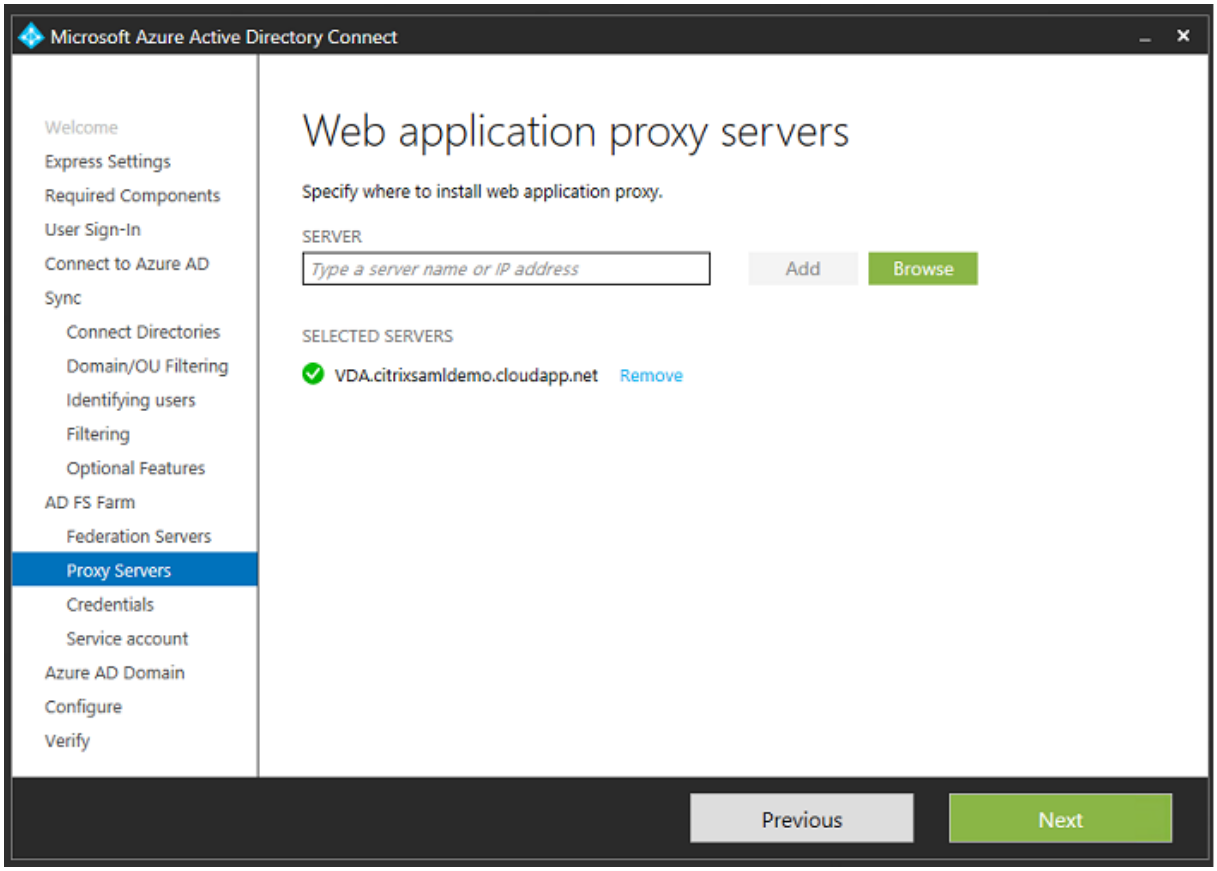
必要に応じて、Azure AD パスワードを Active Directory と同期することができます。これは、通常、ADFS ベースの認証では必要ありません。



証明書の PFX ファイルを AD FS で使用するように選択します。DNS 名として fs.citrixsamldemo.net を指定します。

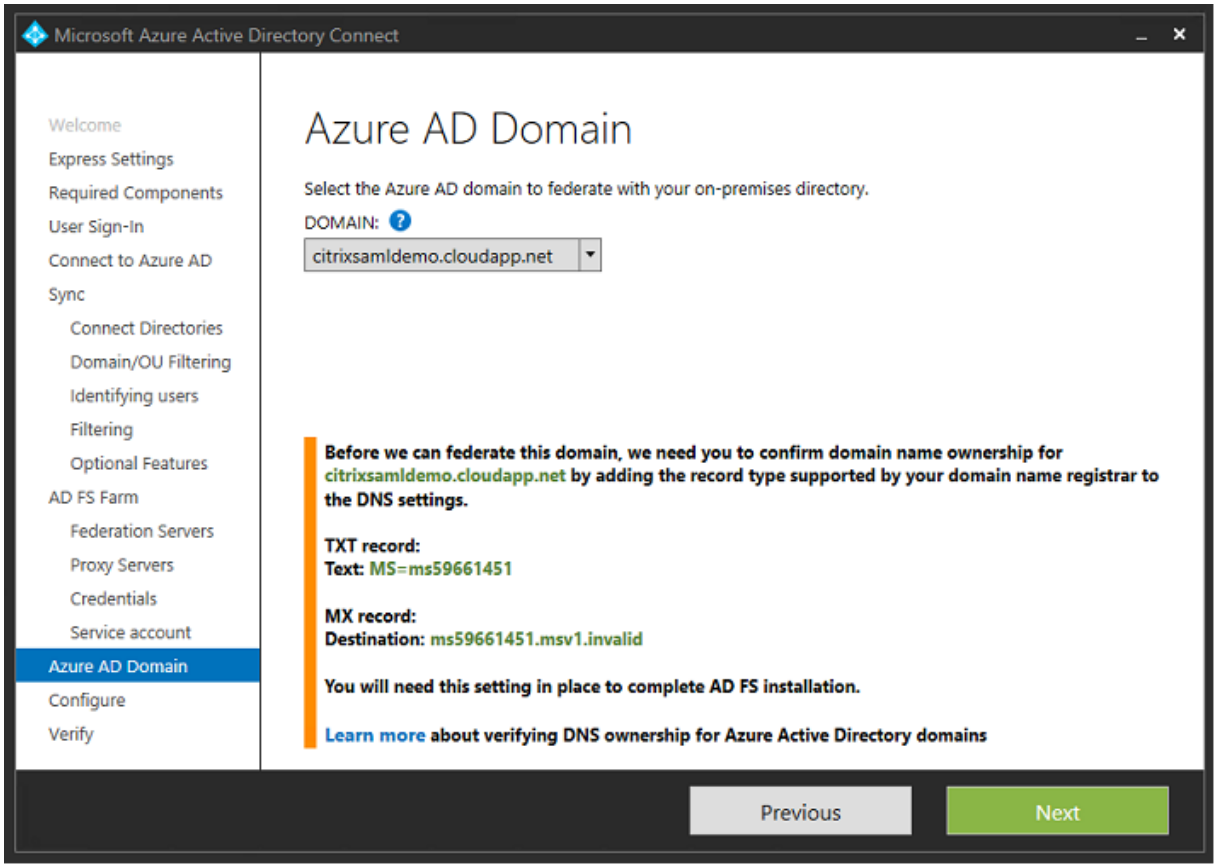


プロキシサーバーの選択を求める画面が表示されたら、wap.citrixsamldemo.net サーバーのアドレスを入力します。Azure AD Connect が構成できるよう、Web アプリケーションプロキシサーバーの管理者として **Enable-PSRemoting –Force** コマンドレットを実行する必要がある場合があります。

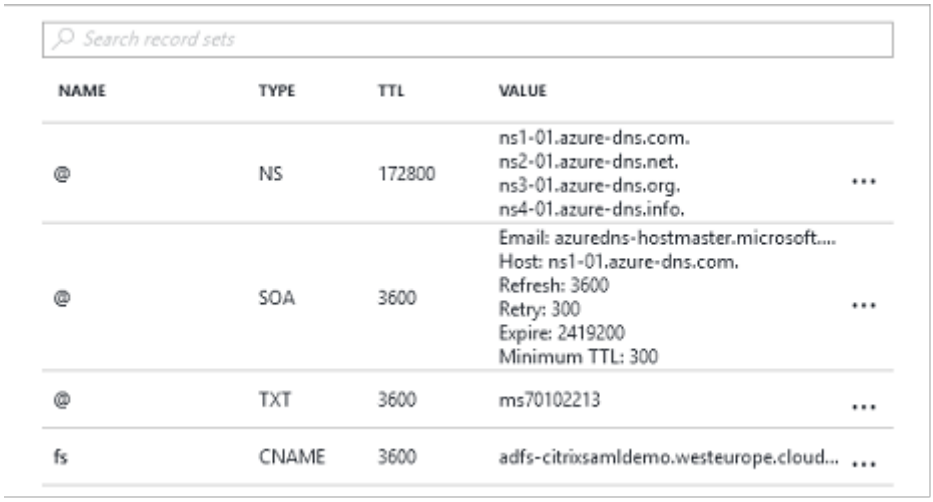


注： Remote PowerShell の信頼性の問題でこの手順に失敗した場合は、Web アプリケーションプロキシサーバーをドメインに参加させてみてください。

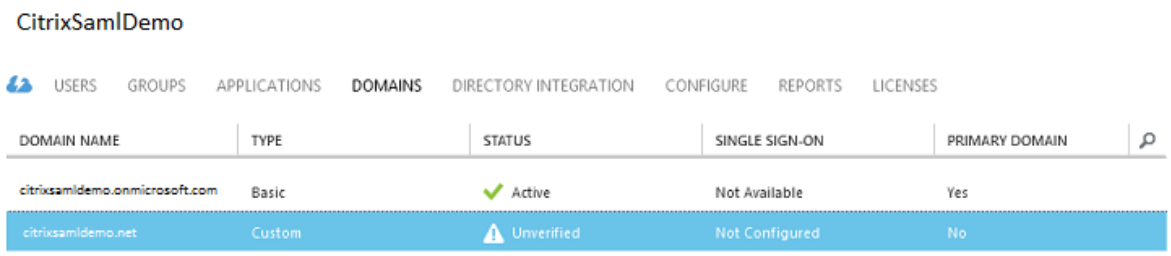
ウィザードの残りの手順については、標準の管理者パスワードを使用して、ADFS のサービスアカウントを作成します。Azure AD Connect により、DNS ゾーンの所有権の検証が求められます。



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。

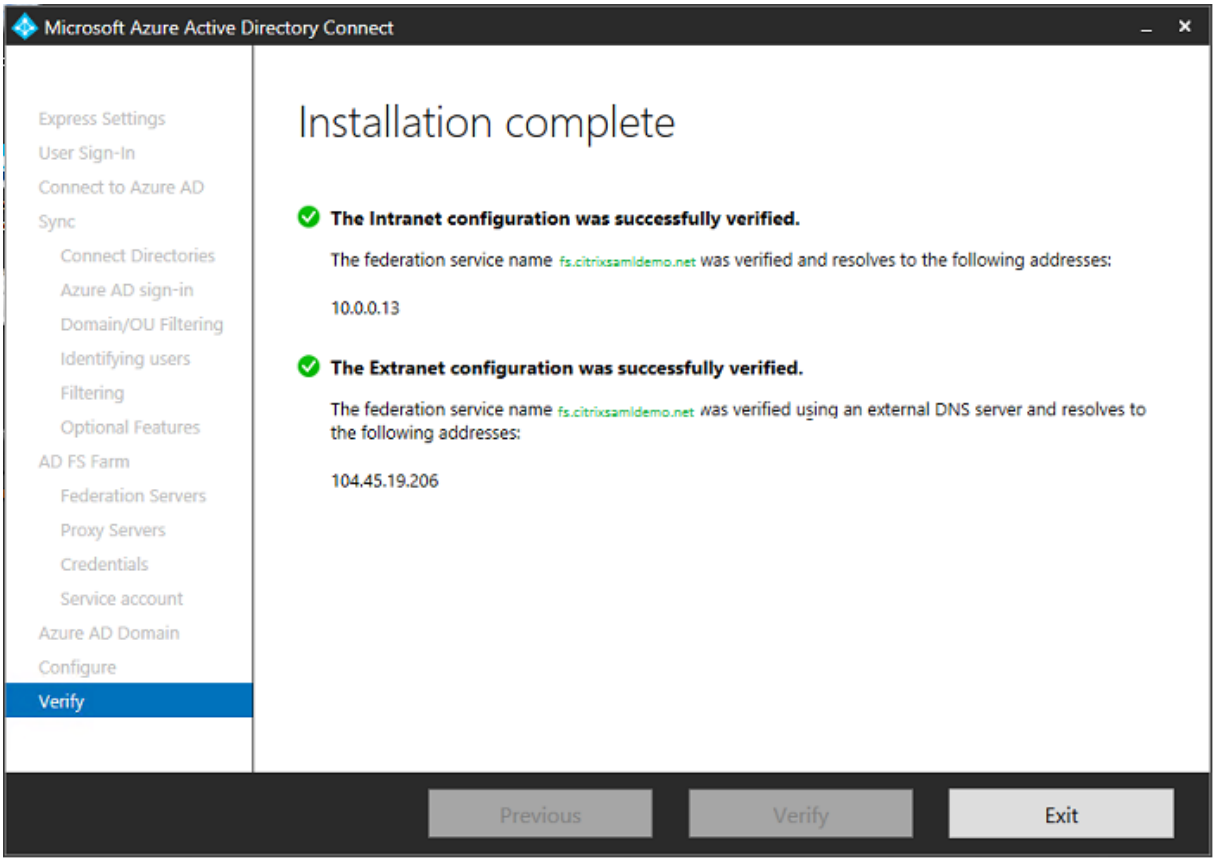


Azure 管理コンソールで［検証］をクリックします。



注：この手順に失敗した場合は、Azure AD Connect を実行する前にドメインを検証します。

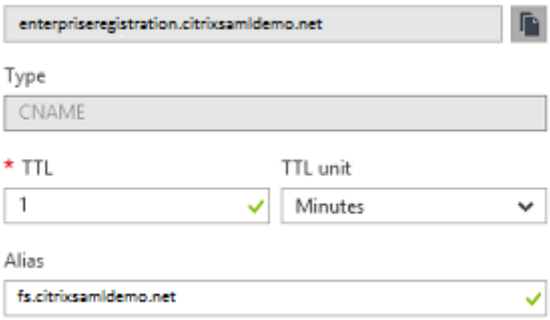
完了すると、外部アドレス fs.citrixsamldemo.net がポート 443 で接続されます。



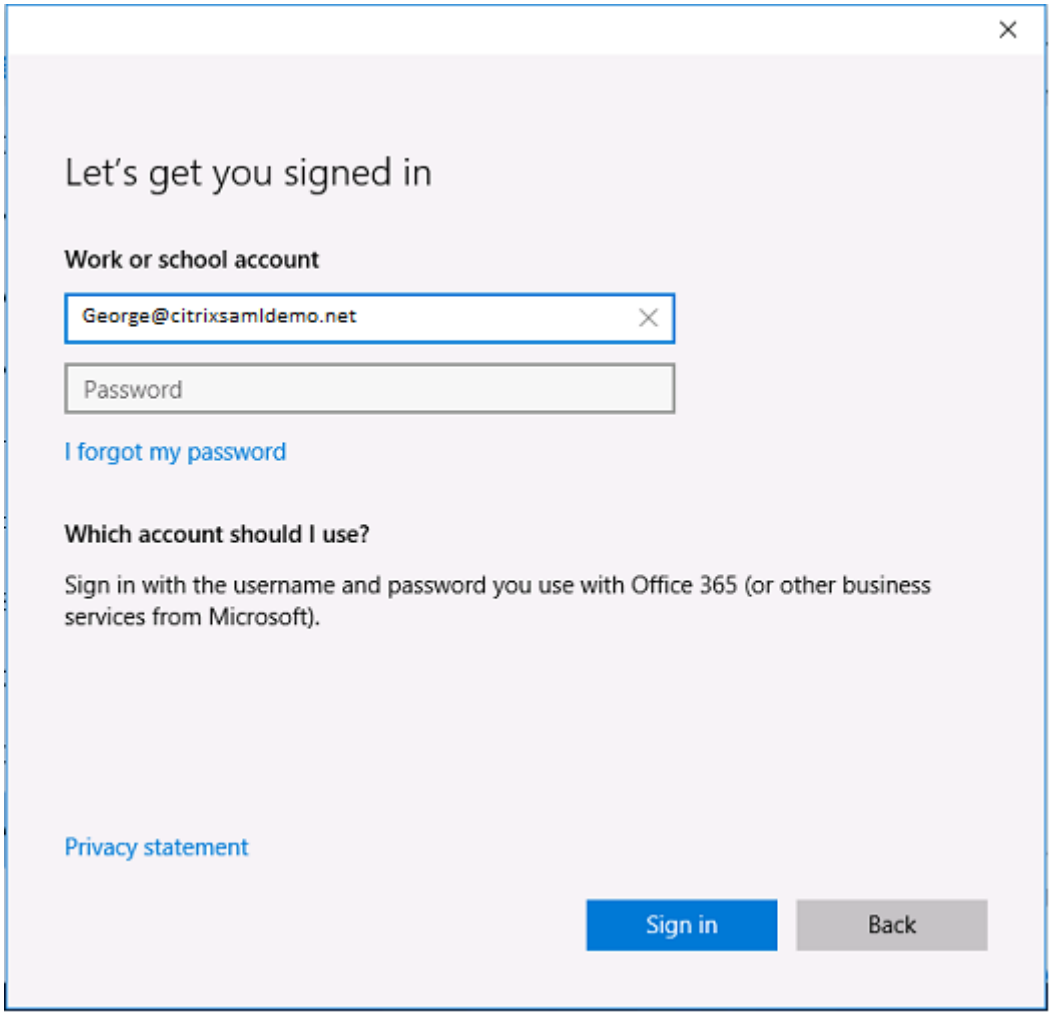
Azure AD への参加の有効化

Windows 10 が Azure AD への参加を実行するよう、メールアドレスを入力すると、ADFS を指す必要がある CNAME DNS レコードの作成に DNS サフィックスが使用されます（enterpriseregistration.<upnsuffix>）。

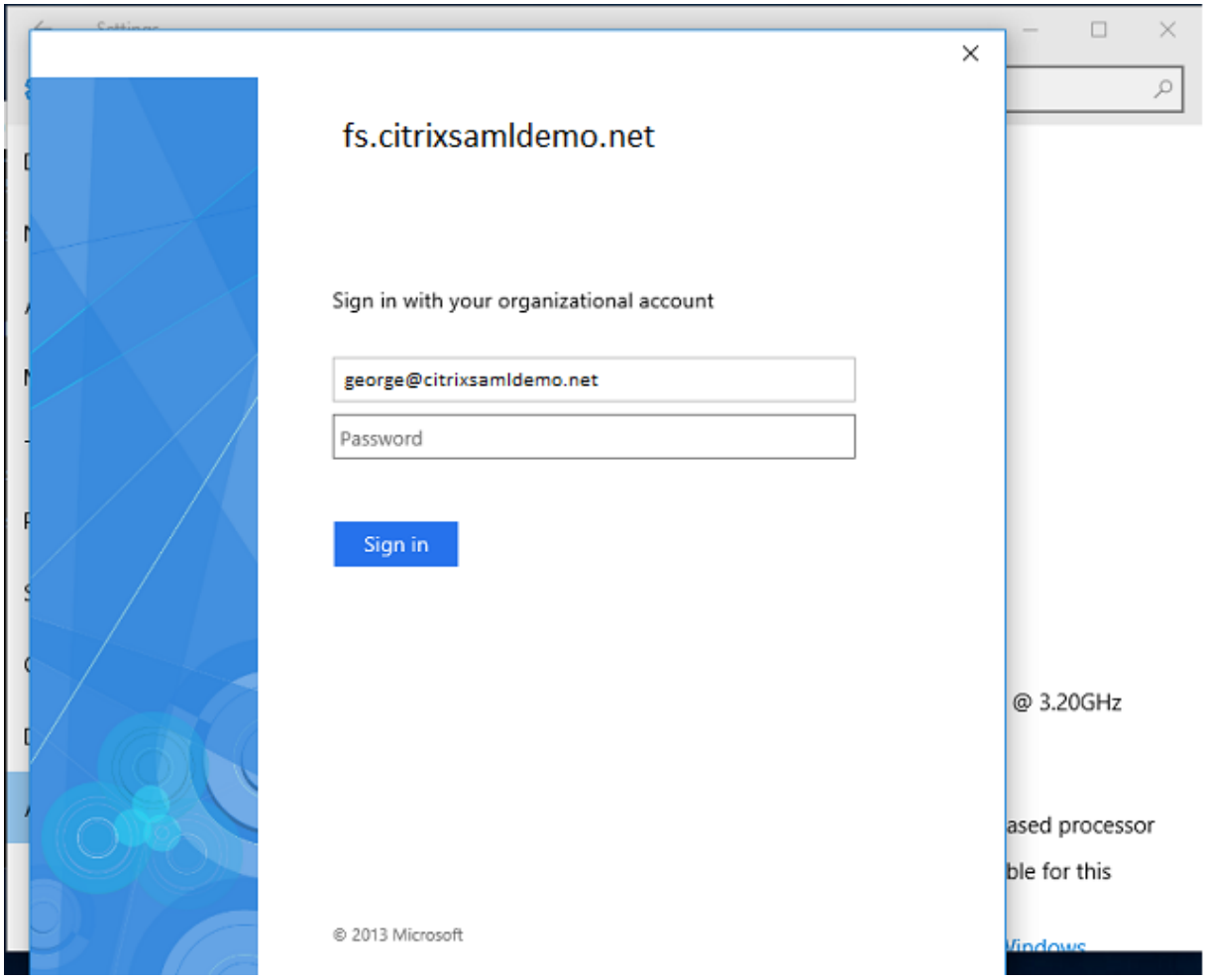
この例では fs.citrixsamldemo.net です。

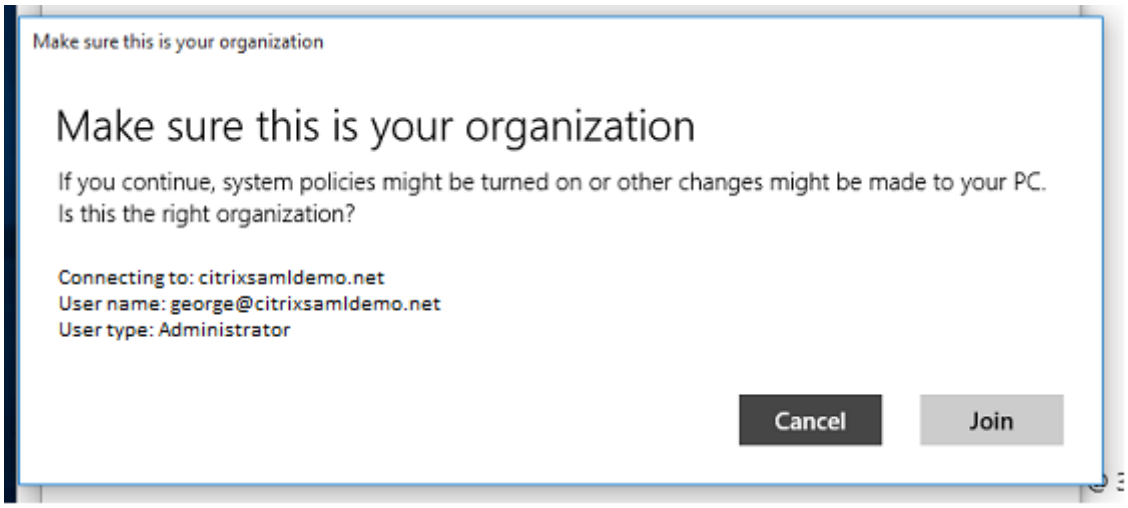


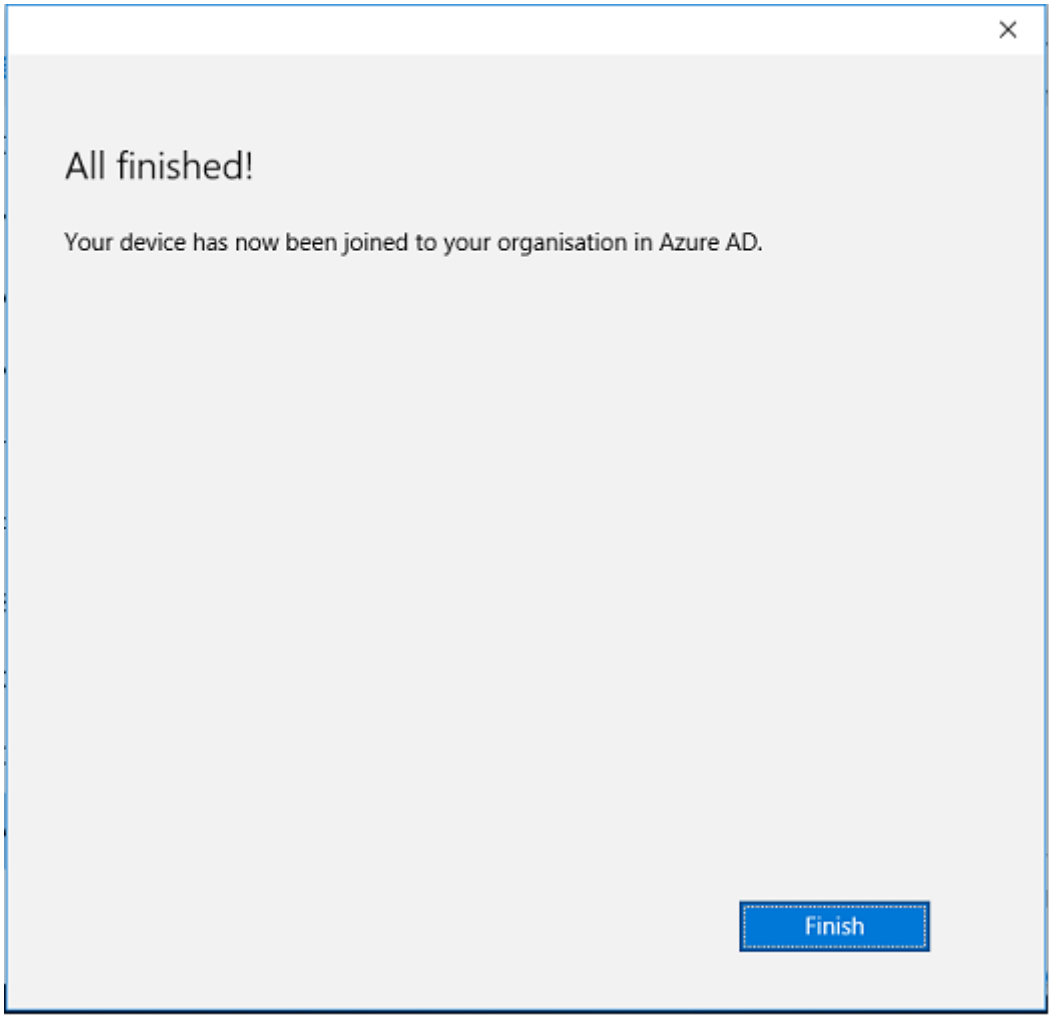
パブリック CA を使用していない場合は、Windows が ADFS サーバーを信頼するよう、ADFS のルート証明書を Windows 10 コンピューターにインストールします。あらかじめ生成された標準のユーザーアカウントを使用して、Azure AD ドメインに参加します。



UPN は、ADFS ドメインコントローラーで認識される UPN と一致する必要があることに注意してください。





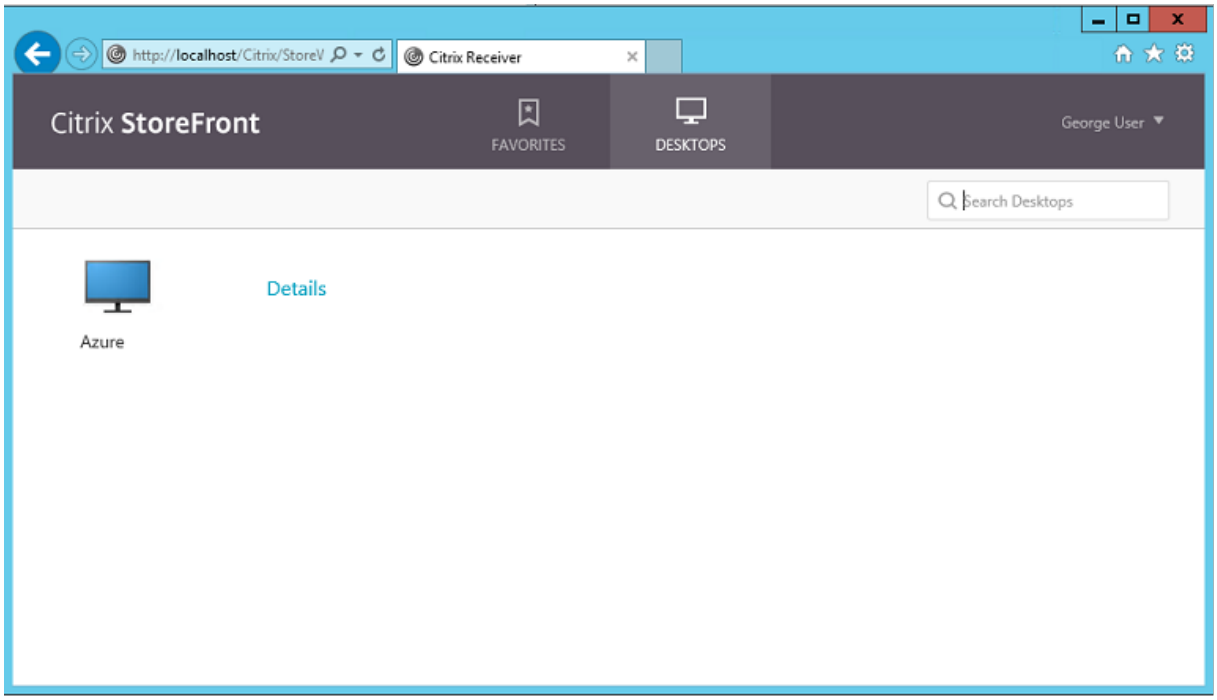


メールアドレスを使用してマシンの再起動とログオンを行い、Azure AD への参加が正常に行われたことを検証します。ログオンすると Microsoft Edge が起動してhttps://myapps.microsoft.comに接続します。この Web サイトでは、シングルサインオンが自動的に使用されます。

XenApp または **XenDesktop** のインストール

通常の方法で、XenApp または XenDesktop ISO から、Delivery Controller および VDA 仮想マシンを Azure に直接インストールすることができます。

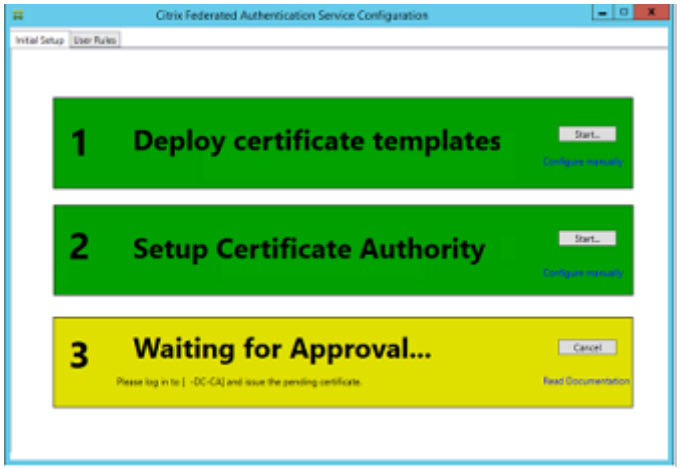
この例では、StoreFront は Delivery Controller と同じサーバーにインストールされています。VDA はスタンドアロンの Windows 2012 R2 用 RDS ワーカーとしてインストールされ、Machine Creation Services とは統合していません（ただしオプションで構成することができます）。作業を続行する前に、ユーザー George@citrixsamldemo.net がパスワードで認証できることを確認します。

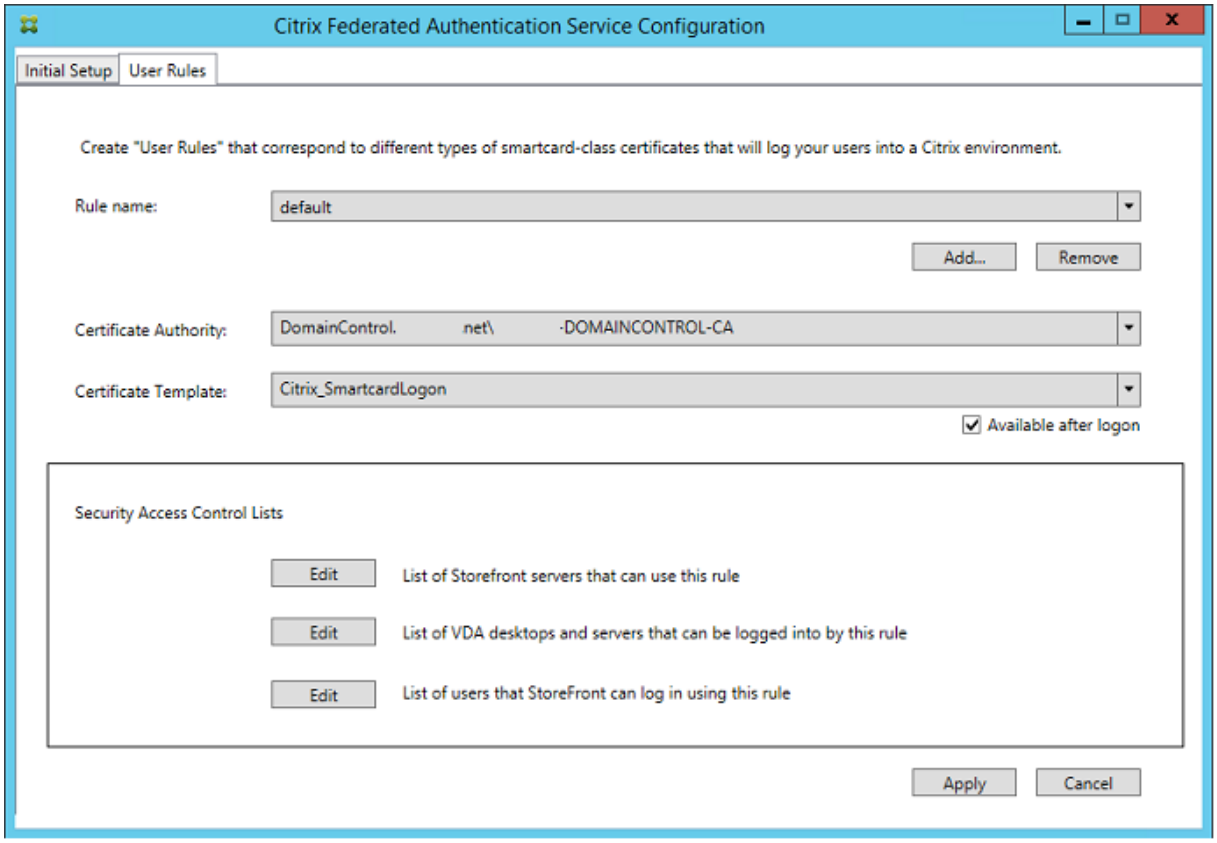


StoreFrontがユーザー資格情報なしに認証できるよう、**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell コマンドレットを Controller で実行します。

フェデレーション認証サービスのインストール

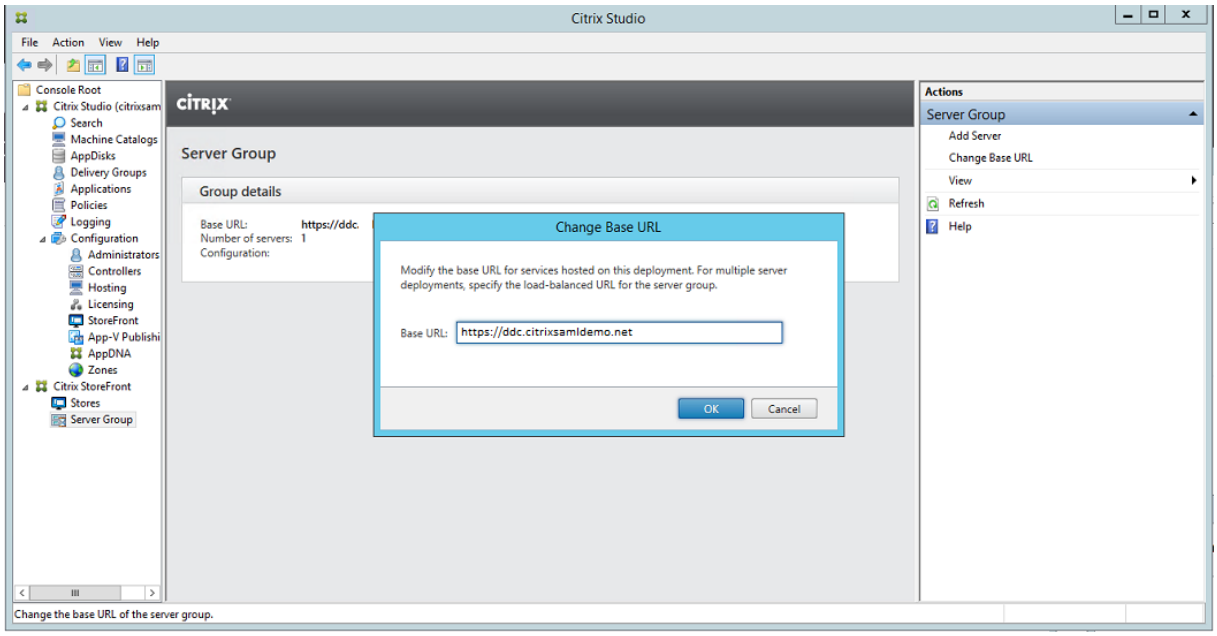
フェデレーション認証サービス（FAS）コンポーネントを ADFS サーバーにインストールして Controller のルールを構成し、信頼された StoreFront として機能するように設定します。



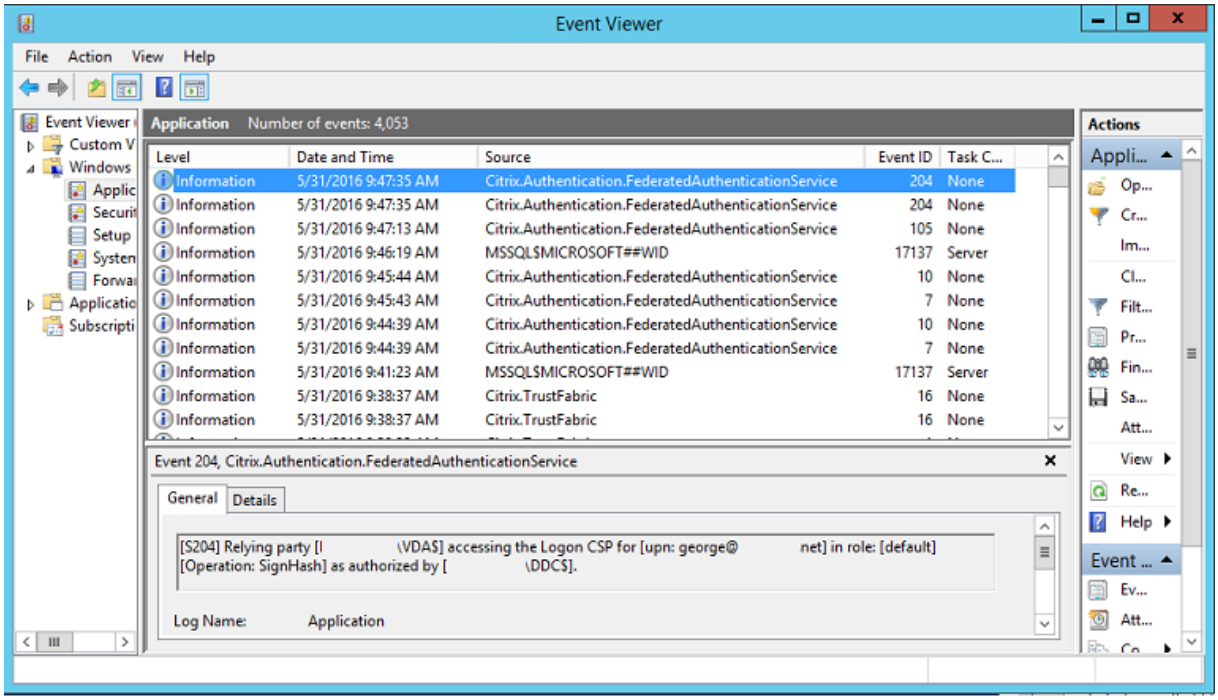


StoreFront の構成

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。

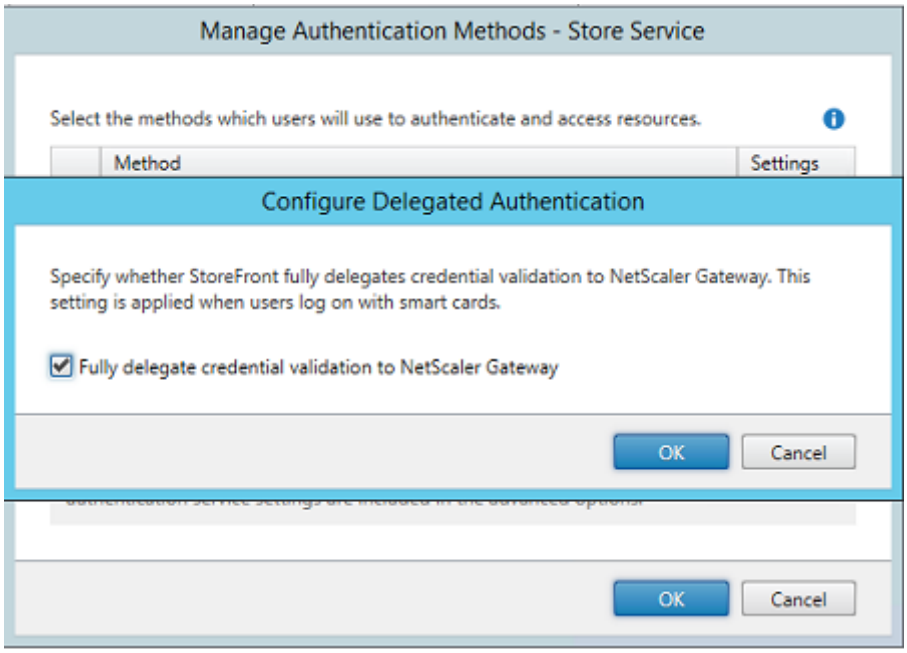


StoreFront で FAS サーバーが使用されるように構成し（「Federated Authentication Service」の PowerShell スクリプトを使用します）、Azure 内で内部テストを行います。FAS サーバーのイベントビューアーをチェックして、ログオンに FAS が使用されることを確認します。

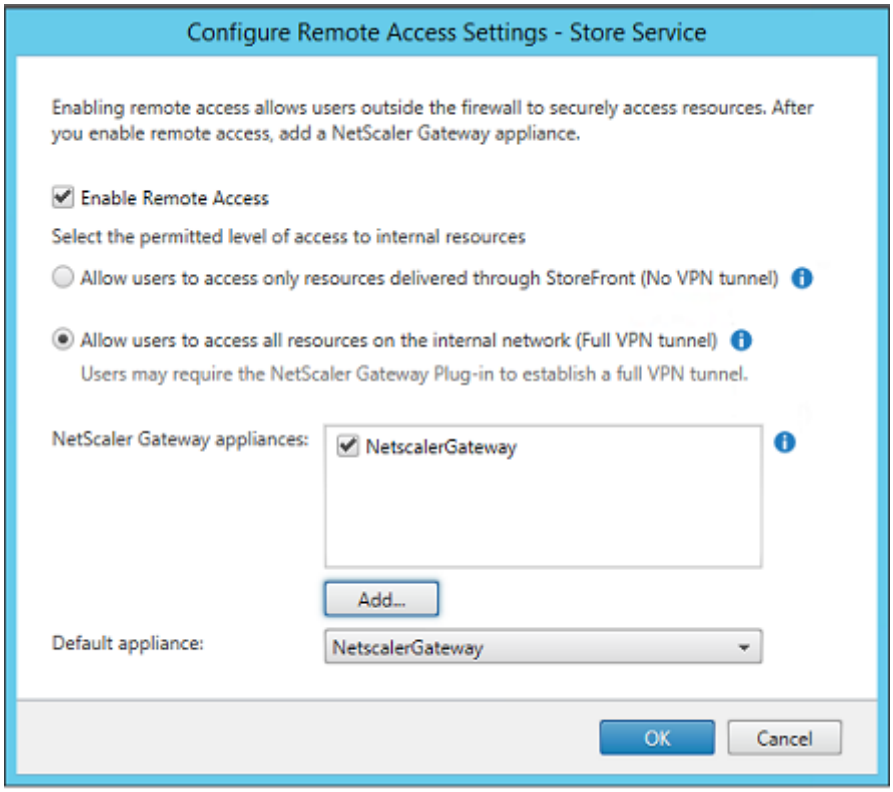


StoreFront が **NetScaler** を使用するように構成

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。

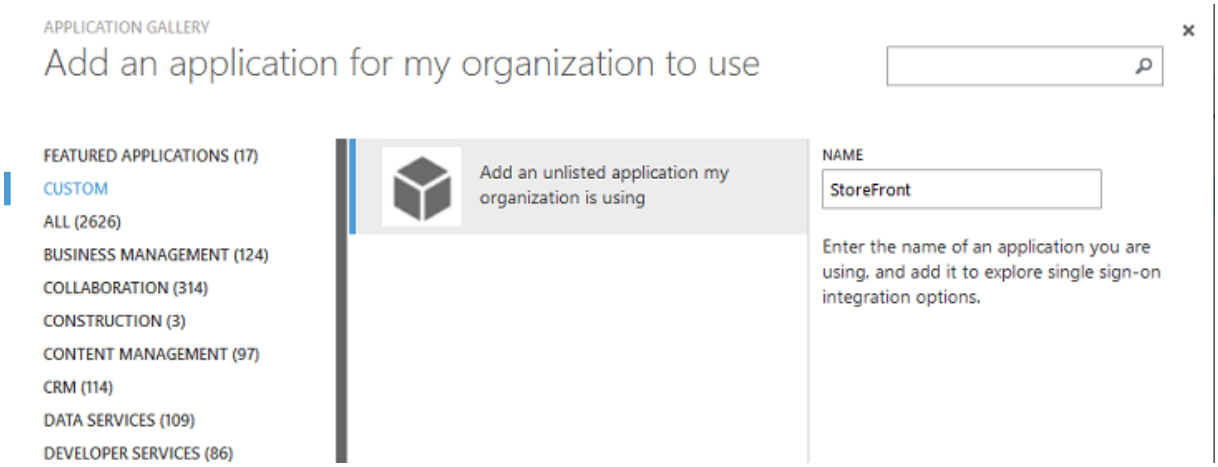


NetScaler 認証オプションを統合するには、Secure Ticket Authority（STA）の構成および NetScaler Gateway アドレスの構成を行います。



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。



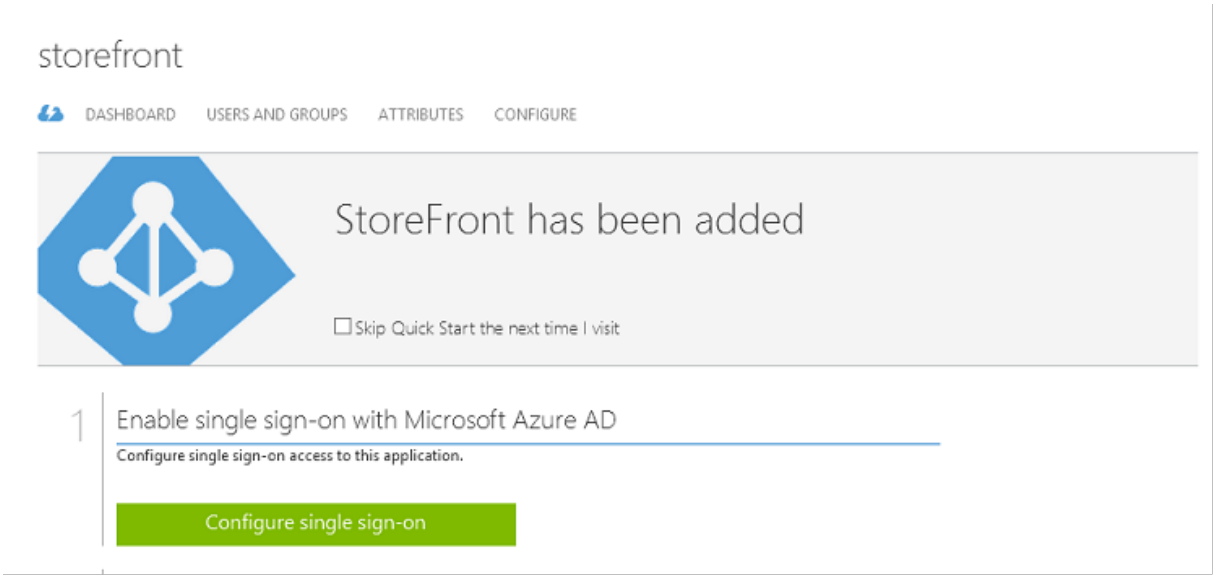
［カスタム］カテゴリの［私の組織で使用している、一覧にないアプリケーションを追加］を選択して、ユーザーが使用する新しいカスタムアプリケーションを作成します。

アイコンの構成

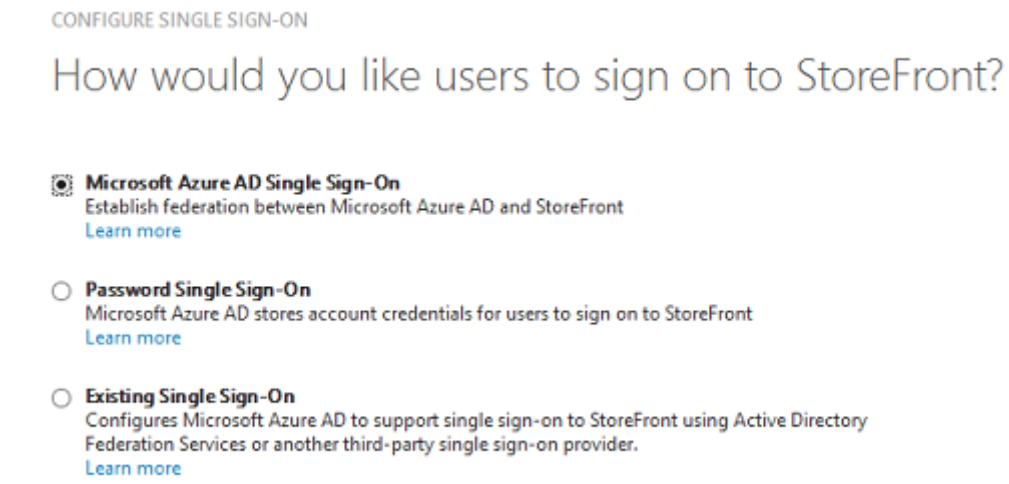
縦横 215 ピクセルの画像を作成して［構成］ページにアップロードし、アプリケーションのアイコンとして使用します。

SAML 認証の構成

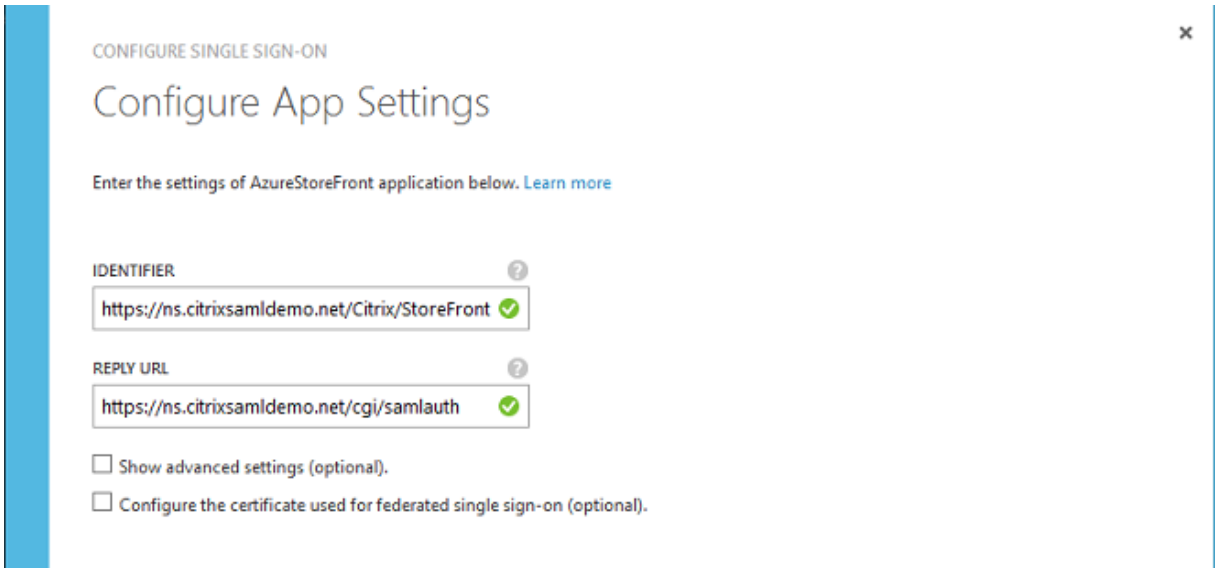
アプリケーションダッシュボードの概要ページに戻り、［シングルサインオンの構成］を選択します。



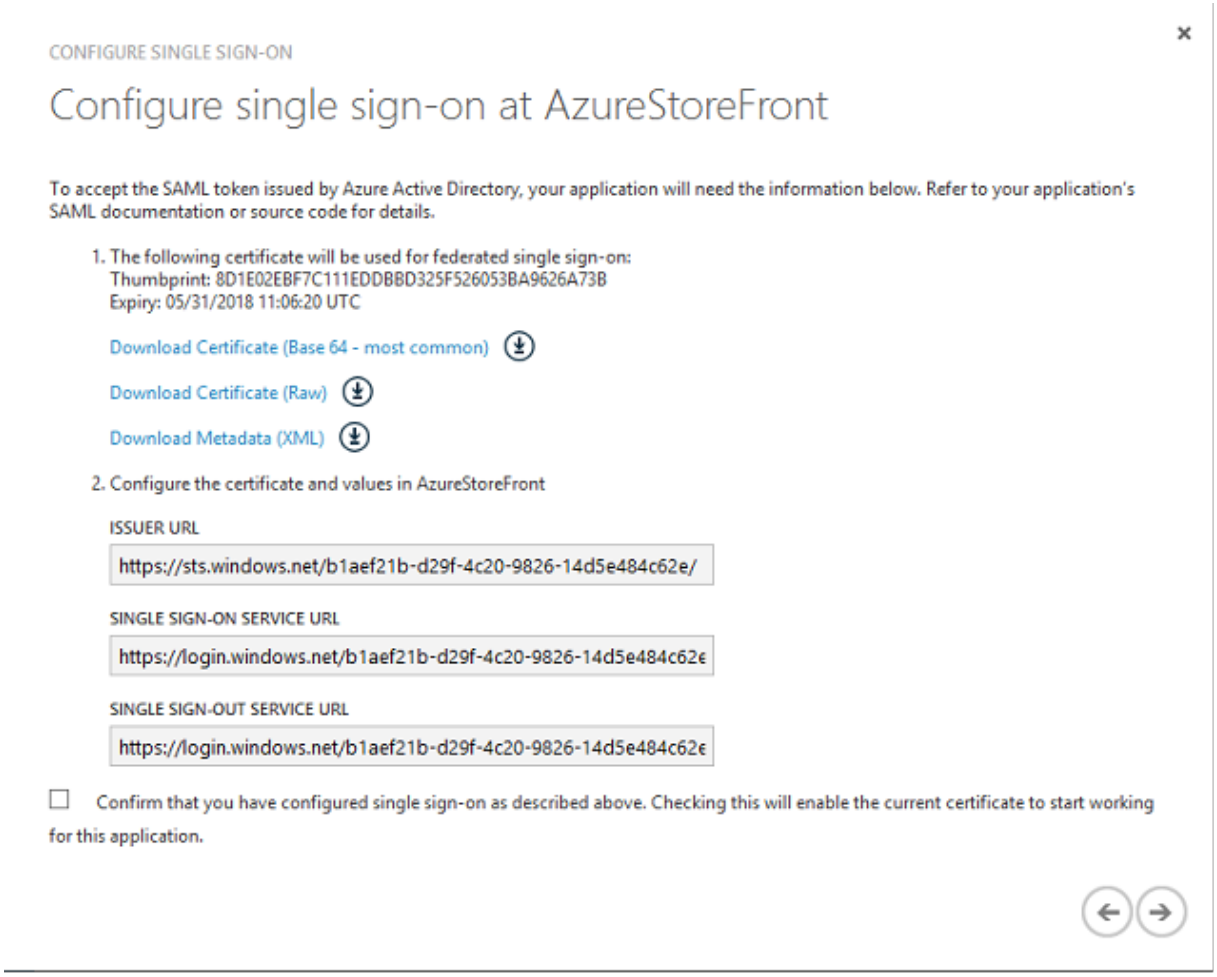
この展開では、［**Microsoft Azure AD** のシングルサインオン］に対応する SAML 2.0 認証を使用します。



［識別子］には任意の文字列を指定できます（NetScaler に提供された構成と一致する必要があります）。この例では、［応答 **URL**］が NetScaler サーバーの/cgi/samlauth になっています。



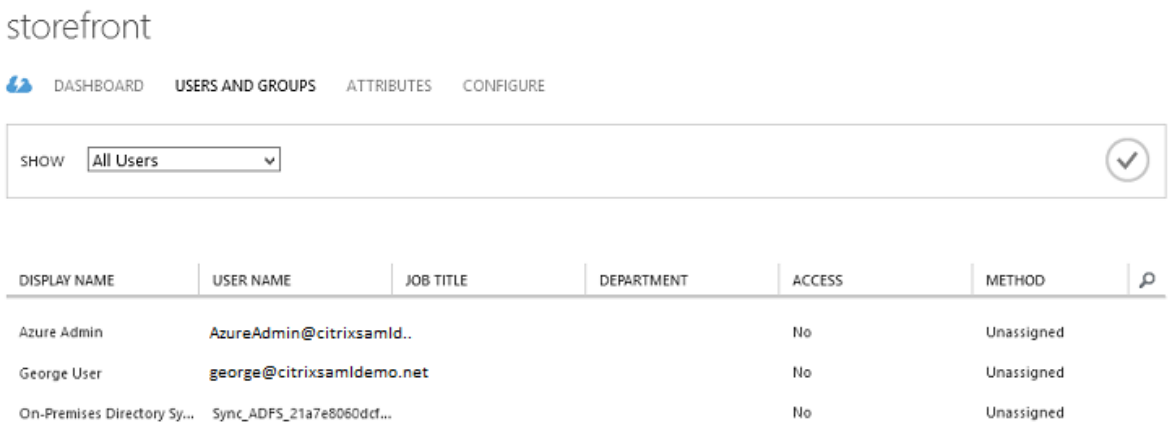
次のページには、NetScaler を Azure AD の証明書利用者として構成するために使用される情報が含まれています。



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。

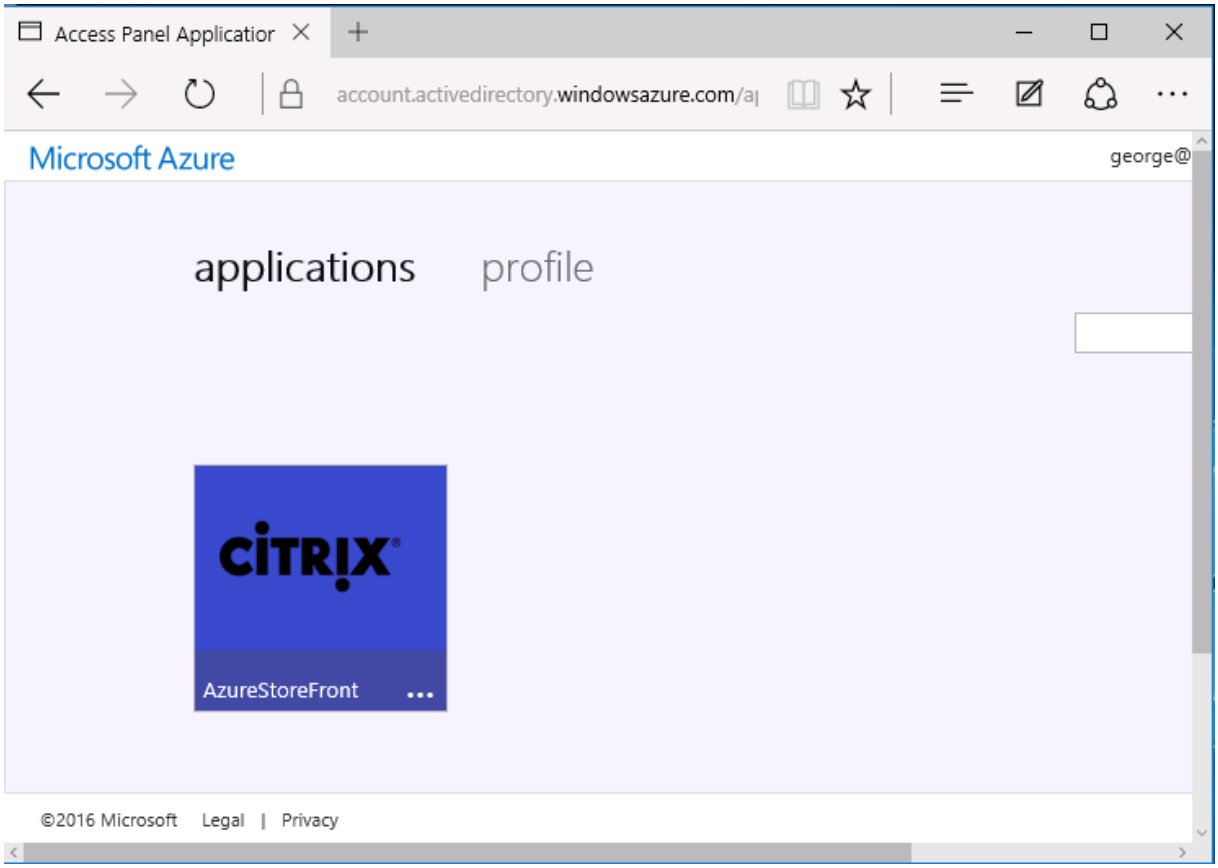
ユーザーへのアプリケーションの割り当て

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、<user>@<domain> パターンに従っていないため、明示的にマップする必要があります。



MyApps ページ

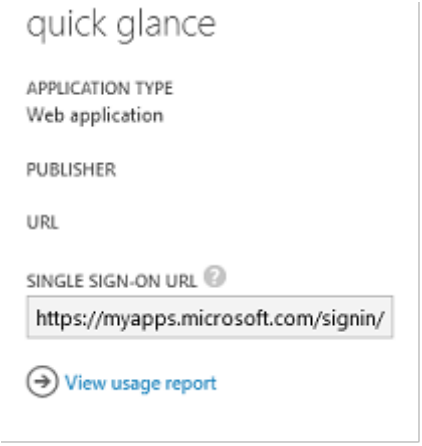
アプリケーションが構成されると、https://myapps.microsoft.comで、Azure アプリケーションのユーザー一覧に表示されます。



Azure AD に参加している場合、ログオンしたユーザーは、Windows 10 により、Azure アプリケーションへのシングルサインオンがサポートされます。アイコンをクリックすると、ブラウザーは前に構成した SAML cgi/samlauth Web ページに移動します。

シングルサインオン **URL**

Azure AD ダッシュボードのアプリケーションに戻ります。アプリケーションに利用できるシングルサインオン URL があることを確認します。この URL は、Web ブラウザーリンクの提供や、StoreFront に直接移動するための、スタートメニューのショートカットの作成に使用されます。



この URL を Web ブラウザーにペーストして、前に構成した NetScaler cgi/samlauth Web ページに、Azure AD がリダイレクトするようにします。これが機能するのは、割り当てられたユーザーだけです。また、シングルサインオンが利用できるのは、Windows 10 の Azure AD に参加しているログオンセッションだけです。（そのほかのユーザーには、Azure AD の資格情報の入力が求められます。）

NetScaler Gateway のインストールと構成

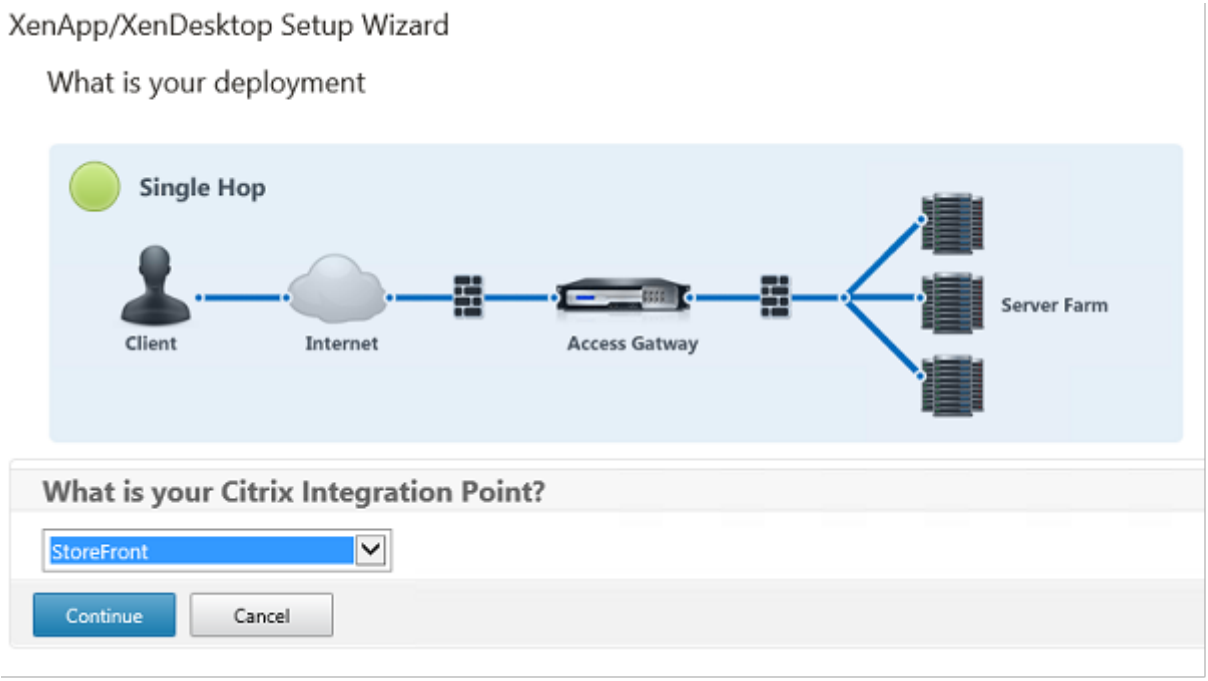
この例では、展開へのリモートアクセスに、NetScaler を実行する独立した仮想マシンを使用します。仮想マシンは Azure ストアで購入できます。この例では、NetScaler 11.0 の「Bring your own License」バージョンを使用しています。

Web ブラウザーのアドレスバーに内部 IP アドレスを入力し、ユーザー認証の際に指定された資格情報を使用して、NetScaler 仮想マシンにログオンします。Azure AD 仮想マシンの nsroot ユーザーのパスワードを変更する必要があることに注意してください。

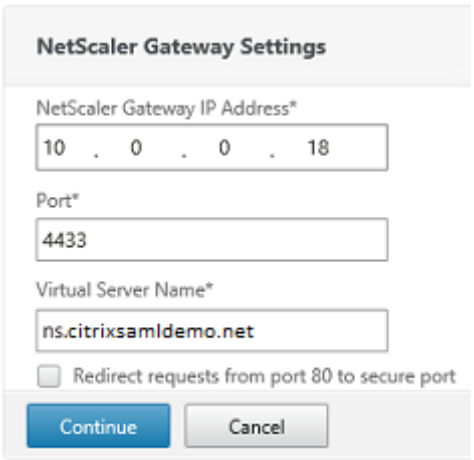
ライセンスを追加し、各ライセンスファイルが追加されたら ［再起動］ を選択して、DNS リゾルバーが Microsoft ドメインコントローラーをポイントするようにします。

XenApp および **XenDesktop** セットアップウィザードの実行

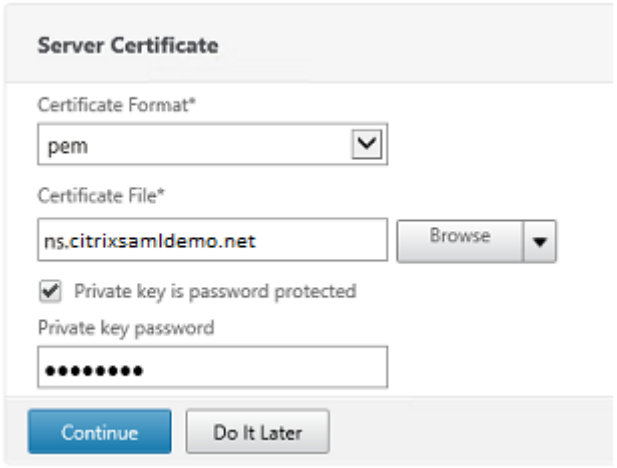
この例では、SAML を使用しない、シンプルな StoreFront 統合を構成することから始めます。この展開が機能するようになってから、SAML のログオンポリシーが追加されます。



NetScaler および StoreFront の標準設定を選択します。Microsoft Azure での使用のため、この例ではポート 443 ではなく、ポート 4433 を構成します。あるいは、ポート転送したり、NetScaler 管理 Web サイトを再マップしたりすることもできます。

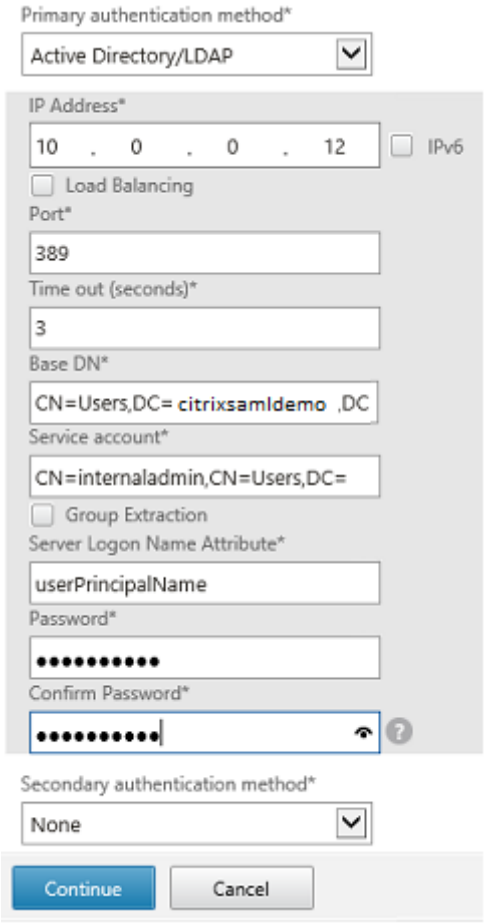


この例では、簡単にするために、ファイルに保存された既存のサーバー証明書と秘密キーをアップロードします。



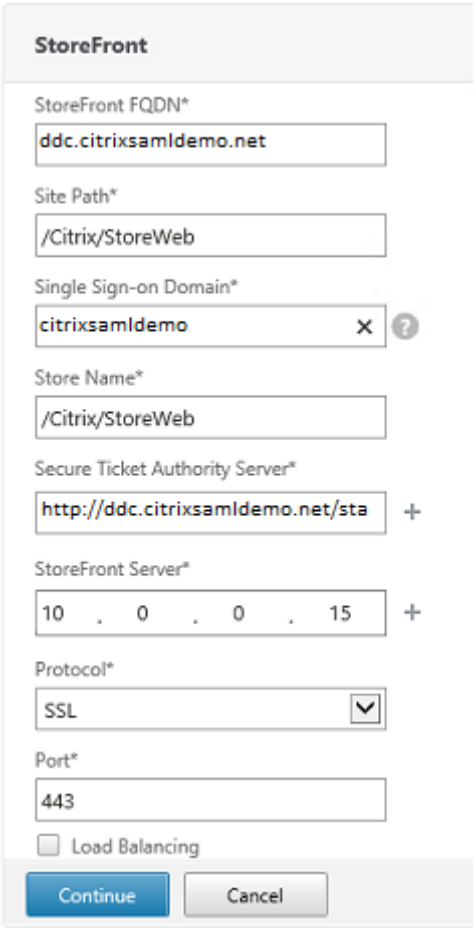
AD アカウント管理のためのドメインコントローラーの構成

ドメインコントローラーはアカウント解決に使用されるため、その IP アドレスをプライマリ認証方法に追加します。ダイアロ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。



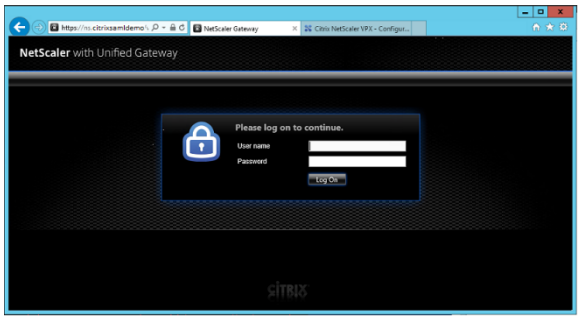
StoreFront アドレスの構成

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。



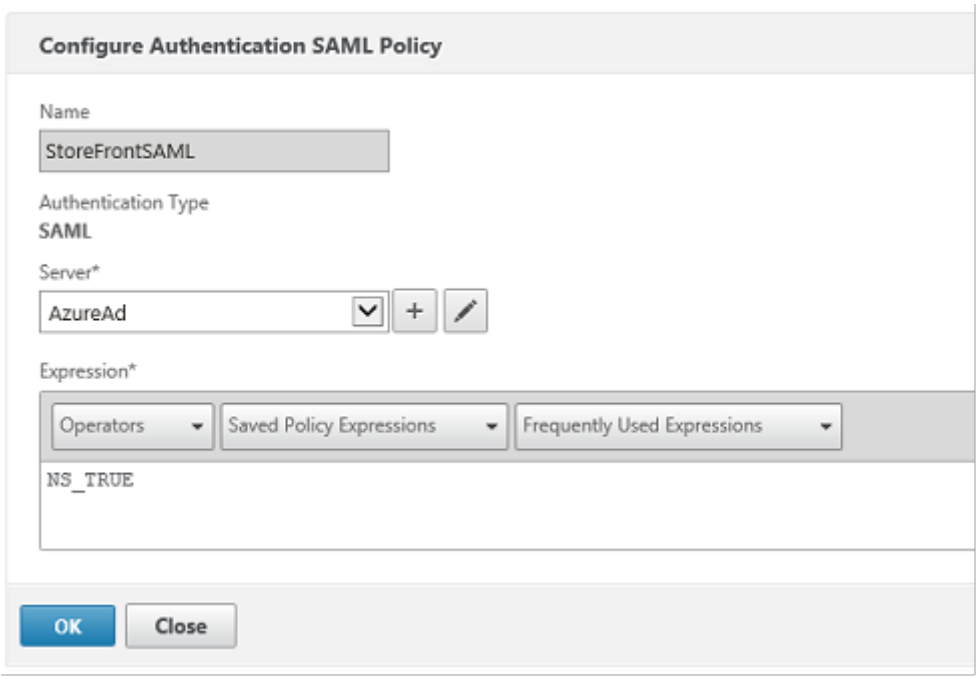
NetScaler の展開を検証

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。

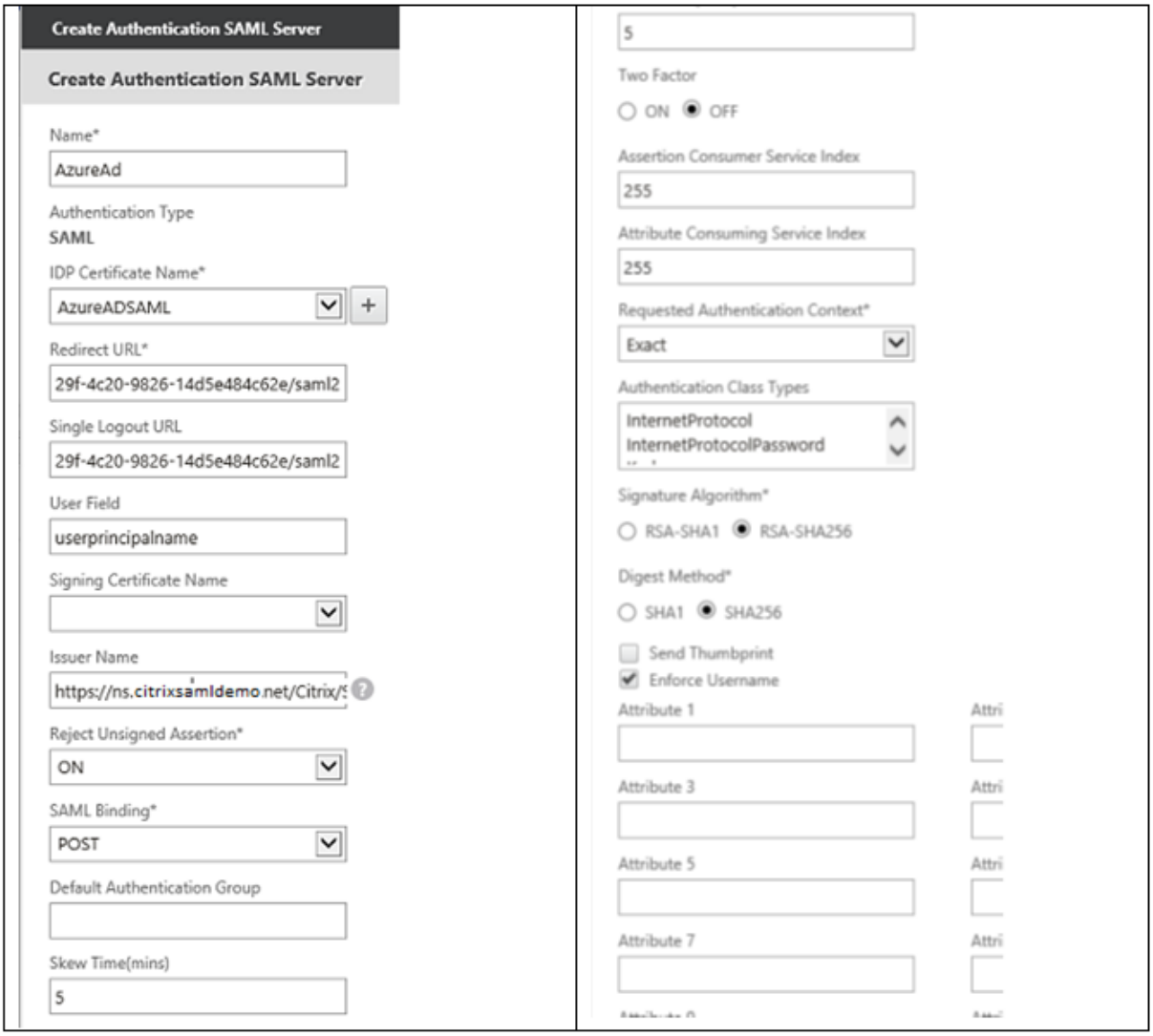


NetScaler SAML 認証サポートの有効化

StoreFront での SAML の使用は、ほかの Web サイトで SAMl を使用するのと同様です。**NS_TRUE** の式を使用して、新しい SAML ポリシーを追加します。



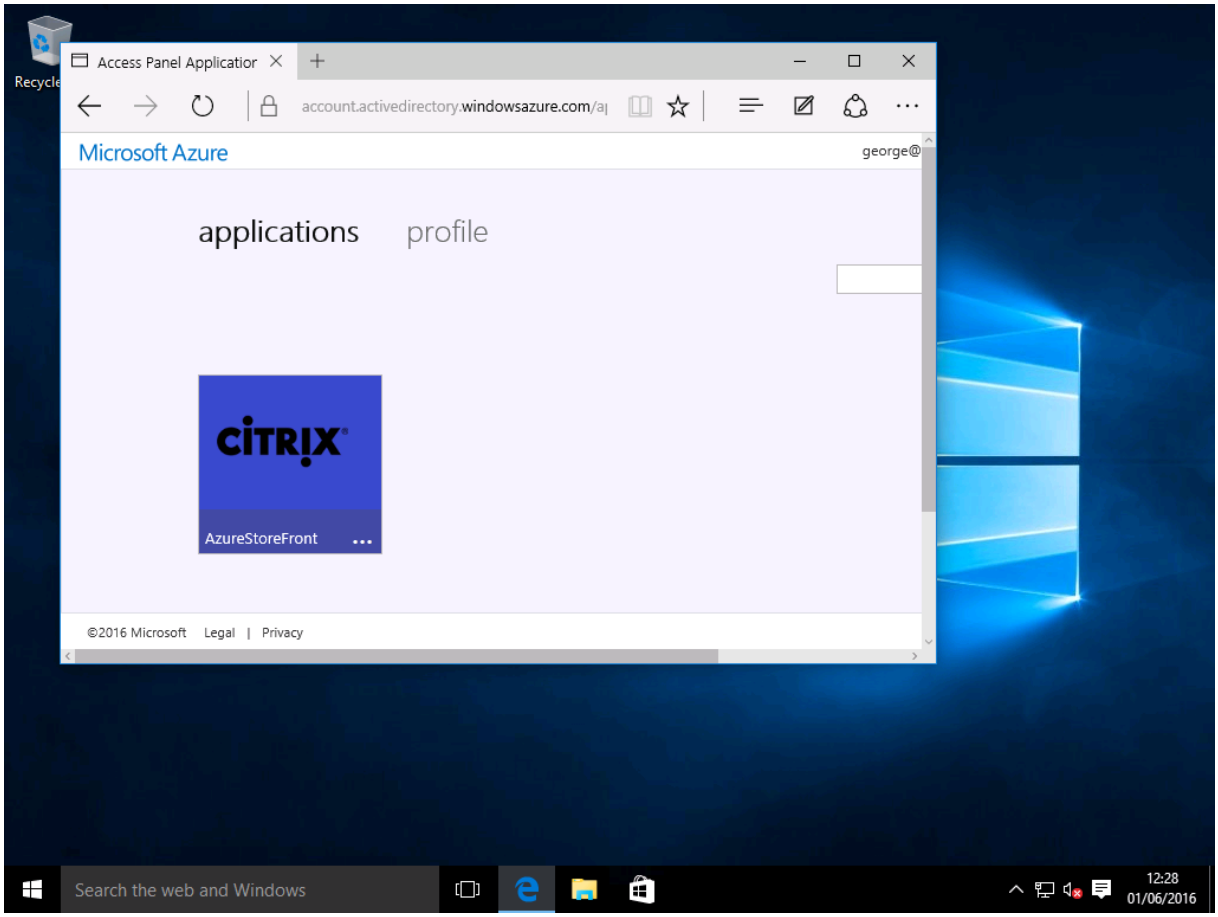
Azure AD から前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。



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。

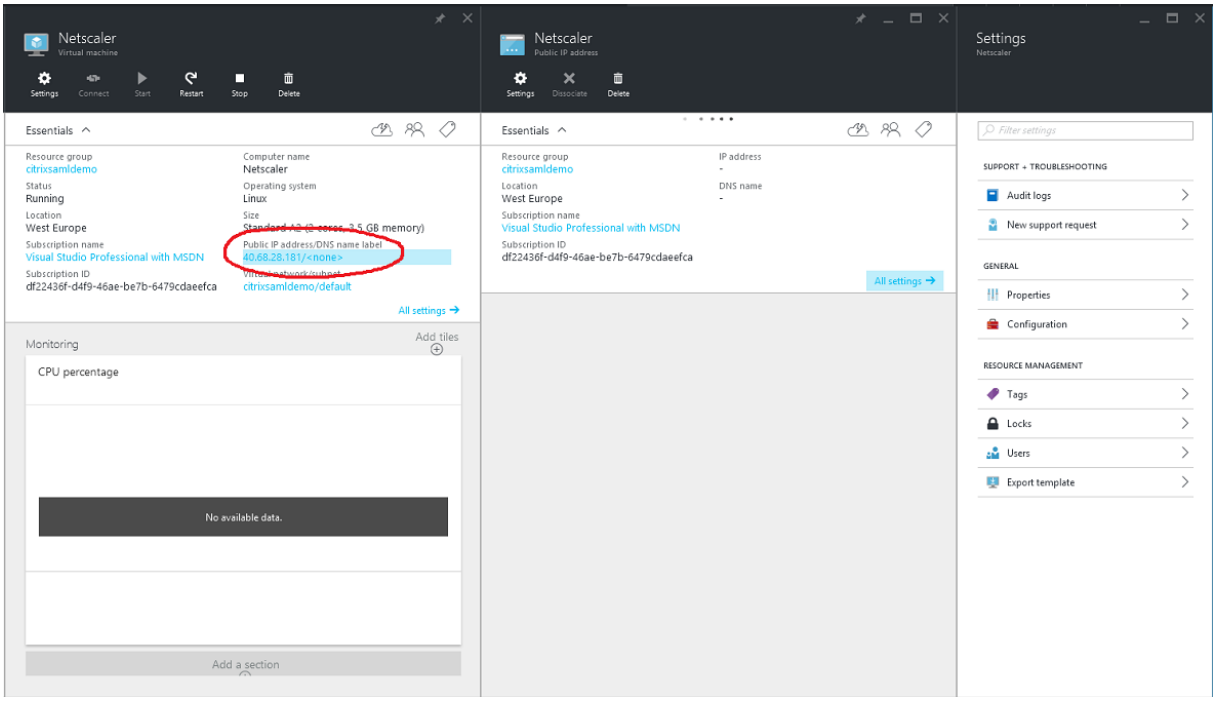
最後に、Azure AD に参加していないマシンも同じ URL で動作することを確認します（ただし、最初の接続時に、Azure AD への明示的なサインオンが 1 回行われます）。

付録

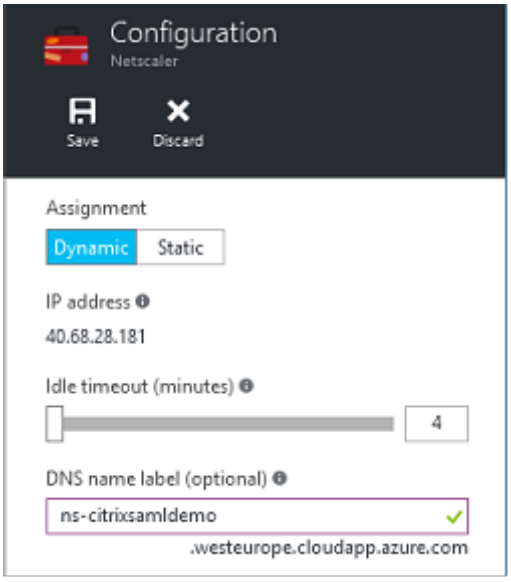
Azure で仮想マシンをセットアップする場合は、構成に必要な標準オプションがいくつかあります。

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、動的に更新された DNS ラベルで参照できる、パブリック IP アドレスも提供されます。



［パブリック **IP** アドレス**/DNS** 名］ラベルの［構成］を選択します。仮想マシンのパブリック DNS アドレスを選択します。これは、ほかの DNS ゾーンファイルでの CNAME 参照に使用でき、IP アドレスが再割り当てされた場合も、すべての DNS レコードが正しく仮想マシンをポイントするようにします。

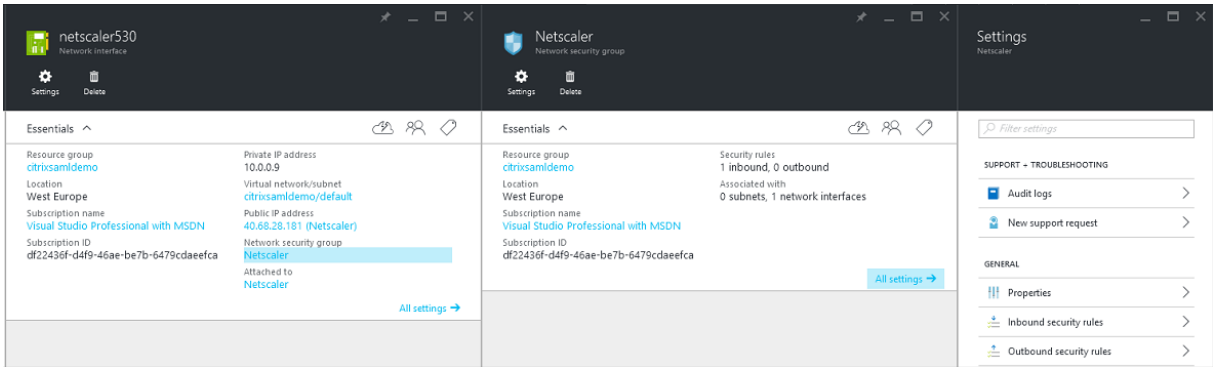


ファイアウォールルールのセットアップ（セキュリティグループ）

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、「フェデレーション認証サービスのアーキテクチャの概要」を参照してください。
- 「フェデレーション認証サービスの構成と管理」では「方法」の記事を紹介しています。

Federated Authentication System の方法：構成と管理

August 24, 2021

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、「フェデレーション認証サービス」を参照してください。
- 「Federated Authentication Service のアーキテクチャの概要」では、FAS の主要アーキテクチャの概要を説明し、より複雑なアーキテクチャに関するそのほかの記事へのリンクを掲載しています。

フェデレーション認証サービスの証明機関の設定

August 24, 2021

この記事では、Citrix フェデレーション認証サービス（FAS）を FAS 管理コンソールでサポートされていない証明機関（CA）サーバーと統合するための詳細設定について説明します。この説明では、FAS が提供する PowerShell API を使用します。この記事に記載されている説明を実行する前に、PowerShell の基礎知識を確認してください。

FAS で使用するための複数 **CA** サーバーのセットアップ

このセクションでは、複数の CA サーバーを使用して証明書を発行するための単一 FAS のセットアップ方法について説明します。これにより、CA サーバーの負荷分散とフェールオーバーが可能になります。

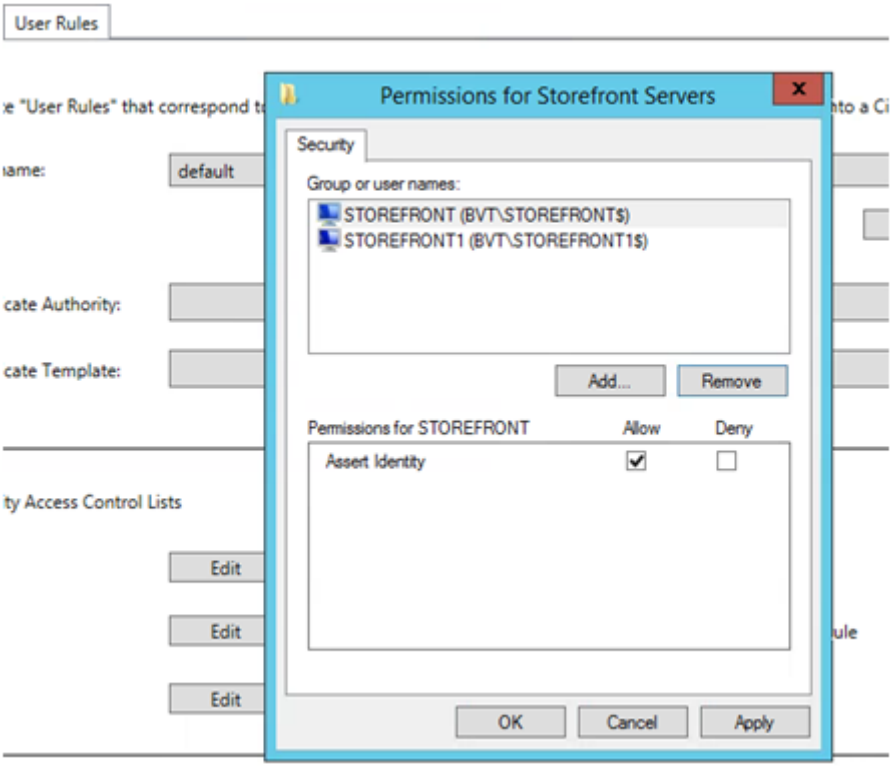
手順 **1**：**FAS** が検出できる **CA** サーバーの数の確認

Get-FASMsCertificateAuthority コマンドレットを使用して、FAS が接続できる CA サーバーを特定します。次の例は、FAS が 3 つの CA サーバーに接続できることを示しています。

```
PS > Add-PSSnapin Citrix*
PS > Get-FasMsCertificateAuthority

Address                         IsDefault   PublishedTemplates
-------                         ---------   ------------------

DC1.bvt.local\bvt-DC1-CA        False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local     False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local     False       {
 Citrix_SmartcardLogon, Citrix_Regis...
```

手順 **2**：既存の証明書定義の変更

ロールの作成には、PowerShell ではなく FAS 管理コンソールを使用することをお勧めします。これにより、後から手動で SDL を追加する手間が省けます。次の例では、アクセスの規則が構成された「default」という名前の役割が作成されています：

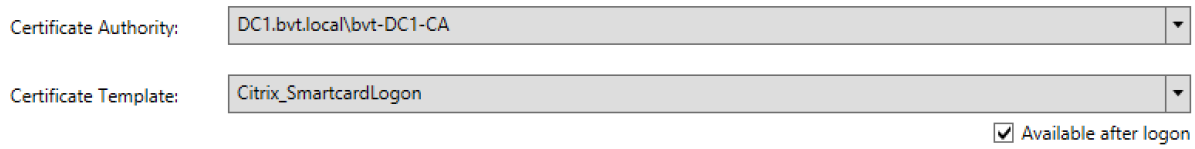


証明機関フィールドに複数の CA を追加するには、PowerShell を使用して証明書定義を構成する必要があります。(複数の CA の追加すこのリリースで FAS 管理コンソールからサポートされていません。)

最初に、証明書定義の名前が必要です。この名前を管理コンソールから特定できない場合は、Get-FASCertificateDefinition コマンドレットを使用してください。

```
PS > Get-FasCertificateDefinition

Name                          : default_Definition
CertificateAuthorities        : {
 DC1.bvt.local\bvt-DC1-CA }

MsTemplate                    : Citrix_SmartcardLogon
AuthorizationCertificate      : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids                    : {
  }

InSession                     : True
```

UI と同等のもの



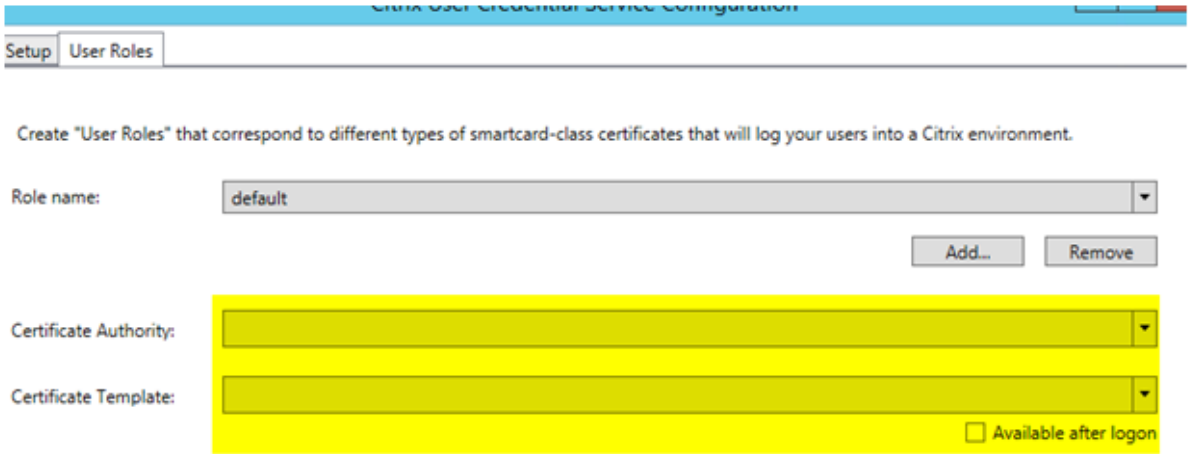
証明書定義の名前が特定できたら、証明書定義を変更して CertificateAuthorities が 1 つではなく一覧で含まれるようにします。

```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

Get-FASCertificateDefinition コマンドレットによって以下が返されます。

```
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
```

複数の CA サーバーで構成した後は、FAS 管理コンソールを使用して FAS を構成できません。ここに示すように、「証明機関」と「証明書テンプレート」フィールドは空になります。



> 注:
>
> コンソールを使用してアクセス規則を修正すると、複数の CA での構成が上書きされます。手順 2 を繰り返す

> だけで、すべての証明機関を再構成することができます。

PowerShell からアクセス規則の ACL を再構成する場合、使用する値が不明な場合は以下の方法をお勧めします。

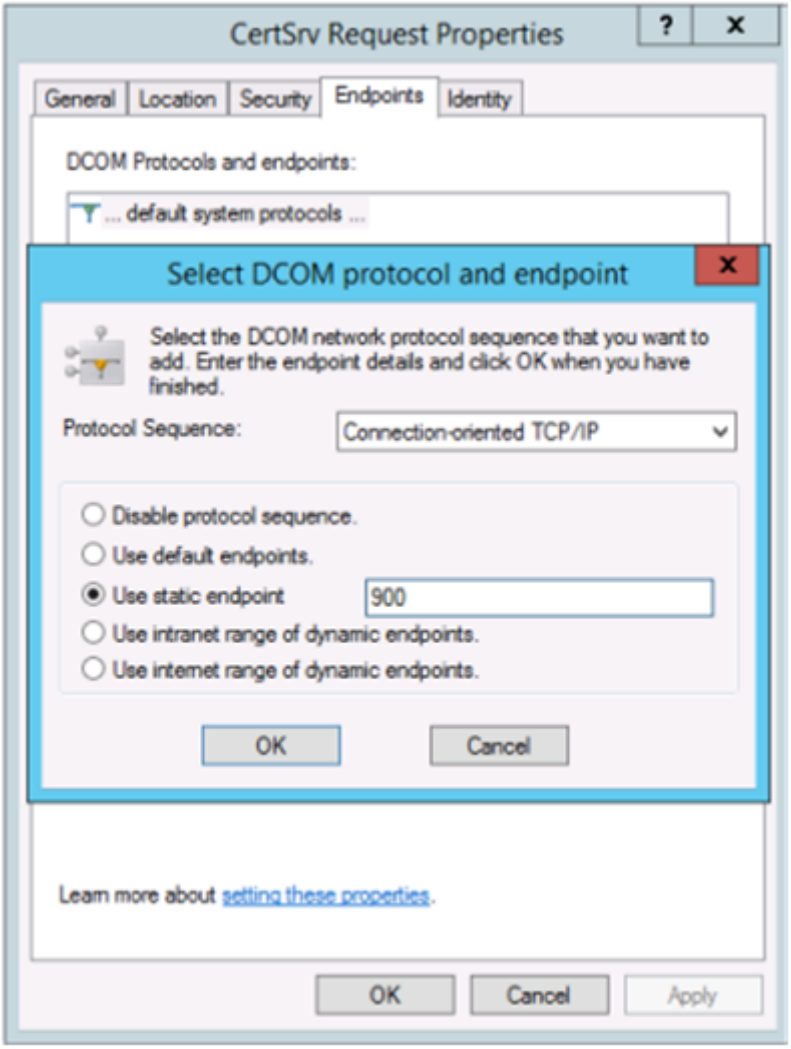
- 同じ CA を使用して別の規則を作成する（例:「テスト」など)。
- 「テスト」規則に必要な ACL を構成する。
- PowerShell を使用して ACL を検査する (Get-FasRule -name “テスト”)。
- PowerShell を使用して元の規則に ACL を適用する（Set-FasRule)。
- 不要になった「テスト」規則を削除する。

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。

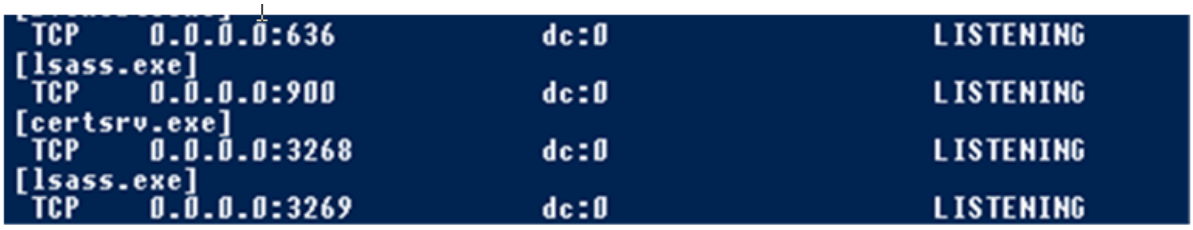
Microsoft CA を TCP アクセス用に構成する

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、certsvr がポート 900 をリスンしていることを確認する必要があります。



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

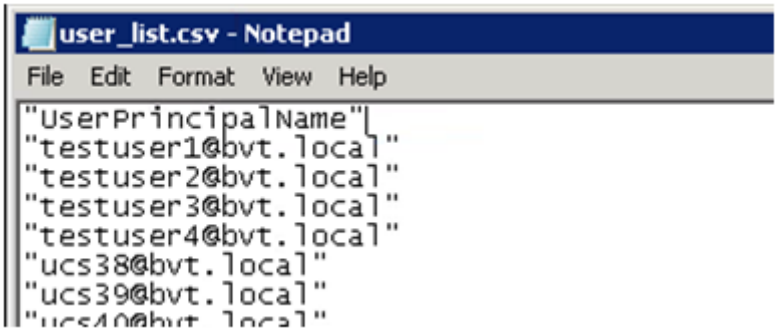
AD に対してクエリを実行し、ユーザーの一覧を次の例のようにファイル（.csv ファイルなど）に保存することにより、証明書の生成を改善することができます。

```
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 -NoTypeInformation -Encoding utf8 -
      delimiter "," $filename
 }
  else {

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
       -NoTypeInformation -Encoding utf8 -delimiter "," $filename
 }

<!--NeedCopy-->
```

Get-ADUser は、ユーザーの一覧を要求するための標準コマンドレットです。上述の例には UserPrincipalName でステータスが「有効」のユーザーのみを一覧表示するためのフィルター引数が含まれています。

SearchBase 引数によって、AD のユーザー検索が制限されます。すべてのユーザーを AD に含めたい場合、これを省略できます。注：このクエリによって、多数のユーザーが返される可能性があります。

CSV の外観は、次のようになります。



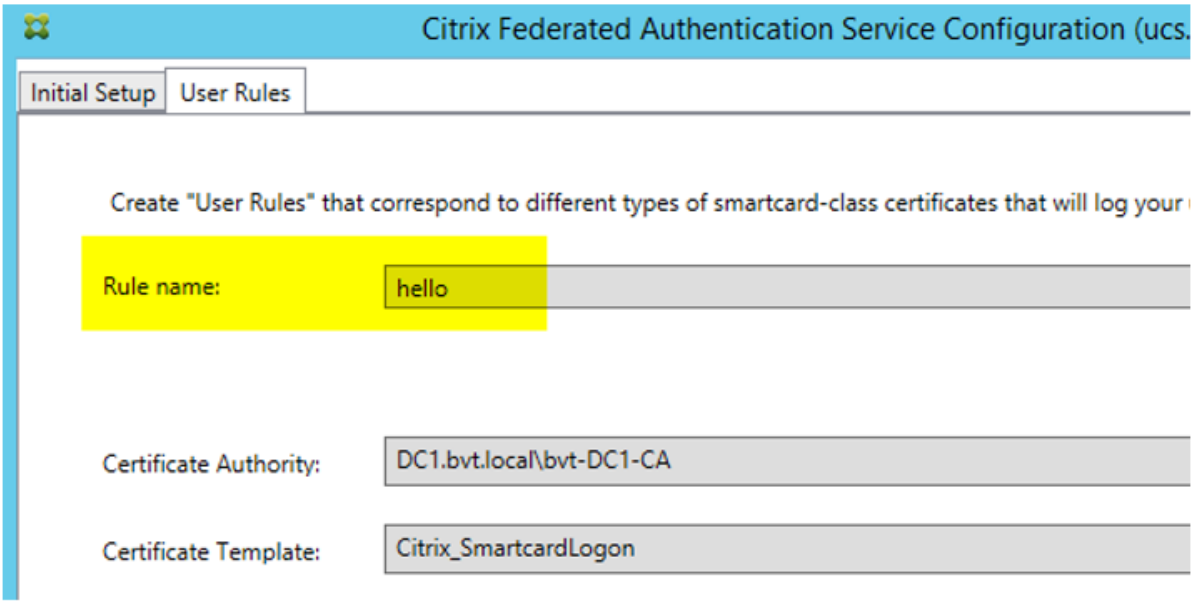
FAS サーバー

以下の PowerShell スクリプトでは、以前生成されたユーザーの一覧を使用してユーザー証明書の一覧が作成されます。

```
Add-PSSnapin Citrix.A*
$csv = "user_list.csv"
$rule = "default" # rule/role in your admin console
$users = Import-Csv -encoding utf8 $csv
foreach ( $user in $users )
{

    $server = Get-FasServerForUser -UserPrincipalNames $user.
       UserPrincipalName
    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

 }

<!--NeedCopy-->
```

複数の FAS サーバーが存在する場合は、特定のユーザーの証明書がメインサーバーで 1 回、フェールオーバーサーバーで 1 回の合計 2 回生成されます。

上述の例は「default」という名前の規則の場合です。規則名が異なる場合（「hello」など）は、スクリプトの $rule 変数を変更してください。



登録機関証明書を更新します

複数の FAS サーバーを使用中の場合は、ログオン中のユーザーに影響することなく FAS 認証証明書を更新できます。注：GUI を使用して FAS の権限を取り消したり再び付与したりすることもできますが、これによって FAS の構成オプションがリセットされます。

以下の手順を実行します。

1. 新しい認証証明書を作成します。`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 <FAS server> -MaintenanceMode $true`
4. 新しい認証証明書を置換します。`Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
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 <FAS server> -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、「フェデレーション認証サービスのアーキテクチャの概要」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。

フェデレーション認証サービスの秘密キー保護

August 24, 2021

はじめに

証明書は FAS サーバーのレジストリに保存されます。関連する秘密キーは、FAS サーバーの Network Service アカウントを使用して保存され、デフォルトでエクスポート不可としてマークされます。

秘密キーには 2 つの種類があります。

- 登録機関（RA）証明書に関連付けられている、Citrix_RegistrationAuthority 証明書テンプレートからの秘密キー
- ユーザー証明書に関連付けられている、Citrix_SmartcardLogon 証明書テンプレートからの秘密キー

RA 証明書には Citrix_RegistrationAuthority_ManualAuthorization（デフォルトで 24 時間有効）および Citrix_RegistrationAuthority（デフォルトで 2 年間有効）の 2 つの種類があります。

FAS 管理コンソールの初回セットアップの手順 3 で、管理者が［許可する］をクリックすると、FAS サーバーによってキーペアが生成され、証明書署名要求（CSR）が Citrix_RegistrationAuthority_ManualAuthorization 証明書の証明機関（CA）に送信されます。これは一時的な証明書であり、デフォルトで 24 時間有効です。CA は自動的に証明書を発行しません。証明書を発行するには、管理者による CA での手動の権限許可が必要です。証明書が FAS サーバーに発行されると、FAS は Citrix_RegistrationAuthority_ManualAuthorization 証明書を使用して Citrix_RegistrationAuthority 証明書（デフォルトで 2 年間有効）を自動的に取得します。FAS サーバーは、Citrix_RegistrationAuthority 証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorization の証明書とキーを削除します。

RA 証明書ポリシーは秘密キーを所有するものすべてに対して、テンプレートで構成されたユーザーセットに対する証明書要求の発行を許可するため、RA 証明書に関連付けられた秘密キーは特に機密です。結果として、このキーを管理するものはだれでも、セット内のユーザーと同様、環境に接続できます。

次のいずれかを使用して、組織のセキュリティ要件に準拠して秘密キーが保護されるように FAS サーバーを構成できます:

- Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー（RA 証明書およびユーザー証明書両方の秘密キー用）。
- トラステッドプラットフォームモジュール（TPM）チップを使用した Microsoft プラットフォームキー記憶域プロバイダー（RA 証明書の秘密キー用）、および Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー（ユーザー証明書の秘密キー用）。

- ハードウェアセキュリティモジュール（HSM）ベンダーの HSM デバイスを使用した暗号サービスまたはキー記憶域プロバイダー（RA 証明書およびユーザー証明書両方の秘密キー用）。

秘密キーの構成設定

3 つのオプションのうちいずれかを使用して FAS を構成します。テキストエディターを使用して、Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルを編集します。ファイルのデフォルトの場所は FAS サーバーの Program Files\Citrix\Federated Authentication Service フォルダーです。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

FAS は、サービスの起動時にのみ構成ファイルを読み込みます。いずれかの値が変更された場合、新しい設定を反映させるために FAS を再起動する必要があります。

Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルの関連する値を次のとおり設定します：

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**（CAPI と CNG API の切り替え）

値	コメント
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	コメント
Microsoft Enhanced RSA および AES Cryptographic Provider	デフォルトは CAPI プロバイダーです
Microsoft ソフトウェアキー記憶域プロバイダー	デフォルトは CNG プロバイダーです
Microsoft プラットフォームキー記憶域プロバイダー	デフォルトは TPM プロバイダーです。TPM はユーザーキーにはお勧めしません。TPM は RA キーにのみお使いください。FAS サーバーを仮想化環境で実行する予定の場合は、TPM およびハイパーバイザーのベンダーに仮想化がサポートされているかどうかを確認してください。
HSM_Vendor CSP/Key 記憶域プロバイダー	HSM ベンダーによって提供されます。値はベンダーによって異なります。FAS サーバーを仮想化環境で実行する予定の場合は、HSM ベンダーに仮想化がサポートされているかどうかを確認してください。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType**（CAPI API の場合のみ必要）

値	コメント
24	Default。Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24 を参照します。CAPI で HSM を使用する場合、および HSM ベンダーで別のタイプを指定されている場合以外は、常に 24 である必要があります。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**（FAS が秘密キー操作を実行する必要がある場合は、ここで使用されている値を使用します）。秘密キーの「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合は、TPM キーストレージの使用が許可されます。

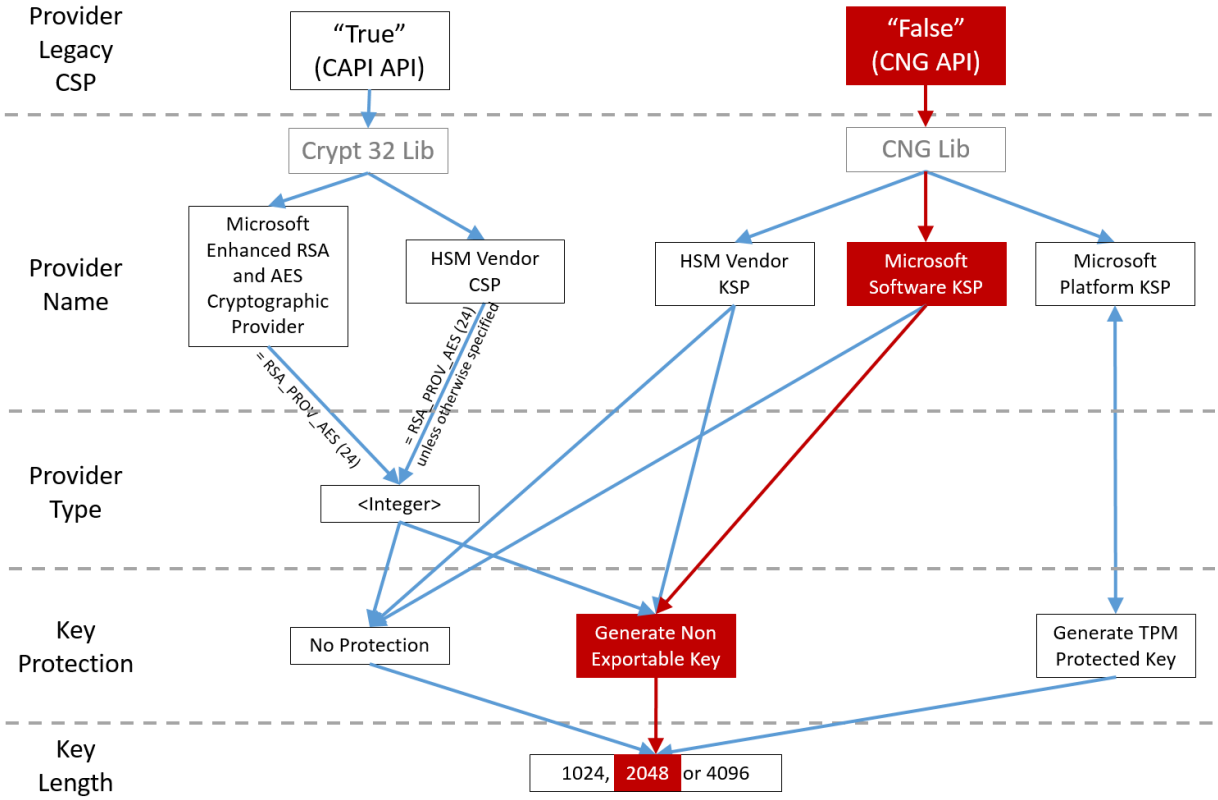
値	コメント
NoProtection	秘密キーをエクスポートできます。
GenerateNonExportableKey	Default。秘密キーをエクスポートできません。

値	コメント
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単位で指定）

値	コメント
2048	デフォルト値です。1024 または 4096 を使用することもできます。

構成ファイルの設定を以下に図解します（インストール時のデフォルト設定は赤で示しています）。



構成シナリオの例

例 **1**

この例では、Microsoft ソフトウェアキー記憶域プロバイダーを使用して格納されている RA 証明書の秘密キーおよびユーザー証明書の秘密キーについて説明します。

これはデフォルトのインストール後の構成です。追加の秘密キー構成は不要です。

例 **2**

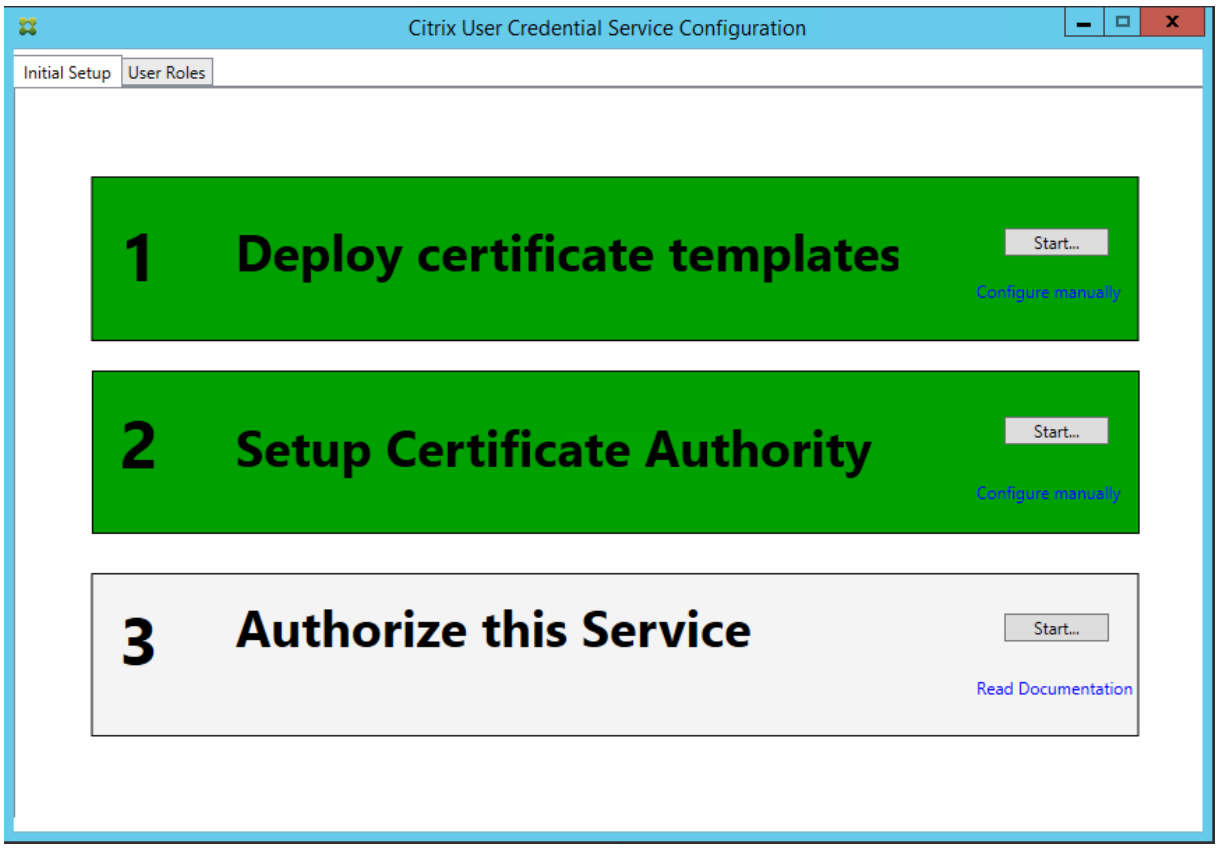
この例は、Microsoft プラットフォームキー記憶域プロバイダーを使用して FAS サーバーのマザーボードのハードウェア TPM に格納されている RA 証明書秘密キー、および Microsoft ソフトウェアキー記憶域プロバイダーを使用して格納されているユーザー証明書秘密キーを示しています。

このシナリオでは、FAS サーバーのマザーボード上の TPM は TPM の製造元のドキュメントに基づいて BIOS で有効化され、その後 Windows で初期化されているものとみなしています。詳しくは、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)?redirectedfrom=MSDNを参照してください。

PowerShell の使用（推奨）

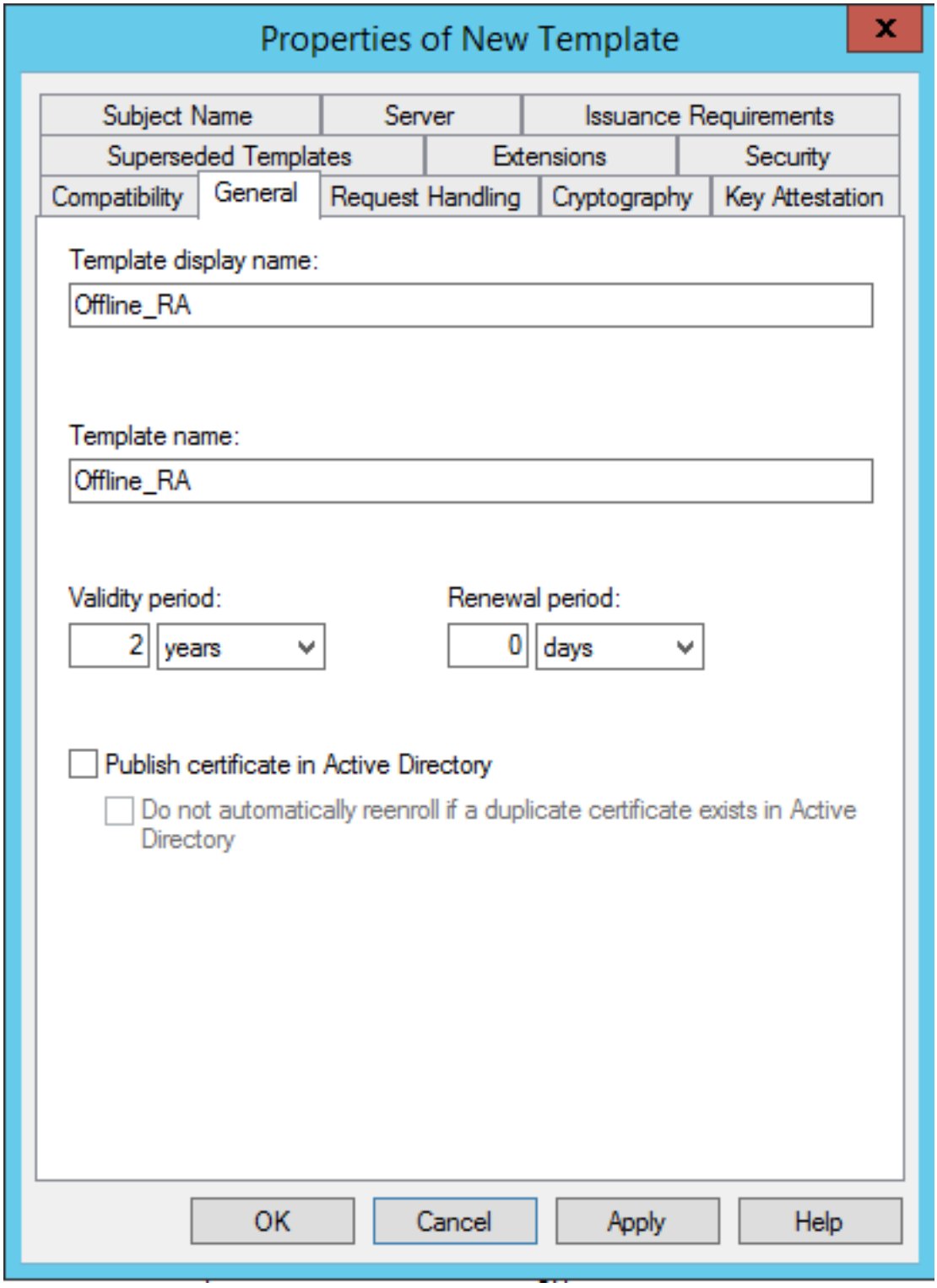
PowerShell を使用して、RA 証明書をオフラインで要求できます。これは、CA がオンラインの CSR で RA 証明書を発行しないようにする組織にお勧めです。FAS 管理コンソールを使用してオフラインの RA CSR を行うことはできません。

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_ManualAuthor**
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.FederatedAuthenticationService.V1

手順 **5**：RSA キーペアを FAS サーバーの TPM 内で生成し、FAS サーバーで次の PowerShell コマンドレットを入力して CSR を作成します。注：一部の TPM ではキーの長さが制限されます。デフォルトでは、証明書のキーの長さは 2048 ビットに制限されています。ハードウェアでサポートされているキーの長さを指定してください。

New-FasAuthorizationCertificateRequest -UseTPM $true -address

例：

New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net

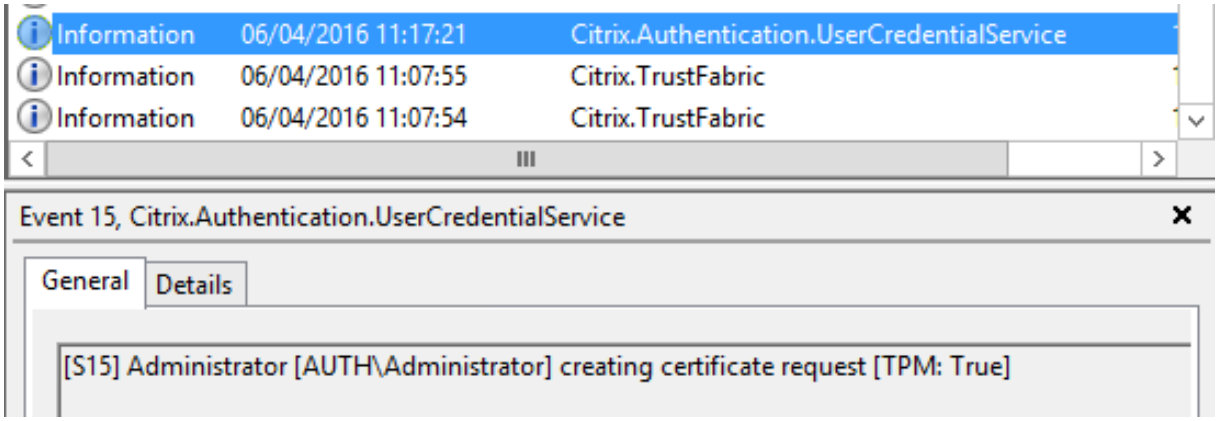
以下が表示されます。

```
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
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfRORW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Dy/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g22DY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaElWXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TD15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

メモ：

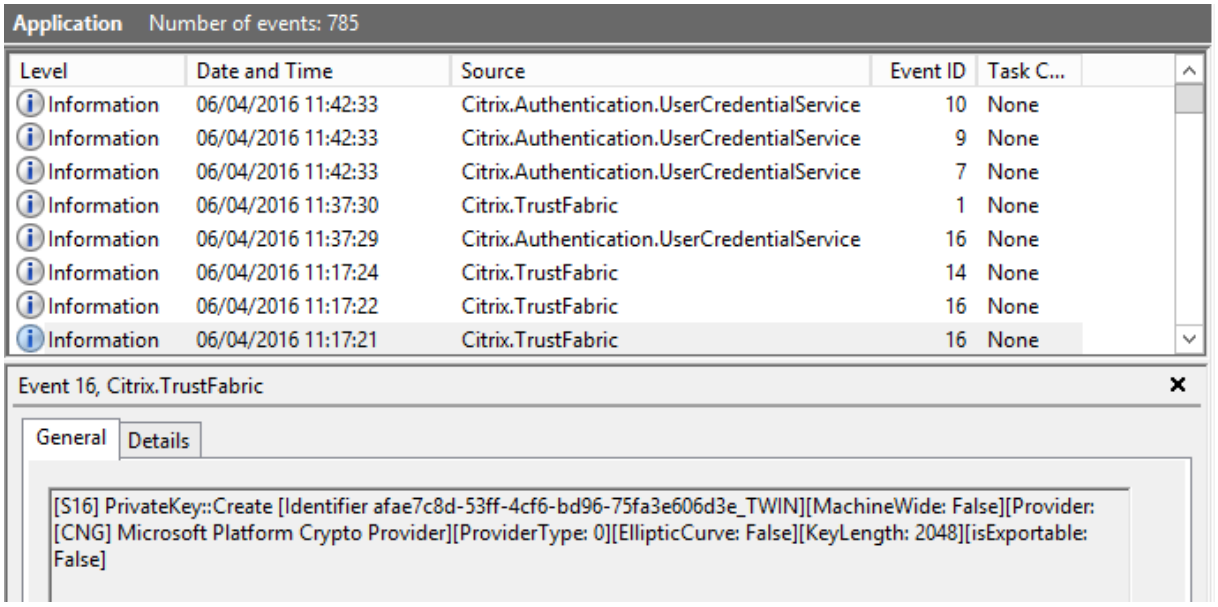
- Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は後続の手順で必要です。
- この PowerShell コマンドレットは、RA 証明書の秘密キーの生成に使用される一時的な「上書き」と認識してください。
- このコマンドレットを実行する場合、FAS サービスが開始されるときに構成ファイルから読み込まれる値がチェックされ、使用するキーの長さが決定されます（デフォルトは 2048 です）。
- この手動の PowerShell によって開始される RA 証明書秘密キー操作で-UseTPM が $true に設定されているため、ファイルからの値で 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。



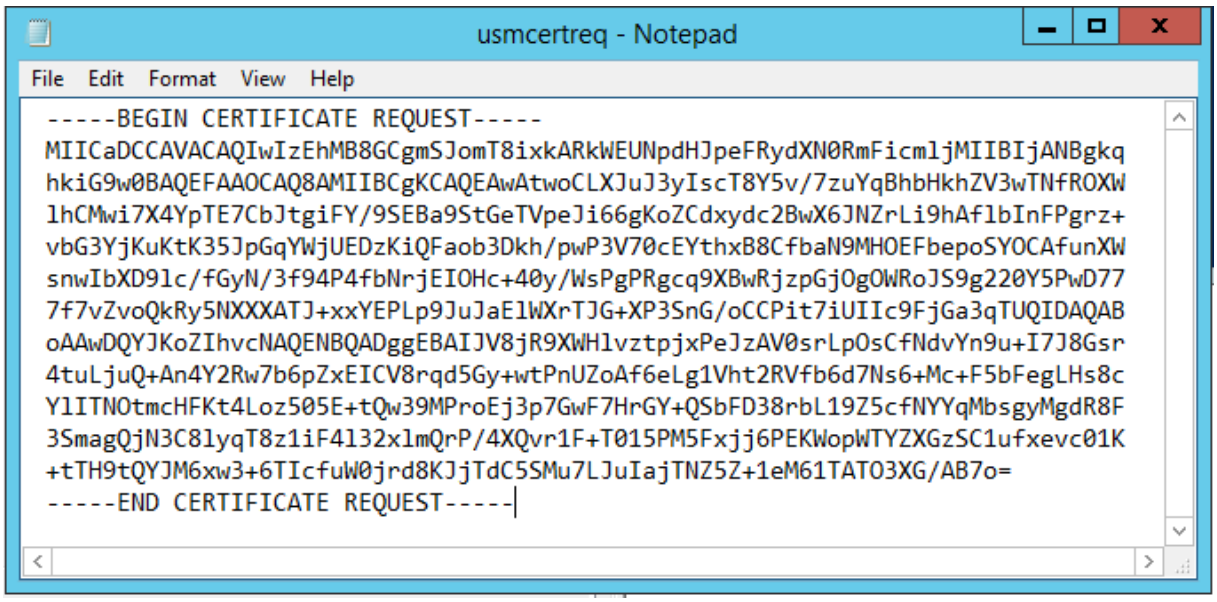
「[TPM:True]」を確認します。

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：

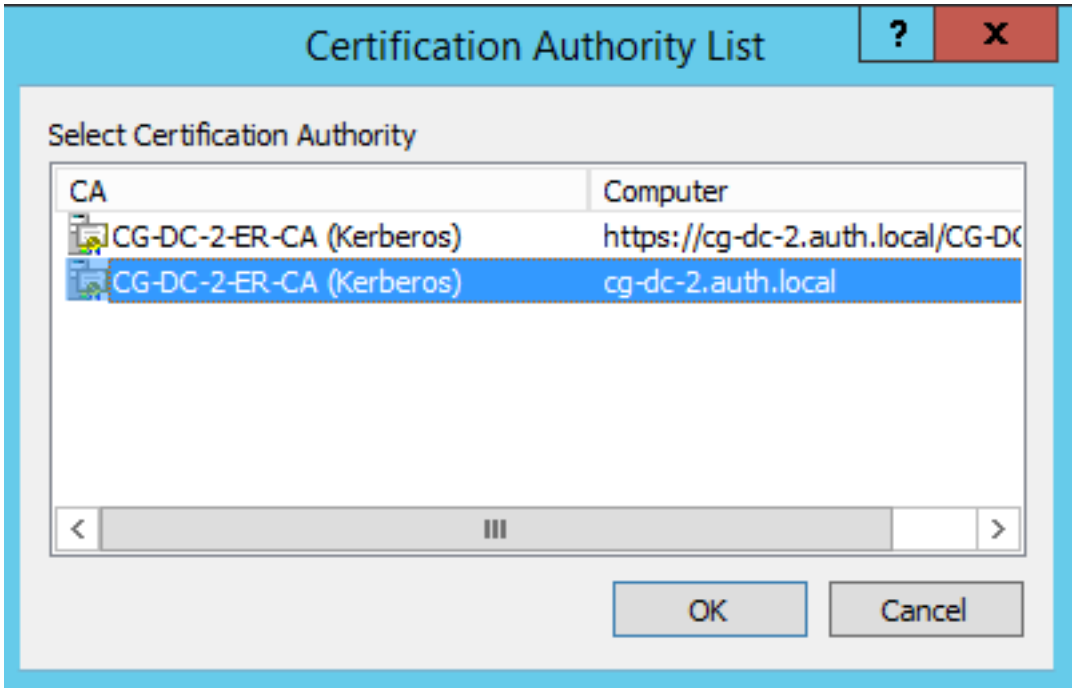
certreq -submit -attrib “certificatetemplate:< 手順 2 の証明書テンプレート >” < 手順 6 の証明書要求ファイル >

例：

certreq -submit -attrib “certificatetemplate:Offline_RA” C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

以下が表示されます。

この時点で、「証明機関の一覧」ウィンドウが表示される可能性があります。この例の CA では http（上部）および DCOM（下部）登録の両方が有効です。使用できる場合は DCOM オプションを選択します。

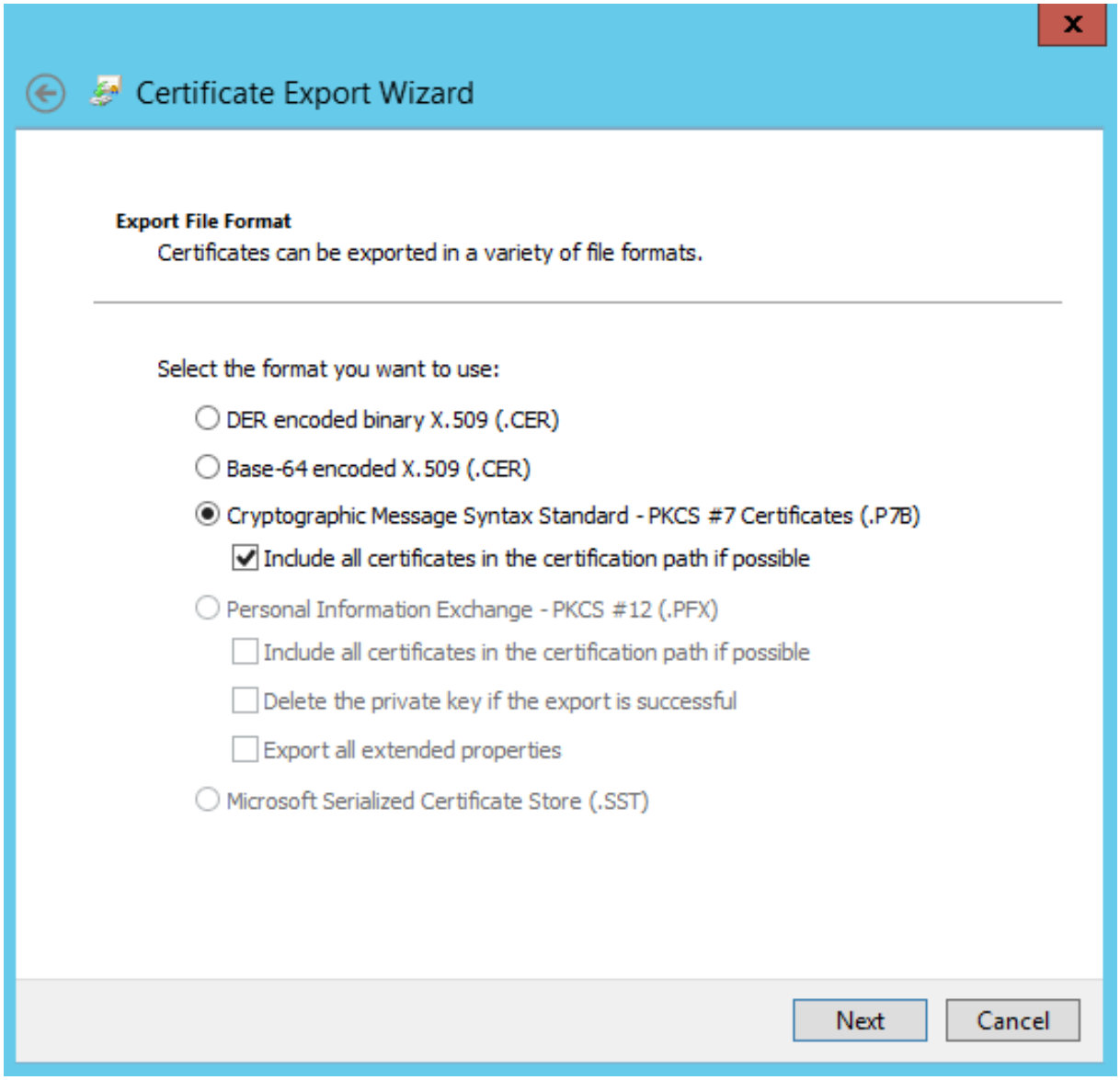


CA が指定されると、PowerShell によって RequestID が表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

手順 **8**: CA サーバーの CA MMC スナップインで、［保留中の要求］をクリックします。要求 ID を記録します。要求を右クリックし、［発行］を選択します。

手順 **9**:［発行した証明書］ノードを選択します。発行したばかりの証明書（要求 ID が一致する証明書）を見つけます。証明書をダブルクリックして開きます。［詳細］タブをクリックします。［ファイルへコピー］をクリックします。証明書のエクスポートウィザードが開きます。［次へ］をクリックします。次のファイル形式のオプションを選択します。



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>
```

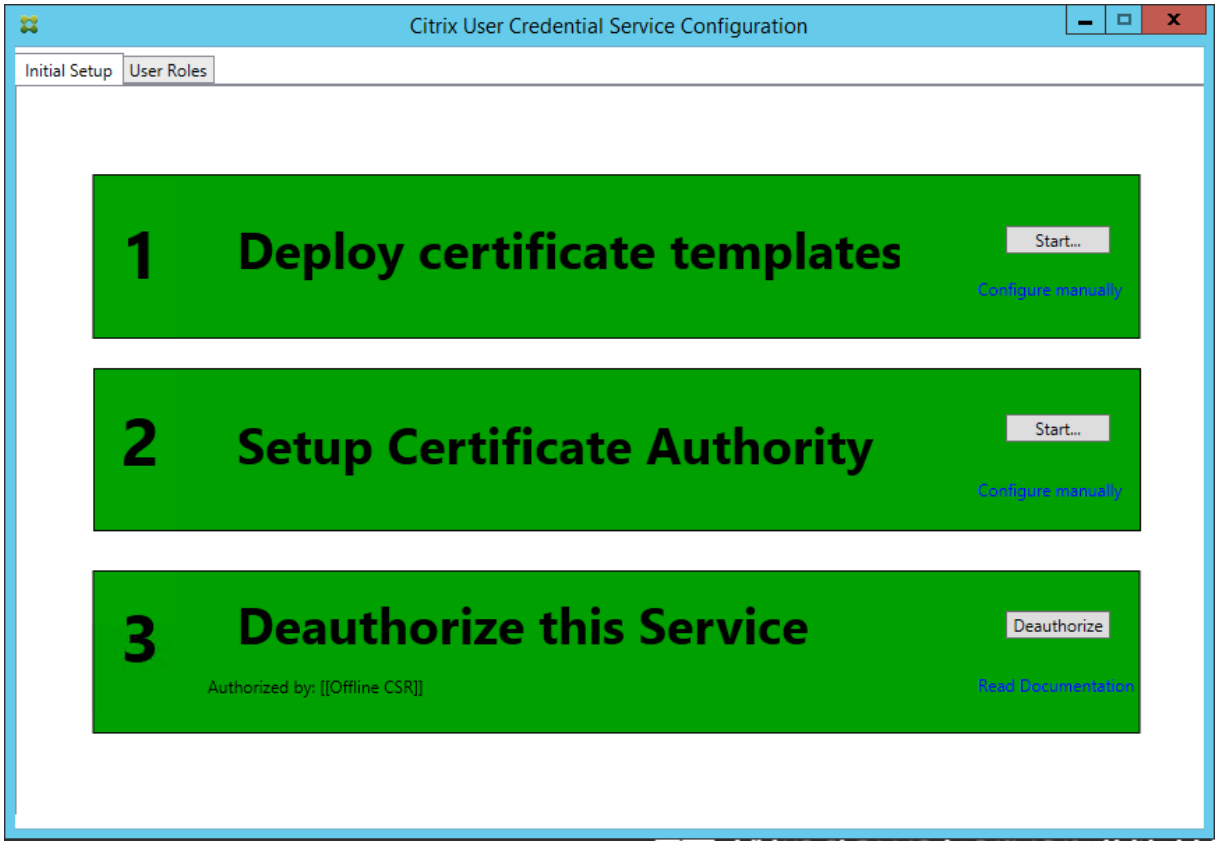
例：

```
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-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

手順 **12**：FAS 管理コンソールを終了して再起動します。



手順「このサービスを許可する」が緑色になり、表示が「このサービスの許可を取り消す」に変更されます。下部のエントリには、「認証元：オフライン CSR」と表示されます。

手順 **13**：FAS 管理コンソールで ［ユーザーロール］タブを選択し、メインの FAS 記事の記述に従って設定を編集します。

注：管理コンソールから FAS の許可を取り消すと、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.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

一部の TPM ではキーの長さが制限されています。デフォルトのキーの長さは、2048 ビットです。ハードウェアでサポートされているキーの長さを指定してください。

手順 **2**：サービスを許可します。

手順 **3**：CA サーバーから、保留中の証明書要求を手動で発行します。RA 証明書が取得されたら、管理コンソールのセットアップ順序の手順 3 が緑色に変わります。この時点で、RA 証明書の秘密キーは TPM で生成されています。証明書はデフォルトで 2 年間有効です。

手順 **4**：次のように構成ファイルを編集し直します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

注：FAS は TPM で保護されたキーでユーザー証明書を生成できますが、TPM は大規模の展開には速度が遅すぎる可能性があります。

手順 **5**： Citrix フェデレーション認証サービスを再起動します。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。

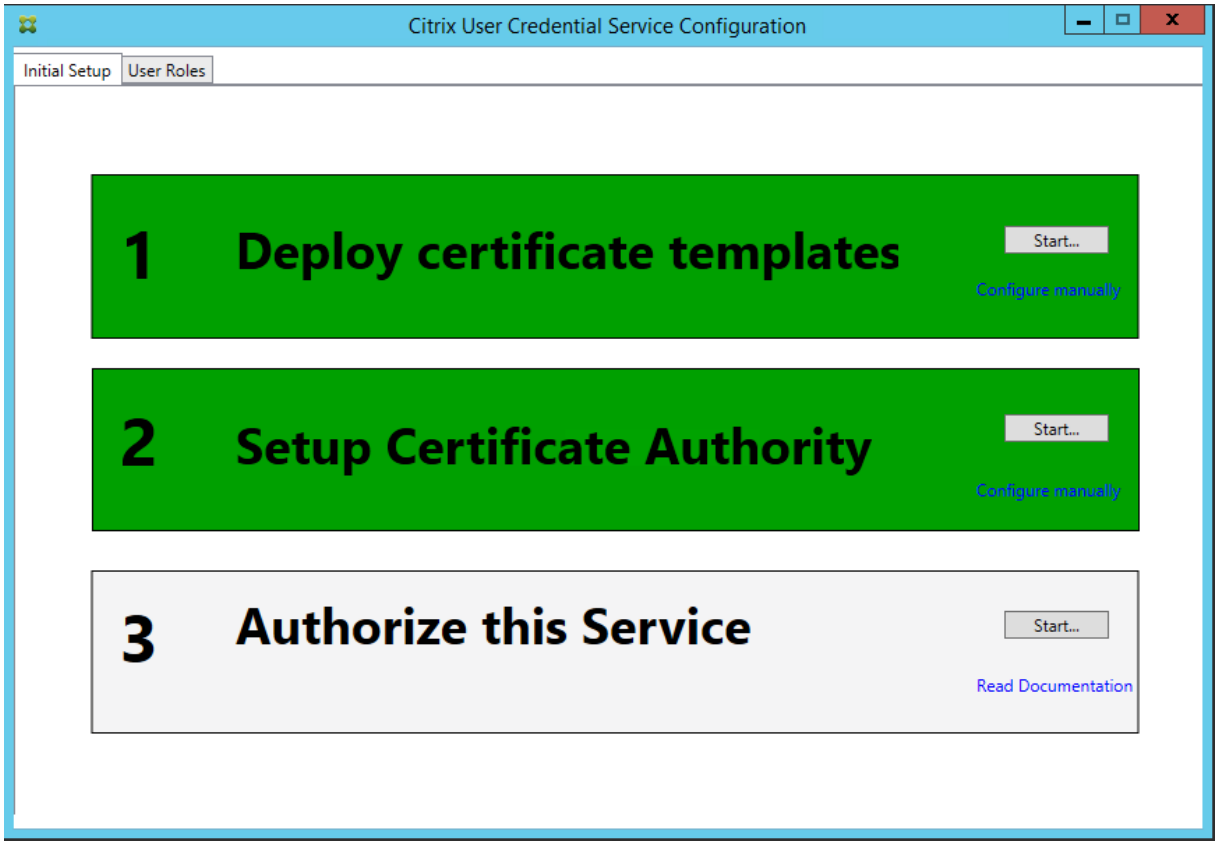
注：管理コンソールから FAS の許可を取り消すと、ユーザー規則が削除されます。

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.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

このシナリオでは、HSM が CNG を使用していると想定しているため、ProviderLegacyCsp の値は false に設定されています。HSM が CAPI を使用している場合は、ProviderLegacyCsp の値は true に設定されます。HSM ベンダーのドキュメントで、HSM が CAPICN と CNG のどちらを使用しているかを確認してください。また、非対称 RSA キー生成でサポートされているキーの長さについても、HSM ベンダーのドキュメントで確認してください。この例では、キーの長さはデフォルトの 2048 ビットに設定されています。指定したキーの長さがお使いのハードウェアでサポートされていることを確認してください。

手順 **4**: Citrix フェデレーション認証サービスを再起動して、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]
```

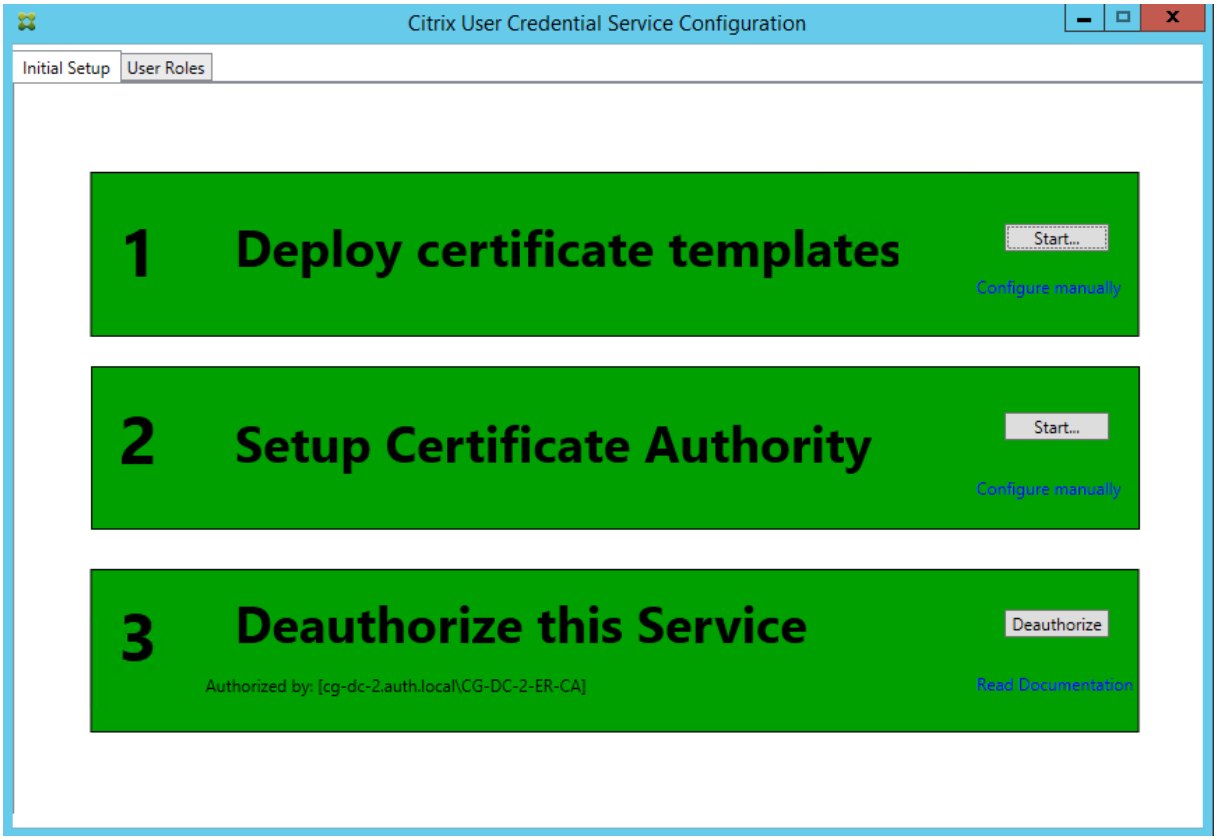
注: [Provider: [CNG] HSM_Vendor's Key Storage Provider] となっています。

手順 **7**: CA サーバーの CA MMC で、［保留中の要求］ノードを選択します:

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

要求を右クリックし、［発行］を選択します。

手順「このサービスを許可する」が緑色になり、表示が「このサービスの許可を取り消す」に変更されます。下部のエントリには、「認証元: [\]」と表示されます。



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 の許可を取り消すと、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 <FAS server FQDN>

例：

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-----
                     MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     Gl0/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

ユーザー証明書の一覧を取得するには、以下を入力します:

Get-FasUserCertificate –address <FAS server FQDN>

例:

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。

フェデレーション認証サービスのセキュリティとネットワークの構成

August 24, 2021

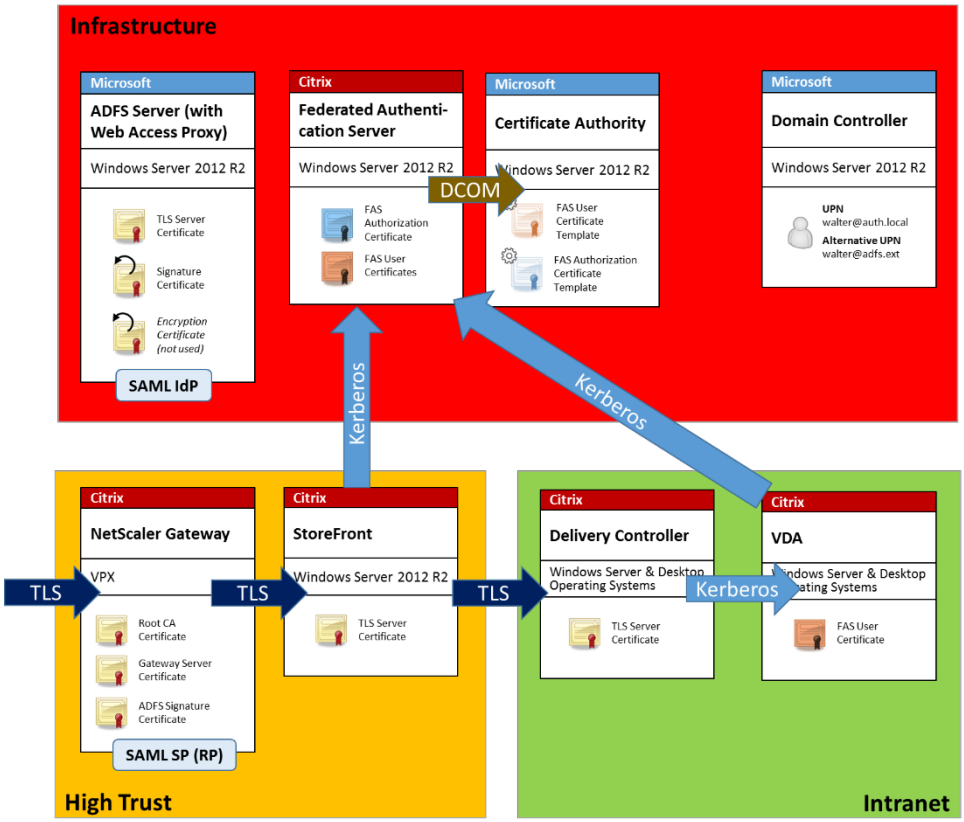
Citrix フェデレーション認証サービス（FAS）は、Microsoft Active Directory および Microsoft 証明機関（CA）と密接に統合しています。ドメインコントローラーやそのほかの重要なインフラストラクチャと同様に、セキュリティポリシーを展開することによって、システムの適切な管理と保護を行うことが重要です。

このドキュメントでは、FAS を展開する場合に考慮する、セキュリティ問題の概要について説明します。また、インフラストラクチャのセキュリティ保護に役立つ利用可能な機能の概要についても説明します。

ネットワークアーキテクチャ

次の図は、FAS 展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FAS サーバーは、CA やドメインコントローラーと共に、セキュリティ上重要なインフラストラクチャの一部として扱われる必要があります。フェデレーション環境では、Citrix NetScaler および Citrix StoreFront はユーザー認証を行うことが信頼されたコンポーネントです。そのほかの XenApp および XenDesktop コンポーネントは、FAS 導入の影響を受けません。



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
フェデレーション認証サービス	[受信] StoreFront および VDA から HTTP 経由で Kerberos、[送信] DCOM から Microsoft CA
NetScaler	[受信] クライアントマシンから HTTPS、[受信/送信] HTTPS と StoreFront サーバー間、[送信] HDX から VDA
StoreFront	[受信] NetScaler から HTTPS、[送信] HTTPS から Delivery Controller、[送信] Kerberos から HTTP 経由で FAS
Delivery Controller	[受信] StoreFront サーバーから HTTPS、[受信/送信] VDA から HTTP 経由で Kerberos
VDA	[受信/送信] Delivery Controller から HTTP 経由で Kerberos、[受信] NetScaler Gateway から HDX、[送信] Kerberos から HTTP 経由で FAS
Microsoft CA	[受信] 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\<fqdn> Kerberos ID を検証します。FAS サーバーにアクセスするすべてのサーバーは、同じインデックスに同一の FQDN を持つ必要があります。そうでない場合は、StoreFront および VDA が別の FAS サーバーに接続することがあります。

構成ミスを防ぐために、環境内のすべてのマシンに、単一のポリシーを適用することをお勧めします。FAS サーバーの一覧に変更を加える場合、特にエントリの削除や順序の変更は、注意して行ってください。

この GPO の管理は、FAS サーバーのインストールおよび運用停止を担当する FAS 管理者（またはドメイン管理者）に限定する必要があります。FAS サーバーの運用停止直後に、その FQDN を再度使用しないように注意してください。

証明書テンプレート

FAS から提供される Citrix_SmartcardLogon 証明書テンプレートを使用しない場合、証明書のコピーを変更できます。以下の変更がサポートされています。

証明書テンプレートの名前の変更

Citrix_SmartcardLogon の名前を変更する場合、所属組織のテンプレート命名標準に従って、以下を行う必要があります。

- 証明書テンプレートのコピーを作成し、所属組織のテンプレート命名標準に従ってその名前を変更します。
- 管理ユーザーインターフェイスではなく、管理 FAS への FAS PowerShell コマンドを使用します。（管理ユーザーインターフェイスは、Citrix のデフォルトのテンプレート名での使用のみを対象としています。）
  - Microsoft MMC 証明書テンプレートスナップインか Publish-FasMsTemplate コマンドを使用して、自身のテンプレートを公開し、
  - New-FasCertificateDefinition コマンドにより、自身のテンプレートの名前を使用して FAS を構成します。

全般プロパティの変更

証明書テンプレートの有効期間を変更できます。

更新期間は変更しないでください。FAS は証明書テンプレートのこの設定を無視します。FAS は有効期間の半ばで証明書を自動的に更新します。

要求処理プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。FAS では常に、［秘密キーのエクスポートを許可する］と ［同一キーで更新する］はオフにされています。

暗号プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。

FAS で提供される該当の設定については、「フェデレーション認証サービスの秘密キー保護」を参照してください。

キーの構成証明プロパティの変更

これらのプロパティは変更しないでください。FAS ではキーの構成証明はサポートされません。

優先テンプレートプロパティの変更

これらのプロパティは変更しないでください。FAS では優先テンプレートはサポートされません。

拡張プロパティの変更

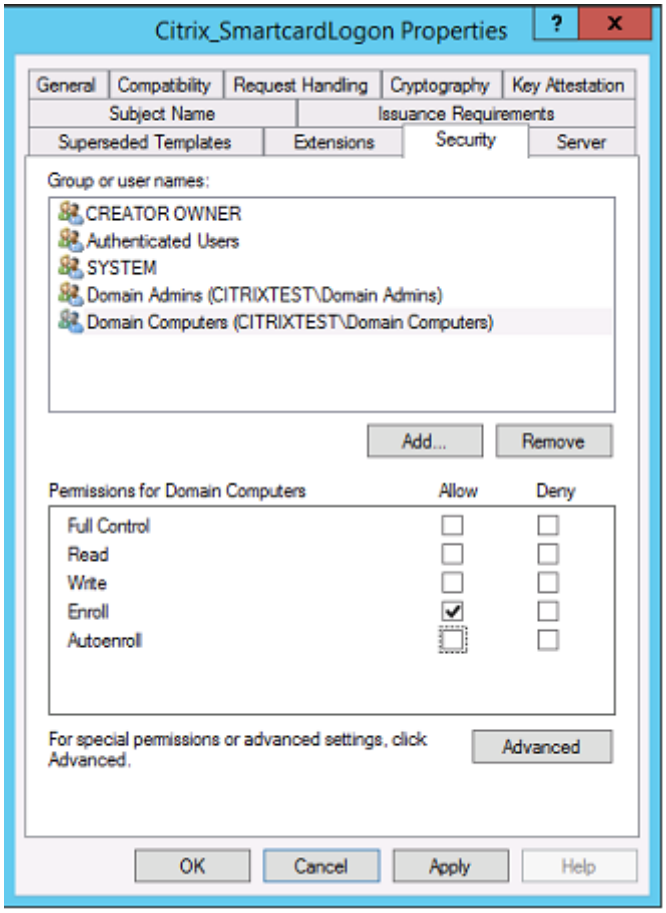
所属組織のポリシーに合わせてこれらの設定を変更できます。

注：不適切な拡張設定を行うと、セキュリティの問題が発生したり、証明書が使用できなくなる場合があります。

セキュリティプロパティの変更

FAS サーバーのマシンアカウントにのみ読み取り権限および登録権限が許可されるように、これらの設定を変更することをお勧めします。FAS サービスには、それ以外の権限は必要ありません。ただし、他の証明書テンプレートと同様、次の項目も追加できます：

- 管理者がテンプレートに対して読み取りまたは書き込みできるようにする
- 認証ユーザーがテンプレートに対して読み取りできるようにする



サブジェクト名プロパティの変更

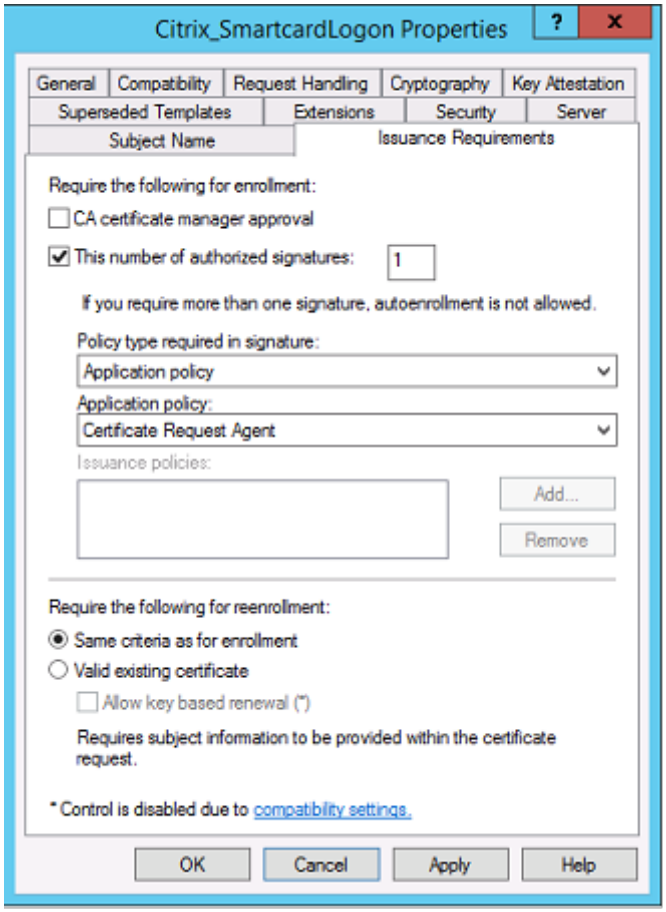
必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

サーバープロパティの変更

推奨はされませんが、必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

発行要件プロパティの変更

これらの設定は変更しないでください。これらは以下のように設定する必要があります。



互換性プロパティの変更

これらの設定は変更できます。この設定は、**Windows Server 2003 CA**（スキーマバージョン 2）以上とする必要があります。ただし、FAS がサポートするのは Windows Server 2008 以降の CA のみです。上記の説明のとおり、**Windows Server 2008 CA**（スキーマバージョン 3）または **Windows Server 2012 CA**（スキーマバージョン 4）を選択することにより使用可能となる追加設定は、FAS では無視されます。

証明機関の管理

CA 管理者の任務は、CA サーバーの構成、および CA サーバーが使用する証明書用秘密キーの発行です。

テンプレートの公開

エンタープライズ管理者の提供するテンプレートに基づいた証明書を証明機関が発行するには、CA 管理者がテンプレートの公開を選択する必要があります。

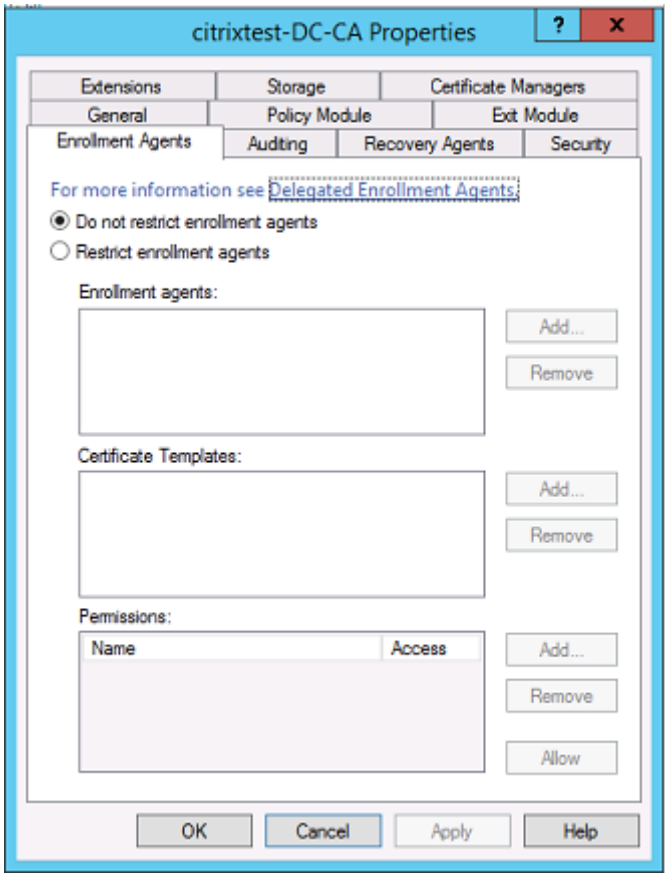
シンプルなセキュリティ対策としては、FAS サーバーのインストール時にのみ RA 証明書テンプレートを公開するか、またはオフラインの証明書発行手続きを選択することです。いずれの場合も、CA 管理者は RA 証明書の要求の承認において全面的なコントロールを維持し、FAS サーバーの承認に関するポリシーを持つ必要があります。

ファイアウォールの設定

一般的に、CA 管理者は、CA のネットワークファイアウォール設定も管理して、受信接続の制御を行います。CA 管理者は、DCOM TCP およびファイアウォールルールを構成し、FAS サーバーだけが証明書を要求できるようにすることができます。

登録の制限

デフォルトでは、RA 証明書のすべての保持者が、アクセス可能な証明書テンプレートを使用して、ユーザーに証明書を発行することができます。これを、CA プロパティの「登録エージェントの制限」で、特権のないユーザーグループに制限する必要があります。



ポリシーモジュールと監査

高度な展開には、カスタムセキュリティモジュールを使用して、証明書の発行の追跡と拒否を行うことができます。

FAS の管理

FAS にはいくつかのセキュリティ機能があります。

アクセス制御リスト（**ACL**）による **StoreFront**、ユーザー、および **VDA** の制限

FAS セキュリティモデルの中心となるのが、機能にアクセスできる Kerberos アカウントの管理です。

アクセスベクトル	説明
StoreFront [IdP]	これらの Kerberos アカウントは、ユーザーが正しく認証されたと宣言することを信頼されています。Kerberos アカウントのいずれかが危害を受けた場合には、証明書が作成され、FAS の構成で許可されたユーザーに証明書が使用されます。
VDA [証明書利用者]	これらは、証明書および秘密キーへのアクセスが許可されたマシンです。このグループ内の危害を受けた VDA アカウントによるシステム攻撃の範囲が制限されるよう、IdP が取得した資格情報ハンドルも必要です。
ユーザー	IdP がどのユーザーをアサートするかを管理します。CA の「制限付き登録エージェント」構成オプションと重複していることに注意してください。一般的に、アクセス制御リストには、特権のないアカウントのみを加えることをお勧めします。これにより、危害を受けた StoreFront アカウントが、権限をより高い管理者レベルに高めることを防ぎます。特に、ドメイン管理者のアカウントは、このアクセス制御リ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（ACL）は、個別に構成することができます。

CA およびテンプレートの構成

証明書テンプレートおよび CA は、それぞれ異なるアクセス権のために構成することができます。高度な構成は、環境に応じて、権限の度合いが異なる証明書を使用するよう選択する場合があります。たとえば、「外部」と識別されたユーザーには、「内部」ユーザーよりも権限が弱い証明書が発行されることがあります。

セッション中および認証の証明書

FAS 管理者は、認証に使用された証明書を、ユーザーのセッションで使用するかどうか管理します。たとえば、より権限のある「ログオン」証明書はログオン時にのみ使用するように、セッションでは「署名」証明書のみ使用可能にすることができます。

秘密キー保護およびキー長

FAS 管理者は、FAS が秘密キーをハードウェアセキュリティモジュール（HSM）、またはトラステッドプラットフォームモジュール（TPM）に保存するよう構成できます。少なくとも RA 証明書の秘密キーは、TPM に保存して保護することをお勧めします。このオプションは、「オフライン」証明書要求手続きの中で提供されます。

同様に、ユーザー証明書の秘密キーも TPM または HSM に保存できます。すべてのキーは「エクスポート不可能」として生成し、キー長は 2048 ビット以上でなければなりません。

イベントログ

FAS サーバーによって、詳細な構成およびランタイムイベントのログが提供されるため、監査と侵入検出に役立てることができます。

管理アクセスと管理ツール

FAS には、リモート管理の機能（相互認証の Kerberos）およびツールが含まれています。「ローカル管理者グループ」のメンバーが、FAS の構成を全面的に管理します。この一覧は、注意して維持する必要があります。

XenApp、**XenDesktop**、および **VDA** の管理者

「Active Directory パスワード」は FAS の「資格情報ハンドル」にそのまま置き換えられるため、一般的には、FAS の利用によって Delivery Controller や VDA 管理者のセキュリティモデルが変更されることはありません。Controller および VDA の管理グループのメンバーは、信頼されたユーザーに限定する必要があります。監査とイベントログを維持する必要があります。

一般的な **Windows** サーバーセキュリティ

すべてのサーバーにパッチを完全に適用し、標準のファイアウォールとアンチウィルスソフトウェアを使用する必要があります。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、「フェデレーション認証サービスのアーキテクチャの概要」を参照してください。
- 「フェデレーション認証サービスの構成と管理」ではそのほかの「方法」記事を紹介しています。

フェデレーション認証サービスによる **Windows** ログオンの問題のトラブルシューティング

August 24, 2021

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
- ルートおよび中間証明書ストア：通常、証明書ログオンシステムは単一の証明書のみを提供できるため、チェーンが使用中の場合、すべてのマシン上の中間証明書ストアがこれらの証明書を含んでいる必要があります。ルート証明書は信頼されたルートストアに、最後から 2 番目の証明書は NTAuth ストアにある必要があります。
- ログオン証明書拡張とグループポリシー：EKU や他の証明書ポリシーを強制的に検証するように Windows を構成できます。Microsoft のドキュメントサイトを参照してください: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN。

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。

レジストリポリシー	説明
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。
EnumerateECCCerts	楕円曲線認証を有効化します。
X509HintsNeeded	証明書に一意のユーザープリンシパル名（UPN）が含まれないか、複数の解釈が可能な場合、このオプションを使用すると、ユーザーが手動で Windows ログオンアカウントを指定できます。
UseCachedCRLOnlyAnd、IgnoreRevocationUnknownErrors	失効チェックを無効にします（通常ドメインコントローラー上で設定）。

- ドメインコントローラー証明書：Kerberos 接続を認証するには、すべてのサーバーが適切な「ドメインコントローラー」証明書を持っている必要があります。これらは、［Local Computer Certificate Personal Store］MMC スナップインメニューを使用して要求できます。

UPN 名と証明書マッピング

ユーザー証明書は、一意のユーザープリンシパル名（UPN）をサブジェクトの別名拡張機能に含めることをお勧めします。

Active Directory での **UPN** 名

デフォルトで、Active Directory のすべてのユーザーは、パターン <samUsername>@<domainNetBios> および <samUsername>@<domainFQDN> に基づく暗黙的 UPN を持っています。利用できるドメインおよび FQDN は、フォレストに対応する RootDSE エントリに含まれています。RootDSE で、単一のドメインに対して複数の FQDN アドレスが登録されていることがあることに注意してください。

また、Active Directory のすべてのユーザーは明示的な UPN と altUserPrincipalNames を持っています。これらはユーザーの UPN を指定する LDAP エントリです。

UPN でユーザーを検索する場合、Windows は、まず（UPN を参照するプロセスの ID に基づいて）現在のドメインで明示的な UPN を、続けて代替 UPN を探します。一致するものがない場合、暗黙的 UPN を探しますが、これはフォレストの異なるドメインで解決されることがあります。

証明書マッピングサービス

証明書に明示的な UPN が含まれない場合、Active Directory は各使用に対して正確な公開証明書を「x509certificate」属性に保管するオプションを持っています。そのような証明書をユーザーに解決するために、コンピューターは直接この属性を問い合わせることができます（デフォルトでは単一のドメインで）。

用意されているオプションを使用すると、ユーザーがユーザーアカウントを指定してこの検索の速度を上げたり、この機能がクロスドメイン環境で使用されるようにしたりできます。

フォレストに複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active Directory の rootDSE が証明書マッピングサービスの場所を指定します。これは通常グローバルカタログマシンに置かれ、フォレスト内のすべての x509certificate 属性のキャッシュビューを持っています。このコンピューターは、証明書だけに基づいて任意のドメインでユーザーアカウントを効率的に検出するために使用できます。

ログオンドメインコントローラーの選択制御

ある環境に複数のドメインコントローラーが含まれる場合、認証にどのドメインコントローラーが使用されているかを把握して制限すると、ログを有効化して取得するのに便利です。

ドメインコントローラーの選択制御

Windows に対して、ログオンで特定の Windows ドメインコントローラーを強制的に使用させるために、lmhosts ファイル（\Windows\System32\drivers\etc\lmhosts）を構成することで、Windows マシンが使用するドメインコントローラーのリストを明示的に設定することができます。

通常その場所には「lmhosts.sam」という名のサンプルファイルがあります。単に次の 1 行を追加します。

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

ここで、「1.2.3.4」は、「mydomain」ドメインで「dcnetbiosname」という名前が付けられているドメインコントローラーの IP アドレスです。

再起動後に、Windows マシンはその情報を使用して mydomain にログオンします。デバッギングが完了したら、この構成を取り消す必要があることに注意してください。

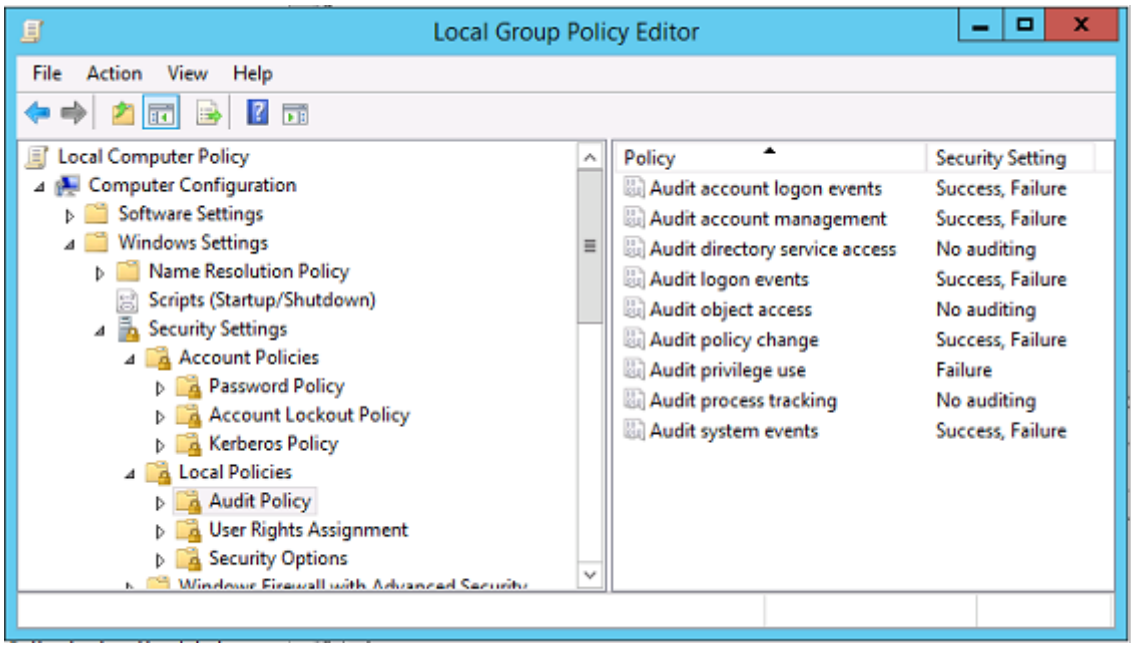
使用中のドメインコントローラーの識別

Windows はログオン時に、ユーザーをログオンさせたドメインコントローラーを MSDOS 環境変数に設定します。これを参照するには、コマンドプロンプトで「**echo %LOGONSERVER%**」を実行します。

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。certutil –verify user.cer

CAPI ログの有効化

ドメインコントローラーとユーザーマシンでは、イベントビューアーを開いて、Microsoft/Windows/-CAPI2/Operational Logs のロギングを有効化します。

CAPI ログは、次のレジストリキーで制御できます。CurrentControlSet\Services\crypt32

値	説明
DiagLevel（DWORD）	詳細度レベル（0～5）
DiagMatchAnyMask（QUADWORD）	イベントフィルター（すべてに 0xffffff を使用）
DiagProcessName（MULTI_SZ）	プロセス名（たとえば、LSASS.exe）によるフィルター

CAPI のログ

メッセージ	説明
チェーンの構築	LSA が CertGetCertificateChain をコールしました（結果含む）
失効確認	LSA が CertVerifyRevocation をコールしました（結果含む）
X509 オブジェクト	詳細モードでは、証明書と証明書失効リスト（CRL）が AppData\LocalLow\Microsoft\X509Objects にダンプされます
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

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	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0xffffffff

ハイブ	値の名前	値［DWORD］
CurrentControlSet\Services\Kd	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

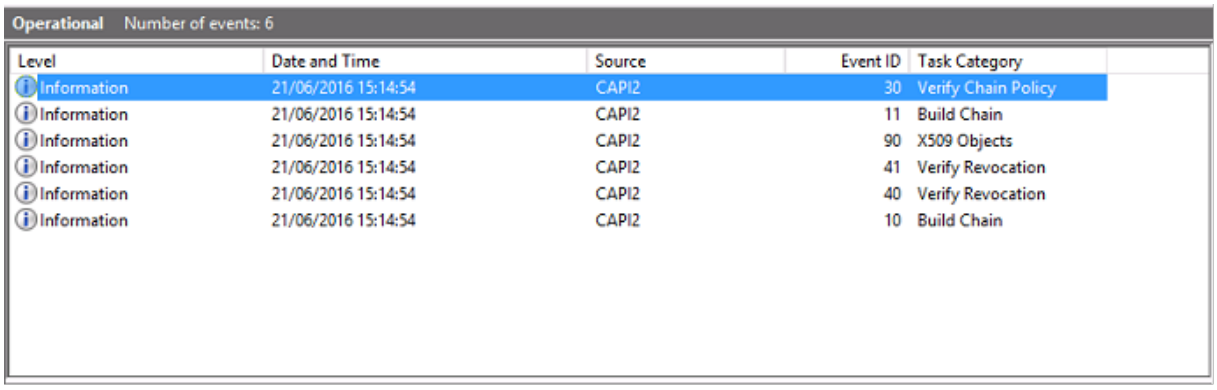
イベントログメッセージ

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。



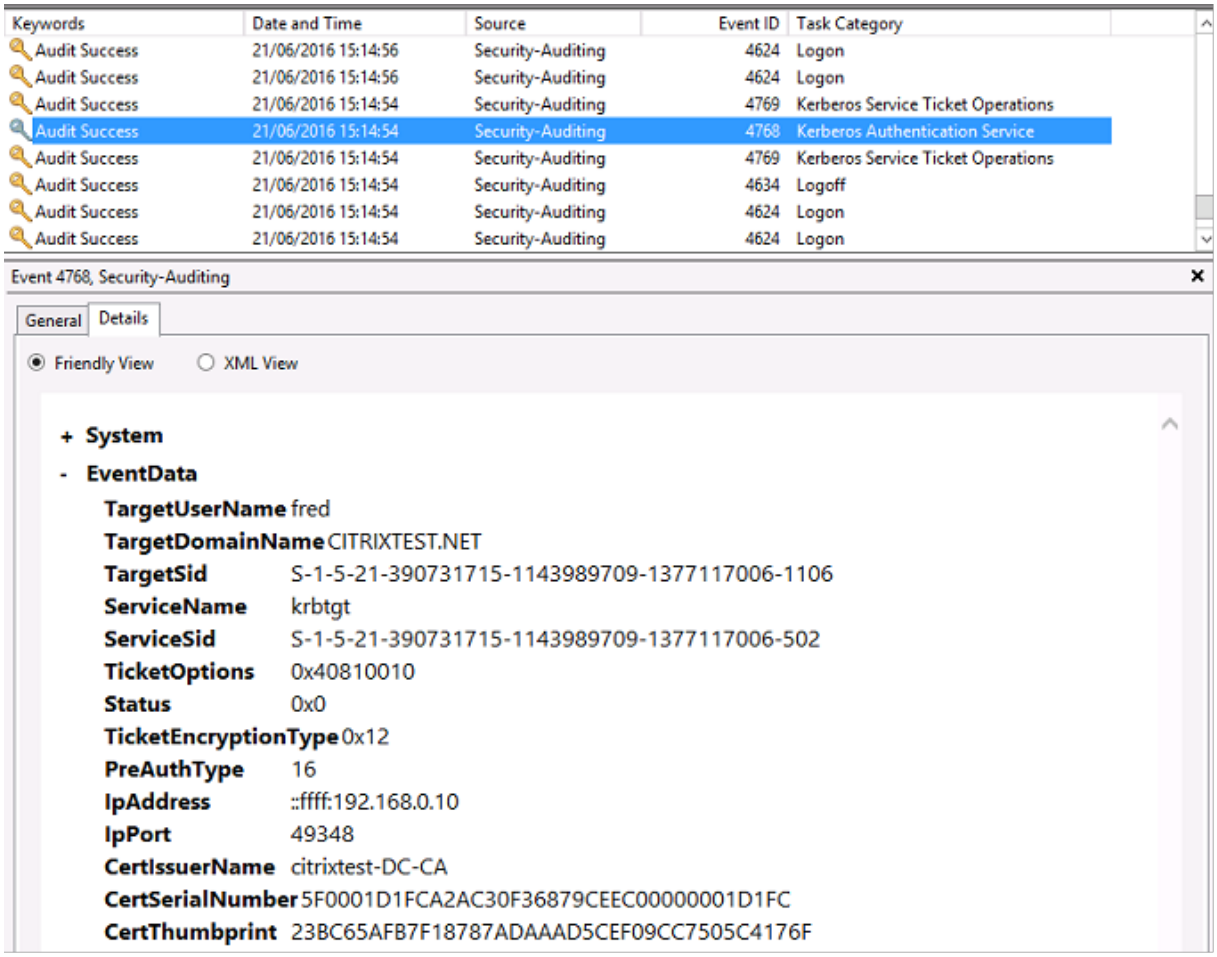
最終イベントログメッセージは、VDA によって提供される証明書に基づいてチェーンを作成するドメインコントローラー上に lsass.exe を表示し、その妥当性（失効など）を検証します。結果は「ERROR_SUCCESS」として戻されます。

- **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

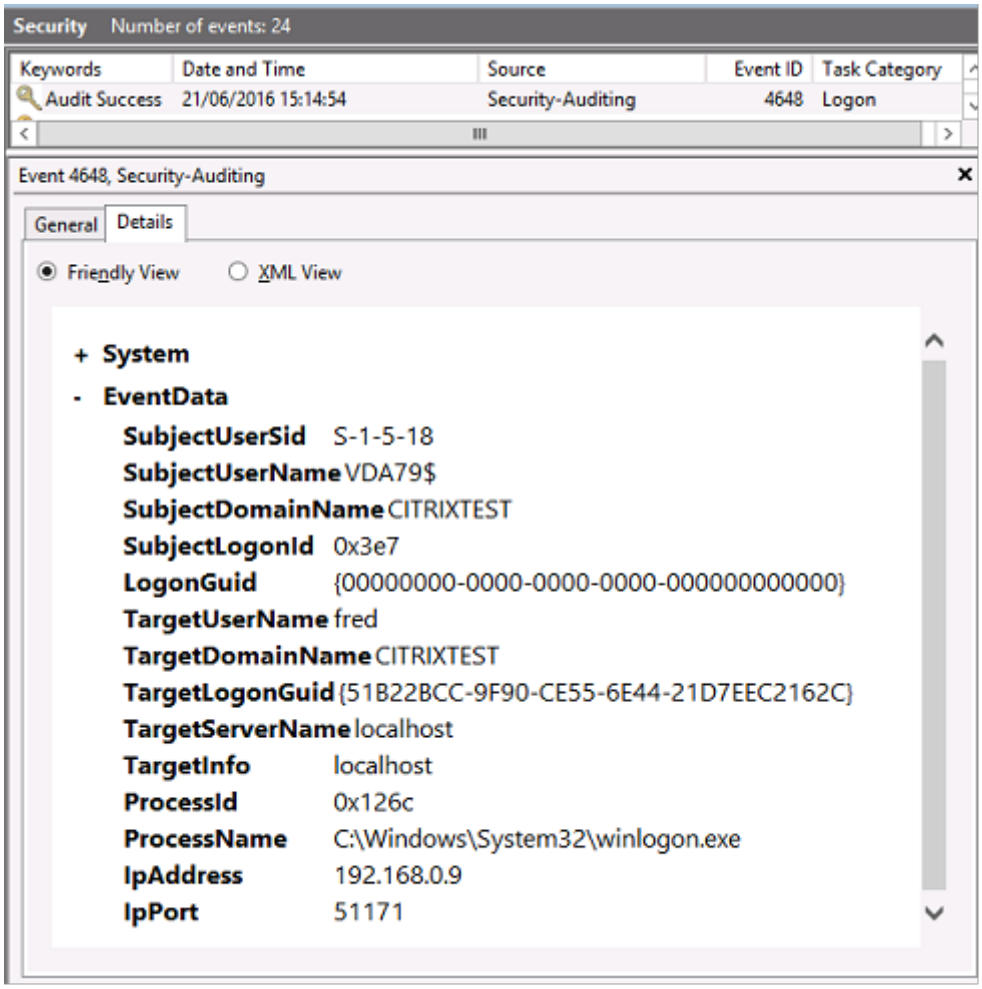
ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは 4768 で、証明書を使用して Kerberos Ticket Granting Ticket（krbtgt）を発行します。

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。



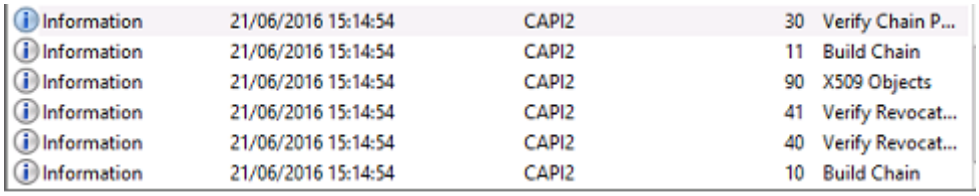
VDA セキュリティログ

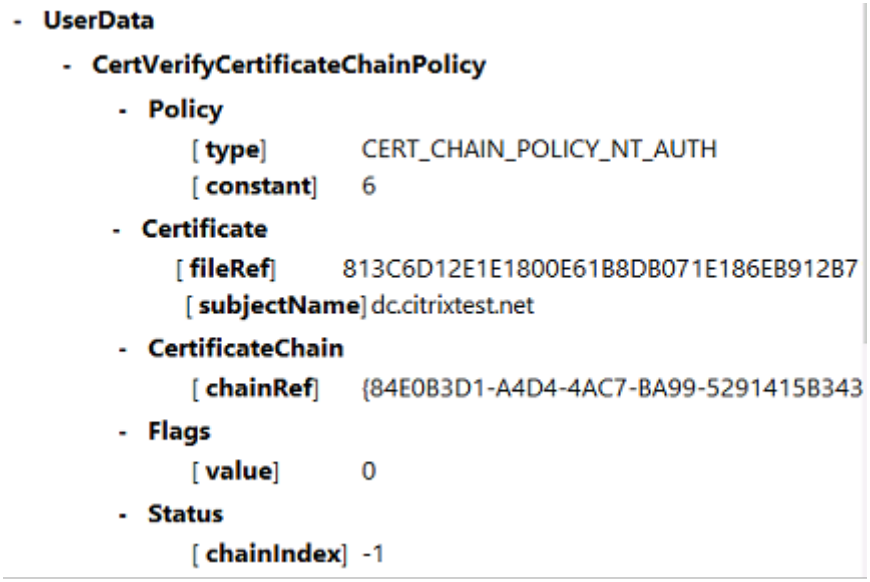
ログオンイベントに対応する VDA セキュリティ監査ログはイベント ID が 4648 のエントリで、winlogon.exe により記録されます。



VDA CAPI ログ

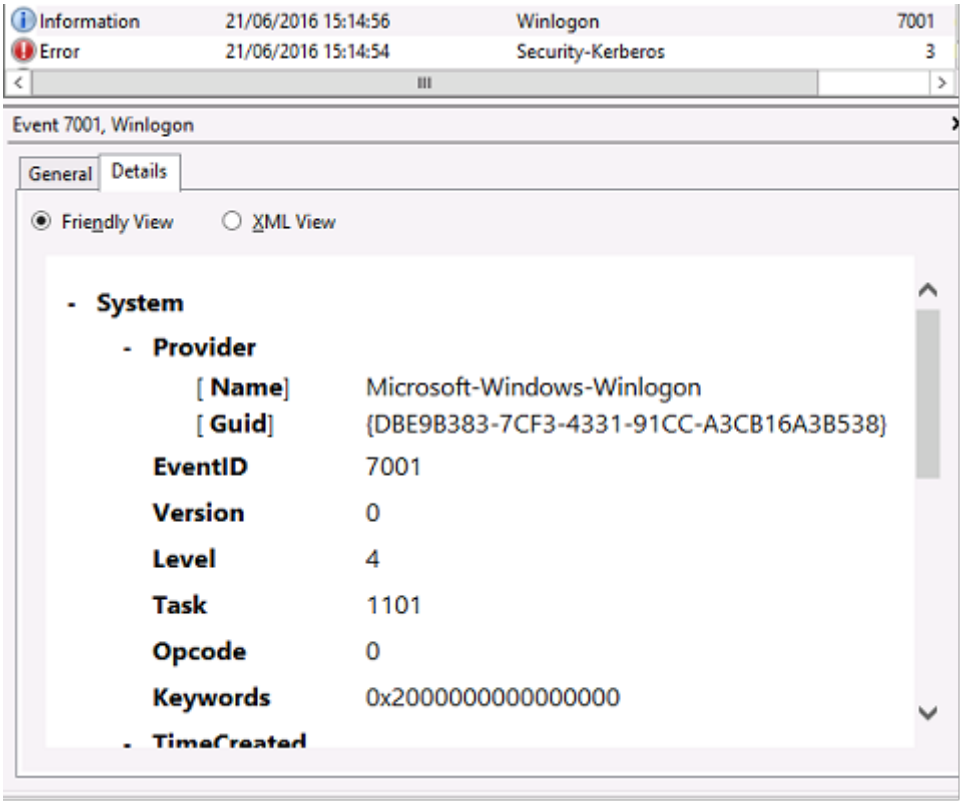
このサンプルの VDA CAPI ログは、lsass.exe から単一のチェーンビルドおよび検証シーケンスを示しており、ドメインコントローラー証明書（dc.citrixtest.net）を検証しています。





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。この記事の「*Kerberos* ログ」を参照してください。
システムにログオンできませんでした。資格情報を確認できませんでした。	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。
要求がサポートされていません	CTX206156 の記述に従って、「ドメインコントローラー」および「ドメインコントローラーの認証」証明書をドメインコントローラーに再登録します。これは通常試す価値があります。既存の証明書が有効に見える場合でも同様です。
システムにログオンできませんでした。認証のために使用されたスマートカード証明書が信頼できませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。ドメイン不参加のコンピューターへのスマートカード証明書のインストール手順は、CTX206156 を参照してください。この記事の証明書と公開キー基盤も参照してください。
アカウントでスマートカードログオンがサポートされていないためログオンできません。	ワークグループユーザーアカウントが、スマートカードログオンに対して完全には構成されていません。
要求されたキーが存在しません	証明書が秘密キーを参照しており、アクセスできません。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。

表示されるエラーメッセージ	説明および参照先
有効なスマートカード証明書が見つかりませんでした。	T 証明書の拡張子が正しく設定されていないか、RSA キーが短すぎます（2048 ビット未満）。有効なスマートカード証明書の生成について詳しくは、CTX206901 を参照してください。
スマートカードがブロックされています	スマートカードがロックされています（たとえば、ユーザーが不正確な PIN を複数回入力しました）。管理者は、スマートカードベンダー提供のツールを使用してカードの PIN ロック解除コード（puk）を取得し、ユーザー PIN をリセットできる場合があります。puk コードが利用できないかロックアウトされている場合、カードを工場出荷時の設定にリセットする必要があります。
不正な要求	スマートカード秘密キーが、ドメインコントローラーが必要とする暗号化をサポートしていません。たとえば、ドメインコントローラーが「秘密キー復号化」を要求したのに、スマートカードが署名しかサポートしていないことがあります。これは通常、証明書の拡張子が正しく設定されていないか、RSA キーが短すぎることを示します（2048 ビット未満）。有効なスマートカード証明書の生成について詳しくは、CTX206901 を参照してください。

関連情報

- スマートカードログオン用のドメインを構成します：https://support.citrix.com/article/CTX206156
- スマートカードログオンポリシー：https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN
- CAPI ログの有効化：https://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

フェデレーション認証サービスの **PowerShell** コマンドレット

August 24, 2021

シンプルな展開ではフェデレーション認証サービス管理コンソールも使用できますが、PowerShell インターフェイスにはより詳細なオプションがあります。コンソールでは使用できないオプションを使用する場合は、PowerShell のみを使用して構成を行うことをお勧めします。

次のコマンドによって FAS PowerShell コマンドレットが追加されます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

PowerShell ウィンドウでは、Get-Help <*cmdlet name*> を使用して、コマンドレットのヘルプを表示できます。

次のリンク先にある zip ファイルには、すべての FAS PowerShell SDK コマンドレットのヘルプファイルが含まれています。このファイルを使用するにはリンクをクリックします。zip ファイルがダウンロードされます。続いて、ローカルフォルダーに内容を展開します。index.html ファイルには、すべてのコマンドレットの一覧が、各コマンドレットヘルプファイルへのリンクとともに記載されています。

フェデレーション認証サービスの PowerShell コマンドレットのヘルプファイル

グラフィック

April 29, 2019

Citrix HDX グラフィックは広範囲な一連のグラフィックアクセラレーションと、XenApp および XenDesktop からのリッチグラフィックアプリケーションの配信を最適化するエンコード技術を備えています。このグラフィック技術は、グラフィックを多用する仮想アプリケーションをリモートで使用する際に、物理デスクトップを使う場合と同じ操作性を提供します。

グラフィックにはハードウェアまたはソフトウェアレンダリングが使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティのライブラリが必要です。たとえば、Windows には DirectX ベースのグラフィックのための WARP ラスタライザーが含まれています。他のソフトウェアレンダラーを使うことも可能です（OpenGL ソフトウェアアクセラレータなど）。ハードウェアレンダリング（ハードウェアアクセラレーション）にはグラフィックプロセッサ（GPU）が必要です。

HDX グラフィックは、一般的なユースケースのほとんどの場合に最適化された、デフォルトのエンコーディング構成を備えています。Citrix ポリシーを使用すると、IT 管理者は異なる要件を満たすさまざまなグラフィック関連の設定を構成し、望ましいユーザーエクスペリエンスを実現することもできます。

Thinwire

Thinwire とは、XenApp および XenDesktop で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。グラフィックは、ユーザー入力（たとえば、キー入力やマウス操作）の結果として生成されます。

HDX 3D Pro

XenApp および XenDesktop の HDX 3D Pro 機能を使用すると、ハードウェアアクセラレーションにグラフィック処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。

Windows デスクトップ OS のための GPU アクセラレーション

HDX 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりデスクトップ OS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

GPU パススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数の GPU を装着して、各仮想マシンに GPU を 1 つずつ割り当てることができます。

GPU 仮想化を使用すると、複数の仮想マシンで単一の物理 GPU によるグラフィック処理能力に直接アクセスできるようになります。

Windows サーバー OS のための GPU アクセラレーション

HDX 3D Pro 機能により、Windows サーバー OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。また、ワークロードが CPU と GPU で分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Framehawk

Framehawk は、ブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE セルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawk はスペクトル干渉や多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供しています。

OpenGL ソフトウェアアクセラレータ

OpenGL ソフトウェアアクセラレータは、ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、コンピューター支援設計、およびコンピューター支援製造などの OpenGL アプリケーションで使用するソフトウェアラスタライザーです。OpenGL ソフトウェアアクセラレータを使用すると、グラフィックカードを装着しなくてもユーザーに良好なユーザーエクスペリエンスを提供できる場合があります。

関連情報

- Thinwire

- HDX 3D Pro
- 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
- Framehawk
- OpenGL ソフトウェアアクセラレータ

Framehawk

August 24, 2021

Framehawk は、ブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE セルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawk はスペクトル干渉や多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供しています。Framehawk は、少量のパケット損失がユーザーエクスペリエンスを低下させる可能性がある、長距離（低速）ブロードバンドネットワーク接続を利用しているユーザーに適している場合があります。このユースケースではアダプティブトランスポートを使用することをお勧めします。詳しくは、「アダプティブトランスポート」を参照してください。

Citrix ポリシーテンプレートを使用し、組織に適した方法で、一連のユーザーとアクセスシナリオ用に Framehawk を実装します。Framehawk は、ラップトップやタブレットなど、単一画面でのモバイルユースケースをターゲットにしています。リアルタイムの対話的なパフォーマンスによってサーバーリソースの追加コストやブロードバンド接続の要件の正当性が証明される場合に Framehawk を使用します。

Framehawk はどのようにして円滑なユーザーエクスペリエンスを維持するか

Framehawk は人間の目をソフトウェアとして実装したもので、フレームバッファーの中に何があるかを確認したり、画面上のさまざまなコンテンツの種類を識別したりするものと考えてください。ユーザーにとって重要なものはなんでしょうか。画面エリアが動画や動くグラフィックのように急速に変化している場合は、多少のピクセルが失われていても、新しいデータですぐに上書きされますから、人間の目にとっては大したことではありません。

しかし、通知エリアやツールバーのアイコン、読み始めたいところまでユーザーがスクロールした後のテキストのように画面で変化しない領域は、人間の目が細部にまでこだわるところです。ユーザーは、このようなエリアではピクセルが完璧であることを期待します。**0** と **1** の観点で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にとって適切なものであることです。

Framehawk は、次世代 QoS 信号増幅器に加え、ワークロードをきめ細かく、より効率的に識別するための時間をベースにしたヒートマップを搭載しています。Framehawk はデータ圧縮に加えて、自動自己回復変換を使用します。また、データの再送信を回避し、クリック応答、線形性、一貫したリズムを維持します。損失の多いネットワーク接続では、Framehawk は補間を使って損失を隠すため、ユーザーは良好なイメージ品質を感じながら、流れるようなエクスペリエンスを楽しむことができます。さらに、Framehawk のアルゴリズムはさまざまな種類のパケット損失をインテリジェントに区別します。たとえば、ランダム損失（補正のためにさらにデータを送信）と輻輳損失（チャネルはすでに渋滞しているので追加のデータは送信しない）などです。

Citrix Receiver の Framehawk Intent Engine は、上スクロールと下スクロール、ズーム、左または右方向への移動、読み込み、入力などの一般的な操作を区別します。エンジンはまた、共有ディクショナリを使用して、Virtual Delivery Agent（VDA）への通信を管理します。ユーザーが読もうとしているテキストは、高い品質で表示されなければなりません。スクロールはすばやく、スムーズであることが必要です。また、一時停止もできなければなりません。これにより、ユーザーはアプリケーションやデスクトップとのやりとりを常に制御できる立場でいられます。

ネットワーク接続のリズムを測定すること（自転車のチェーンの張力にたとえて「ギアリング」）により、Framehawk ロジックはよりすばやく反応し、遅延の大きな接続でも優れたエクスペリエンスを実現します。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を実現するために TCP を使用しています。そのため、損失率の高いネットワークや過負荷状態のネットワークでは、パケットを再送信しなければならず、これがユーザーエクスペリエンスの低下につながります。Enlightened Data Transport（EDT）レイヤー上で Thinwire を使用可能にすることによって、高遅延ネットワーク接続上での TCP 制限に対処しています。

Framehawk は、UDP（ユーザーデータグラムプロトコル）上に作成されたデータ転送レイヤーを使用します。Framehawk とその他の UDP ベースのプロトコルのパフォーマンスを比較すればわかるとおり、UDP は、Framehawk で損失性を打開する方法のほんの一部に過ぎません。UDP は、Framehawk を際立たせる、人間を主体にした技術の重要な基礎を提供します。

Framehawk で必要な帯域幅

ブロードバンドワイヤレスの意味は、接続を共有するユーザーの人数、接続の品質、使用しているアプリなどいくつかの要素によって変わります。最適なパフォーマンスを上げるには、基本の 4Mbps または 5Mbps に、同時に使用しているユーザー 1 人につき約 150Kbps を加えることを Citrix ではお勧めします。

Thinwire の帯域幅の推奨は、通常、基本の 1.5Mbps に、ユーザー 1 人につき 150Kbps を追加します。詳しくは、XenApp および XenDesktop 帯域幅ブログを参照してください。Thinwire over TCP では 3% のパケットが失われるため、有益なユーザーエクスペリエンスを保証するには、Framehawk よりもかなり大きな帯域幅が必要であることがわかります。

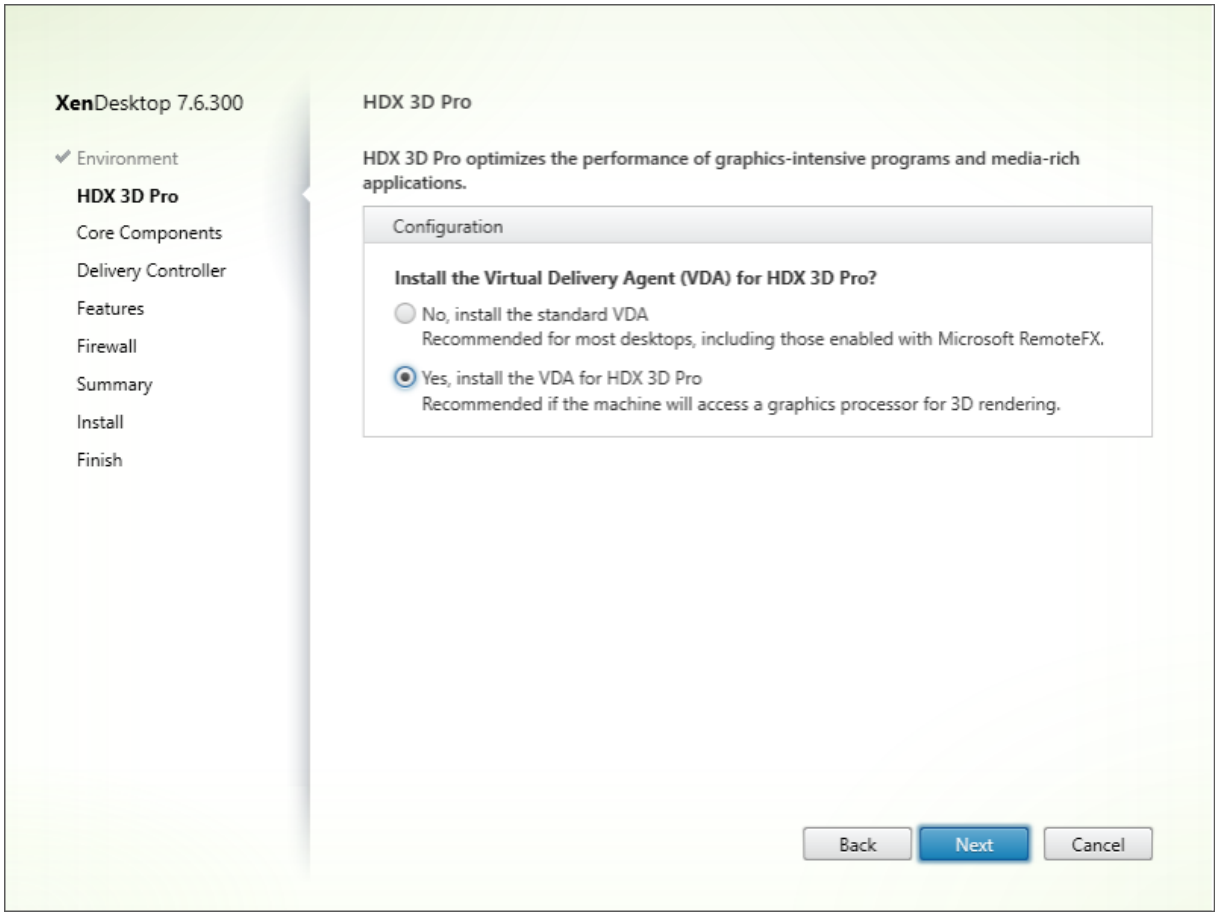
Thinwire は、ICA プロトコルのディスプレイリモート処理では、プライマリチャネルのままです。Framehawk は、デフォルトで無効になっています。Citrix は必要に応じて有効、無効を切り替えることで、組織のブロードバンドワイヤレスアクセスシナリオに対応することを推奨します。Framehawk は、Thinwire よりかなり多くのサーバーリソース（CPU とメモリ）を必要とすることに注意してください。

Framehawk および **HDX 3D Pro**

Framehawk では、XenApp（サーバー OS）および XenDesktop（デスクトップ OS）アプリの両方で、すべての HDX 3D Pro のユースケースがサポートされます。遅延が 400～500 ミリ秒、パケット損失が 1～2% の顧客環境で

検証されました。そのため、AutoCAD や Siemens NX などの一般的な 3D モデリングアプリで素晴らしい対話操作性が得られます。これにより、移動中や、国外または劣悪なネットワーク環境で作業を行う場合も、より大規模な CAD モデルを表示させて操作できるようになりました。（長距離ネットワーク接続上で 3D アプリケーションを提供する必要がある組織は、アダプティブトランスポートを使用することをお勧めします。詳しくは、「アダプティブトランスポート」を参照してください。）

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。



このように選択すると、HDX は Citrix ビデオドライバーでなく GPU ベンダーのビデオドライバーを使用します。通常のデフォルトである Selective H.264 エンコーディングを使用するアダプティブ表示でなく、Thinwire 上の全画面 H.264 エンコーディングをデフォルトとします。

要件および考慮事項

Framehawk では、少なくとも、VDA 7.6.300 およびグループポリシー管理 7.6.300 が必要です。

エンドポイントには、少なくとも、Citrix Receiver for Windows 4.3.100、または Citrix Receiver for iOS 6.0.1 が必要です。

デフォルトでは Framehawk では、双方向のユーザーデータグラムプロトコル（UDP）ポート範囲（3224～3324）

を使用して Framehawk 表示チャネルデータが Citrix Receiver と交換されます。この範囲は、ポリシー設定 **Framehawk** 表示チャネルポートの範囲でカスタマイズできます。クライアントと仮想デスクトップの間の同時接続 1 つにつき、固有のポートが 1 つ必要になります。XenApp サーバーなど、マルチユーザー OS 環境では、同時ユーザーセッションを上限までサポートするために、十分な数のポートを定義してください。VDI デスクトップのようなシングルユーザー OS では、UDP ポートを 1 つ定義すれば十分です。Framehawk は最初に定義されたポートを使用しようとし、範囲内で指定された最後のポートまで進みます。これは、NetScaler Gateway を通過する場合と、StoreFront サーバーへの直接内部接続の両方に当てはまります。

リモートアクセスの場合は、NetScaler Gateway を必ず展開してください。デフォルトでは、NetScaler は、クライアント Citrix Receiver と Gateway の間での暗号化通信のために UDP ポート 443 を使用します。双方向通信を確実に行うためには、外側のファイアウォールすべてで、このポートを開いておく必要があります。この機能は Datagram Transport Layer Security（DTLS）と呼ばれます。

> 注:
>
> Framehawk/DTLS 接続は、FIPS アプライアンスではサポートされません。

暗号化された Framehawk 接続は、NetScaler Gateway Version 11.0.62 および NetScaler Unified Gateway Version 11.0.64.34 からサポートされています。

NetScaler High Availability（HA）は、XenApp および XenDesktop 7.12 以降でサポートされています。

Framehawk を実装する前に、以下のベストプラクティスを検討してください:

- セキュリティ管理者に問い合わせ、Framehawk 用に定義された UDP ポートがファイアウォールで開かれていることを確認してください。インストール中にファイアウォールが自動的に構成されることはありません。
- 多くの場合、NetScaler Gateway は DMZ にインストールされ、外側だけでなく内側もファイアウォールで守られます。外側のファイアウォールで UDP ポート 443 が開いていることを確認してください。デフォルトのポート範囲を使用している環境では、内側のファイアウォールで UDP ポート 3224〜3324 が開いていることを確認してください。

構成

> 注意:
>
> 大きなパケット損失が発生していると思われるユーザーについてのみ、Framehawk を有効化することが推奨されます。また、Framehawk を、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。

Framehawk は、デフォルトで無効になっています。この機能を有効にすると、ユーザーのグラフィックスおよび入力に対して、サーバーで Framehawk の使用が試みられます。何らかの理由で前提条件が満たされていない場合、接続はデフォルトモード（Thinwire）で確立されます。

Framehawk に影響を与えるポリシー設定は以下のとおりです:

- Framehawk ディスプレイチャネル: この機能を有効または無効にします。

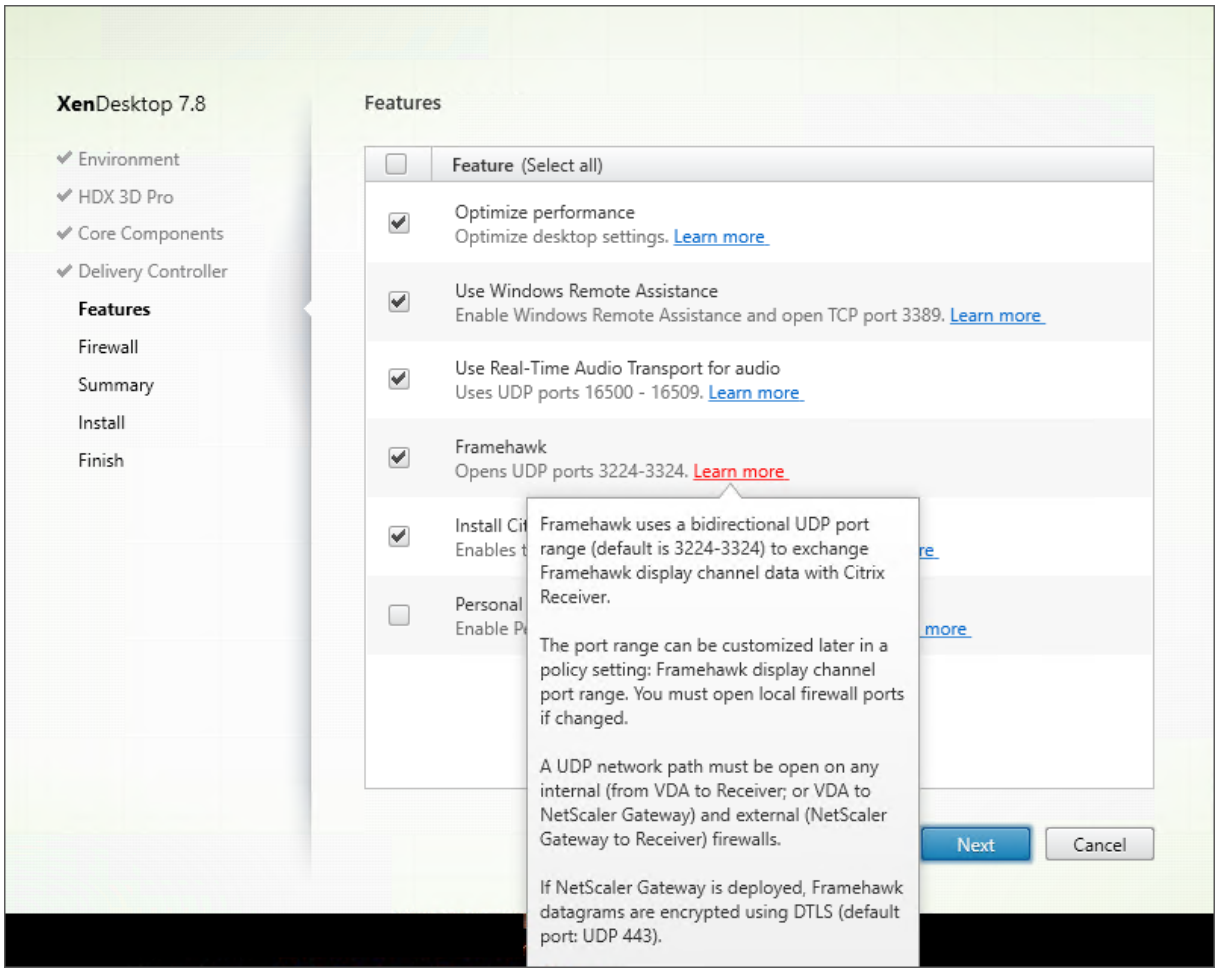
- Framehawk ディスプレイチャネルのポート範囲：ユーザーデバイスと Framehawk ディスプレイチャネルデータの交換に VDA で使用する UDP ポート番号の範囲（最小ポート番号と最大ポート番号）を指定します。VDA は、各ポートの使用を試行します。まず、最小のポート番号から始めて、2 回目以降の試行では 1 つずつ番号を増やしていきます。ポートは、受信トラフィックと送信トラフィックに使用されます。

Framehawk ディスプレイチャネル用のポートの開放

XenApp および XenDesktop 7.8 より、VDA インストーラーの ［機能］手順で、ファイアウォールを再構成する新たなオプションが使用できるようになりました。このチェックボックスをオンにすると、Windows のファイアウォールで UDP ポート 3224～3324 が開放されます。以下の場合は、手動でファイアウォールを構成する必要があります。

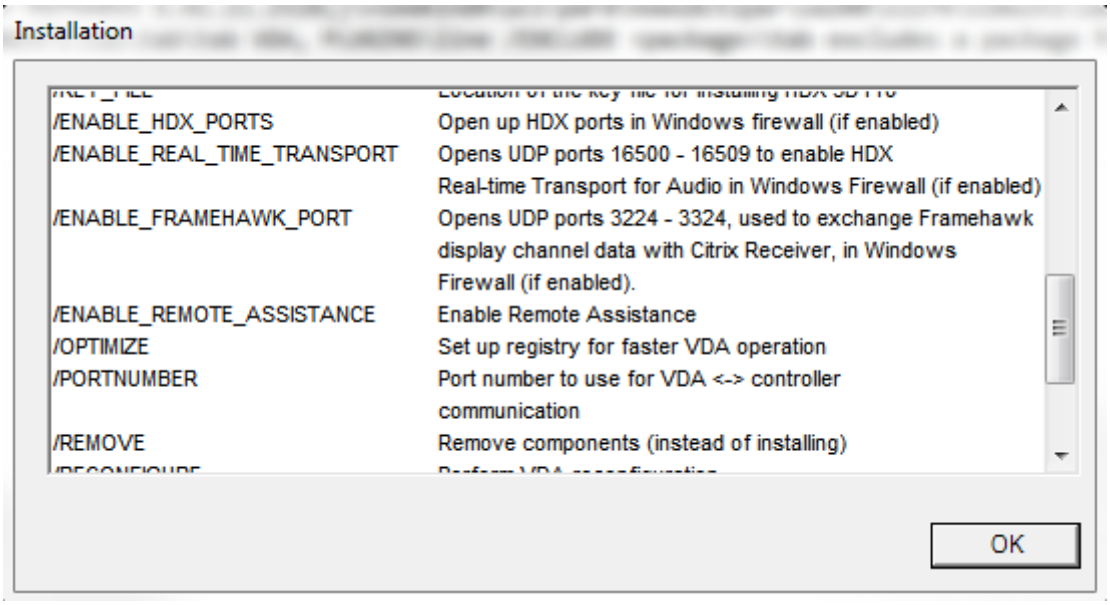
- ネットワークファイアウォールの場合。
  または
- デフォルトのポート範囲がカスタマイズされている場合。

これらの UDP ポートを開放するには、［**Framehawk**］チェックボックスをオンにします：



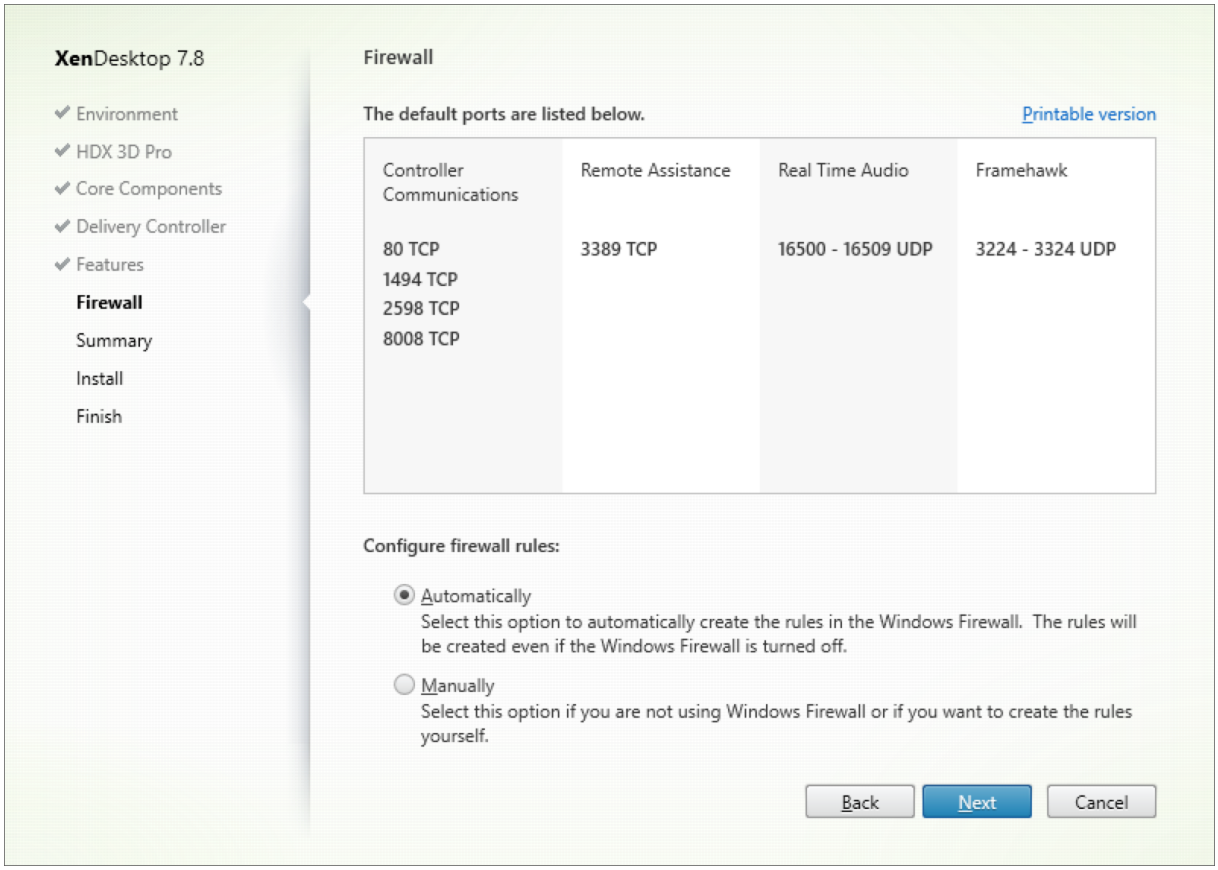
コマンドラインで**/ENABLE_FRAMEHAWK_PORT** を使用して、Framehawk 用に UDP ポートを開放すること

もできます。

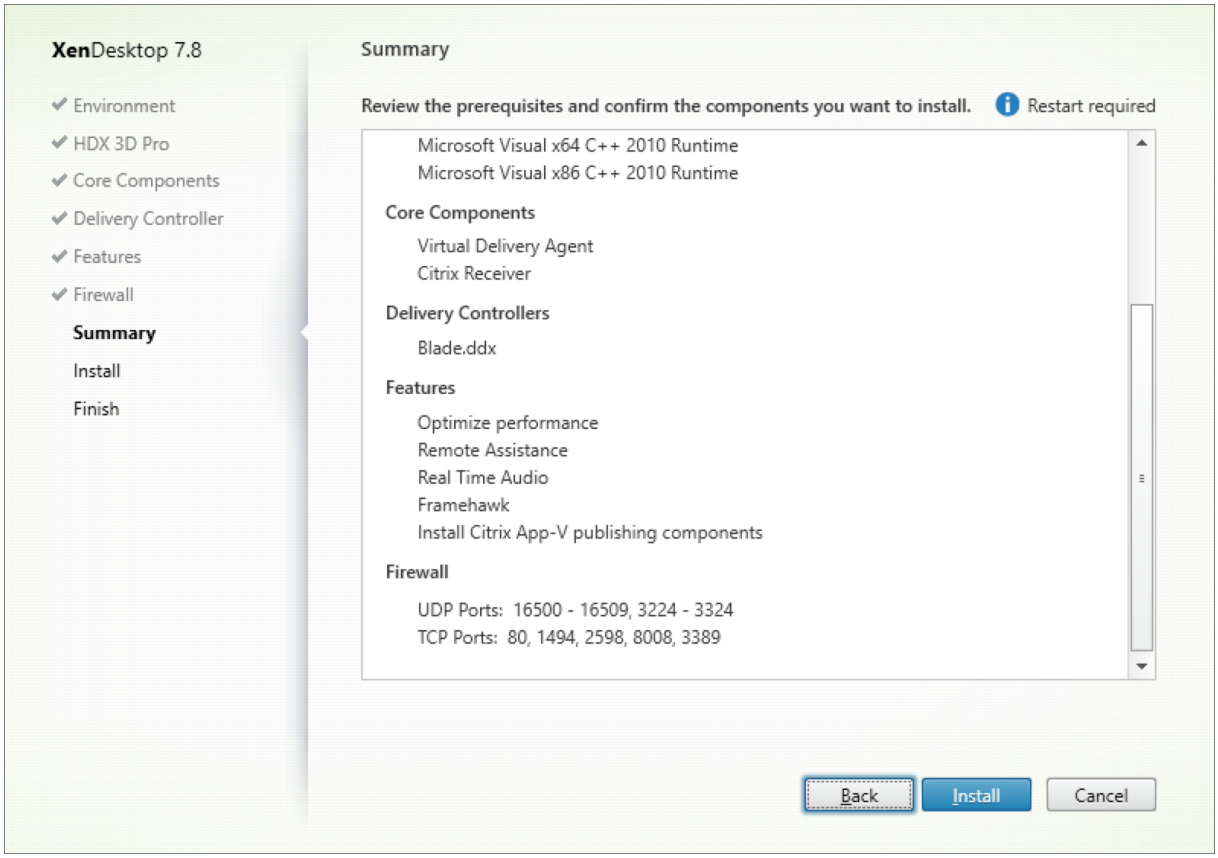


Framehawk の **UDP** ポートの割り当ての確認

インストール中に、Framehawk 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 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を参照します。つまり、VPN vServer には、パブリック IP アドレスが割り当てられていて、ユーザーはこの IP アドレスに直接接続します。
- Unified Gateway を伴う NetScaler とは、Gateway VPN vServer がターゲットとして Content Switching vServer（CS）にバインドされた展開を言います。この展開では、CS vServer はパブリック IP アドレスを持ち、Gateway VPN vServer はダミーの IP アドレスを持ちます。

NetScaler Gateway で Framehawk のサポートを可能にするには、Gateway VPN vServer レベルで DTLS パラメーターを有効化する必要があります。このパラメーターを有効化し、XenApp または XenDesktop でコンポーネントが正常に更新されると、Gateway VPN vServer とユーザーデバイスの間で、Framehawk のオーディオ、ビデオ、およびインタラクティブなトラフィックが暗号化されるようになります。

Framehawk でサポートされるのは、NetScaler Gateway、Unified Gateway、および NetScaler Gateway とグローバルサーバー負荷分散の組み合わせです。

Framehawk では、次のシナリオはサポートされません。

- HDX Insight
- IPv6 モードの NetScaler Gateway
- NetScaler Gateway のダブルホップ
- クラスターセットアップ付き NetScaler Gateway

シナリオ	**Framehawk** のサポート
NetScaler Gateway	はい
NetScaler ＋グローバルサーバー負荷分散	はい
Unified Gateway を伴う NetScaler	はい。注：サポートされるのは Unified Gateway バージョン 11.0.64.34 以降です。
HDX Insight	いいえ
IPv6 モードの NetScaler Gateway	いいえ
NetScaler Gateway のダブルホップ	いいえ
NetScaler Gateway 上に Secure Ticket Authority を複数配置	はい
High Availability 機能付き NetScaler Gateway	はい
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 **NetScaler** の構成

NetScaler Gateway で Framehawk のサポートを可能にするには、Gateway VPN vServer レベルで DTLS パラメーターを有効化してください。このパラメーターを有効化し、XenApp または XenDesktop でコンポーネントが正常に更新されると、Gateway VPN vServer とユーザーデバイスの間で、Framehawk のオーディオ、ビデオ、およびインタラクティブなトラフィックが暗号化されるようになります。

リモートアクセスのために、NetScaler Gateway で UDP 暗号化を実現するには、この構成が必須です。

Framehawk をサポートするように NetScaler を構成する場合：

- 外側のファイアウォールすべてで UDP ポート 443 が開いていることを確認します
- 外側のファイアウォールすべてで CGP ポート（デフォルトは 2598）が開いていることを確認します
- VPN 仮想サーバーの設定で DTLS を有効化します
- SSL 証明書とキーのペアのバインドをいったん解除してから、再びバインドします NetScaler バージョン 11.0.64.34 以降をお使いの場合、この手順を行う必要はありません。

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ても、無視してください。

旧バージョンの **NetScaler Gateway** における手順

11.0.64.34 より古いバージョンの NetScaler Gateway を使用している場合は、以下の手順に従います。

1. サーバー証明書の［バインド］画面を再度開き、証明書のキーペアをバインドするために、［+］をクリックします。
2. 前述の証明書のキーペアを選択し、［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ても、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、Citrix 製品ドキュメントサイトでUnified Gatewayの情報を参照してください。
2. ターゲット *vServer* として CS *vServer* にバインドされている VPN vServer 上で、DTLS パラメーターを有効にします。

制限事項

クライアントデバイス上に古い NetScaler Gateway 仮想サーバーの DNS エントリがある場合、アダプティブトランスポートと Framehawk は UDP トランスポートではなく TCP トランスポートへフォールバックすることがあります。TCP トランスポートへのフォールバックが発生する場合は、クライアントの DNS キャッシュをクリアし、UDP トランスポートを使用して再接続しセッションを確立させます。

ほかの **VPN** 製品のサポート

NetScaler Gateway は、Framehawk で必要な UDP 暗号化をサポートする唯一の SSL VPN 製品です。ほかの SSL VPN や誤ったバージョンの NetScaler Gateway が使用された場合、Framehawk ポリシーの適用に失敗する可能性があります。従来型の IPSec VPN 製品では、変更を加えなくとも Framehawk がサポートされます。

Framehawk をサポートする **Citrix Receiver for iOS** の構成

以前のバージョンの Citrix Receiver for iOS を Framehawk をサポートするように構成するには、default.ica を手作業で編集する必要があります。

1. StoreFront サーバーで、c:\inetpub\wwwroot\にある自分のストアの App_Data ディレクトリにアクセスします。
2. default.ica ファイルを開き、[WFClient] セクションに「Framehawk=On」という行を追加します。
3. 変更を保存します。

この手順により、iOS デバイス上の互換性のある Citrix Receiver から Framehawk セッションを確立できるようになります。Receiver for Windows を使用している場合、この手順は必要ありません。

> 注:
>
> iOS バージョン 7.0 以降の Receiver を使用している場合、default.ica ファイルにパラメーター **Framehawk=On** を明示的に追加する必要はありません。

Framehawk のモニター

Citrix Director から Framehawk の利用状況とパフォーマンスをモニターすることができます。HDX 仮想チャネル詳細ビューには、あらゆるセッションで、Framehawk のトラブルシューティングやモニターに役立つ情報が表示されます。Framehawk 関連のメトリックスを確認するには、［グラフィック **- Framehawk**］を選択します。

Framehawk 接続が確立されていれば、詳細ページに「プロバイダー **=VD3D**」および「接続済み **=** はい」と表示されます。仮想チャネルの状況がアイドルであるのは正常です。これは、モニターの対象がシグナリングチャネルで、これは最初のハンドシェイク中にしか使用されないからです。このページには、接続に関するその他の有益な統計も表示されます。

問題が発生した場合は、Framehawk のトラブルシューティングブログを参照してください。

HDX 3D Pro

August 24, 2021

XenApp と XenDesktop の HDX 3D Pro 機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、

OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。標準 VDA または HDX 3D Pro VDA の選択について詳しくは、「手順 5：HDX 3D Pro モードを有効にするかどうかを選択する」を「VDA のインストール」の記事内で参照してください。

サポートされているすべての Citrix Receiver は、3D グラフィックとともに使用できます。複雑な 3D ワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、最新バージョンの Citrix Receiver for Windows および Citrix Receiver for Linux をお勧めします。サポートされている Citrix Receiver のバージョンについて詳しくは、「Lifecycle Milestones for Citrix Receiver」を参照してください。

これらの 3D グラフィック処理アプリケーションとして次のものがあります：

- コンピューター支援設計（CAD）、コンピューター支援製造（CAM）、およびコンピューター支援エンジニアリング（CAE）アプリケーション
- 地理情報システム（GIS）ソフトウェア
- 医療画像処理のための画像保存通信システム（PACS）
- 最新バージョンの OpenGL、DirectX、NVIDIA CUDA、OpenCL、および WebGL を使用するアプリケーション
- 並列計算に NVIDIA Compute Unified Device Architecture（CUDA）GPU を使用する計算集約型の非グラフィックアプリケーション

HDX 3D Pro では、さまざまな帯域幅において最適なユーザーエクスペリエンスが提供されます。

- WAN 接続の場合：帯域幅が 1.5Mbps の WAN 接続でもインタラクティブなユーザーエクスペリエンスが提供されます。
- LAN 接続の場合：LAN 接続ではローカルデスクトップに匹敵するユーザーエクスペリエンスが提供されます。

  ユーザーが使用する複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えて、グラフィック処理をユーザー側から中央管理が可能なデータセンター内に移管できます。

HDX 3D Pro により、Windows デスクトップ OS マシンと Windows サーバー OS マシンでの GPU アクセラレーションが提供されます。詳しくは、「Windows デスクトップ OS のための GPU アクセラレーション」および「Windows サーバー OS のための GPU アクセラレーション」を参照してください。

HDX 3D Pro は、次のハイパーバイザーが提供する GPU パススルーや GPU 仮想化、およびベアメタルと互換性があります：

- Citrix XenServer
  - NVIDIA GRID および Intel GVT-d による GPU パススルー
  - NVIDIA GRID および Intel GVT-g による GPU 仮想化
- Microsoft Hyper V
  - NVIDIA GRID および AMD による GPU パススルー（Discrete Device Assignment）
- VMware vSphere
  - NVIDIA GRID、Intel、および AMD IOMMU による GPU パススルー（vDGA）

- NVIDIA GRID および AMD MxGPU による GPU 仮想化

サポート対象の XenServer バージョンについては、「Citrix XenServer のハードウェア互換性リスト」を参照してください。

HDX Monitor を使用すると、HDX 仮想テクノロジの操作と構成を検証して、HDX の問題を診断して解決できます。このツールの詳細およびダウンロード方法については、https://taas.citrix.com/hdx/download/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

August 24, 2021

HDX 3D Pro 機能により、Windows サーバー OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。また、ワークロードが CPU と GPU で分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Windows Server はマルチユーザーオペレーティングシステムなので、XenApp によってアクセスされる GPU は複数のユーザーによって共有でき、GPU 仮想化（vGPU）の必要はありません。

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

GPU 共有

GPU 共有により、リモートデスクトップセッションで動作する OpenGL アプリケーションおよび DirectX アプリケーションで GPU ハードウェアによるレンダリング処理が可能になります。これにより、以下の効果があります。

- ベアメタルまたは仮想マシン上で使用でき、アプリケーションのスケーラビリティとパフォーマンスが向上します。
- 複数の同時接続セッションで GPU リソースを共有できます（ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません）。
- 特別な設定は必要ありません。

複数の GPU を持つグラフィックカードを装着したり、複数のグラフィックカードを装着したりして、ハイパーバイザー上に複数の GPU をインストールして各 GPU を特定の仮想マシンに（1 対 1 で）割り当てることができます。ただし、サーバー上で異なるグラフィックカードを混在させることは推奨されません。

仮想マシンでは、GPU への直接パススルーアクセスが必要です。この機能は、Citrix XenServer、VMware vSphere vDGA、および Intel GVT-d で提供されます。HDX 3D Pro と GPU パススルーを併用すると、サーバー上の各 GPU で単一のマルチユーザー仮想マシンをサポートできます。

GPU 共有は、特定のグラフィックカードに依存するものではありません。

- ハイパーバイザー上では、そのハイパーバイザーの GPU パススルー機能でサポートされるハードウェアプラットフォームとグラフィックカードを選択してください。XenServer の GPU パススルー機能でテストされたハードウェアの一覧については、「GPU Pass-through Devices」を参照してください。
- ベアメタルを実行するときは、オペレーティングシステムで単一のディスプレイアダプターを有効にすることをお勧めします。複数の GPU がハードウェアに取り付けられている場合は、デバイスマネージャーを使用して 1 つだけ残して無効にします。

GPU 共有でのスケーラビリティは、以下の要素により異なります。

- 実行するアプリケーション
- 消費されるビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションでは、ビデオ RAM の不足をより効果的に処理できます。ハードウェアの負荷が過剰になると、グラフィックカードドライバーが不安定になったり異常停止したりすることがあります。このような問題を避けるには、同時接続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、https://www.techpowerup.com/gpuz/で提供されています。

DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、DDI（Display Driver Interface）Version 9ex、10、または 11 をサポートする GPU が搭載されたサーバーでのみ使用可能です。

- Windows Server 2008 R2 では、DirectX および Direct3D で単一 GPU を使用するために特別な設定は不要です。
- Windows Server 2016 および Windows Server 2012 の RD Session Host サーバー上のリモートデスクトップサービス（RDS）セッションでは、デフォルトのアダプターとして Microsoft 基本レンダリングドライバーが使用されます。Windows 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［すべてのリモートデスクトップサービスセッションにハードウェアの既定のグラフィックスアダプターを使用する］を有効にします。
- WPF アプリケーションでのレンダリングにサーバーの GPU が使用されるようにするには、Windows サーバー OS セッションを実行するサーバー上で以下のレジストリキーを設定します。
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

CUDA または **OpenCL** アプリケーション用の **GPU** アクセラレーション機能

ユーザーセッションで実行中の CUDA および OpenCL アプリケーションの GPU アクセラレーションは、デフォルトで無効です。

CUDA アクセラレーション POC 機能を有効にするには、以下のレジストリを設定します。

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA”=dword:0000000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA”=dword:00000001

OpenCL アクセラレーション POC 機能を有効にするには、以下のレジストリを設定します。

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:00000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:00000001

Windows デスクトップ **OS** のための **GPU** アクセラレーション

October 22, 2021

する X 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりデスクトップ OS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

GPU パススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数の GPU を装着して、各仮想マシンに GPU を 1 つずつ割り当てることができます。

GPU 仮想化を使用すると、複数の仮想マシンで単一の物理 GPU によるグラフィック処理能力に直接アクセスできるようになります。このハードウェア GPU 共有により、より専門的で複雑な設計作業を行うユーザーに適したデスクトップが提供されます。NVIDIA GRID カード（「NVIDIA GRID」参照）の GPU 仮想化では、非仮想化オペレーティングシステムで動作するものと同じ NVIDIA グラフィックドライバーが使用されます。GPU 仮想化ではさらに、Intel GVT-g 搭載の Intel Iris Graphics を採用した第 5 世代および第 6 世代の Intel CPU もサポートされます。これらの Intel プロセッサーのファミリについて詳しくは、「第 5 世代 Intel Core プロセッサー」および「第 6 世代 Intel Core i5 プロセッサー」を参照してください。GPU 仮想化は、AMD FirePro S シリーズのサーバーカードでもサポートされています。「AMD Professional Graphics の仮想化ソリューション」を参照してください。

HDX 3D Pro の機能は以下のとおりです：

- WAN およびワイヤレス接続でのパフォーマンスを最適化する Adaptive H.264 ベースの深圧縮。HDX 3D Pro のデフォルトでは、CPU ベースの全画面 H.264 圧縮が使用されます。ハードウェアエンコーディングは、NVENC をサポートする NVIDIA カードで使用されます。
- 特殊なユースケースのための無損失圧縮オプション。HDX 3D Pro では CPU ベースの無損失コーデックも提供され、医療用画像処理などピクセル単位での精密なグラフィックが求められるアプリケーションがサポートされます。真の無損失圧縮はネットワークおよび処理リソースに対する負荷が非常に高いため、特殊なユースケースでのみ使用することをお勧めします。

  無損失圧縮を使用すると、以下のように動作します。

  - 表示しているフレームに非可逆圧縮が適用されているのか無損失圧縮が適用されているのかを示すインジケーターがユーザーの通知領域に表示されます。このインジケーターは、ポリシーの［表示品質］設定で［操作時は低品質］が選択されている場合に便利です。送信されたフレームが無損失の場合、このインジケーターが緑色になります。
  - ユーザーは、無損失スイッチを使ってセッション内でいつでも［常に無損失］モードを有効にできます。セッション内で［無損失］を選択または選択解除するには、アイコンを右クリックするか、ショートカット Alt+Shift+1 を使用します。

    無損失圧縮の場合：HDX 3D Pro では、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：HDX 3D Pro では、デフォルトのコーデックまたはポリシーで指定されているコーデックが使用されます。

    無損失スイッチの設定は保持されず、次回のセッションではリセットされます。すべてのセッションで無損失コーデックが使用されるようにするには、ポリシーの［表示品質］設定で［常に無損失］を選択します。

- デフォルトのショートカットである ALT+SHIFT+1 を無効にし、セッション内で無損失を選択または選択解除できます。HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator で新しいレジストリ設定を構成します。
  - 名前：HKLM_HotKey、種類：String
  - 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。
  - 例：
    * F10 には、以下を設定します：K=0x79
    * Ctrl + F10 には、以下を設定します：C=1, K=0x79
    * Alt + A には、以下を設定します：A=1, K=a または A=1, K=A または K=A, A=1
    * Ctrl + Alt + 5 には、以下を設定します：C=1, A=1, K=5 または A=1, K=5, C=1
    * Ctrl + Shift + F5 には、以下を設定します：A=1, S=1, K=0x74

> 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、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- 複数および高解像度モニターのサポート。デスクトップ OS マシンでは、最大で 4 つのモニターが構成されたユーザーデバイスがサポートされます。ユーザーはそれらのモニターを自由に配置でき、解像度や向きが異なるモニターを組み合わせて使用できます。モニターの数は、ホストコンピューターの GPU、ユーザーデバイス、および使用できる帯域幅による制限を受けます。HDX 3D Pro では、ホストコンピューター上の GPU でサポートされるすべてのモニター解像度がサポートされます。

  HDX 3D Pro ではまた、Windows XP デスクトップでは、デュアルモニター構成が限定的にサポートされます。これについて詳しくは、「Windows XP または Windows Vista 上の VDA」を参照してください。

- 動的解像度仮想デスクトップまたはアプリケーションのウィンドウのサイズを任意に変更できます。注：解像度は、VDA のセッションウィンドウのサイズを変更することでのみ変更できます。VDA セッション内での解像度の変更（［コントロールパネル］>［デスクトップのカスタマイズ］>［ディスプレイ］>［画面の解像度］で変更）はサポートされていません。

- NVIDIA GRID アーキテクチャのサポート。HDX 3D Pro の GPU パススルーおよび GPU 共有では、NVIDIA GRID カードがサポートされます（「NVIDIA GRID)。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 を使用する HDX 3D Pro がサポートされます。

- NVIDIA GRID vGPU および AMD MxGPU を使用する VMware vSphere/ESX のサポート。

- Windows Server 2016 の Discrete Device Assignment を使用した Microsoft HyperV のサポート。

- Intel Xeon Processor E3 ファミリによるデータセンターグラフィックのサポート。HDX 3D Pro では、サポートされる Intel プロセッサファミリで、マルチモニター（最大 3 つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。詳しくは、「https://www.citrix.com/intel」および「https://www.intel.com/content/www/us/en/servers/data-center-graphics.html」を参照してください。

- AMD FirePro S シリーズのサーバーカードでの AMD RapidFire のサポート。HDX 3D Pro では、マルチモニター（最大 6 つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。注：HDX 3D Pro による AMD MxGPU（GPU 仮想化）のサポートで対応しているのは、VMWare vSphere の vGPU のみです。GPU パススルーに対応しているのは、XenServer と Hyper-V です。詳しくは、「AMD 仮想化ソリューション」を参照してください。

- NVIDIA GPU の高パフォーマンスビデオエンコーダーと Intel Iris Pro グラフィックプロセッサへのアクセス。この機能は、ポリシー設定（デフォルトで有効）によって制御され、H.264 エンコーディングのハードウ

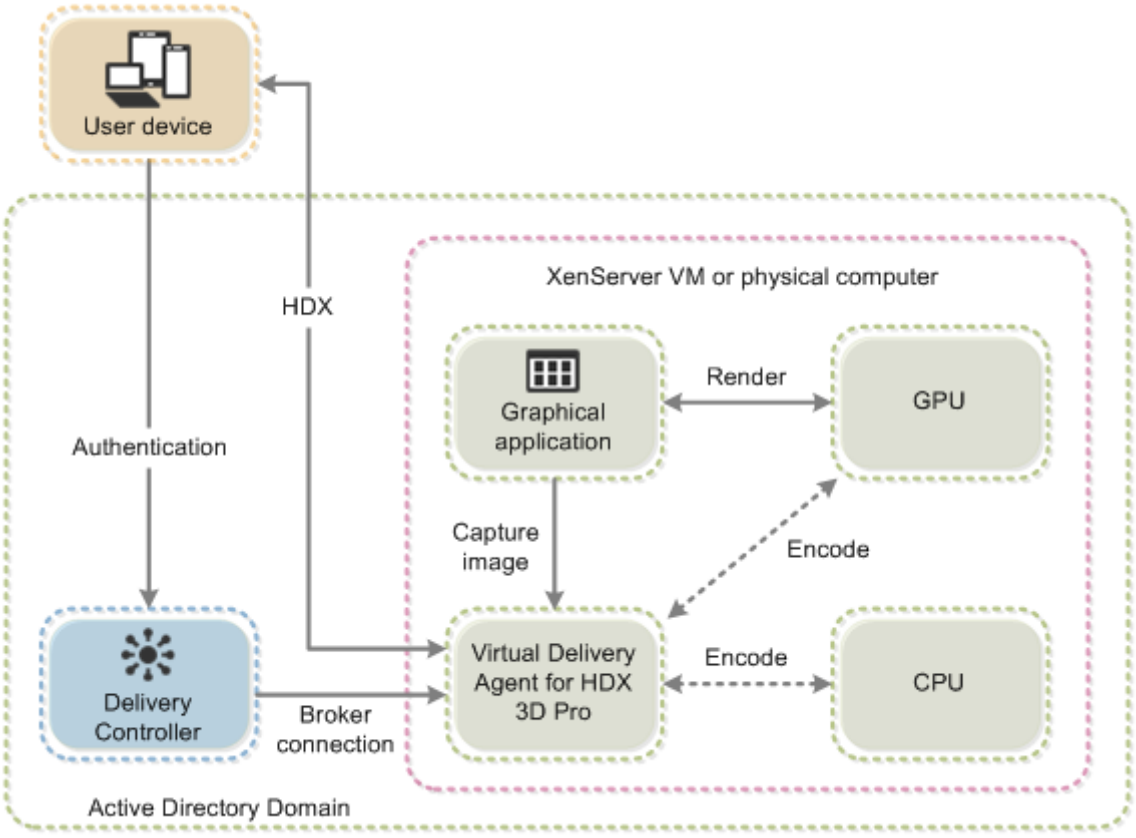
ェアエンコーディングが許可されます（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して CPU ベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

以下の図を参照してください：

- ユーザーが Citrix Receiver にログオンして仮想アプリケーションまたはデスクトップにアクセスすると、Controller がユーザーを認証して VDA for HDX 3D Pro と通信し、グラフィックアプリケーションをホストしているコンピューターへの接続を仲介します。

VDA for HDX 3D Pro はホスト上の適切なハードウェアを使って、デスクトップ全体またはグラフィックアプリケーションだけのビューを圧縮します。

- デスクトップまたはアプリケーションのビューおよびそれに対するユーザーの応答は、Citrix Receiver と VDA for HDX 3D Pro 間の直接 HDX 接続を介して、ホストコンピューターとユーザーデバイス間で転送されます。



VDA for HDX 3D Pro のインストール

VDA for Windows Desktop OS をインストーラーのグラフィカルインターフェイスでインストールする場合は、［HDX 3D Pro］ページで［はい］をクリックします。コマンドラインでインストールする場合は、XenDesktop VdaSetup.exe コマンドに/enable_hdx_3d_pro オプションを指定します。

HDX 3D Pro をアップグレードするには、既存の HDX 3D for Professional Graphics コンポーネントと VDA の両方をアンインストールしてから VDA を HDX 3D Pro モードでインストールしてください。同様に、Windows Desktop OS で標準の VDA モードを 3D Pro モードに切り替える場合も、標準の VDA をアンインストールしてから VDA を HDX 3D Pro モードでインストールしてください。

標準モード	HDX 3D Pro モード
一般的に、グラフィックのハードウェアアクセラレーションおよびリモート PC アクセスに最適です。	5 つ以上のモニターが必要でない限り、一般的にグラフィックハードウェアアクセラレーションのあるデータセンターデスクトップに最適です。
リモート PC アクセスには、あらゆる GPU を使用できます（アプリケーション互換性の制限あり）: Windows 7、8、8.1 では、DirectX 用 GPU アクセラレーションの機能レベルは最大 9.3 です。一部の DirectX 10、11、12 アプリケーションは、DirectX 9 へのフォールバックをしない場合、実行されないことがあります。Windows 10 の場合、GPU アクセラレーションはウィンドウ表示の DirectX 10、11、および 12 アプリに提供されます。DX 9 アプリは WARP によってレンダリングされます。DX アプリを全画面モードで使用できません。GPU ベンダーによってサポートされている場合はリモートセッションでの OpenGL アプリケーションアクセラレーション（現時点では NVIDIA のみ）。	任意の GPU による GPU アクセラレーションをサポートしますが、コンソールのブランキング、非標準画面解像度、および True Multi Monitor サポートには NVIDIA GRID、Intel Iris Pro または AMD RapidFire グラフィックスが必要です。広範なアプリケーション互換性のためにグラフィックベンダーのドライバーを活用します: GPU がサポートするすべての 3D API（DirectX または OpenGL）。Intel Iris Pro（Win10 のみ）、NVIDIA GRID および AMD RapidFire での全画面 3D アプリサポート。カスタムドライバー拡張および API のサポート（CUDA や OpenCL など）。
任意のモニター解像度（上限は Windows OS およびパフォーマンスによって決まります）および最大 8 つのモニター。	最大で 4 つのモニターをサポートします。
Intel Iris Pro グラフィックプロセッサで利用可能な H.264 ハードウェアエンコーディング。	Intel Iris Pro グラフィックスプロセッサおよび NVIDIA カードを搭載して H.264 ハードウェアエンコーディングが使用可能です。

NVIDIA ドライバーのインストールとアップグレード

NVIDIA GRID API では、GPU のフレームバッファーに対する直接アクセスが提供され、スムーズでインタラクティブなユーザーエクスペリエンスのための最速のフレームレートが提供されます。NVIDIA ドライバーをインストールしてから VDA for HDX 3D Pro をインストールすると、NVIDIA GRID がデフォルトで有効になります。

仮想マシン上で NVIDIA GRID を有効にするには、デバイスマネージャーで Microsoft 基本ディスプレイアダプターを無効にします。**NVFBCEnable.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 NVFBCEnable ツールを使って NVIDIA GRID を有効にします。

NVIDIA GRID を無効にするには、**NVFBCEnable.exe -disable -noreset** コマンドを実行してから VDA を再起動します。

Intel グラフィックドライバーのインストール

VDA をインストールする前に Intel グラフィックドライバーをインストールできます。次の手順は、VDA for HDX 3D Pro をインストールした後、または Intel ドライバーが更新された後にのみ必要です。

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:
>
> 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。

ブランチオフィスなど、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。

OpenGL ソフトウェアアクセラレータ

November 28, 2018

OpenGL ソフトウェアアクセラレータは、ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、および CAD/CAM アプリケーションなどの OpenGL アプリケーションで使用するソフトウェアラスタライザーです。OpenGL ソフトウェアアクセラレータを使用すると、グラフィックカードを装着しなくてもユーザーに良好なユーザーエクスペリエンスを提供できる場合があります。

> 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、一部のアプリケーションがサポートされない場合があるため、すべてのアプリケーションで動作確認を行ってください。この機能は、Windows OpenGL ラスタライザーで十分なパフォーマンスが得られない場合の解決策として使用してください。OpenGL ソフトウェアアクセラレータがアプリケーションをサポートする場合は、GPU ハードウェアのコストを削減する手段として使用できます。

OpenGL ソフトウェアアクセラレータはインストールメディアのサポートフォルダーに収録されており、すべての VDA プラットフォームをサポートしています。

OpenGL ソフトウェアアクセラレータは、以下の場合に使用します:

- グラフィック処理ハードウェアのないサーバーで、XenServer やほかのハイパーバイザーの仮想マシン上で動作する OpenGL アプリケーションで十分なパフォーマンスが得られない。一部のアプリケーションでは、Windows に付属の Microsoft OpenGL ソフトウェアラスタライザーよりも高いパフォーマンスが得られる場合があります。これは、OpenGL アクセラレータで SSE4.1 および AVX が使用されるためです。OpenGL アクセラレータは、Version 2.1 までの OpenGL を使用するアプリケーションをサポートします。
- ワークステーション上で動作するアプリケーションでは、まずそのワークステーションのグラフィックアダプターで提供されるデフォルトの OpenGL サポート機能を使用してテストを行います。一般的に、最新バージョンのグラフィックカードを使用すると最高のパフォーマンスが得られます。グラフィックカードのバージョンが低い場合、または十分なパフォーマンスが得られない場合は、OpenGL ソフトウェアアクセラレータを使用してテストを行います。
- 3D OpenGL アプリケーションが CPU ベースのソフトウェアラスタライザーで適切に配信されていない場合は、OpenGL の GPU ハードウェアアクセラレーションを使用することでパフォーマンスが向上することがあります。この機能は、ベアメタルまたは仮想マシン上で使用できます。

Thinwire

August 24, 2021

はじめに

Thinwire とは、XenApp および XenDesktop で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。

正常なディスプレイリモートソリューションでは、ローカル PC と同様の、高度にインタラクティブなユーザーエクスペリエンスが提供されます。Thinwire では、幅広く複合的、効果的な画像解析および圧縮技術の使用により、これを実現しています。Thinwire ではサーバーのスケーラビリティが最大化され、消費する帯域幅は他のディスプレイリモートテクノロジより少なくできます。

このバランスのために Thinwire は大部分の一般的なビジネスユースケースに合致しており、XenApp および XenDesktop のデフォルトのディスプレイリモートテクノロジとして使用されています。

Thinwire または Framehawk

Thinwire は、デスクトップの一般的なワークロード、たとえば、デスクトップ、オフィスの生産性、またはブラウザベースのアプリケーションを提供するために使用してください。Thinwire は、マルチモニター、高解像度、または高 DPI のシナリオや、ビデオとビデオ以外の混在コンテンツを持つワークロードにも推奨されます。

Framehawkは、パケット損失が断続的に高くなることがあるブロードバンドワイヤレス接続を使用するモバイルワーカーに使用してください。

HDX 3D Pro

デフォルトの構成では、Thinwire は 3D や高度にインタラクティブなグラフィックを提供できますが、VDA for Desktop OS のインストール時に HDX 3D Pro モードを有効化することが、そのようなシナリオに適切な選択です。Thinwire の 3D Pro モードは、全画面の H.264 エンコードでのグラフィック送信のための構成です。これにより、3D Pro グラフィックは、より滑らかなエクスペリエンスを実現できます。詳しくは、「HDX 3D Pro」および「Windows デスクトップ OS のための GPU アクセラレーション」を参照してください。

要件および考慮事項

- Thinwire は、Windows Server 2012 R2、Windows Server 2016、Windows 7、および Windows 10 など、最新のオペレーティングシステムに最適化されています。Windows Server 2008 R2 には、従来のグラフィックモードをお勧めします。ビルトインのCitrix ポリシーテンプレートである「高サーバースケーラビ

リティ - レガシ OS」と「WAN の最適化 - レガシ OS」を使用して、これらのユースケースに推奨されるポリシー設定の組み合わせを提供します。

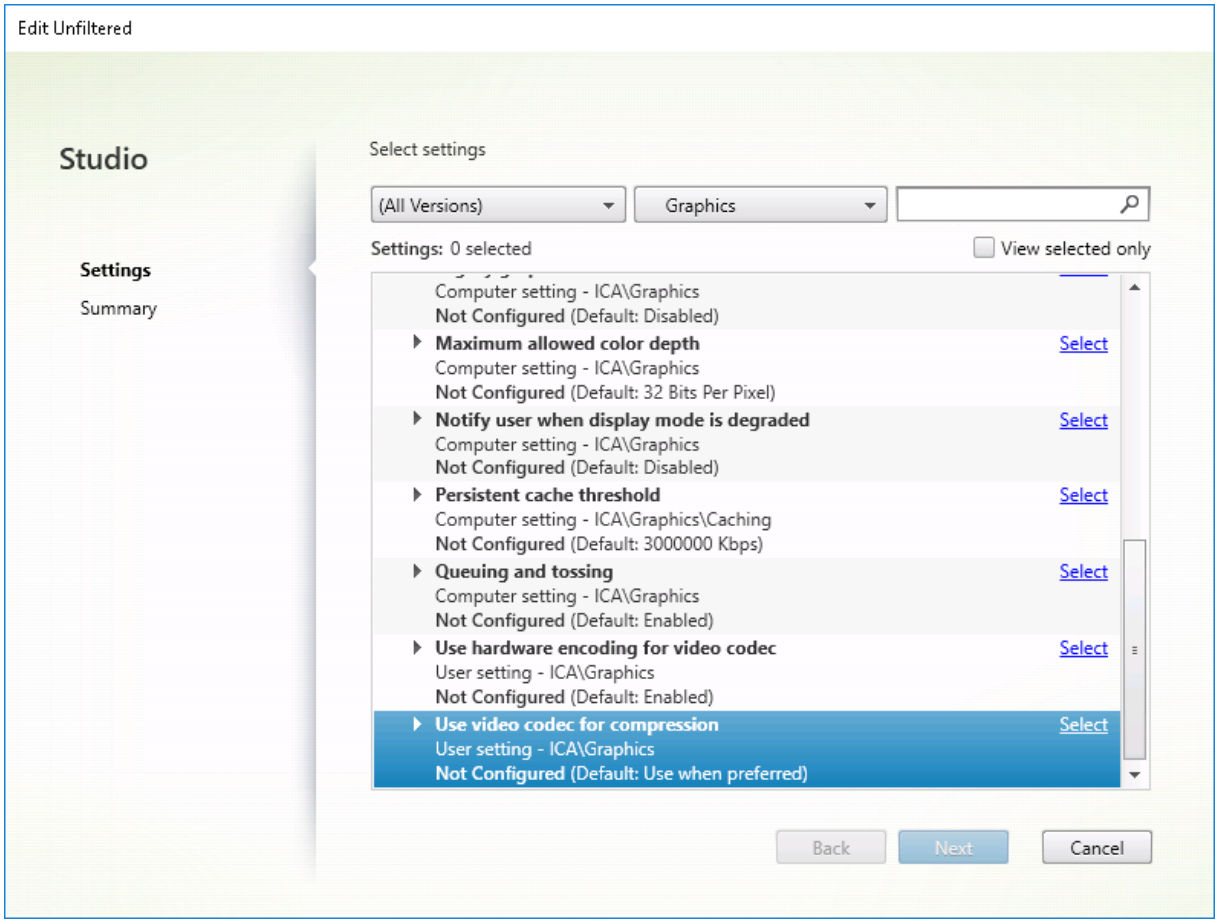
- Thinwire の動作を制御する ［圧縮にビデオコーデックを使用する］ポリシー設定は、XenApp および XenDesktop 7.6 FP3 以降の VDA バージョンで利用できます。［選択された場合ビデオコーデックを使用する］オプションは、VDA バージョン XenApp および XenDesktop 7.9 以降のデフォルト設定です。
- Thinwire はすべての Citrix Receiver でサポートされています。ただし一部の Citrix Receiver は、他でサポートされない Thinwire 機能（たとえば、帯域幅使用が低下した場合の 8 または 16 ビットグラフィック）をサポートする場合があります。そのような機能のサポートは、Citrix Receiver によって自動的にネゴシエートされます。
- Thinwire は、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwire が使用するリソース量は調整可能ですが、帯域幅の使用状況がその結果増大することがあります。
- 低帯域幅または高遅延のシナリオでは、8 または 16 ビットグラフィックを有効化して対話操作性を改善することを検討できますが、特に 8 ビットの色数で、表示品質が影響を受ける場合があります。

構成

Thinwire はデフォルトのディスプレイリモートテクノロジです。

次のグラフィックポリシー設定はデフォルトを設定し、さまざまなユースケースに代替選択肢を提供します。

- 圧縮にビデオコーデックを使用する
  - 選択された場合ビデオコーデックを使用するこれがデフォルトの設定です。追加の構成は必要ありません。この設定をデフォルトとして保持することにより、すべての Citrix 接続で Thinwire が選択され、デスクトップの一般的なワークロードで、スケーラビリティ、帯域幅、および優れた画質の点で、確実に最適化されます。
- このポリシー設定の他のオプションは、さまざまなユースケースでの他のテクノロジとの組み合わせでも Thinwire を使用し続けます。例:
  - ［領域をアクティブに変更］。Thinwire のアダプティブ表示テクノロジは、動画（ビデオ、3D インモーション）を識別し、画像が動く画面の部分でのみ H.264 を使用します。
  - ［画面全体に使用］。特に 3D グラフィックを多用する事例で、Thinwire を全画面 H.264 を使用して配信して、ユーザーエクスペリエンスと帯域幅の改善を最適化します。



次の視覚表示ポリシー設定など、いくつかの他のポリシー設定は、ディスプレイリモートテクノロジのパフォーマンスを微調整するために使用でき、また、Thinwire によってすべてサポートされます。

- 単純なグラフィックスの優先色深度
- ターゲットフレーム数
- 表示品質

さまざまなビジネスユースケースに対してシトリックスが推奨するポリシー設定の組み合わせを取得するには、組み込みのCitrix ポリシーテンプレートを使用します。「高サーバースケーラビリティ」および「最高品位ユーザーエクスペリエンス」テンプレートはどちらも、組織の優先順位やユーザーの予期に最も適したポリシー設定との組み合わせで Thinwire を使用します。

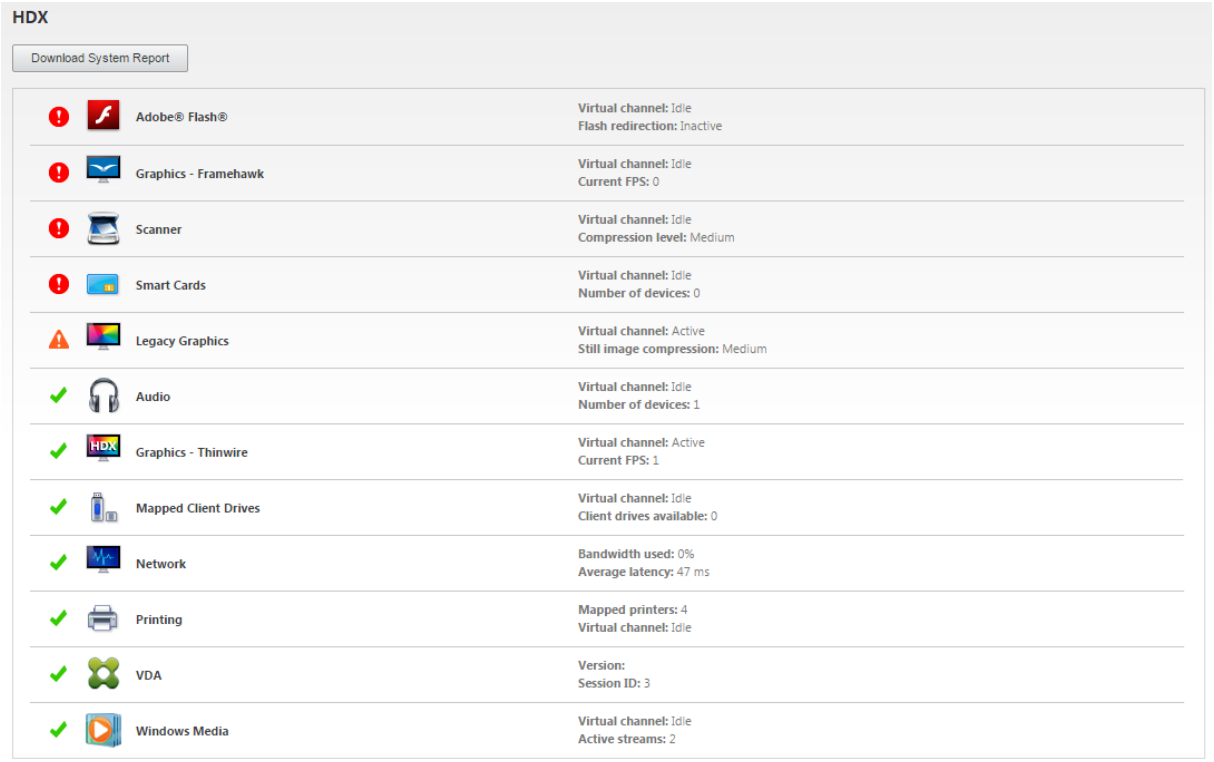
Thinwire のモニター

Citrix Director から Thinwire の利用状況とパフォーマンスをモニターすることができます。HDX 仮想チャネル詳細ビューには、あらゆるセッションで、Thinwire のトラブルシューティングやモニターに役立つ情報が表示されます。Thinwire 関連の測定基準を表示するには:

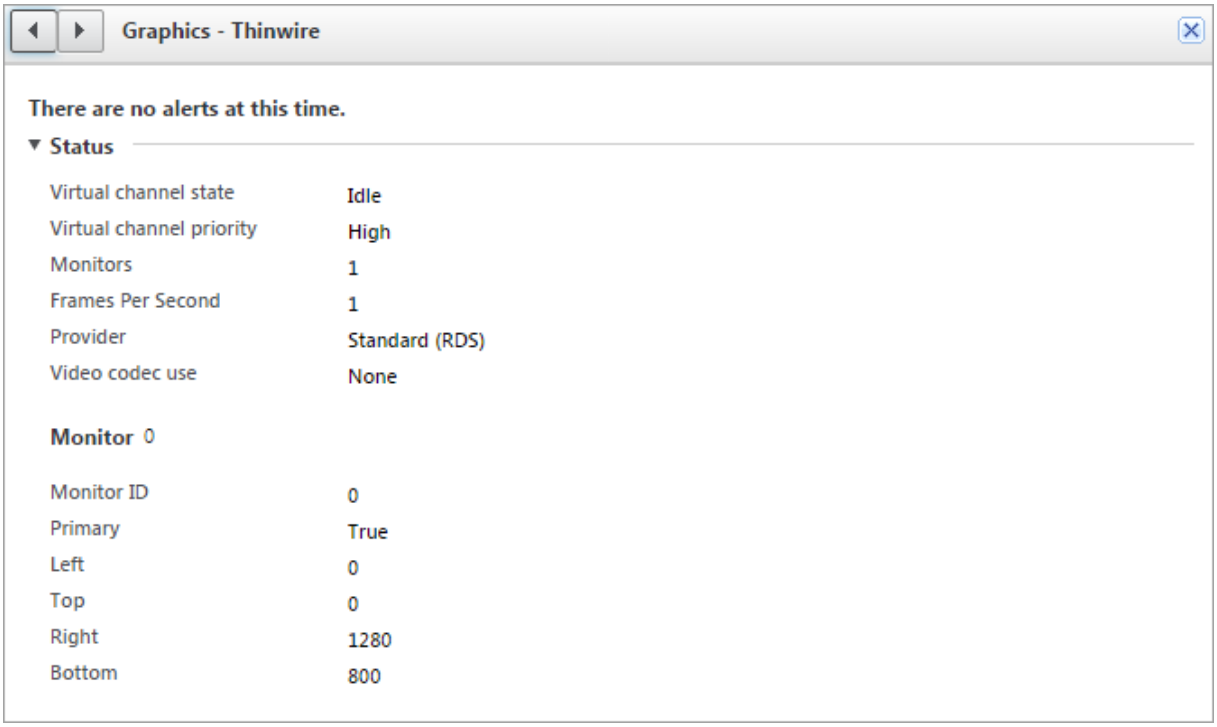
1. Director で、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて ［詳細］をクリックします。または、［フィルター］>［セッション］>［すべてのセッション］を選択し、アクティブな

セッションを開いて［詳細］をクリックすることもできます。

2. ［**HDX**］パネルまで下にスクロールします。



1. ［グラフィック **- Thinwire**］を選択します。



マルチメディア

August 24, 2021

HDX 技術スタックは、マルチメディアアプリケーションの配信を次の 2 つの相補的なアプローチでサポートします。

- サーバー側でレンダリングするマルチメディア配信
- クライアント側でレンダリングするマルチメディアリダイレクト

これにより、良好なユーザーエクスペリエンスを保ちながら、サーバースケーラビリティを向上させ、ユーザーごとのコストを削減するあらゆる種類のマルチメディアフォーマットを配信できます。

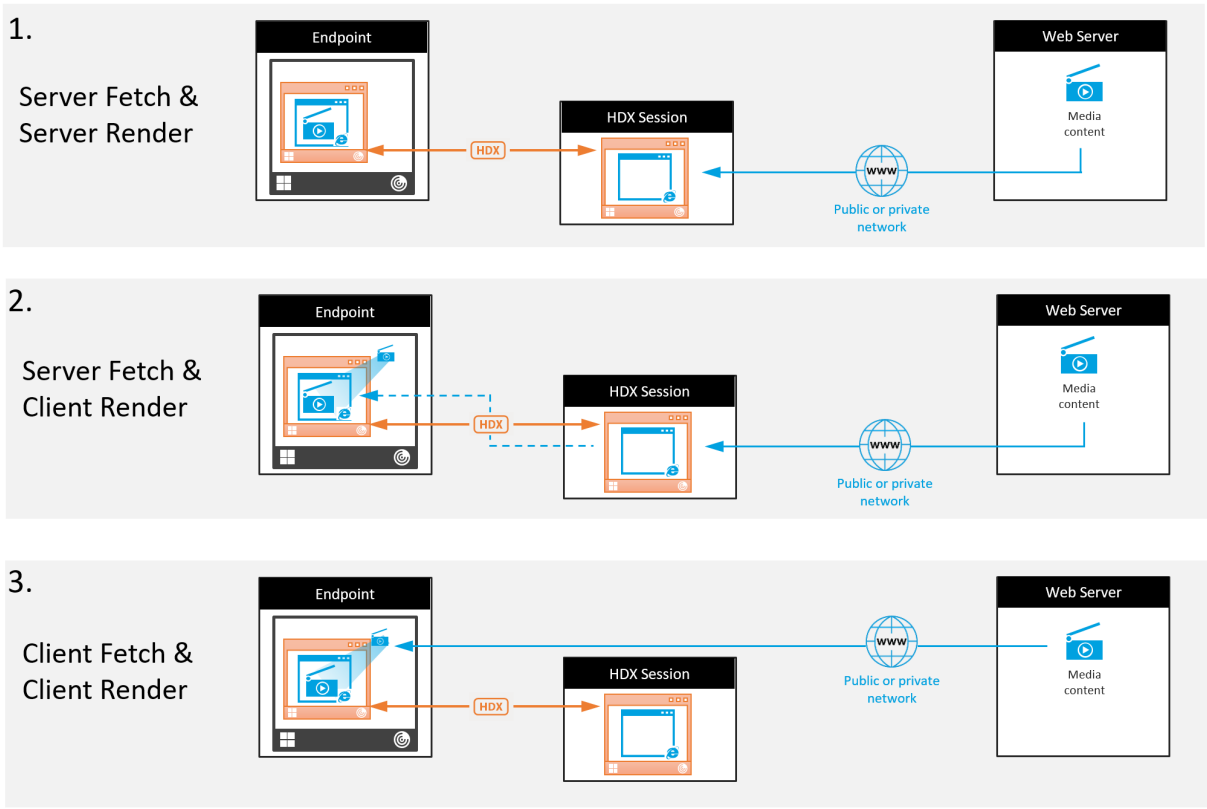
サーバー側でレンダリングするマルチメディア配信で、オーディオとビデオコンテンツは、アプリケーションによって XenApp または XenDesktop サーバー上でデコードおよびレンダリングされます。コンテンツは圧縮され、ICA プロトコルでユーザーデバイス上の Citrix Receiver に配信されます。この方法は、さまざまなアプリケーションとメディア形式に対して、最大レートの互換性を提供します。ビデオ処理は数値計算であるため、サーバー側でレンダリングされたマルチメディア配信はオンボードのハードウェアアクセラレーションの利点を大幅に活かすことがきます。たとえば、DirectX Video Acceleration（DXVA）のサポートは、H.264 デコーディングを別のハードウェアで実行することで、CPU をオフロードします。Intel Quick Sync と NVIDIA NVENC の機能により、ハードウェアアクセラレーション用の H.264 エンコーディングが利用できるようになりました。

ほとんどのサーバーにビデオ圧縮用のハードウェアアクセラレーションがないため、すべてのビデオ処理をサーバーの CPU で実行する場合は、サーバースケーラビリティに悪影響を及ぼします。高サーバースケーラビリティを維持するために、多くのマルチメディア形式をユーザーデバイスにリダイレクトして、ローカル側でレンダリングできます。Windows Media リダイレクトは、一般的に Windows Media Player に関連した、さまざまな種類のメディア形式に対してサーバーをオフロードします。

Flash リダイレクトは、ユーザーデバイス上でローカルに実行される Flash Player に Adobe Flash ビデオコンテンツをリダイレクトします。
HTML5 ビデオが普及し、シトリックスはこのタイプのコンテンツに対してリダイレクトテクノロジを導入しました。また、一般的なアドレス帳リダイレクト機能である、ホストからクライアントへのリダイレクトとローカルアプリアクセスを、マルチメディアコンテンツに適用できます。

これらの機能を含めて、リダイレクトを構成しない場合は、HDX はサーバー側でのレンダリングを実行します。
リダイレクトを構成する場合、HDX はサーバー側でフェッチし、クライアント側でレンダリング、またはクライアント側でフェッチし、クライアント側でレンダリングのいずれかを実行します。これらの方法が失敗した場合、HDX は必要に応じてサーバー側でのレンダリングにフォールバックし、フォールバック防止ポリシーの対象になります。

サンプルシナリオ



シナリオ **1.**（サーバー側でフェッチし、サーバー側でレンダリング）**:**

1. サーバーはメディアファイルをソースからフェッチし、デコードし、コンテンツをオーディオデバイスまたはディスプレイデバイスに対して再生します。
2. サーバーは再生されたイメージまたはサウンドをディスプレイデバイスまたはオーディオデバイスからそれぞれ抽出します。
3. オプションとしてサーバーが抽出されたファイルを圧縮し、クライアントに送信します。

このアプローチでは、（抽出されたイメージやサウンドが効率的に圧縮されていない場合は）高 CPU コストと高帯域幅コストを負担することになり、サーバースケーラビリティは低くなります。

Thinwire とオーディオの仮想チャネルがこのアプローチを処理します。このアプローチの利点により、クライアントのハードウェアとソフトウェアの要件が削減されます。このアプローチでは、デコーディングはサーバーで実行され、より多くの種類のデバイスとフォーマットに対応します。

シナリオ **2.**（サーバー側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、オーディオまたはディスプレイデバイスに対してデコードおよび再生される前に、メディアコンテンツをインターセプトできることを前提としています。圧縮されたオーディオ/ビデオコンテンツは、クライアントに送信され、ローカルでデコードおよび再生されます。このアプローチの利点により、デコーディングとプレゼンテーションはクライアントデバイスにオフロードされ、サーバーの CPU サイクルが節約されます。

ただし、このアプローチでは、クライアントにハードウェアとソフトウェアの要件が一部追加されます。クライアン

トは、受信する可能性のあるそれぞれのフォーマットをデコードできる必要があります。

シナリオ **3.**（クライアント側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、ソースからフェッチされる前に、メディアコンテンツの URL をインターセプトできることを前提としています。URL は、メディアコンテンツがローカルでフェッチ、デコード、および再生されたクライアントに送信されます。このアプローチは概念的に単純です。この利点により、制御コマンドのみがサーバーから送信されるため、サーバーの CPU サイクルと帯域幅の両方が節約されます。ただし、メディアコンテンツは、クライアントに常にアクセスできるわけではありません。

フレームワークとプラットフォーム

デスクトップオペレーティングシステム（Windows、Mac OS X、および Linux）は、マルチメディアアプリケーションのよりすばやく簡単な開発を可能にする、マルチメディアフレームワークを提供します。次の表に、より一般的なマルチメディアフレームワークの一部を示します。各フレームワークはメディア処理を複数の段階に分割して、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows（98 以降）
Media Foundation	Windows（Vista 以降）
Gstreamer	Linux
Quicktime	Mac OS X

メディアリダイレクト機能によるダブルホップのサポート

メディアリダイレクト	サポート
HDX Flash リダイレクト	いいえ
Windows Media リダイレクト	はい
HTML5 ビデオリダイレクト	はい
オーディオリダイレクト	なし

関連情報

- オーディオ機能
- Flash リダイレクト
- HTML5 マルチメディアリダイレクション
- Windows Media リダイレクト

- 一般コンテンツリダイレクト

オーディオ機能

October 22, 2021

ポリシーに以下の Citrix 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」、「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
>
> TCP ではなくユーザーデータグラムプロトコル（UDP）を使ってオーディオを配信するのが最も良いのですが、DTLS を使った UDP オーディオ暗号化は NetScaler Gateway と Citrix Receiver 間でのみ有効です。そのため、TCP トランスポートが望ましい場合もあります。TCP は、VDA と Citrix Receiver 間の、エンドツーエンドの TLS 暗号化をサポートします。

音質

一般的に、音質を高くするほど、オーディオデータの転送に必要な帯域幅が大きくなり、サーバーの CPU にも負担がかかります。オーディオデータを圧縮すると、セッションのパフォーマンスと音質とのバランスを考慮しながら、ユーザーの操作感を最適化できます。これを行うには、サウンドファイルに適用する圧縮レベルを制御するには、Citrix ポリシーを使用します。

デフォルトでは、TCP トランスポート使用時の「音質」ポリシー設定は［高 - 高品位オーディオ］に設定されており、UDP トランスポート使用時（推奨）は［中 - スピーチに最適化］に設定されています。高品位オーディオ設定では HiFi ステレオオーディオが提供されますが、ほかの品質設定よりも多くの帯域幅が消費されます。最適化されていないボイスチャットアプリケーションやビデオチャットアプリケーション（ソフトフォンなど）でこの設定を使用すると、リアルタイムの音声通信に不適切な遅延が発生することがあります。「スピーチに最適化」ポリシー設定は、選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオにお勧めです。

衛星、ダイヤルアップ接続など帯域幅が制限されている場合、音質を ［低］に設定することで、帯域幅の消費を最少にすることができます。この状況では、低帯域幅接続のユーザーに対して別のポリシーを作成し、高帯域幅接続のユーザーに影響しないようにします。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイスの［クライアント側オーディオ設定］が有効になっていることを確認してください。詳しくは、後述の「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

クライアントオーディオリダイレクト

サーバー上で実行しているアプリケーションからユーザーデバイス上のスピーカーまたはヘッドフォンなどのサウンドデバイスでオーディオが再生されるようにするには、［クライアントオーディオリダイレクト］設定をデフォルトの

まま（[許可]）にします。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。ただし、[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。

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。ユーザーデバイスの [クライアント側オーディオ設定] が有効になっていることを確認してください。詳しくは、後述の「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、[クライアントマイクリダイレクト] 設定をデフォルトのまま（[許可]）にします。

ユーザーデバイスとの信頼関係が設定されていないサーバー上のセッションでマイクを使用しようとすると、セキュリティに関する警告がユーザーに表示されます。この場合、クライアント側のマイクへのアクセスを許可するかどうかをユーザーが選択できます。この警告は、ユーザーが Citrix Receiver 側で無効にできます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイスの [クライアント側オーディオ設定] が有効になっていることを確認してください。詳しくは、後述の「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

オーディオプラグアンドプレイ

ポリシーの [オーディオプラグアンドプレイ] 設定では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。この設定項目は、デフォルトで [有効] になっています。[オーディオプラグアンドプレイ] を使用すると、ユーザーのセッションが確立されるまでプラグを差し込まなくても、オーディオデバイスが認識されるようにできます。

この設定項目は、Windows サーバー OS マシンのみに適用されます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。

オーディオリダイレクトの最大帯域幅（**Kbps**）とオーディオリダイレクトの最大帯域幅（**%**）

ポリシーの [オーディオリダイレクトの最大帯域幅（Kbps）] 設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。ポリシーの [オーディオリダイレクトの最大帯域幅（%）] 設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。これらの設定には、デフォルトで 0 が指定されており、帯域幅に制限はありません。両方の設定を構成した場合、より高い制限（より小さい値）の設定が適用されます。

設定について詳しくは、「帯域幅のポリシー設定」を参照してください。ユーザーデバイスの [クライアント側オーディオ設定] が有効になっていることを確認してください。詳しくは、後述の「ユーザーデバイス側のオーディオ設定ポリシー」を参照してください。

UDP でのオーディオリアルタイムトランスポートとオーディオ UDP ポートの範囲

ポリシーの
[UDP でのオーディオリアルタイムトランスポート］設定は、デフォルトで［有効］が選択されています（インストール時に選択した場合）。これにより、サーバーの UDP ポートが開き、［UDP でのオーディオリアルタイムトランスポート］設定が有効な接続でそのポートが使用されます。ネットワークで輻輳やパケット損失などが生じる環境で最適なユーザーエクスペリエンスを提供するため、オーディオの UDP/RTP を構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオでは、EDT より UDP オーディオが優先されます。UDP は再送のないパケット損失が認められており、パケット損失が頻繁な場合でも接続に遅延が発生しません。

> 重要:
>
> NetScaler 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 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 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。ユーザーデバイスの［クライアント側オーディオ設定］が有効になっていることを確認してください。詳しくは、後述の「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管理用テンプレートの構成」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 コンポーネント］>［Citrix Receiver］>［ユーザーエクスペリエンス］の順に開きます。
3. ［**Client audio settings**］を開き、［未構成］、［有効］、または［無効］をクリックします。
   - 未構成。デフォルトでは、オーディオリダイレクトは高品質オーディオ、または以前に構成したカスタムのオーディオ設定で有効になります。
   - 有効。オーディオリダイレクトは、選択したオプションで有効になります。
   - **Disabled**（無効）：オーディオリダイレクトは無効化されます。
4. ［有効］をクリックした場合は、音質を選択します。UDP オーディオでは、［中］（デフォルト）を使用してください。
5. UDP オーディオでは、［**Enable Real-Time Transport**］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 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 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\<Store Name>\App_Data\default.ica を開きます。
2. ［アプリケーション］セクションに以下の項目を記入します。

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

ユーザーデータグラムプロトコル（UDP）オーディオは、default.ica の編集で有効になっている場合、そのストアを使用するすべてのユーザーに対して有効化されます。

マルチメディア会議でのエコーの解消

オーディオまたはビデオ会議にユーザーが参加したときに、音声にエコーがかかって聞こえることがあります。通常、この問題はスピーカーとマイクが近すぎる場合に発生します。このため、オーディオまたはビデオ会議ではヘッドセットを使用することをお勧めします。

HDX には、会議中のエコーを最小限に抑えるためのエコーキャンセル機能が用意されており、デフォルトで有効になっています。エコーキャンセル機能の効果は、スピーカーとマイクとの距離により異なります。デバイスは、近すぎず、かつ遠すぎないところに配置してください。

エコーキャンセル機能を無効にするには、レジストリ設定を変更します。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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\Advance

- 64 ビットシステム: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation

2. [値のデータ] ボックスの値を FALSE に変更します。

ソフトフォン

ソフトフォンは、電話インターフェイスとして動作するソフトウェアです。コンピューターや他のスマートデバイスからインターネット経由で電話するには、ソフトフォンを使用します。ソフトフォンを使うことにより、画面を使って電話番号をダイヤルしたり、他の電話関連の機能を実行したりできます。

XenApp および XenDesktop は、ソフトフォンの配信に対するいくつかの代替手段をサポートします。

- 制御モード。ホストされたソフトフォンが物理的な電話セットを制御します。このモードでは、XenApp または XenDesktop サーバーを通過するオーディオトラフィックはありません。
- **HDX RealTime** に最適化されたソフトフォンのサポート。このメディアエンジンはユーザーデバイス上で実行され、ボイスオーバー IP（VoIP）トラフィックがピアツーピアで流れます。たとえば、以下を参照してください:
  - Microsoft Skype for Business と Lync の配信を最適化するHDX RealTime Optimization Pack
  - Jabber 用のCisco Virtualization Experience Media Engine（VXME）
  - one-X Communicator および one-X Agent 用のAvaya VDI Communicator
- ローカルアプリケーションアクセス。XenApp および XenDesktop の機能により、ソフトフォンなどのアプリケーションは、エンドユーザーの Windows デバイス上ではローカルで実行されますが、その仮想/公開デスクトップとはシームレスに統合されています。これにより、ユーザーデバイスへのすべてのオーディオ処理の負荷が軽減されます。詳しくは、「ローカルアプリアクセスと URL リダイレクト」を参照してください。
- **HDX RealTime** の汎用ソフトフォンのサポート。VoIP-over-ICA。

汎用ソフトフォンのサポート

汎用ソフトフォンのサポートにより、データセンターの XenApp または XenDesktop 上に、未変更のソフトフォンをホストすることができます。オーディオトラフィックは、Citrix ICA プロトコルを介して（UDP/RTP を優先的に使用して）、Citrix Receiver を実行しているユーザーデバイスに送信されます。

汎用ソフトフォンのサポートは、HDX RealTime の機能です。ソフトフォンの配信に対するこのアプローチは、以下の場合に特に有効です。

- ソフトフォンの配信に最適なソリューションがなく、ローカルアプリケーションアクセスが可能な Windows デバイス上にユーザーがいない。
- ソフトフォンの最適化された配信に必要とされるメディアエンジンが、ユーザーデバイスにインストールされていないか、ユーザーデバイス上で実行しているオペレーティングシステムのバージョンで利用できない。このシナリオでは、汎用 HDX RealTime が価値のあるフォールバックソリューションを提供します。

XenApp および XenDesktop を使用したソフトフォンの配信には、考慮事項が 2 つあります:

- ソフトフォンアプリケーションがどのように仮想/公開デスクトップに配信されるか。

- エンドユーザーのヘッドセット、マイクロフォン、およびスピーカー、または USB 電話セット間でオーディオがどのように配信されるか。

XenApp および XenDesktop には、汎用ソフトフォンの配信をサポートする多くのテクノロジが含まれています:

- リアルタイムオーディオの高速エンコードと帯域幅の効率性のための、スピーチに最適化されたコーデック。
- 遅延の少ないオーディオスタック。
- ネットワーク遅延が変動する場合、オーディオをスムーズにするサーバー側のジッターバッファー。
- QoS のパケットのタグ付け（DSCP および WMM）
  - RTP パケットの DSCP タグ付け（レイヤー 3）
  - WiFi の WMM タグ付け

Windows、Linux、Chrome、および Mac 用の Citrix Receiver バージョンは、VoIP にも対応しています。Citrix Receiver for Windows は以下の機能を提供します:

- クライアント側のジッターバッファー - ネットワーク遅延が変動する場合でもオーディオを確実にスムーズにします。
- エコーキャンセル - ヘッドセットを使用しないユーザー向けに、マイクとスピーカの距離を調整します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッション開始前にプラグインする必要はありません。いつでもプラグインできます。
- オーディオデバイスルーティング - ユーザーはヘッドセットの音声通信以外に、スピーカーに着信音を直接送信できます。
- マルチストリーム ICA - ネットワーク上で柔軟な QoS（サービス品質）ベースのルーティングを有効にします。
- ICA は、4 つの TCP と 2 つの UDP ストリームをサポートします。UDP ストリームの 1 つは、RTP 上でリアルタイムオーディオをサポートします。

Citrix Receiver の機能の概要については、『Citrix Receiver Feature Matrix』を参照してください。

システム構成の推奨事項

クライアントのハードウェアとソフトウェア: 音質の最適化のために、最新バージョンの Citrix Receiver とアコースティックエコーキャンセル（AEC）付きの高品質なヘッドセットをお勧めします。Windows、Linux、および Mac 用の Citrix Receiver バージョンは VoIP をサポートします。また、Dell Wyse は ThinOS（WTOS）の VoIP サポートを提供します。

CPU 検討事項: VDA 上の CPU 使用率を監視して、それぞれの仮想マシンに 2 つの仮想 CPU を割り当てる必要があるかどうかを決定します。リアルタイムの音声およびビデオはデータ量が多いです。2 つの仮想 CPU を構成すると、スレッドの切り替え遅延を減らすことができます。そのため、XenDesktop VDI 環境で 2 つの vCPU を構成することをお勧めします。

物理 CPU はセッションを超えて共有できるため、2 つの仮想 CPU を持つことは、必ずしも物理 CPU の数を倍にすることではありません。

セッション画面の保持機能に使われる Citrix Gateway Protocol（CGP）により、CPU の消費も増加します。高品質のネットワーク接続では、この機能を無効にして、VDA の CPU 消費を削減することができます。前述のいずれの手順も、強力なサーバーでは必要ないかもしれません。

UDP オーディオ： UDP によるオーディオは、ネットワークの輻輳やパケット損失に対する強力な耐性を提供します。利用できるのであれば、TCP から代えることをお勧めします。

LAN/WAN の設定：ネットワークの適切な設定は、リアルタイムオーディオの高い品質には極めて重要です。通常、過度のブロードキャストパケットはジッターを発生させる場合があるため、仮想 LAN（VLAN）を構成する必要があります。IPv6 が有効なデバイスでは、大量のブロードキャストパケットが発生する場合があります。IPv6 のサポートが不要な場合は、それらのデバイスで IPv6 を無効にできます。QoS（サービス品質）をサポートするように構成してください。

WAN 接続使用時の設定：
LAN および WAN 接続を経由したボイスチャットを使用できます。WAN 接続では、音質は接続の遅延、パケット損失、およびジッターにより異なります。WAN 接続を経由してソフトフォンを配信する場合、高い QoS（サービス品質）を保つため、データセンターとリモートオフィス間には Citrix SD-WAN を使用することをお勧めします。Citrix SD-WAN は、UDP を含むマルチストリーム ICA をサポートします。また、単一の TCP ストリームの場合は、さまざまな ICA 仮想チャネルの優先度を識別し、優先度の高いリアルタイムの音声データを優先的に扱うことができます。

直接ワークロード接続を使用すると、Gateway 経由の認証後に Citrix SD-WAN で UDP を使用したオーディオを暗号化できます。

HDX 構成を検証するには、Director またはHDX Monitorを使用してください。

リモートユーザーの接続：NetScaler Gateway 11 は DTLS をサポートし、UDP/RTP トラフィックをネイティブに（TCP でカプセル化せずに）送信します。
ポート 443 を介した UDP トラフィックに対してファイアウォールを双方向に開く必要があります。

コーデックの選択と帯域幅の消費：
ユーザーデバイスとデータセンターの Virtual Delivery Agent（VDA）間には、中品質オーディオとも呼ばれる、スピーチに最適化されたコーデック設定を使用することをお勧めします。VDA プラットフォームと IP-PBX 間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。次に例を示します：

- G711 はより優れた音質を提供するものの、通話あたり 80～100 キロビットの帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。
- G729 の音質は高く、通話あたり 30～40 キロビットの低帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。

ソフトフォンアプリケーションの仮想デスクトップへの配信

XenDesktop 仮想デスクトップにソフトフォンを配信するには、次の 2 つの方法があります。

- アプリケーションは、仮想デスクトップイメージにインストールできます。
- アプリケーションは、Microsoft App-V を使用して、仮想デスクトップにストリーム配信できます。このアプローチでは、仮想デスクトップイメージに手が加えられないため、管理上の利点があります。仮想デスクトップにストリーム配信された後、アプリケーションはその環境で、通常の方法でインストールされたかのように実行します。すべてのアプリケーションが App-V 互換であるわけではありません。

ユーザーデバイスとのオーディオの配信

汎用 HDX RealTime は、ユーザーデバイスとのオーディオの配信を次の 2 つの方法でサポートします。

- **Citrix** オーディオ仮想チャネル。オーディオ転送専用に設計されているため、通常は Citrix オーディオ仮想チャネルをお勧めします。
- 汎用 **USB** リダイレクト。ユーザーデバイスが XenApp または XenDesktop サーバーへの LAN または LAN のような接続上にある場合は、ボタンやディスプレイといったヒューマンインターフェイスデバイス（HID）を持つオーディオデバイスのサポートに有効です。

Citrix オーディオ仮想チャネル

双方向の Citrix オーディオ仮想チャネル（CTXCAM）は、ネットワーク上でオーディオを効率的に配信することができます。汎用 HDX RealTime は、ユーザーのヘッドセットまたはマイクからオーディオを取り出して圧縮し、ICA 経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力も圧縮され、ユーザーのヘッドセットまたはスピーカーに向けて反対方向に送信されます。この圧縮は、ソフトフォン自体で使われる圧縮（G.729、G.711 など）とは関係ありません。スピーチに最適化されたコーデック（中品質）で行われます。その特性はボイスオーバー IP（VoIP）に最適です。高速エンコード機能を備え、ピーク時でもおよそ 1 秒間に 56 キロビット（それぞれの方向で 28Kbps ずつ）しかネットワーク帯域幅を消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studio のコンソールで明示的に選択する必要があります。デフォルトは、HD オーディオコーデック（高品質）です。このコーデックは HiFi ステレオ録音には最適ですが、スピーチに最適化されたコーデックと比較してエンコードが遅くなります。

汎用 ***USB*** リダイレクト

Citrix 汎用 USB リダイレクトテクノロジ（CTXGUSB 仮想チャネル）は、複合デバイス（オーディオプラス HID）とアイソクロナス USB デバイスを含む、USB デバイスのリモート処理に一般的な手段を提供します。USB プロトコルはネットワークの遅延に影響を受けやすく、相当量のネットワーク帯域幅を必要とするため、このアプローチは LAN 接続のユーザーに制限されます。ソフトフォンによっては、アイソクロナス USB リダイレクトが有効です。このリダイレクトは優れた音質と少ない遅延を提供しますが、オーディオトラフィックに最適化されているため、Citrix オーディオ仮想チャネルが優先されます。主な例外は、データセンターに LAN 接続されているユーザーデバイスに取り付けられた USB 電話など、ボタンが付いたオーディオデバイスを使う場合です。この場合は、汎用 USB リダイレクトが、信号をソフトフォンに送ることで機能を制御する電話セットまたはヘッドセットのボタンをサポートします。これは、デバイス上でローカルに動作するボタンでの問題ではありません。

Web ブラウザーコンテンツのリダイレクト

August 24, 2021

Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート（ユーザーの Web ページの表示領域）のみがエンドポイントにリダイレクトされます。
ブラウザーコンテンツリダイレクトは、VDA のブラウザーのユーザーインターフェイス（アドレスバー、ツールバー

など）はリダイレクトしません。

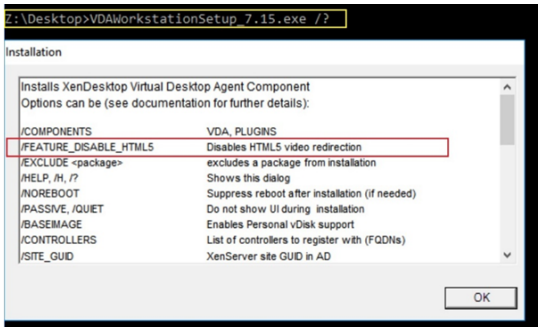
システム要件

これらの要件は、XenApp および XenDesktop 7.15 LTSR CU5 の BCR.msi に特化したものです。XenApp、XenDesktop のその他のバージョン、Citrix Virtual Apps and Desktops で使用されているブラウザーコンテンツリダイレクトのシステム要件は含まれません。

- Delivery Controller および VDA の両方にバージョン 7.15 LTSR CU5 以降。
- Windows 向け Citrix Workspace アプリ 1809 以降。
- Citrix Receiver for Linux 13.9.1 以降。
- BCR.msi - シトリックスのダウンロードページからダウンロードできます。
- Chrome（Web ブラウザーコンテンツのリダイレクト拡張機能を Chrome ウェブストアからインストール）または Internet Explorer 11（Browser Helper Object（BHO）の Citrix HDXJsInjector を有効化）。

インストール

1. コマンドライン「/FEATURE_DISABLE_HTML5」オプションを使用して、VDA にバージョン 7.15 LTSR CU5 をインストールまたはアップグレードします。



   このオプションは HTML5 ビデオリダイレクション機能を削除するため、BCR.msi の実行前に完了する必要があります。BCR.msi は、インストール中にこの機能を再度追加し、ブラウザーコンテンツリダイレクトサービスも追加します。この手順が完了したら、services.msc コンソールを開き、**Citrix HDX HTML5 Video Redirection Service** が表示されていないことを確認します。

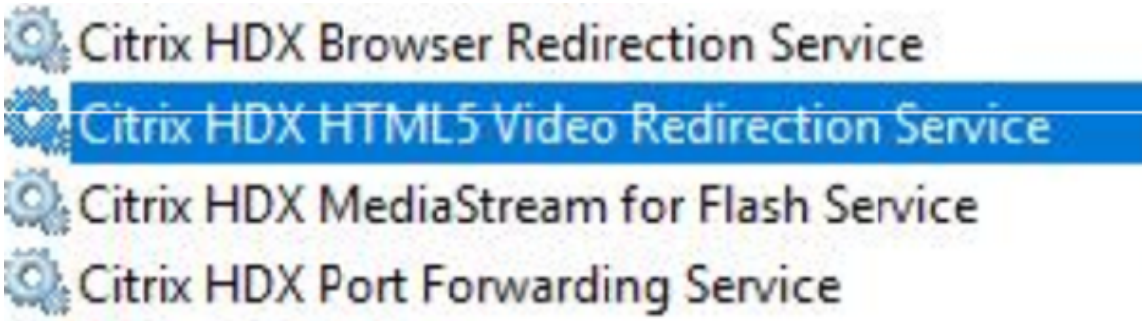
2. BCR.msi でブラウザーコンテンツリダイレクトサービスのインストールを開始します。システムに応じて、BCR.msi のファイルは次の場所にインストールされます:

   C:\Program Files\Citrix\ICAService

   または

   C:\Program Files (x86)\Citrix\ICAService

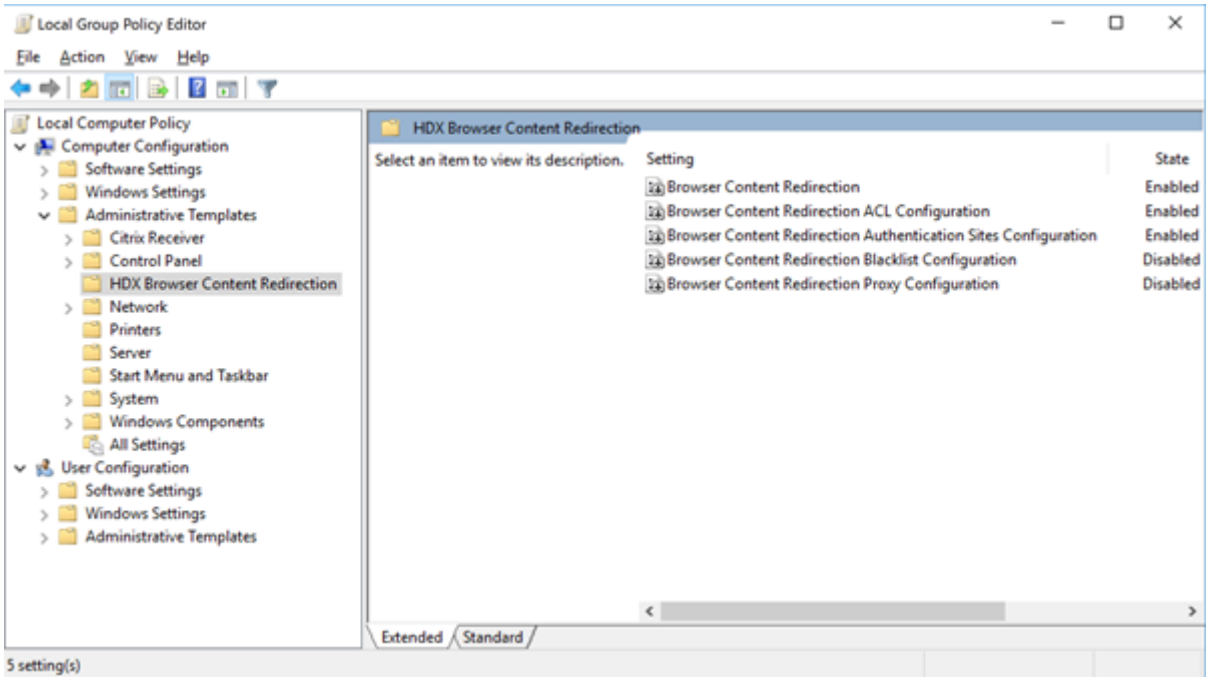
   インストールが高速であるため、ダイアログボックスがすぐに閉じることがあります。この場合、services.msc に戻ってサービスが追加されたことを確認します。



ポリシー

VDA で HKEY_LOCAL_MACHINE レジストリを使用して、またはグループポリシー管理コンソールで Citrix 管理テンプレートの **HDX Browser Content Redirection** を使用してポリシーを制御できます。

Citrix Virtual Apps and Desktops（XenApp および XenDesktop）、XenApp 7.15 LTSR または XenDesktop 7.15 LTSR、コンポーネント の順に移動し、citrix.comダウンロードページからテンプレートをダウンロードできます。Citrix Studio にはこれらのポリシーは含まれません。



ポリシー情報について詳しくは、「Web ブラウザーコンテンツのリダイレクトのポリシー設定」を参照してください。トラブルシューティングについて詳しくは、Knowledge Center のCTX230052を参照してください。

Flash リダイレクト

August 24, 2021

> 重要
>
> 2017 年 7 月 25 日、Adobe は Flash の製品終了（EOL）を発表しました。Flash Player のアップデートおよび配布は、2020 年末に停止される予定です。
>
> Microsoft は、Adobe の発表した終了日より前に Internet Explorer での Flash のサポートから撤退していくことを発表しました。2020 年末までに、Flash は Windows から削除されます。これによって、ユーザーは Internet Explorer で Flash を有効にしたり、実行したりすることができなくなります。
>
> シトリックスでは、Microsoft ポリシーに合わせて、2020 年末まで HDX Flash リダイレクトの保守およびサポートを継続します。Flash リダイレクトコードが除外される XenApp および XenDesktop のバージョンは決定していませんが、可能な限り速やかに HTML5 ビデオリダイレクションに切り替えることをお勧めします。HTML5 ビデオリダイレクションは、マルチメディアコンテンツの制御に最適です。例えば、企業のコミュニケーションビデオ、トレーニングビデオ、またはサードパーティがコンテンツをホストする時などに使用できます。
>
> HTML5 ビデオリダイレクションについて詳しくは、「HTML5 マルチメディアリダイレクト」を参照してください。

Flash リダイレクト機能を有効にすると、ほとんどの Adobe Flash コンテンツ（アニメーション、ビデオ、アプリケーションなど）が LAN または WAN で接続されたユーザー側の Windows デバイスおよび 32 ビット Linux x86 デバイス上で処理（レンダリング）され、サーバーリソースおよびネットワークの負荷が軽減されます。これにより、スケーラビリティおよびユーザーエクスペリエンスが向上します。Flash リダイレクトを構成するには、サーバー側およびクライアント側の設定が必要です。

> 注意：
>
> Flash リダイレクトでは、ユーザーデバイスとサーバー間で頻繁な相互通信が行われます。ユーザーデバイスとサーバー間でセキュリティ境界による分離が不要な環境でのみ、この機能を使用してください。また、ユーザーデバイスでは、信頼するサーバーでのみこの機能を使用するように設定する必要があります。Flash リダイレクトを使用するにはユーザーデバイス上に Adobe Flash Player をインストールする必要があるため、ユーザーデバイス上の Flash Player の安全性が確認されている場合にのみ Flash リダイレクトを有効にしてください。

Flash リダイレクトは、クライアント側およびサーバー側でサポートされます。クライアント側で第 2 世代の Flash リダイレクトがサポートされる場合、Flash コンテンツはクライアント側でレンダリングされます。Flash リダイレクト機能では、以下で説明する WAN 接続、インテリジェントフォールバック、URL 互換性リストがサポートされます。

Flash リダイレクトは、サーバー上の Windows イベントログを使用して Flash イベントのログを記録します。このイベントログには、Flash リダイレクトが使用されたかどうか、および問題に関する詳細が記録されます。Flash リダイレクトのすべてのイベントで、以下の共通の情報が記録されます：

- Flash リダイレクトのイベントは、アプリケーションログに記録されます。
- Windows 10、Windows 8 および Windows 7 が動作するコンピューターでは、Flash リダイレクトのログは［アプリケーションとサービスログ］ノードに記録されます。
- ソースには「Flash」と記録されます。

- 分類には「なし」と記録されます。

HDX Flash の互換性に関する最新の更新については、CTX136588を参照してください。

サーバー側での **Flash** リダイレクトの構成

サーバー側で Flash リダイレクト機能を構成するには、Citrix ポリシーで以下の設定項目を使用します。詳しくは、「Flash リダイレクトのポリシー設定」を参照してください。

- デフォルトでは、Flash リダイレクトは有効になっています。特定の Web ページの Flash コンテンツでこのデフォルト設定を上書きするには、［Flash URL 互換性リスト］設定を使用します。
- ［Flash インテリジェントフォールバック］設定により、小さい Flash ムービー（広告で使用されるものなど）が検出され、それらがユーザーデバイスではなくサーバー側でレンダリングされます。この最適化を使用しても、Web ページや Flash アプリケーションのロード時に中断や障害は発生しませんデフォルトでは、Flash インテリジェントフォールバックは有効になっています。サイズにかかわらずすべての Flash コンテンツがユーザーデバイス側でレンダリングされるようにするには、この設定項目を無効にします。一部の Flash コンテンツが正常にリダイレクトされない場合がある点に注意してください。
- ［Flash サーバー側コンテンツフェッチ URL 一覧］設定を使用すると、特定の Web サイトの Flash コンテンツがいったんサーバー上にダウンロードされ、それがユーザーデバイスに転送されてレンダリングされるようになります。（Flash リダイレクトのデフォルトでは、Flash コンテンツがクライアント側フェッチでユーザーデバイス上に直接ダウンロードされます）。Flash リダイレクトのデフォルトでは、Flash コンテンツがユーザーデバイス上にダウンロードされ、そこでレンダリングされます。この設定項目を使用する場合はユーザーデバイス側の［サーバー側のコンテンツの取得を有効にする］設定が必要で、イントラネット上の内部用 Flash アプリケーションで使用されます。詳しくは、後述の説明を参照してください。この機能はほとんどのインターネットサイトでも動作するため、ユーザーデバイスが直接インターネットに接続できない環境（XenApp/XenDesktop サーバー経由でインターネットに接続している場合など）で使用できます。
  注：サーバー側コンテンツのフェッチ機能は、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。

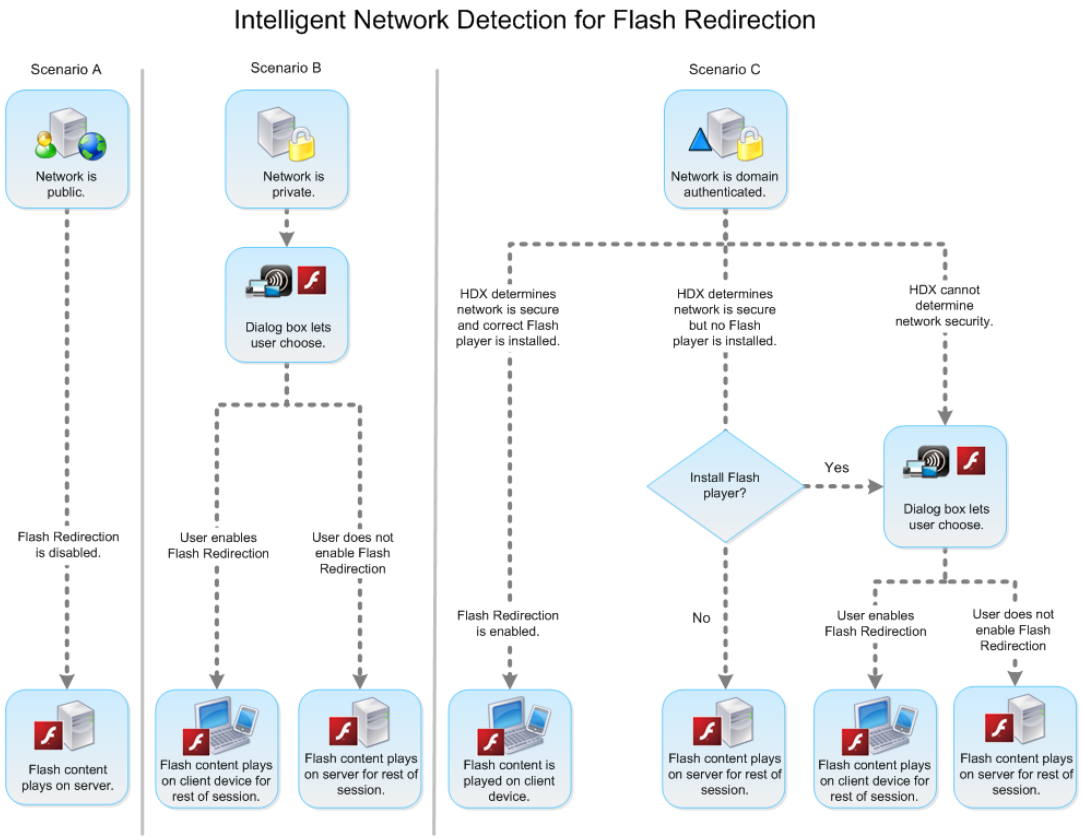
Flash リダイレクトの動作を変更する：

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）。

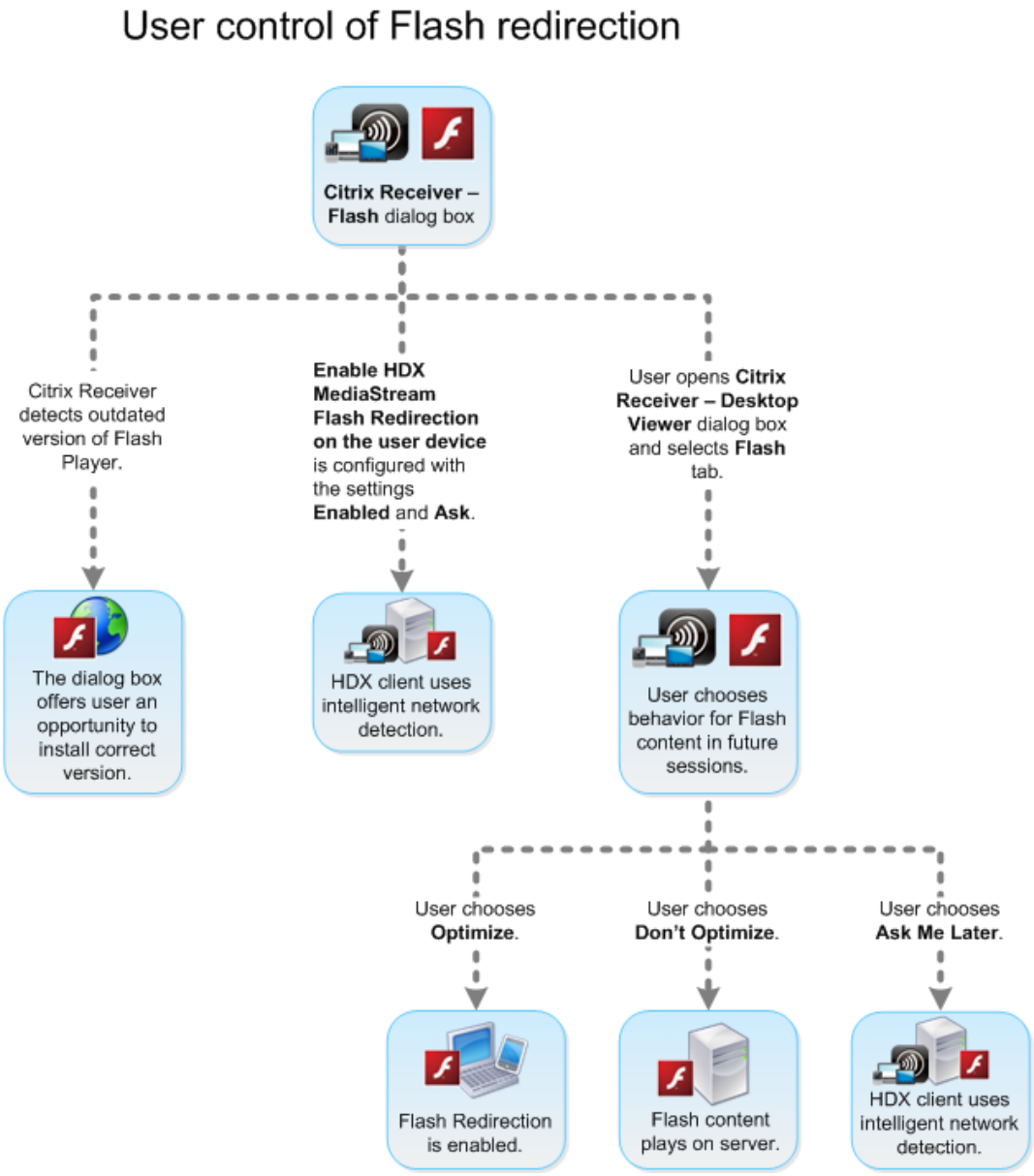
ポリシー設定が未構成である場合、Desktop Lock 環境ではデフォルトで Flash リダイレクトが有効になります。

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 世代のみ有効］を選択します。これにより、要件が満たされる場合は Flash コンテンツがユーザーデバイス側で処理され、満たされない場合はサーバー側で処理されます。
    - 常に Flash リダイレクトを行うには、［常に有効］を選択します。これにより、Flash コンテンツが常にユーザーデバイス側で処理されます。
    - Flash リダイレクトを無効にするには、［常に無効］を選択します。これにより、Flash コンテンツが常にサーバー側で処理されます。
    - クライアント側のネットワークのセキュリティレベルを検出して Flash リダイレクトの使用を決定するには、［確認］（デフォルト）を選択します。ネットワークのセキュリティレベルを検出できない場合は、Flash リダイレクト機能を使用するかどうかを確認するメッセージがユーザーに表示されます。ネットワークのセキュリティレベルを検出できない場合は、Flash リダイレクト機能を使用するかどうかを確認するメッセージがユーザーに表示されます。
      次の図は、さまざまなネットワークで Flash リダイレクトがどのように処理されるかを示しています。



インテリジェントネットワーク検出機能は、ユーザー側で有効または無効にすることができます。これを行うには、［Citrix Receiver - Desktop Viewer 基本設定］ダイアログボックスの［Flash］タブで、［最適化する］または［最適化しない］を選択します。ここに表示されるオプションは、次の図のように、ユーザーデバイスでの Flash リダイレクトの構成により異なります。



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。

サーバー側コンテンツのフェッチを有効にする:

Flash リダイレクトのデフォルトでは、Adobe Flash コンテンツがユーザーデバイス上に直接ダウンロードされ、そこで処理されます。サーバー側コンテンツのフェッチを有効にすると、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、サーバー側コンテンツのフェッチは、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:
>
> サーバー側コンテンツのフェッチ機能は、RTMP（Real Time Messaging Protocol）を使用した Flash アプリケーションをサポートしません。このようなサイトは、サーバー側で処理されます。

Flash リダイレクトでは、サーバー側コンテンツのフェッチを有効にする 3 つのオプションがサポートされています。これらの中には、サーバー側で取得したコンテンツをユーザーデバイス上にキャッシュするためのものが含まれています。これにより、再使用されるコンテンツがユーザーデバイス上にキャッシュされるため、パフォーマンスが向上します。このキャッシュコンテンツは、ユーザーデバイス上でキャッシュされるほかの HTTP コンテンツとは別に保存されます。

いずれかの有効オプションが選択されている場合に、クライアント側での SWF ファイル取得に失敗すると自動的にサーバー側コンテンツ取得にフォールバックされます。

サーバー側コンテンツのフェッチを有効にするには、クライアントデバイス側およびサーバー側での設定が必要です。

1. [設定] の一覧で、[サーバー側のコンテンツの取得を有効にする] を選択して [ポリシー設定] をクリックします。
2. [未構成]、[有効]、または [無効]（デフォルト）を選択します。[有効] を選択する場合は、[サーバー側のコンテンツの取得の状態] 一覧で以下のいずれかのオプションを選択します。

オプション	説明
無効	サーバー側でのコンテンツ取得を無効にします。サーバー上の [Flash サーバー側でのコンテンツ取得 URL リスト] 設定は無視されます。サーバー側でのコンテンツ取得へのフォールバックも無効になります。
有効	[Flash サーバー側コンテンツフェッチ URL 一覧] 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コンテンツのフェッチを有効にします。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。

オプション	説明
有効（永続キャッシュ）	[Flash サーバー側コンテンツフェッチ URL 一覧］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コンテンツのフェッチを有効にします。サーバー側コンテンツのフェッチ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 サーバー側コンテンツフェッチ URL 一覧］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コンテンツのフェッチを有効にします。サーバー側コンテンツのフェッチ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** サーバーにリダイレクトする:

Flash コンテンツの取得をリダイレクトするには、第 2 世代の Flash リダイレクト機能である URL［クライアント側のコンテンツの取得の URL 書き換え規則］設定を使用します。この機能を構成する場合、2 つの URL のパターンを指定します。ユーザーデバイスが最初のパターン（「一致パターン」）と一致する Web サイトからコンテンツを取得しようとすると、2 つ目のパターン（「置換パターン」）により指定された Web サイトにリダイレクトされます。

この設定を使って、コンテンツ配信ネットワーク（CDN）の機能を補うことができます。Flash コンテンツを配信する一部の Web サイトでは、ユーザーからのコンテンツ要求が、そのユーザーに最も近い Web サイトにリダイレクトされます。これを、「CDN リダイレクト」と呼びます。Flash リダイレクトによるクライ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。［未構成］がデフォルトで選択されています。［無効］を選択すると、次の手順で指定する URL 書き換え規則がすべて無視されます。
3. この設定を有効にした場合は、［表示］をクリックします。Perl 正規表現構文を使って［値の名前］ボックスに一致パターンを入力し、［値］ボックスに置換パターンを入力します。

Flash リダイレクトの最小バージョンチェック

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

Citrix Receiver for Windows または Citrix Receiver for Linux を使って VDA にアクセスするクライアントデバイスに対する Flash リダイレクトに必要な最小バージョンを指定するためのレジストリ設定を追加できます。このセキュリティ機能により、古い Flash バージョンが使用されないことが保証されます。

ServerFlashPlayerVersionMinimum は、ICA サーバー（VDA）上で必要な Flash Player の最小バージョンを指定する文字列値です。

ClientFlashPlayerVersionMinimum は、ICA クライアント（Citrix Receiver）上で必要な Flash Player の最小バージョンを指定する文字列値です。

これらのバージョン文字列は、「10」、「10.2」、または「10.2.140」のように指定できます。メジャーおよびマイナーのビルド番号のみ比較されます。レビジョン番号は無視されます。たとえば、メジャー番号のみ「10」と指定されたバージョン文字列の場合、マイナーおよびビルド番号は 0 であるという前提になります。

FlashPlayerVersionComparisonMask は、DWORD 値です。0 と設定すると、ICA サーバー上の Flash Player に対する ICA クライアント上の Flash Player のバージョンの比較が無効になります。比較マスクにはほかの値がありますが、0 以外のマスクの意味は変わることがあるため、それらを使用するべきではありません。必要なクライアント対して比較マスクを 0 に設定することをお勧めします。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、クライアントとサーバーの最小チェックも正常に完了する必要があります。

サブキー ClientID0x51 は Citrix Receiver for Linux を指定します。サブキー ClientID0x1 は Citrix Receiver for Windows を指定します。このサブキーには、文字列”ClientID” に 16 進数のクライアント製品 ID（0 で始まるものがない）を付けて名前が付けられます。

32 ビット **VDA** のレジストリ構成例:

[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\HdxMedi
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\Clien
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）“ClientFlashPlayerVersion-Minimum”=”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

“ClientFlashPlayerVersionMinimum”=”16.0.0”[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMed

“FlashPlayerVersionComparisonMask”=dword:00000000 “ClientFlashPlayerVersionMinimum”=”11.2.0”

HTML5 マルチメディアリダイレクション

August 24, 2021

HTML5 マルチメディアリダイレクションは、HDX MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 のオーディオとビデオを含むようにしたものです。マルチメディアコンテンツのオンライン配信の拡大、特にモバイルデバイスへの拡大により、ブラウザー業界はオーディオやビデオを再生するより効率的な方法を開発してきました。

Flash が標準となりましたが、Flash はプラグインが必要で、すべてのデバイスで稼働するわけではなく、また、モバイルデバイスでは大量のバッテリーを消費します。Youtube、NetFlix.com などの企業や Mozilla、Google、Microsoft のブラウザーの新バージョンは HTML5 に移行しており、これが新しい標準になっています。

HTML5 ベースのマルチメディアには、専用プラグインを超える以下のような多数の利点があります：

- 企業非依存型の標準（W3C）
- 簡素化されたデジタル著作権管理（DRM）ワークフロー
- プラグインが原因のセキュリティの問題がないことによる優れたパフォーマンス

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする、HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、（単一品質でエンコードされた）1 つのファイルが HTTP Web サーバーからダウンロードされている間に、ブラウザーがそれを再生します。ビデオは、受け取られるとハードドライブに保存され、ハードドライブから再生されます。ビデオを再度視聴する場合、ブラウザーがキャッシュからビデオをロードします。

プログレッシブダウンロードの例については、「HTML5 ビデオリダイレクションのテストページ」を参照してください。使用するブラウザーの開発者ツールを使用して、Web ページ内のビデオエレメントを調べ、以下のような HTML5 ビデオタグ内のソース（MP4 コンテナフォーマット）を探します：


```
<video src="https://www.citrix.com/content/dam/citrix61/en_us/images/
offsite/html5-redirect.mp4"controls=""style="width:800px;"></video>
```

HTML5 と Flash の比較

機能	HTML5	Flash
専用のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
異なるプラットフォームでの実行速度	High	低速
iOS でサポート	はい	いいえ
リソース使用率	低い	高い
より高速なロード	はい	いいえ

要件

MP4 フォーマットでのプログレッシブダウンロードのリダイレクトのみがサポートされます。WebM、および DASH/HLS などのアダプティブビットレートストリーミングのテクノロジはサポートされません。

サポート対象:

- サーバー側でレンダリング
- サーバー側でフェッチし、クライアント側でレンダリング
- クライアント側でフェッチしレンダリング

これらはポリシーを使って制御されます。詳しくは、「マルチメディアのポリシー設定」を参照してください。

Citrix Receiver の最小バージョン:

- Citrix Receiver for Windows 4.5
- Citrix Receiver for Linux 13.5

最小の VDA ブラウザーバージョンと Windows OS のバージョン/ビルド/SP:

- **Internet Explorer 11.0**
  - Windows 10 x86（1607 RS1）および x64（1607 RS1）
  - Windows 7 x86 および x64
  - Windows Server 2016 RTM 14393（1607）
  - Windows Server 2012 R2
  - Windows Server 2008 R2

- **Firefox 47**。Firefox 証明書ストアに証明書を手動で追加するか、Windows の信頼された機関からの証明書ストアで証明書を探すように Firefox を構成します。詳しくは、「https://wiki.mozilla.org/CA:AddRootToFirefox」を参照してください。
  - Windows 10 x86（1607 RS1）および x64（1607 RS1）
  - Windows 7 x86 および x64
  - Windows Server 2016 RTM 14393（1607）
  - Windows Server 2012 R2
  - Windows Server 2008 R2
- **Chrome 51**
  - Windows 10 x86（1607 RS1）および x64（1607 RS1）
  - Windows 7 x86 および x64
  - Windows Server 2016 RTM 14393（1607）
  - Windows Server 2012 R2
  - Windows Server 2008 R2

HTML5 ビデオリダイレクションソリューションのコンポーネント

- **HdxVideo.js** - Web サイト上のビデオコマンドを傍受する JavaScript フック。HdxVideo.js は、セキュア WebSocket（SSL/TLS）を使用して WebSocketService と通信します。
- **WebSocket SSL** 証明書
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp/XenDesktop Engineering、CN = Citrix XenApp/XenDesktop HDX In-Product CA）
    場所：［証明書 - ローカルコンピューター］>［信頼されたルート証明機関］>［証明書］
  - エンドエンティティ（リーフ）の場合：**Citrix XenApp/XenDesktop HDX Service**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp/XenDesktop Engineering、CN = Citrix XenApp/XenDesktop HDX Service）
    場所：［証明書 - ローカルコンピューター］>［個人］>［証明書］
- **WebSocketService.exe** - ローカルシステムで稼働し、SSL の終了とユーザーセッションマッピングを実行します。127.0.0.1 ポート 9001 でリッスンする TLS Secure WebSocket です。
- **WebSocketAgent.exe** - ユーザーセッションで稼働し、WebSocketService コマンドの指示に従ってビデオをレンダリングします。

HTML5 ビデオリダイレクションを有効にするには

このリリースでは、この機能は管理対象 Web ページでのみ利用できます。HTML5 マルチメディアコンテンツが利用可能な Web ページに HdxVideo.js JavaScript（XenDesktop および XenApp のインストールメディアに含まれています）を追加する必要があります。たとえば、社内研修サイトのビデオなどです。

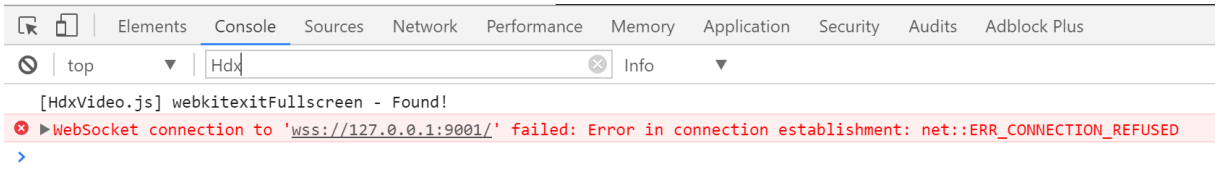
youtube.com のようにアダプティブビットレート技術（HTTP ライブストリーミング（HLS）、Dynamic Adaptive

Streaming over HTTP（DASH）など）をベースにした Web サイトは、サポートされていません。

詳しくは、「マルチメディアのポリシー設定」を参照してください。

トラブルシューティングのヒント

Web ページで HdxVideo.js を実行しようとすると、エラーが発生する場合があります。JavaScript が読み込みに失敗した場合、HTML5 リダイレクションメカニズムはエラーになります。使用するブラウザーの開発者ツールウィンドウでコンソールを調べて、HdxVideo.js に関連するエラーがないことを確認してください。例:



Windows Media リダイレクト

August 24, 2021

Windows Media リダイレクトは、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。サーバーではなくクライアントデバイスでメディアランタイムファイルを再生することで、Windows Media リダイレクトはマルチメディアファイルの再生に必要な帯域幅を減少させます。Windows Media リダイレクトは、仮想 Windows デスクトップで実行中の Windows Media Player および互換プレーヤーのパフォーマンスを向上させます。

Windows メディアのクライアント側でのコンテンツ取得の要件が満たされない場合、メディア配信は自動的にサーバー側での取得を使用します。その方法はユーザーにとって透過的です。XenDesktop Collector を使用して、HostMMTransport.dll から Citrix Diagnosis Facility（CDF）トレースを実行すると、その使用方法を決定できます。

Windows Media リダイレクトは、ホストサーバーでのメディアパイプラインをインターセプトし、ネイティブの圧縮フォーマットでメディアデータをキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスはパイプラインを再作成し、ホストサーバーから受信したメディアデータの展開およびレンダリングを行います。Windows Media リダイレクトは Windows オペレーティングシステムを実行中のクライアントデバイスで正しく動作します。これらのデバイスは、ホストサーバーに存在したパイプラインを再構築するために必要なマルチメディアフレームワークを備えています。Linux クライアントは、メディアパイプラインを再構築するために、同様のオープンソースメディアフレームワークを使用します。

[**Windows Media** リダイレクト］ポリシー設定で、この機能を制御します。デフォルトは ［許可］です。この設定は、通常、セッション内で再生されるオーディオおよびビデオの品質が向上して、クライアントデバイス上のファイルを再生しているときの品質に近くなります。まれに、Windows Media リダイレクトによるメディアの再生品質

が、基本的な ICA 圧縮および通常のオーディオ機能での品質よりも悪い場合があります。その場合は、[**Windows Media** リダイレクト] 設定をポリシーに追加し、その値を [禁止] にすることで、機能を無効にできます。

ポリシーの設定について詳しくは、「マルチメディアのポリシー設定」を参照してください。

一般コンテンツリダイレクト

April 29, 2019

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれを Windows デスクトップデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト

一般的ではないユースケースでの、ホストからクライアントへのリダイレクト機能の使用を検討します。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。この種類のリダイレクト機能は、サーバー OS の VDA でのみサポートされ、デスクトップ OS の VDA ではサポートされません。

ローカルアプリアクセスと **URL** リダイレクト

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。

USB とクライアント側ドライブの考慮事項

HDX テクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なときに汎用 **USB** リダイレクトを提供します。

関連情報

- クライアントフォルダーのリダイレクト
- ホストからクライアントへのリダイレクト
- ローカルアプリアクセスと URL リダイレクト
- USB とクライアント側ドライブの考慮事項
- マルチメディア

クライアントフォルダーのリダイレクト

February 3, 2020

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、シトリックス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。
    a) キー（HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection）を作成します。
    b) REG_DWORD 値を作成します。
        - 値の名前：CFROnlyModeAvailable
        - 種類：REG_DWORD
        - データ：「1」に設定します。
2. ユーザーデバイス側で以下を行います。
    a) 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。
    b) 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。
    c)［カスタム］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。
    d) 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。

ホストからクライアントへのリダイレクト

August 24, 2021

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

ホストからクライアントへのリダイレクトは、コンテンツのリダイレクト機能の一種です。この機能は、サーバー OS の VDA でのみサポートされ、デスクトップ OS の VDA ではサポートされません。

- ホストからクライアントへのリダイレクト機能を有効にすると、URL はサーバー VDA でインターセプトされてからユーザーデバイスに送信されます。これらの URL は、ユーザーデバイス上の Web ブラウザーまたはマルチメディアプレーヤーで開かれます。
- ホストからクライアントへのリダイレクト機能を有効にしても、ユーザーのデバイスから URL に接続できない場合は、その URL がサーバー VDA に戻されます。
- ホストからクライアントへのリダイレクト機能が無効な場合、URL はサーバー VDA 上の Web ブラウザーまたはマルチメディアプレーヤーで開きます。
- ホストからクライアントへのリダイレクト機能を有効な場合、ユーザーがこの機能を無効にすることはできません。

ホストからクライアントへのリダイレクトは、以前はサーバーからクライアントへのリダイレクトと呼ばれていました。

ホストからクライアントへのリダイレクト機能の使用に適した状況

一般的ではない特定の状況では、パフォーマンス、互換性、コンプライアンスなどの理由から、ホストからクライアントへのリダイレクト機能の使用が必要となることがあります。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。

パフォーマンス:

ホストからクライアントへのリダイレクト機能を使用すると、ユーザーデバイスにアプリケーションがインストールされていれば、VDA 上のアプリケーションではなくこのアプリケーションを使用することができ、パフォーマンスを改善できます。

ただし、VDA では Adobe Flash などのマルチメディアコンテンツは既に最適化されているため、ホストからクライアントへのリダイレクト機能によりパフォーマンスが改善されるのは特定の状況に限られます。まず、ホストからクライアントへのリダイレクト機能ではなく、以下の表に示した他のアプローチ（ポリシー設定）を使用することを検討してください。これらの設定は柔軟性が高く、特に低性能のユーザーデバイスでは、一般的にユーザーエクスペリエンスも向上します。

互換性:

以下の場合、ホストからクライアントへのリダイレクト機能を使用して互換性を確保できます。

- HTML およびマルチメディア以外のコンテンツタイプを使用する場合（例：カスタム URL タイプ）
- VDA のマルチメディアプレーヤーのマルチメディアリダイレクト機能ではサポートされていない旧式のメディア形式を使用する場合（Real Media など）
- 特定のコンテンツタイプのアプリケーションを使用するユーザーがごく少数であり、それらのユーザーがこのアプリケーションを各ユーザーデバイスにインストール済みの場合
- VDA では特定の Web サイトにアクセスできない場合（例：内部 Web サイトから別組織の Web サイトへのアクセス）

コンプライアンス：

以下の場合、ホストからクライアントへのリダイレクト機能を使用してコンプライアンスを確保できます。

- アプリケーションまたはコンテンツのライセンス契約により VDA 経由の公開が許可されていない場合
- 組織のポリシーにより VDA へのドキュメントのアップロードが許可されていない場合

一部の状況は、環境が複雑な場合や、ユーザーデバイスと VDA を所有する組織が異なる場合に起こりやすくなります。

ユーザーデバイスに関する考慮事項

環境によっては、さまざまな種類のユーザーデバイスが存在する場合があります。

ユーザーデバイス	状況または環境	コンテンツのリダイレクトのアプローチ
タブレット	-	次表のすべての機能
ラップトップ PC	-	次表のすべての機能
デスクトップ PC	ユーザーがユーザーデバイスにインストール済みの多様なアプリケーションを使用する場合	次表のすべての機能
デスクトップ PC	ユーザーが使用するのが、ユーザーデバイスにインストール済みである少数かつ既知のアプリケーションに限られている場合	ローカルアプリアクセス
デスクトップ PC	ユーザーがユーザーデバイスにインストール済みのアプリケーションを使用しない場合	マルチメディアリダイレクトまたは Flash リダイレクト
デスクトップアプライアンス	ベンダーがマルチメディアリダイレクトまたは Flash リダイレクトをサポートしている場合	マルチメディアリダイレクトまたは Flash リダイレクト

ユーザーデバイス	状況または環境	コンテンツのリダイレクトのアプローチ
シンクライアント	ベンダーがマルチメディアリダイレクト、Flash リダイレクト、ホストからクライアントへのリダイレクトをサポートしている場合	次表のすべての機能
ゼロクライアント	ベンダーがマルチメディアリダイレクトまたは Flash リダイレクトをサポートしている場合	マルチメディアリダイレクトまたは Flash リダイレクト

使用するコンテンツリダイレクト機能を決める際は、次の例を参考にしてください。

URL リンク	状況または環境	コンテンツのリダイレクトのアプローチ
Web ページまたはドキュメント	VDA が URL にアクセスできない場合	ホストからクライアントへのリダイレクト
Web ページ	Web ページに Adobe Flash が含まれる場合	Flash リダイレクト
マルチメディアファイルまたはストリーム	互換性のあるマルチメディアプレーヤーが VDA にインストールされている場合	マルチメディアリダイレクト
マルチメディアファイルまたはストリーム	互換性のあるマルチメディアプレーヤーが VDA にインストールされていない場合	ホストからクライアントへのリダイレクト
ドキュメント	VDA に当該種類のドキュメント用のアプリケーションがインストールされていない場合	ホストからクライアントへのリダイレクト
ドキュメント	ユーザーデバイスへのドキュメントのダウンロードが禁止されている場合	リダイレクト不可
ドキュメント	VDA へのドキュメントのアップロードが禁止されている場合	ホストからクライアントへのリダイレクト
カスタムの URL タイプ	VDA にカスタム URL タイプ用のアプリケーションがインストールされていない場合	ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクト機能は、Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux、Citrix Receiver for HTML5、Citrix Receiver for Chrome でサポートされています。

ホストからクライアントへのリダイレクト機能を使用するには、ユーザーデバイスに Web ブラウザー、マルチメディアプレーヤー、またはコンテンツに対応したその他のアプリケーションをインストールする必要があります。ユーザーデバイスがデスクトップアライアンス、シンクライアント、またはゼロクライアントである場合、適切なアプリケーションがインストールされていること、および性能が十分であることを確認してください。

ローカルアプリケーションアクセスを有効にしたユーザーデバイスでは別のコンテンツリダイレクトメカニズムが使用されるため、ホストからクライアントへのリダイレクト機能は必要ありません。

Citrix の各種ポリシーを使用して、不適切なデバイスについてホストからクライアントへのコンテンツリダイレクト機能を禁止できます。

ホストからクライアントへのリダイレクト機能が使用される状況

ホストからクライアントへのリダイレクト機能は、URL が以下の場合に使用されます。

- アプリケーションにハイパーリンクとして埋め込まれている場合（電子メールメッセージやドキュメントなど）
- VDA アプリケーションのメニューまたはダイアログボックスから選択された場合（アプリケーションで Windows ShellExecuteEx API が使用されているとき）
- Windows の［ファイル名を指して実行］ダイアログボックスに入力された場合

Web ブラウザー内の URL（Web ページの URL 内および Web ブラウザーのアドレスバーに入力された URL のどちらでも）に対しては、ホストからクライアントへのリダイレクト機能は使用されません。

> 注
>
> ユーザーが（[規定のプログラムを設定する］などを使用して）VDA 上のデフォルトの Web ブラウザーを変更した場合、この変更によりアプリケーションのホストからクライアントへのリダイレクト機能が影響を受ける可能性があります。

ホストからクライアントへのリダイレクト機能が有効な場合、URL を開くアプリケーションは、URL の種類とコンテンツの種類の両方に関するユーザーデバイスの設定で決まります。例:

- コンテンツタイプが HTML である HTTP URL は、デフォルトの Web ブラウザーで開かれます。
- コンテンツタイプが PDF である HTTP URL は、デフォルトの Web ブラウザーまたは別のアプリケーションのどちらかで開かれます。

ユーザーデバイスの設定は、ホストからクライアントへのコンテンツリダイレクト機能では制御できません。ユーザーデバイスの設定を制御しない場合は、ホストからクライアントへのコンテンツリダイレクト機能ではなく、Flash リダイレクトおよびマルチメディアリダイレクトを使用してください。

ホストからクライアントへのリダイレクト機能が有効な場合、次の種類の URL はユーザーデバイスでローカルに開かれます。

- HTTP（Hypertext Transfer Protocol）

- HTTPS（Secure Hypertext Transfer Protocol）
- RTSP（RealPlayer および QuickTime）
- RTSPU（RealPlayer および QuickTime）
- PNM（従来の RealPlayer）
- MMS（Microsoft Media Server）

ホストからクライアントへのリダイレクト機能の URL タイプのリストを変更して、カスタム URL タイプなどの URL タイプを削除および追加できます。

ホストからクライアントへのリダイレクト機能の有効化

ホストからクライアントへのリダイレクト機能を有効にするには、まず Citrix ポリシー設定を有効にします。

ホストからクライアントへのリダイレクトポリシーの設定については、「ファイルリダイレクトのポリシー設定」に記載されています。デフォルトでは、この設定は無効になっています。

さらに、VDA の OS によっては、サーバー VDA のレジストリキーとグループポリシーの設定も必要になります。

- サーバー VDA が Windows Server 2008 R2 SP1 である場合、レジストリキーとグループポリシーを設定する必要はありません。
- サーバー VDA が Windows Server 2012、Windows Server 2012 R2、または Windows Server 2016 である場合、レジストリキーとグループポリシーの設定が必要になります。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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。

レジストリの変更

1. 以下の「**Reg file start**」と「**Reg file end**」の間にあるテキストをコピーして、メモ帳に貼り付けます。
2. ［名前を付けて保存］で［ファイルの種類］を ［すべてのファイル］、［ファイル名］を「**ServerFTA.reg**」に指定して、メモ帳ファイルを保存します。
3. Active Directory のグループポリシーを使用して、**ServerFTA.reg** ファイルをサーバーに配布します。

```
--  Reg file start --

Windows Registry Editor Version 5.00


[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]
```



```
7
8  @="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"
9
10
11 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]
12
13 @="ServerFTA"
14
15
16 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]
17
18 "ApplicationDescription"="Server FTA URL."
19
20 "ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.
      exe,0"
21
22 "ApplicationName"="ServerFTA"
23
24
25
26 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\
      URLAssociations]
27
28 "http"="ServerFTAHTML"
29
30 "https"="ServerFTAHTML"
31
32
33
34 [HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]
35
36 "Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"
37
38 -- Reg file end -- ---
```

グループポリシーの変更

XML ファイルを作成します。この XML ファイルに、以下の「**xml file start**」と「**xml file end**」の間にあるテキストをコピーして貼り付け、「**ServerFTAdefaultPolicy.xml**」という名前で保存します。

```
1  -- xml file start --
2
```



```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>

-- xml file end -- ---
```

現在のグループポリシー管理コンソールで、［コンピューターの構成］>［管理用テンプレート］>［**Windows** コンポーネント］>［エクスプローラー］>［既定の関連付け構成ファイルの設定］の順に開いて、作成した ServerFTAdefaultPolicy.xml ファイルを指定します。

ホストからクライアントへのリダイレクト機能の **URL** タイプリストの変更

ホストからクライアントへのリダイレクト機能の URL タイプのリストを変更するには、サーバー VDA で次のレジストリキーを設定します。

キー: HKLM\Software\Wow6432Node\Citrix\SFTA

リストから URL タイプを削除するには、DisableServerFTA と NoRedirectClasses を設定します。

値の名前：DisableServerFTA

種類：REG_DWORD

データ：1

名前：NoRedirectClasses
種類：REG_MULTI_SZ
データ：http、https、rtsp、rtspu、pnm、mms のいずれかの組み合わせを指定します。1 つの行に 1 つの値を入力してください。例:

http

https

rtsp

リストに URL タイプを追加するには、ExtraURLProtocols を設定します。

値の名前：ExtraURLProtocols

種類：REG_MULTI_SZ

データ：URL タイプの組み合わせを指定します。各 URL タイプにはサフィックスとして「://」を追加し、複数の値はセミコロンで区切って入力します。例：

customtype1://;customtype2://

特定の **Web** サイトのセットについてホストからクライアントへのリダイレクト機能を有効にする

特定の Web サイトのセットについてホストからクライアントへのリダイレクト機能を有効にするには、サーバー VDA で次のレジストリキーを設定します。

キー: HKLM\Software\Wow6432Node\Citrix\SFTA

値の名前：ValidSites

種類：REG_MULTI_SZ

データ：FQDN（完全修飾ドメイン名：Fully-Qualified Domain Name）の組み合わせを指定します。1 つの行に 1 つの FQDN を入力してください。FQDN には、左端にのみワイルドカードを含めることができます。ワイルドカードを含む FQDN は単一レベルのドメインと照合されます。これは RFC 6125 の規則に準拠しています。例：

```
www.example.com
```

```
*.example.com
```

ローカルアプリアクセスと **URL** リダイレクト

August 24, 2021

はじめに

ローカルアプリ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 でローカルアプリアクセスが有効な場合、URL リダイレクトにより、ホストされるデスクトップセッションからローカルアクセスアプリケーションを起動できます。URL リダイレクトでは、複数の URL アドレスでアプリケーションを起動できます。デスクトップセッションで、Web ブラウザー内に埋め込まれたリンクをクリックすると、Web ブラウザーの URL ブラックリストに基づいてローカルの Web ブラウザーが起動します。ブラックリストにない URL をクリックすると、デスクトップセッション内の Web ブラウザーが再度使用されます。

URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できるリダイレクト機能は、サーバー FTA（File Type Association：ファイルタイプの割り当て）リダイレクトの 1 つである「ホストからクライアントへのコンテンツのリダイレクト」のみです。この FTA では、http、http、rtsp、mms など、特定のプロトコルがクライアント側に転送されます。たとえば、http の埋め込みリンクを開くときに、クライアント側のアプリケーションが使用されます。特定の URL のリダイレクトを有効にしたり無効にしたりすることはできません。

ローカルアプリ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、「ローカルアプリアクセスのポリシー設定」を参照してください。

すべての URL を VDA 側の Web ブラウザーで開くこともできますが、以下の URL についてはエンドポイント上の Web ブラウザーで開くためのポリシーを構成できます。

- ジオ/ロケール情報 — ユーザーの現在位置の情報に基づいて適切なページを自動的に表示する msn.com や news.google.com などの Web サイト。たとえば、イギリスにあるデータセンターで提供される VDA にインドのクライアントから接続する場合、in.msn.com ではなく uk.msn.com が表示されます。
- マルチメディアコンテンツ — メディアリッチな Web サイト。クライアント側で処理されるように設定すると、ユーザーエクスペリエンスが向上し、狭帯域幅接続での使用帯域幅や処理能力が改善されます。Flash リダイレクト機能を使用することもできますが、URL リダイレクトを使用すると Silverlight などほかの種類のメディアにも対応できます。これにより、環境のセキュリティも向上します。つまり、管理者により許可された URL だけがクライアント側で処理され、ほかの URL はすべて VDA 側で処理されます。

URL リダイレクトに加えて、FTA リダイレクトも使用できます。この機能では、セッションで特定のファイルを開くときにローカルのアプリケーションが使用されます。ローカルアプリでファイルを開くには、そのローカルアプリがそのファイルにアクセスできる必要があります。つまり、ローカルアプリケーションで開くことができるのは、ネットワーク共有上またはクライアントドライブ上にあるファイル（クライアント側ドライブのマッピング機能）のみです。たとえば、PDF ファイルを開く場合、ローカルにインストールされている PDF リーダーでファイルが表示され

ます。ローカルアプリケーションはファイルに直接アクセスできるため、ファイルを開くときに ICA によるネットワーク転送は発生しません。

要件、考慮事項、および制限事項

ローカルアプリアクセスは VDA for Windows Server OS および VDA for Windows Desktop OS でサポートされるオペレーティングシステムでサポートされ、Citrix Receiver for Windows Version 4.1（以降）が必要です。次の Web ブラウザーがサポートされています:

- Internet Explorer 11 以降。Internet Explorer 8、9、または 10 も使用できますが、Microsoft は Internet Explorer 11 をサポートしており、Citrix も Internet Explorer 11 の使用を推奨しています。
- Firefox 3.5～21.0
- Chrome 10

ローカルアプリアクセスや 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。
  - ローカルアプリアクセスをウィンドウ表示モードの仮想デスクトップで使用するなど、単一の仮想デスクトップをすべてのモニター上で表示しない場合、ユーザーエクスペリエンスに混乱が生じます。
  - マルチモニター環境でアプリケーションの表示を 1 つのモニターで最大化すると、それ以降のアプリケーションはほかのモニターに表示されず、すべてのアプリケーションがそのモニター上に表示されます。
  - この機能は、単一 VDA での使用を想定して設計されています。複数の同時接続 VDA を対象とするものではありません。
- 一部のアプリケーションでは、以下の予期されない問題が発生する場合があります。
  - ユーザーが、仮想デスクトップの C ドライブとローカルの C ドライブを混同する場合があります。
  - 仮想デスクトップで使用できるプリンターは、ローカルアプリケーションでは使用できません。
  - 管理者特権が必要なアプリケーションは、ローカルアプリ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。
  - ローカルアプリアクセスでは、ローカルアプリケーションのプロパティ（デスクトップや［スタート］メニューへのショートカットの配置など）が複製されます。ただし、ショートカットキーや読み取り専用属性などのそのほかのプロパティは複製されません。
  - 一部のアプリケーションで、各ウィンドウが正しい重なり順で表示されない場合があります。これにより、一部のウィンドウが非表示になることがあります。
  - マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブ、フォルダーなどのショートカットはサポートされません。
  - カスタムのファイルタイプ、関連付けられたプログラムのないファイル、ZIP ファイル、および隠しファイルはサポートされません。

  - ビット数の異なるローカルアプリケーションと VDA アプリケーションのタスクバーでのグループ化はサポートされません。たとえば、32 ビットのローカルアプリケーションと 64 ビットの VDA アプリケーションは、タスクバーでグループ化されません。
  - アプリケーションは COM を使って起動できません。たとえば、Office アプリケーション内に埋め込まれている Office ドキュメントをクリックしても、プロセス起動が検出されないため、ローカルアプリケーション統合に失敗します。
- ユーザーが、仮想デスクトップセッション内から別の仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
- URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDA セッションのローカルデスクトップフォルダーにユーザーが新しいファイルを作成することはできません。
- ローカルアプリケーションの複数のインスタンスのタスクバーアイコンは、仮想デスクトップのタスクバー設定に基づいて表示されます。ただし、ローカルで実行されているアプリケーションのショートカットは、このアプリケーションの実行インスタンスのアイコンとはグループ化されません。また、ホストされているアプリケーションの実行インスタンスや、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。
  - ローカルアプリアクセスは、マルチモニターモードでデスクトップアプリケーションのようには動作し

ません。マルチモニターモードでは、スタート画面とデスクトップは別のモニター上で表示されます。

- Windows 8 およびローカルアプリアクセスの 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。

ローカルアプリアクセスと **URL** リダイレクトの構成

Citrix Workspace アプリ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 Workspace アプリをインストールします。Citrix Workspace アプリのインストール時に両方の機能を有効することも、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ことも可能です。
- ポリシーの ［ローカルアプリアクセスを許可する］設定を ［有効］に設定します。URL リダイレクトの URL 許可リストおよび禁止リストのポリシー設定を構成することもできます。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

ローカルアプリアクセスと **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のローカルアプリアクセスを有効にするには、次の手順を実行します:

1. Citrix Studio を開始します。
   - オンプレミス展開の場合、［スタート］メニューから **Citrix Studio** を開きます。
   - クラウドサービス展開の場合、［**Citrix Cloud**］**>** ［**Virtual Apps and Desktops** サービス］**>** ［管理］タブに移動します。
2. Studio のナビゲーションペインで ［ポリシー］を選択します。
3. ［操作］ペインの ［ポリシーの作成］をクリックします。
4. ［ポリシーの作成］ウィンドウで、検索ボックスに「ローカルアプリアクセスを許可する」と入力して、［選択］をクリックします。
5. ［設定の編集］ウィンドウで、［許可］を選択します。デフォルトでは、［ローカルアプリアクセスを許可する］ポリシーは禁止されます。この設定が許可されている場合、VDA により、公開アプリケーションおよびローカルアプリアクセスのショートカットを有効にするかをエンドユーザーが指定できます。（この設定が禁止されている場合、公開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。
6. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトのホワイトリスト」と入力して、［選択］をクリックします。URL リダイレクトの許可リストは、リモートセッションのデフォルトの Web ブラウザーで開く URL を指定します。
7. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。

8. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトのブラックリスト」と入力して、［選択］をクリックします。URL リダイレクトの禁止リストは、エンドポイント上で実行されているデフォルトの Web ブラウザーにリダイレクトされる URL を指定します。
9. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。
10. ［設定］ページで、［次へ］をクリックします。
11. ［ユーザーおよびマシン］ページでポリシーを該当のデリバリーグループに割り当てて、［次へ］をクリックします。
12. ［概要］ページで、設定を確認して ［完了］をクリックします。

Citrix Workspace アプリのインストール中、すべてのローカルアプリケーションで URL リダイレクトを有効にするには、以下の手順を実行します：

1. Citrix Workspace アプリ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 URL リダイレクトを有効にします。これにより、URL リダイレクト機能で使用される Web ブラウザーアドオンも登録されます。
2. コマンドプロンプトで次のいずれかのオプションを付けて適切なコマンドを実行し、Citrix Workspace アプリをインストールします：
   - CitrixReceiver.exe の場合、/`ALLOW_CLIENTHOSTEDAPPSURL`=1を使用します。
   - CitrixReceiverWeb.exe の場合、/`ALLOW_CLIENTHOSTEDAPPSURL`=1を使用します。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには

> 注：
>
> - グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/adml テンプレートファイルをローカルグループポリシーオブジェクト（GPO）に追加します。詳しくは、「グループポリシーオブジェクト管理用テンプレートの構成」を参照してください。
> - Windows 向け Citrix Workspace アプリのテンプレートファイルは、［管理用テンプレート］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Workspace**］フォルダーのローカル GPO にあります（ユーザーが CitrixBase.admx/CitrixBase.adml を%systemroot%\policyDefinitions フォルダーに追加する場合のみ）。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには、以下の手順を実行します：

1. **gpedit.msc** を実行します。
2. ［コンピューターの構成］**>** ［管理用テンプレート］**>** ［従来の管理用テンプレート（**ADM**）］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Workspace**］**>** ［ユーザーエクスペリエンス］の順に移動します。
3. ［ローカルアプリケーションアクセス設定］を選択します。
4. ［有効］を選択し、［**URL** のリダイレクトを許可します］チェックボックスをオンにします。URL リダイレクト機能を使用するには、この記事の「*Web* ブラウザーアドオンの登録」セクションに記載されているコマンドラインを使用して、Web ブラウザーアドオンを登録してください。

公開アプリケーションへのアクセスのみを提供する

次の 2 つのうちいずれかの方法で、公開アプリケーションへのアクセスを提供できます:

レジストリエディターを使用します。

1. Citrix Studio をインストールしたサーバー上で、regedit.exe を実行します。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudioにアクセスします。
3. REG_DWORD のエントリClientHostedAppsEnabledを追加して、値に 1 を設定します（0 を設定するとローカルアプリアクセスが無効になります）。

PowerShell SDK を使用します。

1. Delivery Controller が実行されているマシンで PowerShell を開きます。
2. コマンド: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`を実行します。

クラウドサービス展開で ［ローカルアプリアクセスアプリケーションの追加］にアクセスするには、Citrix Virtual Apps and Desktops Remote PowerShell SDK を使用します。詳しくは、「Citrix Virtual Apps and Desktops Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. 次のコマンドを実行します:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. コマンド: `set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”` を実行します。

上記の手順を完了したら、以下の手順に従って続行します。

1. ［スタート］メニューで ［**Citrix Studio**］を開きます。
2. 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。
3. 中央上部のペインで空白の領域を右クリックし、コンテキストメニューから ［ローカルアプリアクセスアプリケーションの追加］を選択します。また、［操作］ペインで ［ローカルアプリアクセスアプリケーションの追加］をクリックすることもできます。［操作］ペインで［ローカルアプリアクセスアプリケーションの追加］オプションを表示させるには、［更新］をクリックします。
4. ローカルアプリアクセスアプリケーションを公開します。

   - ローカルアプリケーションアクセスウィザードが起動され、［はじめに］ページが表示されます。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。

- ウィザードの指示に従って、［グループ］、［場所］、［識別］、［配信］、［概要］の各ページで操作を行います。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。
- ［グループ］ページで、アプリケーションが追加されるデリバリーグループを選択して ［次へ］をクリックします。
- ［場所］ページで、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、アプリケーションが存在するフォルダーへのパスを入力します。Citrix ではシステム環境変数のパスを使用することをお勧めします（例：%ProgramFiles(x86)%\Internet Explorer\iexplore.exe）。
- ［識別］ページで、既定値をそのまま使用するか、必要な情報を入力して ［次へ］をクリックします。
- ［配信］ページで、このアプリケーションをユーザーに配信する方法を構成して ［次へ］をクリックします。選択したアプリケーションのアイコンを指定できます。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することもできます。
- ［概要］ページで、設定を確認して ［完了］をクリックし、ローカルアプリケーションアクセスウィザードを閉じます。

Web ブラウザーアドオンの登録

> 注：
>
> URL リダイレクト機能に必要な Web ブラウザーアドオンは、コマンドラインでの Citrix Workspace アプリのインストール時に/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に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のアドオンの登録を解除する場合：<*client-installation-folder*>\redirector.exe /unreg<*browser*>
- VDA にアドオンを登録する場合：<*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- VDA のアドオンの登録を解除する場合：<*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

ここで <*browser*> は、「Internet Explorer」、「Firefox」、「Chrome」、または「All」です。

たとえば、Citrix Workspace アプリを実行するデバイスに、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、Windows マルチセッション OS VDA 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 はリダイレクトされません。禁止リストにあってもリダイレクトされません。

URL リダイレクトが正しく機能するためには、Web ブラウザーに表示されるメッセージに従ってアドオンを有効にする必要があります。インターネットオプションを使用するアドオンやメッセージで示されたアドオンが無効の場合、URL リダイレクトは正しく機能しません。

- Firefox アドオンでは、URL が常にリダイレクトされます。

Firefox では、アドオンのインストールを許可するかどうかを確認するメッセージが新しいタブに表示されます。URL リダイレクトが正しく機能するためには、アドオンのインストールを許可します。

- Chrome のアドオンでは、ユーザーがナビゲーションにより開いた最終的な URL（ユーザーが入力したものでない URL）は常にリダイレクトされます。

拡張機能が外部的にインストールされます。この拡張機能を無効にすると、Chrome で URL リダイレクトが動作しなくなります。シークレットモードで URL リダイレクトを使用するには、Web ブラウザーの設定でシークレットモードでの拡張機能の実行を許可する必要があります。

ログオフおよび切断時のローカルアプリケーションの動作の構成

> 注:
>
> 以下の手順どおりに設定を構成しなかった場合、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、デフォルトで、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。

1. ホストされているデスクトップ上で、**regedit.msc** を実行します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State`にアクセスします。

   64 ビットシステムの場合は、`HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State`にアクセスします。
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（仮想デスクトップで使用可能な場合）。
   - 3 — ユーザーが仮想デスクトップからログオフまたは切断した場合、ローカルアプリケーションが終了します。

USB とクライアント側ドライブの考慮事項

August 24, 2021

HDX テクノロジは、一般的な USB デバイスのほとんどに最適化されたサポートを提供します。以下が対象となります:

- モニター
- マウス
- キーボード
- ボイスオーバー IP 電話
- ヘッドセット
- Web カメラ
- スキャナー
- カメラ
- プリンター
- ドライブ
- スマートカードリーダー
- 描画用タブレット
- 署名パッド

最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN 経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDX テクノロジにより、特殊デバイスに次のような最適化されたサポートがないときや、不適切なときに汎用 **USB** リダイレクトを使用できます:

- USB デバイスに追加の高度な機能があり（追加ボタンがあるマウスや Web カメラなど）、それらの機能が最適化されたサポートに含まれていないとき。
- ユーザーが最適化されたサポートに含まれない機能（CD の書き込みなど）を必要とするとき。
- USB デバイスが特殊なデバイス（テスト用機器、測定用機器、工業用コントローラーなど）であるとき。
- アプリケーションが USB デバイスとしてデバイスに直接アクセスする必要があるとき。
- USB デバイスで Windows ドライバーしか使用できないとき。たとえば、スマートカードリーダーに Citrix Receiver for Android で使用できるドライバーがないことがあります。
- Citrix Receiver のバージョンが、該当するタイプの USB デバイスに最適化されたサポートを提供しないとき。

汎用 USB リダイレクトでは、以下に注意してください。

- ユーザーデバイスにデバイスドライバーをインストールする必要はありません。
- USB クライアントドライバーは VDA マシン上にインストールされます。

> 注
>
> - 汎用 USB リダイレクトは、最適化されたサポートと併用できます。汎用 USB リダイレクトを有効にする場合は、整合性の不一致と予期しない動作を避けるために、Citrix のUSB デバイスのポリシー設定で汎用 USB リダイレクトと最適化されたサポートの両方を構成します。
> - 一部の USB デバイスでは、Citrix のポリシー設定のクライアント USB デバイス最適化規則は、汎用 USB リダイレクト専用の設定となります。ここで説明したような最適化されたサポートではありません
> - クライアント USB プラグアンドプレイデバイスリダイレクトは、Picture Transfer Protocol（PTP）や Media Transfer Protocol（MTP）を使用するカメラやメディアプレーヤーなどのデバイスに、最適化されたサポートを提供する関連機能です。クライアント USB プラグアンドプレイリダイレクトは汎用 USB リダイレクトの一部ではありません。サポートされているバージョンについては、「デフォルトのポリシー設定」を参照してください。

USB デバイスのパフォーマンスに関する考慮事項

一部のタイプの USB デバイスの汎用 USB リダイレクトでは、ネットワークの遅延と帯域幅がユーザーエクスペリエンスと USB デバイスの操作に影響を与えます。たとえば、遅延が多く低帯域幅のリンクでタイミングが重要なデバイスが正しく動作しないことがあります。可能な場合は、代わりに最適化されたサポートを使用してください。

3D マウスなどの一部の USB デバイスは、高い帯域幅を使用できる必要があります（通常、これも高帯域幅を必要とする 3D アプリとともに使用）。パフォーマンスの問題は Citrix ポリシーを使って回避することができます。詳しくは、「帯域幅のポリシー設定」（クライアント USB デバイスリダイレクトの場合）および「マルチストリーム接続のポリシー設定」を参照してください。

USB デバイスのセキュリティに関する考慮事項

スマートカードリーダーやフィンガープリントリーダー、署名パッドなどの一部の USB デバイスは、もともとセキュリティを重視します。USB ストレージデバイスなどの他の USB デバイスは、機密扱いである可能性のあるデータの受け渡しに使用できます。

USB デバイスは、しばしばマルウェアの配信に使用されます。このような USB デバイスのリスクを、Citrix Receiver、XenApp、および XenDesktop の構成で減らすことはできますが、すべて取り除くことはできません。このことは、汎用 USB リダイレクトを使用しているか最適化されたサポートを使用しているかにかかわらず当てはまります。

> 重要
>
> セキュリティを重視するデバイスやデータを扱う場合は、TLSまたは IPSec のどちらかを使用して、常に HDX 接続をセキュリティで保護してください。
>
> 必要な USB デバイスのサポートのみを有効にしてください。汎用 USB リダイレクトと最適化されたサポートの両方で、このニーズを満たしてください。
>
> 信用できるソースから入手した USB デバイスのみを使用する、USB デバイスを人がいないオープンな環境

> に置きっぱなしにしない（例：インターネットカフェに Flash デバイスを置きっぱなしにしない）といった、USB デバイスの安全な使用についてのガイダンスをユーザーに提供してください。また、複数のコンピューターで 1 つの USB デバイスを使用することのリスクを説明してください。

汎用 **USB** リダイレクトの互換性

汎用 USB リダイレクトは、USB 2.0 以前のデバイスでサポートされます。USB 3.0 デバイスを USB 2.0 または USB 3.0 ポートに接続した場合も、汎用 USB リダイレクトがサポートされます。汎用 USB リダイレクトは、USB3.0 に導入された超高速などの USB 機能はサポートしません。

次の Citrix Receiver は、汎用 USB リダイレクトをサポートします:

- Citrix Receiver for Windows については、「USB サポートの構成」を参照してください。
- Citrix Receiver for Mac については、Citrix Receiver for Mac の構成を参照してください。
- Citrix Receiver for Linux については、「最適化」を参照してください。
- Citrix Receiver for Chrome OS については、「新機能」を参照してください

Citrix Receiver のバージョンについては、『Citrix Receiver Feature Matrix』を参照してください。

前のバージョンの Citrix Receiver を使用している場合は、Citrix Receiver のドキュメントを参照して、汎用 USB リダイレクトがサポートされていることを確認してください。サポートされる USB デバイスのタイプに関する制限事項については、Citrix Receiver のドキュメントを参照してください。

汎用 USB リダイレクトは VDA for Desktop OS のバージョン 7.6 以上のデスクトップセッションでサポートされます。

汎用 USB リダイレクトは VDA for Server OS のバージョン 7.6 以上のデスクトップセッションでサポートされますが、以下の制限事項があります。

- VDA は Windows Server 2012 R2 または Windows Server 2016 で動作している必要があります。
- USB デバイスドライバーは、完全仮想化サポートなど、Windows 2012 R2 のリモートデスクトップセッションホスト（RDSH）と完全に互換性がある必要があります。

次のような一部のタイプの USB デバイスは、リダイレクトしても役に立たないため、汎用 USB リダイレクトをサポートしません。

- USB モデム。
- USB ネットワークアダプター。
- USB ハブ。USB ハブに接続した USB デバイスは、個別に扱われます。
- USB 仮想 COM ポート。汎用 USB リダイレクトではなく、COM ポートリダイレクトを使用します。

汎用 USB リダイレクトでテストされた USB デバイスについては、CTX123569を参照してください。一部の USB デバイスは、汎用 USB リダイレクトを使用すると正しく動作しません。

汎用 **USB** リダイレクトの設定

汎用 USB リダイレクトを使用する USB デバイスのタイプを制御できます。次の手段で別々に設定できます:

- Citrix ポリシー設定を使って VDA で設定します。詳しくは、「ポリシー設定リファレンス」の「クライアントドライブやデバイスのリダイレクト」、および「USB デバイスのポリシー設定」を参照してください。
- Citrix Receiver で Citrix Receiver に依存するメカニズムを使用します。たとえば、Citrix Receiver for Windows は、管理用テンプレートで制御できるレジストリ設定で設定します。USB リダイレクトのデフォルトでは、特定のクラスの USB デバイスでのみ許可され、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 for Windows のドキュメントの「USB サポートの構成」を参照してください。

別々に設定できることで柔軟性が提供されます。例:

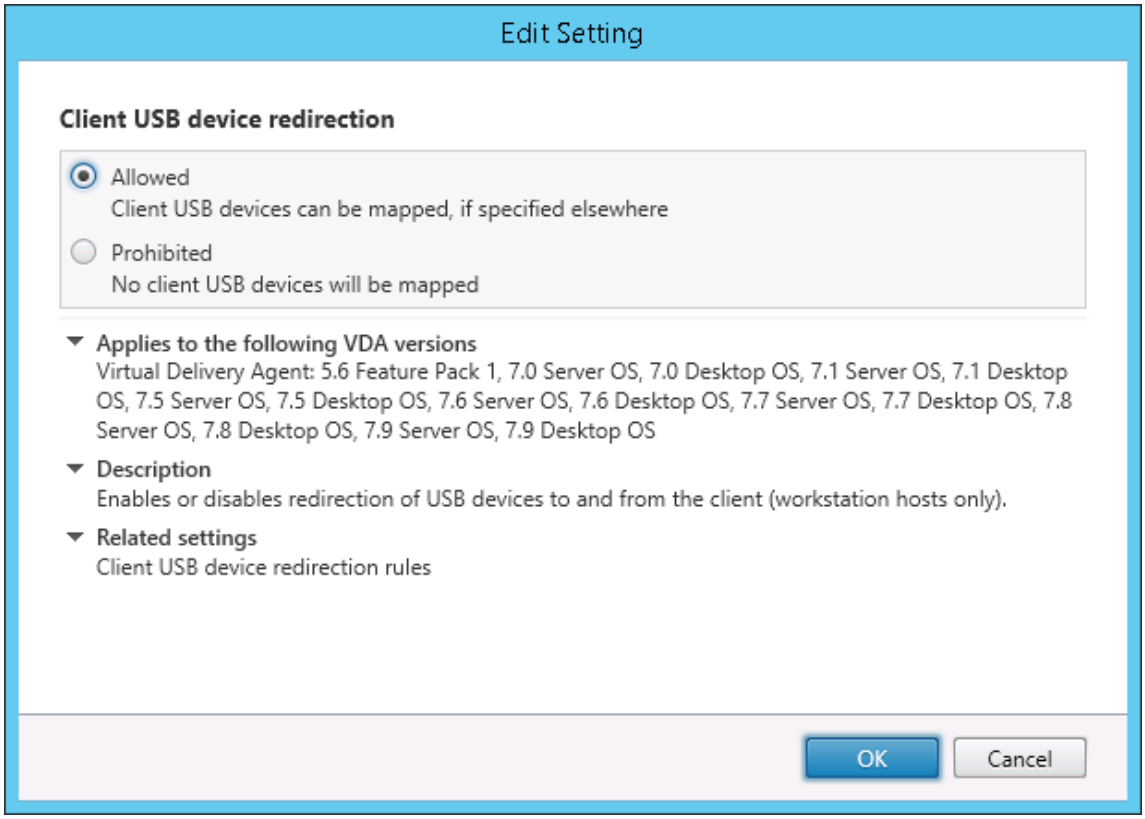
- 2 つの異なる組織または部門が Citrix Receiver と VDA を担当している場合に、それぞれが別に制御を実行できます。このことは、ある組織のユーザーが別の組織のアプリケーションにアクセスするときにも適用されます。
- USB デバイスを、特定のユーザーのみまたは（NetScaler Gateway 経由ではなく）LAN 経由で接続しているユーザーのみに許可する必要がある場合は、Citrix ポリシー設定で制御できます。

汎用 **USB** リダイレクトの有効化

汎用 USB リダイレクトを有効にするには、Citrix ポリシー設定と Citrix Receiver の両方を設定します。

Citrix ポリシー設定で、次の手順に従います:

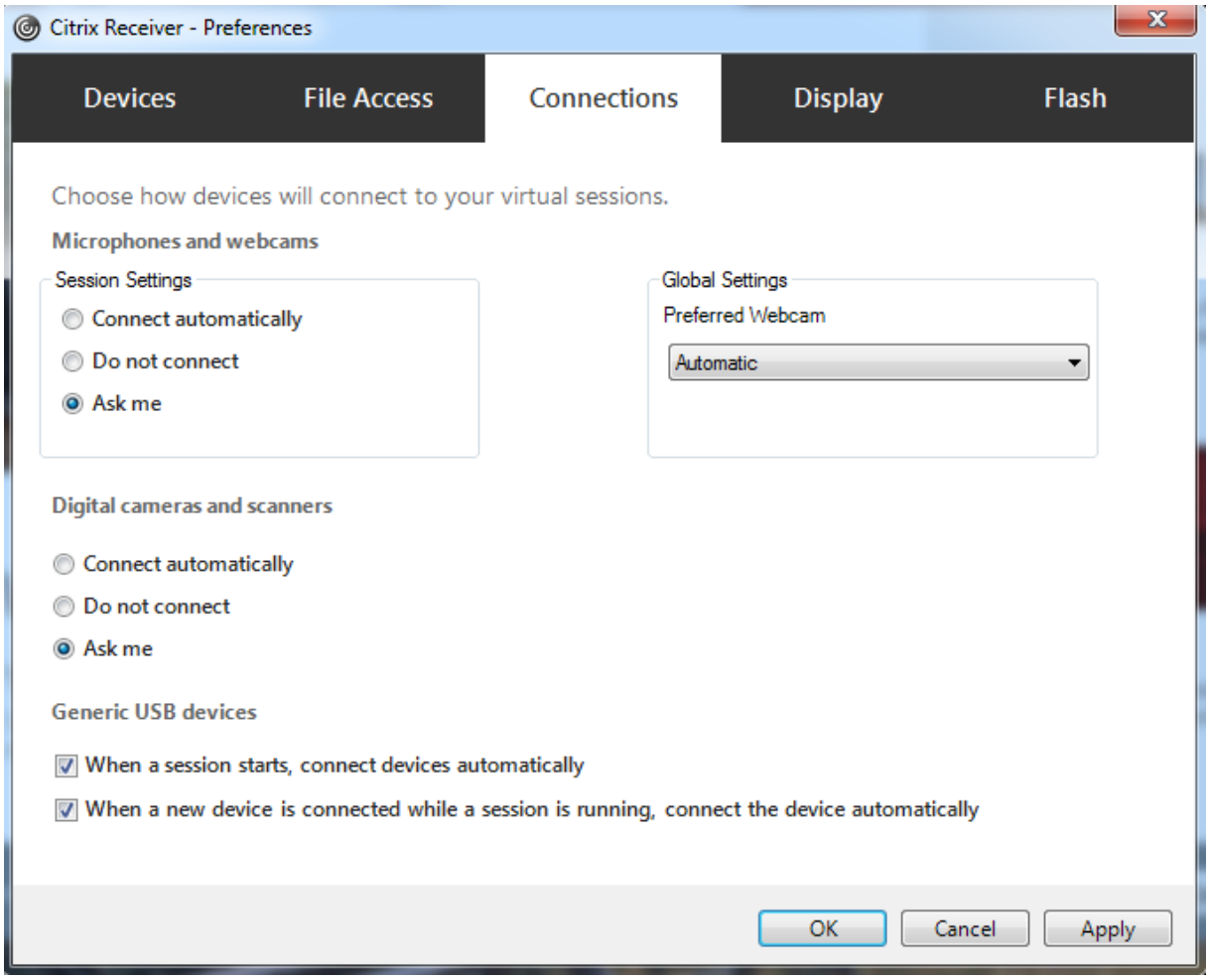
1. ポリシーに ［クライアント USB デバイスリダイレクト］ を追加して、値を ［許可］ に設定します。



2. 必要な場合は、ポリシーに［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 USB ポリシー規則を指定し、リダイレクトする USB デバイスの一覧を変更します。

   Citrix Receiver で、次の手順に従います:

3. ユーザーデバイスに Citrix Receiver をインストールするときに、USB サポートを有効にします。この操作は、管理用テンプレートを使うか、[Citrix Receiver for Windows] > [基本設定] > [接続] で実行できます。



前の手順で VDA の USB ポリシー規則を指定した場合は、Citrix Receiver についても同じポリシー規則を指定します。

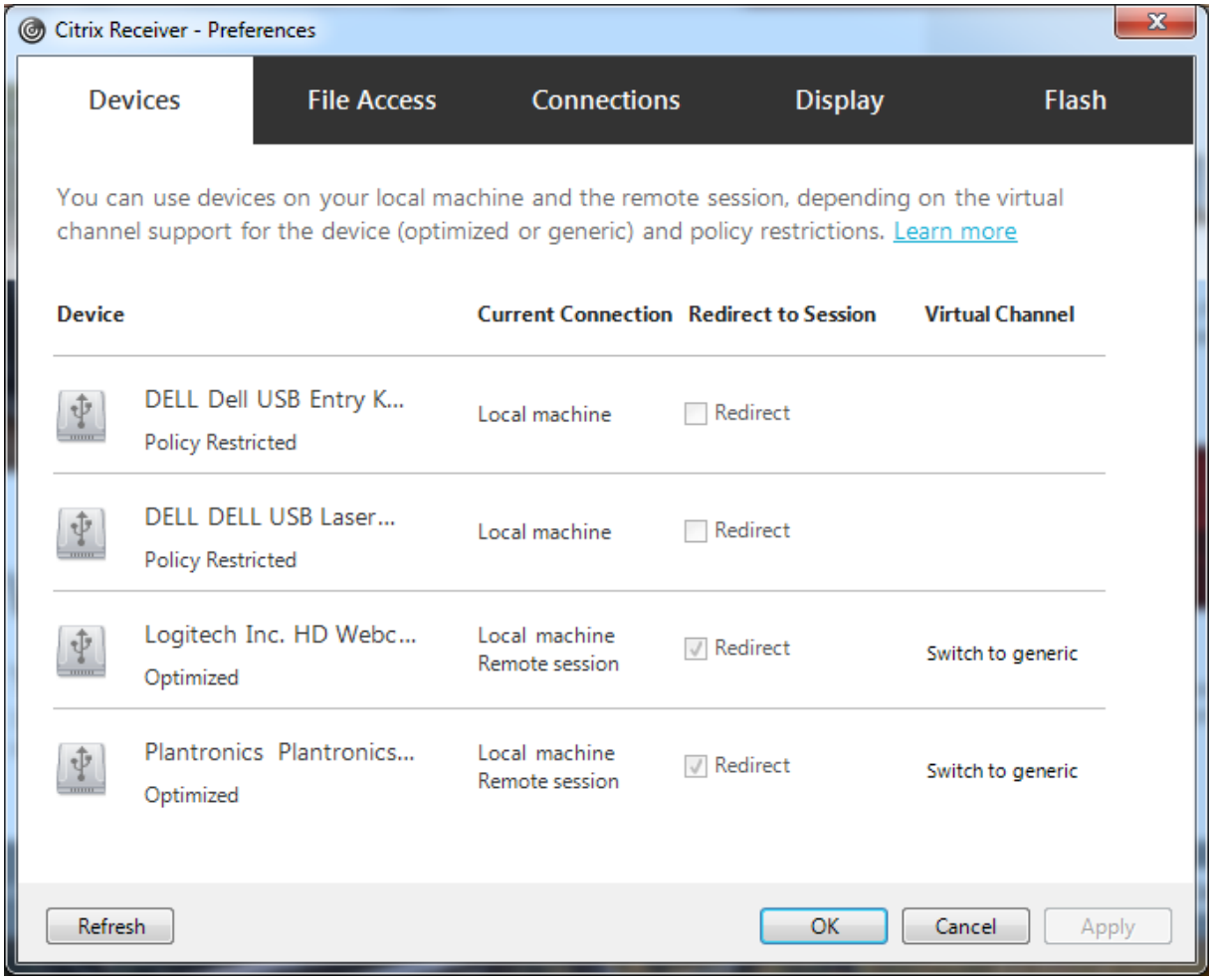
シンクライアントでの USB サポートおよびその構成方法については、デバイスの製造元に問い合わせてください。

汎用 **USB** リダイレクトで使用できる **USB** デバイスタイプの設定

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。また、デスクトップアプライアンスモードで接続バーが表示されていない場合も、USB デバイスが自動的にリダイレクトされます。

ユーザーは、USB デバイスの一覧からデバイスを選択することによって、自動的にリダイレクトされないデバイスを

明示的にリダイレクトすることができます。この手順について詳しくは、Citrix Receiver for Windows のユーザーヘルプ「Desktop Viewer でのデバイスの表示」に説明されています。



最適化されたサポートではなく汎用 USB リダイレクトを使用するには、次のどちらかの手順を実行します。

- Citrix Receiver で、汎用 USB リダイレクトを使う USB デバイスを手動で選択し、［基本設定］ダイアログボックスの［デバイス］タブから ［汎用に切り替え］を選択します。
- USB デバイスタイプの自動リダイレクトを設定することで（たとえば AutoRedirectStorage=1）、汎用 USB リダイレクトを使う USB デバイスを自動選択して、USB ユーザー基本設定を自動接続 USB デバイスに設定します。詳しくは、CTX123015を参照してください。

> 注:
>
> Web カメラと HDX マルチメディアリダイレクトの互換性がない場合は、Web カメラで使用する汎用 USB リダイレクトのみを設定します。

USB デバイスを一覧に表示しないようにしたり、USB デバイスをリダイレクトできないようにしたりするには、Citrix Receiver および VDA のデバイス規則を定義します。

汎用 USB リダイレクトでは、少なくとも USB デバイスクラスとサブクラスを知っておく必要があります。すべての USB デバイスが明確な USB デバイスクラスとサブクラスを持つわけではありません。例:

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーはベンダー定義のクラスまたは HID デバイスクラスを使用できます。

より正確な制御のためには、ベンダー ID、製品 ID、およびリリース ID も知っておく必要があります。この情報はデバイスベンダーから入手できます。

> 重要
>
> 悪意のある USB デバイスが、意図された使用状況にマッチしない USB デバイス特性を示すことがあります。デバイス規則は、この動作を防ぐことを目的としていません。

VDA と Citrix Receiver 両方の USB デバイスリダイレクト規則を指定し、デフォルトの USB ポリシー規則よりも優先することで、汎用 USB リダイレクトを使用できる USB デバイスを制御できます。

VDA の場合:

- グループポリシー規則を介して、サーバー OS マシン上の OS の管理者による上書き規則を編集します。グループポリシー管理コンソールは、インストールメディアにあります。
  - x64 の場合:DVD ルートの\os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - x86 の場合:DVD ルートの\os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Citrix Receiver for Windows の場合:

- 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。DVD のルート \os\lang\Support\Configuration\icaclient_usb.adm）により、Active Directory のグループポリシーを使用してユーザーデバイスを変更できます。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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「*tag*=*value*」式の形式で設定します。

以下のタグがサポートされます。

タグ	説明
VID	デバイス記述子のベンダー ID
PID	デバイス記述子の製品 ID
REL	デバイス記述子のリリース ID
クラス	デバイス記述子またはインターフェイス記述子のクラス。使用可能な USB クラスコードについては、USB Web サイトhttps://www.usb.org/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たとえば、VID=1230 とします。
- 各規則を 1 行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。

> 注
>
> ADM テンプレートを使用する場合は、規則を単一行に（セミコロン区切りのリストとして）作成する必要があります。

例:

- 次の例に、ベンダー ID と製品 ID に関する管理者定義の USB ポリシー規則を示します。

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
                Deny: VID=046D # Deny all Logitech products
<!--NeedCopy-->
```

- 次の例に、クラス、サブクラス、およびプロトコルに関する管理者定義の USB ポリシー規則を示します:

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

USB デバイスの装着と取り外し

ユーザーは、仮想セッションの開始前および開始後に USB デバイスを装着できます。

Citrix Receiver for Windows では、以下の点について考慮してください:

- セッションを開始した後で装着したデバイスは、Desktop Viewer の［USB］メニューに追加されます。
- USB デバイスが正しくリダイレクトされない場合、仮想セッションが開始されてからデバイスを装着することで問題が解決される場合があります。
- データの損失を避けるため、Windows で推奨される手順（［ハードウェアの安全な取り外し］アイコンの使用など）に従って USB デバイスを取り外してください。

USB マスストレージデバイスのセキュリティ制御

USB マスストレージデバイスでは最適化されたサポートが提供されます。これは、XenApp および XenDesktop クライアントドライブのマッピングに含まれています。ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップのドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブのマッピングを構成するには、ICA のポリシー設定の ［ファイルリダイレクトポリシー設定］ セクションの ［クライアント側リムーバブルドライブ］設定を使用します。

USB マスストレージデバイスでは、Citrix ポリシーによって制御される Client 側ドライブのマッピングまたは汎用 USB リダイレクトのどちらか、またはこの両方を使用できます。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用 **USB** リダイレクト
デフォルトで有効。	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
デバイスアクセスが暗号化される	はい、デバイスにアクセスする前に暗号化のロックを解除した場合	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ドライブのマッピングのポリシーの両方が有効な場合、セッション開始前または後に装着されたマスストレージデバイスがクライアント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、自動リダイレクトが構成

されている場合（https://support.citrix.com/article/CTX123015を参照）、セッション開始前または後に装着されたマスストレージデバイスが汎用 USB リダイレクトによりリダイレクトされます。

> 注
>
> USB リダイレクトはより低い帯域幅の接続（50Kbps など）でもサポートされますが、大きなファイルはコピーできません。

クライアント側ドライブのマッピングを使うファイルアクセスの制御

管理者は、ユーザーが仮想環境のファイルをユーザーデバイス上にコピーすることを許可したり禁止したりできます。デフォルトでは、マップされたクライアント側ドライブ上のフォルダーやファイルに対するセッション内での読み取りや書き込みが許可されます。

マップされたクライアント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。

印刷

August 24, 2021

環境でのプリンター管理には、以下の複数の段階があります。

1. 印刷の概念を理解します。
2. 印刷アーキテクチャを計画します。これには、業務上のニーズや既存の印刷インフラストラクチャについての分析と、ユーザーやアプリケーションが現状でどのように印刷を行っているか、および理想的な印刷管理モデルは何かについての評価が含まれます。
3. プリンタープロビジョニングの方法を選択し、印刷設計を展開するためのポリシーを作成して印刷環境を構成します。新しい従業員またはサーバーが追加されたときにポリシーを更新します。
4. 新しい印刷環境を実務環境に展開する前に、その環境をテストします。
5. プリンタードライバーを管理し、印刷のパフォーマンスを最適化して Citrix の印刷環境を維持します。
6. 発生する問題をトラブルシューティングします。

印刷の概念

印刷環境の構築を計画する前に、Citrix 環境での印刷処理の主な概念について理解しておく必要があります。

- 使用できるプリンタープロビジョニングの種類
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーの基本的な管理方法

印刷の概念は、Windows の印刷概念上に構成されています。環境での印刷設定を正しく管理するには、Windows でのネットワークやクライアント印刷のしくみについて熟知しており、それが実際の環境にどのように適用されるのかを理解する必要があります。

印刷プロセス

この環境では、ユーザーによる印刷はすべてアプリケーションをホストするマシン上で開始されます。印刷ジョブはネットワークプリントサーバーまたはユーザーデバイスを介して印刷装置にリダイレクトされます。

仮想デスクトップやアプリケーションのユーザーに提供されるワークスペースは永続的ではありません。ユーザーのセッションが終了すると、そのユーザーのワークスペースはサーバーから削除されます。このため、各セッションの開始時にすべての設定を再構築する必要があります。この結果、ユーザーが新しいセッションを開始するたびに、ユーザーのワークスペースが再構築されます。

ユーザーが印刷を実行すると、以下の処理が行われます。

- ユーザーに提供するプリンターを決定します。この処理は、プリンタープロビジョニングと呼ばれます。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

管理者は、プリンタープロビジョニング、印刷ジョブの送信経路、プリンタープロパティの保存、およびプリンタードライバー管理に関するオプションを変更して、上記の処理をカスタマイズできます。これらのオプションの変更によって環境での印刷パフォーマンスやユーザーエクスペリエンスがどのように変化するのかを検証してください。

プリンタープロビジョニング

セッション用のプリンターを準備する処理は、プリンタープロビジョニングと呼ばれます。通常、この処理は動的に行われます。つまり、セッションで提供されるプリンターは事前定義されておらず、非永続的です。プリンターは、セッションへの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、および変更に応じてセッションの自動作成プリンターが動的に変更されます。この動的プリンター検出は、さまざまなデバイスを使用するモバイルユーザーにとって便利な機能です。

プリンターのプロビジョニングには、主に以下の方法があります:

- ユニバーサルプリントサーバー - Citrixユニバーサルプリントサーバーは、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。ユニバーサルプリントサーバーでは、ユニバーサルプリンタードライバーが使用されます。これにより、サーバー OS マシン上の単一のドライバーを使って、任意のデバイスからネットワーク印刷を実行できます。

リモートの印刷サーバーを使う環境では、Citrix ユニバーサルプリントサーバーの使用をお勧めします。ユニバーサルプリントサーバー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。

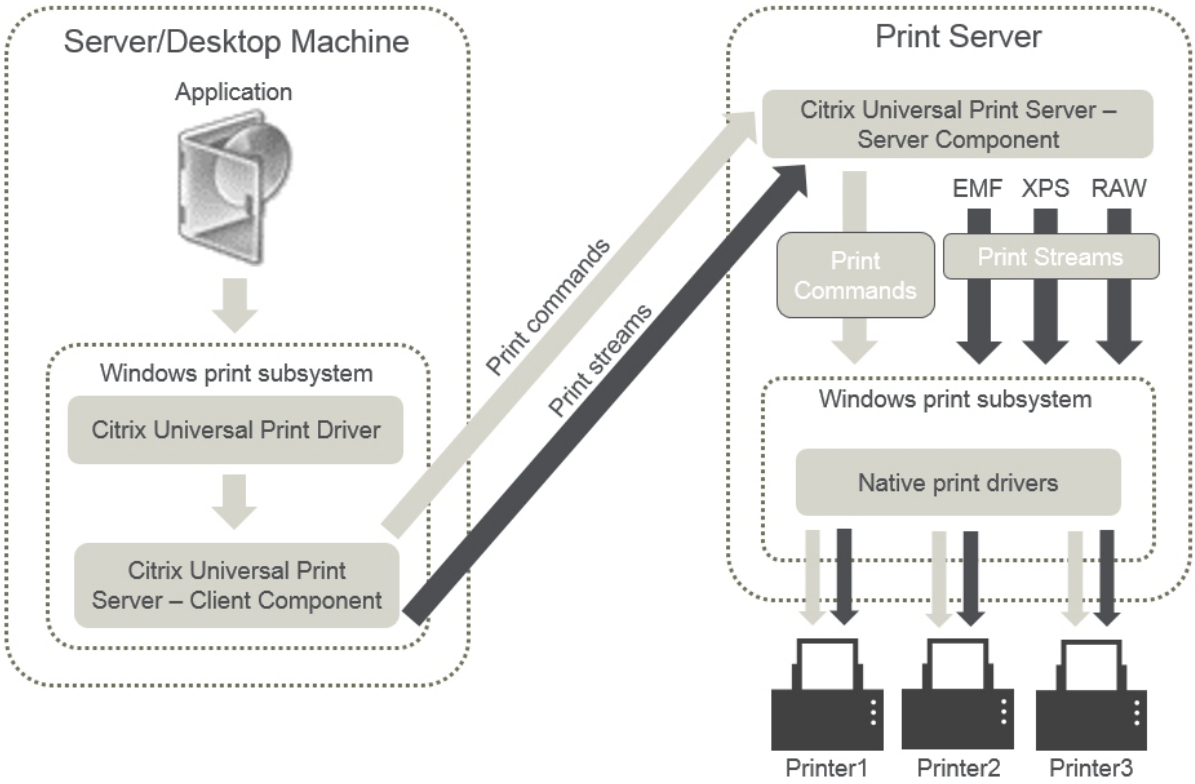
ユニバーサルプリントサーバーの機能は以下のコンポーネントで構成されます。

クライアントコンポーネント、ユニバーサルプリントクライアント - 各サーバー OS マシンでユニバーサルプリントクライアントを有効にして、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し、ユニバーサルプリントドライバーを使用します。

サーバーコンポーネント、ユニバーサルプリントサーバー - 各プリントサーバーにユニバーサルプリントサーバーをインストールして、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し、（セッションプリンターが一元的にプロビジョニングされているかどうかにかかわらず）セッションプリンターにユニバーサルプリントドライバーを使用します。

ユニバーサルプリントサーバー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、ユニバーサルプリントサーバー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 ユニバーサルプリントサーバーを有効にすると、接続されているすべてのネットワークプリンターでユニバーサルプリントサーバーが自動検出されて使用されます。

> 注:
> ユニバーサルプリントサーバーは VDI-in-a-Box 5.3 でもサポートされます。VDI-in-a-Box でのユニバーサルプリントサーバーのインストールについて詳しくは、VDI-in-a-Box のドキュメントを参照してください。

- 自動作成 — 自動作成とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターだけが自動作成されるように構成することを検討します。自動作成するプリンターの数を最小限にすることで、サーバー OS マシンの負荷（メモリや CPU）を軽減できます。また、これによりユーザーログオン時間も短縮されます。

  以下の項目に基づいてプリンターが自動作成されます。

  - ユーザーデバイス上にインストールされたプリンター。
  - セッションに適用されるポリシー。

    管理者は、自動作成に関するポリシーを設定して、作成されるプリンターの数や種類を制御できます。デフォルトでは、ユーザーデバイス上で設定されているすべてのプリンター（ローカル接続のプリンターおよびネットワークプリンター）が自動作成され、ユーザーに提供されます。

  ユーザーがセッションを終了すると、これらのプリンターは削除されます。

  クライアントプリンターおよびネットワークプリンターの自動作成機能を使用する場合、保守作業が必要です。たとえば、プリンターを追加した場合は以下の設定が必要になります:

  - ポリシーの［セッションプリンター］設定を更新します。
  - 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。

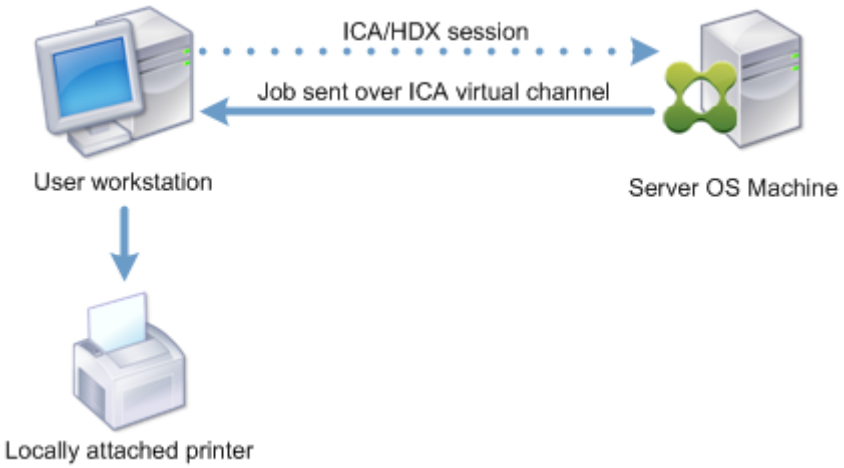
印刷ジョブの送信

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。



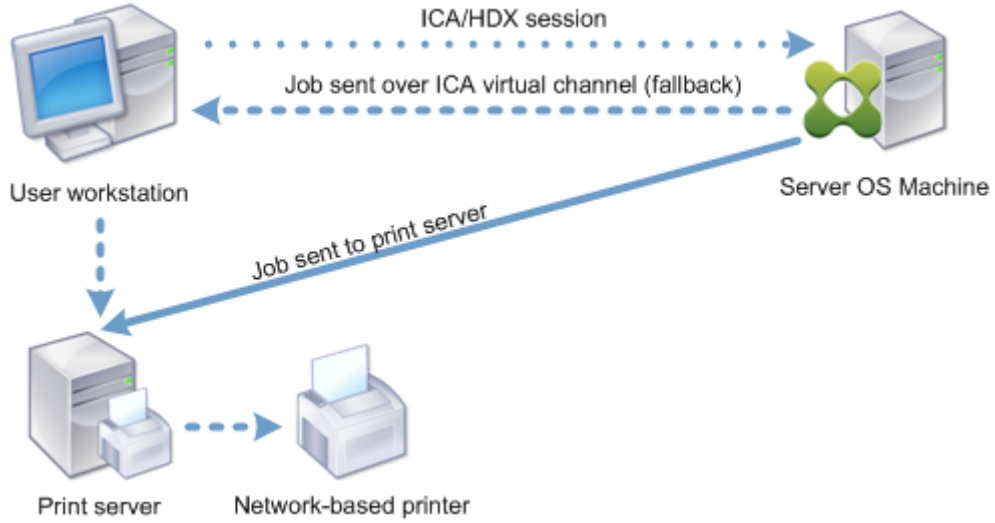
ネットワークベースのプリンター

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。

ユニバーサルプリントサーバーが無効な場合、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

Citrix ユニバーサルプリンタードライバー（UPD）は、デバイスに依存しないプリンタードライバーで、大部分のプリンターに対して互換性があります。Citrix UPD は、以下の 2 つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPD は、XenApp または XenDesktop VDA のインストールの一部としてインストールされます。VDA は、Citrix UPD とともに次のドライバーをインストールします：Citrix ユニバーサルプリンター（EMF ドライバー）および Citrix XPS ユニバーサルプリンター（XPS ドライバー）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

印刷ジョブが開始されると、ドライバーは、エンドポイントデバイスをいっさい変更せずに、アプリケーションの出力を記録して送信します。

クライアントコンポーネント。Citrix UPD は、Citrix Receiver のインストールの一部としてインストールされます。それによって、XenApp または XenDesktop セッションの着信する印刷ストリームがフェッチされます。印刷ストリームはローカルの印刷サブシステムに転送され、そこで印刷ジョブがデバイス固有のプリンタードライバーを使用してレンダリングされます。Citrix UPD のほか、Citrix PDF ユニバーサルプリンタードライバーを、Citrix Receiver for HTML5 および Citrix Receiver for Chrome とともに別々にインストールできます。

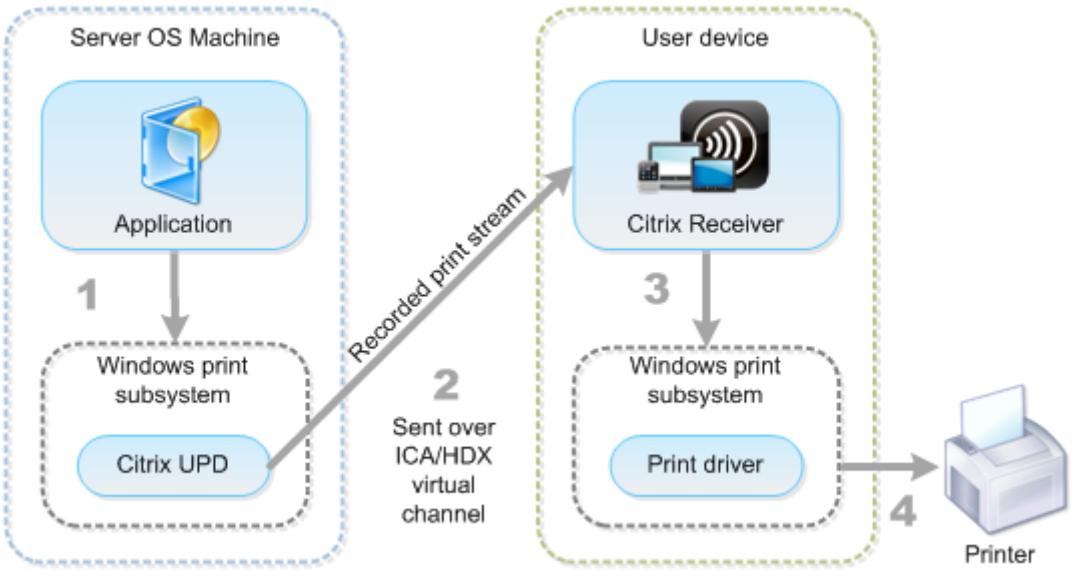
Citrix UPD は次の印刷形式をサポートします。

- 拡張メタファイル形式（**EMF**）、デフォルト。EMF は 32 ビットバージョンの Windows Metafile（WMF）形式です。EMF ドライバーは、Windows ベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPS ドライバーでは XML が使用され、Adobe PDF に似た、プラットフォームに依存しない「電子ペーパー」が作成されます。
- プリンターコマンド言語（**PCL5c** および **PCL4**）。PCL は、もともとインクジェットプリンターのために Hewlett-Packard によって開発された印刷プロトコルです。基本的なテキストおよびグラフィックを印刷するために使用され、HP LaserJet および複合機で広くサポートされています。
- PostScript（**PS**）。PostScript は、テキストおよびベクターグラフィックスを印刷するために使用できるコンピューター言語です。ドライバーは、低コストのプリンターや複合機で広く使われています。

PCL および PS ドライバーは、Mac や UNIX クライアントなど、非 Windows ベースのデバイスを使用する場合に最適です。Citrix UPD がドライバーを使用する順序は、ユニバーサルドライバーの優先度ポリシー設定を使用して変更できます。

Citrix UPD（EMF および XPS ドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリンター機能をサポートします。これらの機能は、ネイティブドライバーが Microsoft の印刷機能テクノロジを使用して利用可能としている場合にのみ、利用できます。ネイティブドライバーでは、印刷機能 XML で、標準化された印刷スキーマキーワードを使用する必要があります。標準化されていないキーワードを使用すると、Citrix のユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

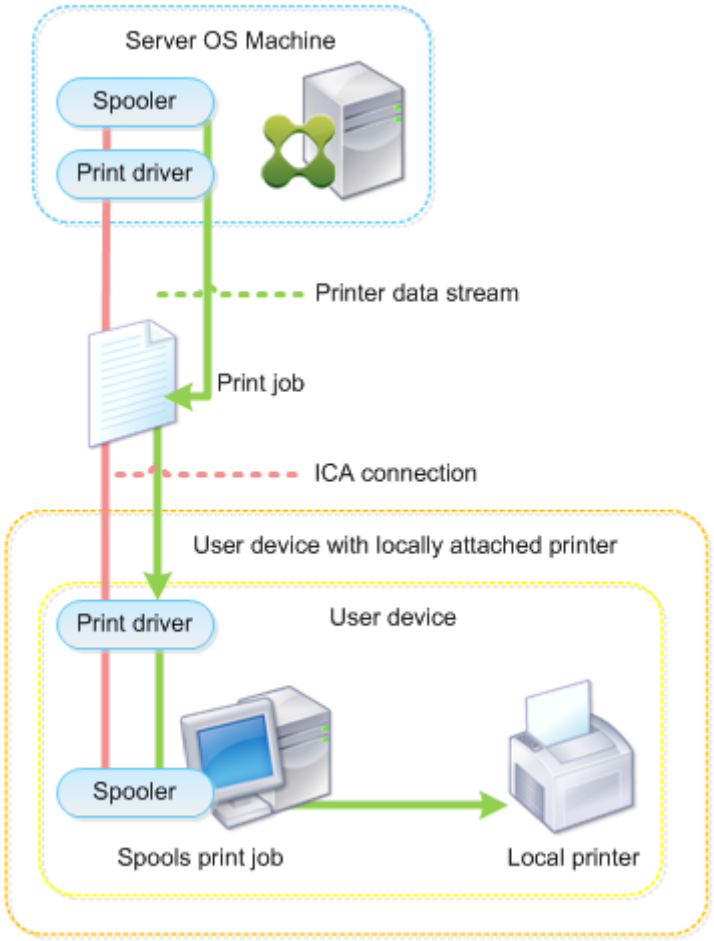
次の図は、ユニバーサルプリンタードライバーコンポーネントとデバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



プリンタードライバーの管理方法を計画する場合、ユニバーサルプリンタードライバーを使用するか、デバイス固有のドライバーを使用するか、またはその両方を使用するかを決定する必要があります。標準ドライバーをサポートする場合は、以下の点を検討する必要があります。

プリンターの自動作成時に、ユーザーデバイスに接続された新しいローカルプリンターが検出されると、必要なプリンタードライバーについてサーバー OS マシンがチェックされます。デフォルトでは、Windows ネイティブドライバーが使用できない場合は、ユニバーサルプリンタードライバーが使用されます。

正しく印刷するには、サーバー OS マシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致する必要があります。次の図は、クライアント印刷経路でサーバーとクライアント上のプリンタードライバーがどのように使用されるかを示しています。



- 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

August 24, 2021

組織のコンピューティング環境やユーザーのニーズに適した印刷環境を設定すると、管理が容易になります。通常、デフォルトの印刷構成でも正しく印刷できますが、ユーザーエクスペリエンスが低下したり、ネットワーク使用が最適化されなかったり、管理上のオーバーヘッドが生じたりする場合もあります。

印刷環境を設定するときは、以下の事項を考慮します。

- 業務上のニーズと既存の印刷インフラストラクチャ。

  組織のニーズに基づいて、印刷環境を設計します。既存の印刷環境（ユーザーが自分でプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるか、など）を確認し、それに沿って印刷環境を構成できます。

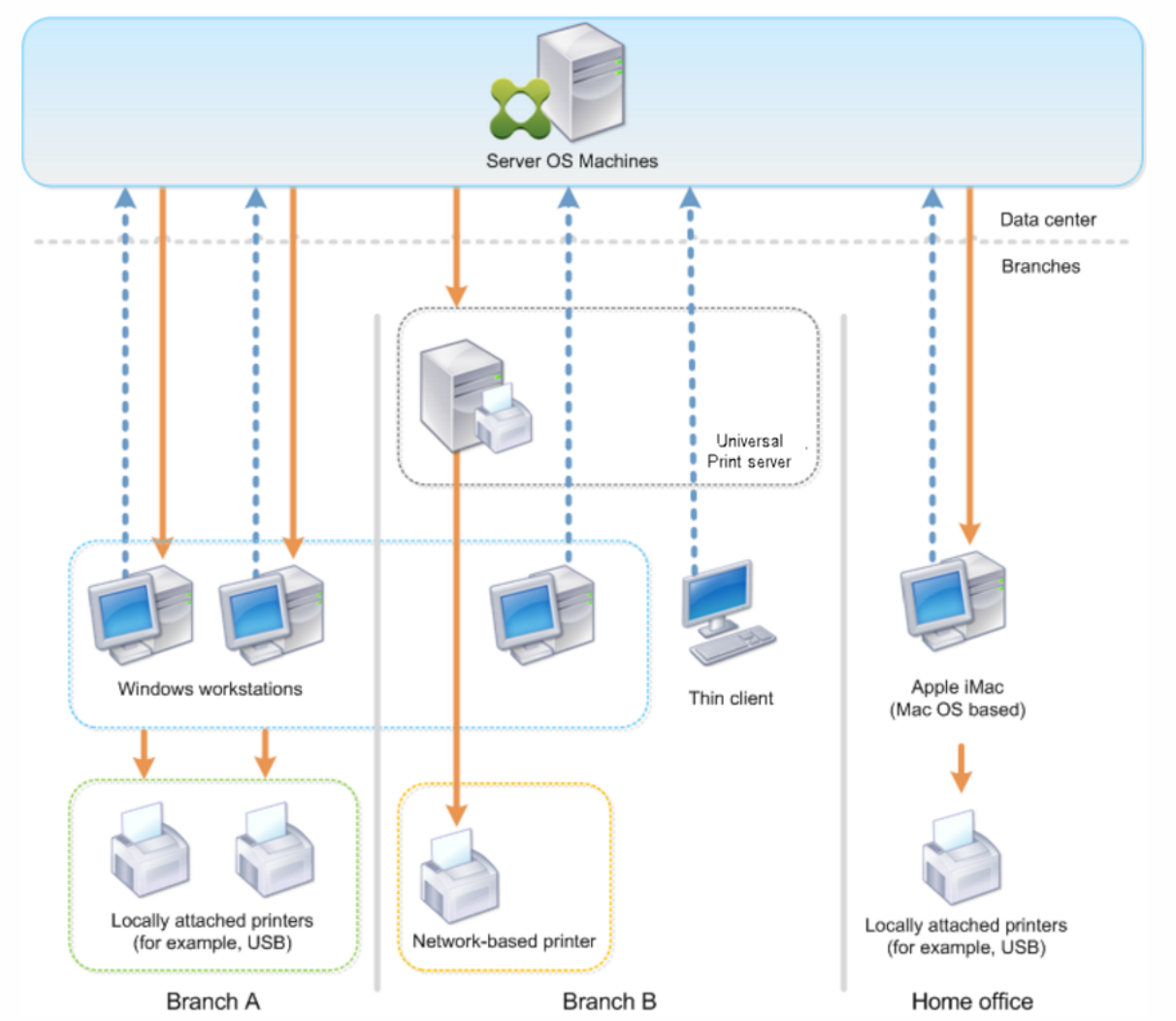
- 組織のセキュリティポリシー。人事部用のプリンターなど、特定のユーザー用に予約されたプリンターがあるかどうかを確認します。
- メインのワークステーションとは離れた場所で印刷するユーザーがいるかどうか。たとえば、複数のワークステーション間を移動しながら作業したり、出張先で印刷したりするユーザーがいるかどうかを確認します。

印刷環境を設計するにあたり、ユーザーがローカルのユーザーデバイス上で印刷する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標にします。

印刷展開の例

次の図は、以下の環境での印刷展開を示しています。

- 支社 **A** - 数台の Windows ワークステーションがある海外の小さなブランチオフィス。すべてのユーザーワークステーションは共有されていないプリンターにローカルで接続されています。
- 支社 **B** - シンクライアントおよび Windows ベースのワークステーションが複数台ある大規模なブランチオフィス。効率を上げるため、この支社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。支社内に置かれている 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

ブランチオフィス 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いるため、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ことなく、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仮想アプリケーションのセッションでも使用できます。

Citrix ユニバーサルプリントサーバー

ブランチオフィス 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 ユニバーサルプリントサーバーが最も効果的な構成になります。

必要なすべてのプリンタードライバーは、ローカルの管理者によりプリントサーバー上にインストールされて管理されます。ネットワーク上のプリンターは、以下のように仮想デスクトップやアプリケーションセッションにマップされます。

- Windows ベースのワークステーションの場合 - ローカルの IT チームの支援により、ユーザーの Windows ワークステーションを適切なネットワークプリンターに接続します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップやアプリケーションのセッションを開始すると、ローカルで構成されたプリンターがセッション内で自動作成されます。仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix ユニバーサルプリントサーバーコンポーネントが構成されているため、ネイティブのプリンタードライバーは不要です。ドライバーをアップデートしたりプリンターキューを変更したりしても、データセンターで何らかの構成を行う必要はありません。

- シンクライアントの場合 - シンクライアントデバイスのユーザーは、仮想デスクトップやアプリケーションのセッション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、シンクライアントのサブセットまたは名前に基づいてポリシーが適用されるように構成します。この構成は「近接プリンター機能」と呼ばれ、ローカルプリンタードライバーのメンテナンスを委任管理モデルに基づいて実行できます。

  プリンターキューを変更または追加する必要がある場合は、Citrix 管理者が環境内でそれぞれの［セッションプリンター］設定を変更する必要があります。

ネットワーク印刷トラフィックは ICA 仮想チャネルの外側で送信されるため、サービス品質（QoS）が実装されます。ICA/HDX トラフィックにより使用されるポート上の送受信ネットワークトラフィックは、ほかのすべてのネットワークトラフィックよりも優先されます。この構成により、大きな印刷ジョブがユーザーセッションに影響を及ぼすことがなくなります。

自動作成されるクライアントプリンターと **Citrix** ユニバーサルプリンタードライバー

ユーザーが自宅で非標準的なワークステーションを使用し、管理されていない印刷装置を使用する場合、ユニバーサルプリンタードライバーを使用してクライアントプリンターを自動作成する構成が最適です。

展開の要約

要約すると、展開例は以下のように構成されています。

- サーバー OS マシン上にはプリンタードライバーがインストールされていません。Citrix ユニバーサルプリンタードライバーのみを使用します。ネイティブのプリンタードライバーへのフォールバックおよびプリンタードライバーの自動インストールは無効です。
- すべてのクライアントプリンターを自動作成するためのポリシーがすべてのユーザーに適用されます。サーバー OS マシンはデフォルトでプリントサーバーに直接アクセスします。必要な構成タスクは、ユニバーサルプリントサーバーコンポーネントの有効化のみです。
- ブランチオフィス B の各階に個別の［セッションプリンター］設定が構成されており、その階のすべてのシンクライアントに適用されます。
- 支社 B には QoS が実装され、優れたユーザーエクスペリエンスが提供されています。

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

August 24, 2021

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 ユニバーサルプリントサーバーを使用します。
- 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。

- ユニバーサルプリントサーバーが無効になります。
- 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。印刷ジョブをネットワーク上に送信できない場合は、ユーザーコンピューターを介して転送されます（リダイレクトされるクライアント印刷ジョブ）。

  この動作は、Citrix ポリシーの［プリントサーバーへの直接接続］設定で［無効］を選択した場合と同等です。

- デフォルトでは、印刷プロパティ（ユーザーの印刷設定とデバイス設定）はユーザーデバイス上に格納されます。クライアント側でこの処理がサポートされない場合、サーバー OS マシン上のユーザープロファイルに印刷プロパティが格納されます。

  この動作は、Citrix ポリシーの［プリンタープロパティの保存］設定で［クライアントに保存できない場合にのみユーザープロファイルに保存する］を選択した場合と同等です。

- セッション内でプリンターが自動作成されるときに、そのサーバー OS マシン上にインストールされている Windows バージョンのプリンタードライバーが使用されます。適切なドライバーがインストールされていない場合、Windows オペレーティングシステムからドライバーがインストールされます。Windows オペレーティングシステムから適切なドライバーをインストールできない場合、Citrix ユニバーサルプリンタードライバーが使用されます。

  この動作は、Citrix ポリシーの［付属のプリンタードライバーの自動インストール］設定で［有効］を選択し、［ユニバーサル印刷］設定で［要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する］を選択した場合と同等です。

  ただし、［付属のプリンタードライバーの自動インストール］を有効にすると、必要以上に多くのプリンタードライバーがインストールされる可能性があります。

注：印刷に関するデフォルト設定を確認するには、新しい Citrix ポリシーを作成し、印刷に関するすべての設定項目で［デフォルト値を使用する］チェックボックスをオンにします。これにより、デフォルトの設定が適用されます。

Always-On ログ

VDA にはプリントサーバーおよび印刷サブシステムのための Always-On ログ機能があります。

ログを ZIP としてまとめてメールで送信、または自動的に Citrix Insight Services にアップロードするには、**Start-TelemetryUpload**PowerShell コマンドレットを使用します。

印刷に関するポリシーと設定

August 24, 2021

Citrix ポリシーでは、ユーザーが公開アプリケーションからプリンターにアクセスするときの以下の動作を制御できます。

- どのようにプリンターを提供するか（どのようにセッションに追加するか）
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーをどのように管理するか

Citrix ポリシーでは、ユーザーが使用するユーザーデバイスやユーザーアカウントなどの条件に応じて、異なる印刷環境を構成できます。

印刷機能の多くは、Citrix の「印刷のポリシー設定」で設定できます。印刷の設定は、Citrix ポリシーの標準的な動作に基づいて適用されます。

プリンター設定は、セッション終了時にプリンターオブジェクトまたは（ユーザーのネットワークアカウントに適切な権限がある場合は）クライアントの印刷装置に格納されます。Citrix Receiver のデフォルトでは、プリンターオブジェクトに格納された設定がまずチェックされ、見つからない場合はほかの場所に格納されている設定が使用されます。

デフォルトでは、ユーザーデバイス（デバイスがこれをサポートする場合）またはサーバー OS マシン上のユーザープロファイルにプリンターのプロパティが格納（または保持）されます。セッションでの作業中にユーザーがプリンターのプロパティを変更すると、その内容はそのマシン上のユーザープロファイルに反映されます。ユーザーがそのマシンに再ログオンしたり再接続したりすると、ユーザープロファイルに保持されたプロパティがユーザーデバイスに継承されます。つまり、ユーザーデバイス上のプリンタープロパティの変更は、ユーザーの次回ログオン時まで反映されません。

印刷設定の場所

Windows の印刷環境では、印刷設定に対する変更をローカルコンピューターに格納したり、ドキュメントファイルに格納したりできます。この環境では、ユーザーが変更した印刷設定を以下の場所に格納できます。

- ユーザーデバイス上 - Windows ユーザーは、ユーザーデバイス側の印刷設定を自分で変更できます。これを行うには、コントロールパネルでプリンターを右クリックして、［印刷設定］を選択します。たとえば、印刷の方向として［横］を選択すると、そのプリンターのデフォルトの方向として横向きが設定されます。
- ドキュメント内 - ワードプロセッサやデスクトップパブリッシングのプログラムでは、印刷の向きなどのドキュメント設定はそのドキュメントファイル内に格納されます。たとえば、Microsoft Word ドキュメントを印刷キューに送ると、ユーザーが指定した印刷の向きやプリンター名などの印刷設定がそのドキュメントファイル内に格納されます。これらのオプションは、次回そのドキュメントを印刷するときのデフォルト設定として表示されます。
- セッションでのユーザーによる変更 - 自動作成されたプリンターでは、ユーザーがセッション内のコントロールパネルで変更したオプション、つまりサーバー OS マシン上で変更されたオプションだけが保持されます。
- サーバー **OS** マシン上 - サーバー OS マシン上の特定のプリンタードライバーに対するデフォルト設定は、そのマシン上に格納されます。

Windows ベースの環境で保持される設定は、ユーザーがどのようにその設定を変更したかにより異なります。つまり、スプレッドシートプログラムなどに表示される印刷設定が、ドキュメントなどほかの場所に格納されている設定と異なることがあります。この結果、特定のプリンターに適用される設定は、セッション内で変化することがあります。

ユーザーの印刷設定の階層構造

印刷に関するユーザー設定はさまざまな場所に格納されるため、特定の優先順位でそれらの設定が処理されます。また、デバイス設定はドキュメント設定とは区別され、より優先されることに注意してください。

デフォルトでは、ユーザーがセッション内で変更したすべての印刷設定、つまり保持された設定が適用され、その後でその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

August 24, 2021

Citrix ユニバーサルプリントサーバー

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。

- ユニバーサルプリントサーバーにより提供されるイメージとフォントのキャッシュ、高度圧縮、最適化、QoS サポートなどの機能は、Windows の印刷プロバイダーでは提供されません。
- ユニバーサルプリンタードライバーでは、Microsoft によって定義されているパブリックな非デバイス依存の設定がサポートされます。ユーザーがプリンターの製造元固有のデバイス設定を使用する必要がある場合は、ユニバーサルプリントサーバーと Windows ネイティブドライバーの両方を提供します。この構成では、ユニバーサルプリントサーバーの長所を維持したままでユーザーに特殊なプリンター機能へのアクセスが提供されます。ここで考慮すべきことは、Windows ネイティブドライバーではメンテナンスが必要になるということです。
- Citrix ユニバーサルプリントサーバーは、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。ユニバーサルプリントサーバーではユニバーサルプリンタードライバーが使用されます。このドライバーはサーバー OS マシン上の単一のドライバーで、シンクライアントやタブレットを含むあらゆるデバイスからのローカル印刷またはネットワーク印刷が可能になります。

ユニバーサルプリントサーバーを Windows ネイティブドライバーと一緒に使うには、ユニバーサルプリントサーバーを有効にします。デフォルトでは、Windows ネイティブドライバーが使用可能な場合はそれが使用されます。使

用できない場合は、ユニバーサルプリンタードライバーが使用されます。Windows ネイティブドライバーのみ、またはユニバーサルプリンタードライバーのみを使用するなど、ユニバーサル印刷機能の動作を変更するには、ポリシーの［ユニバーサル印刷の使用］設定を使用します。

ユニバーサルプリントサーバーのインストール

ユニバーサルプリントサーバーを使用するには、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。詳しくは、「コアコンポーネントのインストール」および「コマンドラインを使ったインストール」を参照してください。

XenApp 6.5 など、UPClient コンポーネントを別個に展開する環境の場合:

1. Windows デスクトップ OS または Windows サーバー OS 用の XenApp および XenDesktop Virtual Delivery Agent（VDA）スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使ったインストール」の説明に従って、コマンドラインを使って VDA を展開します。
3. \Image-Full\Support\VcRedist_2013_RTM から前提条件をインストールします
    - Vcredist_x64 / vcredist_x86
        - 32 ビット展開に対しては x86 のみ、64 ビット展開に対しては両方を実行
4. \Image-Full\x64\Virtual Desktop Components または\Image-Full\x86\Virtual Desktop Components から、cdf の必須コンポーネント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。

ユニバーサルプリントサーバーの **CEIP** からの登録解除

ユニバーサルプリントサーバー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、**HKEY_LOCAL_MACHINE\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、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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。

ユニバーサルプリントサーバーの構成

以下の Citrix ポリシー設定を使用してユニバーサルプリントサーバーを構成します。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。

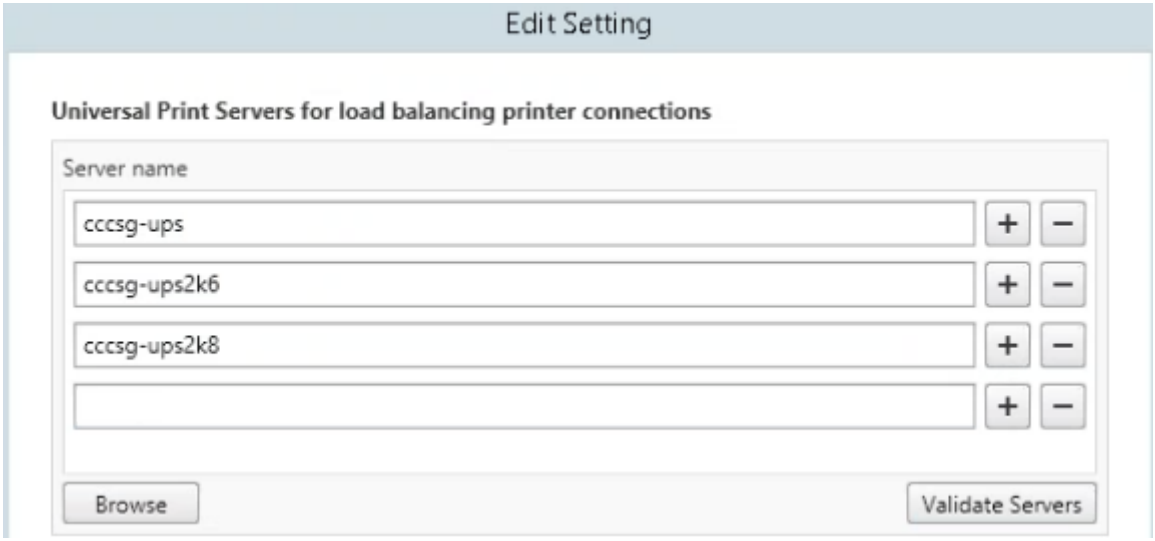
- ユニバーサルプリントサーバーの有効化。ユニバーサルプリントサーバーはデフォルトでは無効になっています。ユニバーサルプリントサーバーを有効にする場合、ユニバーサルプリントサーバーを使用できないときに Windows 印刷プロバイダーにフォールバックするかどうかを選択できます。ユニバーサルプリントサーバーを有効にすると、Windows 印刷プロバイダーと Citrix プロバイダーのインターフェイスを介してネットワークプリンターを追加して列挙できます。
- ユニバーサルプリントサーバー印刷データストリーム（**CGP**）ポート。ユニバーサルプリントサーバー印刷データストリーム CGP（Common 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。
- ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）ポート。ユニバーサルプリントサーバー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 へのユニバーサルプリントサーバー通信用の 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、ユニバーサルプリントサーバー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:<portnumber>

このポート番号は、Studio で HDX ポリシー、ユニバーサルプリントサーバー Web サービス（HTTP/SOAP）ポートと一致する必要があります。

- ユニバーサルプリントサーバー入力データストリームの最大帯域幅（**Kbps**）。各印刷ジョブからユニバーサルプリントサーバーに 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ユニバーサルプリントサーバー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。



- ユニバーサルプリントサーバーのサービス停止のしきい値。ロードバランサーが、反応しないプリントサーバーの復旧を待機する時間を指定します。タイムアウト後、ロードバランサーはそのサーバーが永続的にオフラインであると判定し、その負荷をほかの利用可能なプリントサーバーに再分散します。デフォルト値は 180 秒です。

Delivery Controller で印刷ポリシーを変更した後、そのポリシーの変更が VDA に適用されるまでに数分かかることがあります

ほかのポリシー設定との相互作用 — ユニバーサルプリントサーバーは、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、ユニバーサルプリントサーバー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。

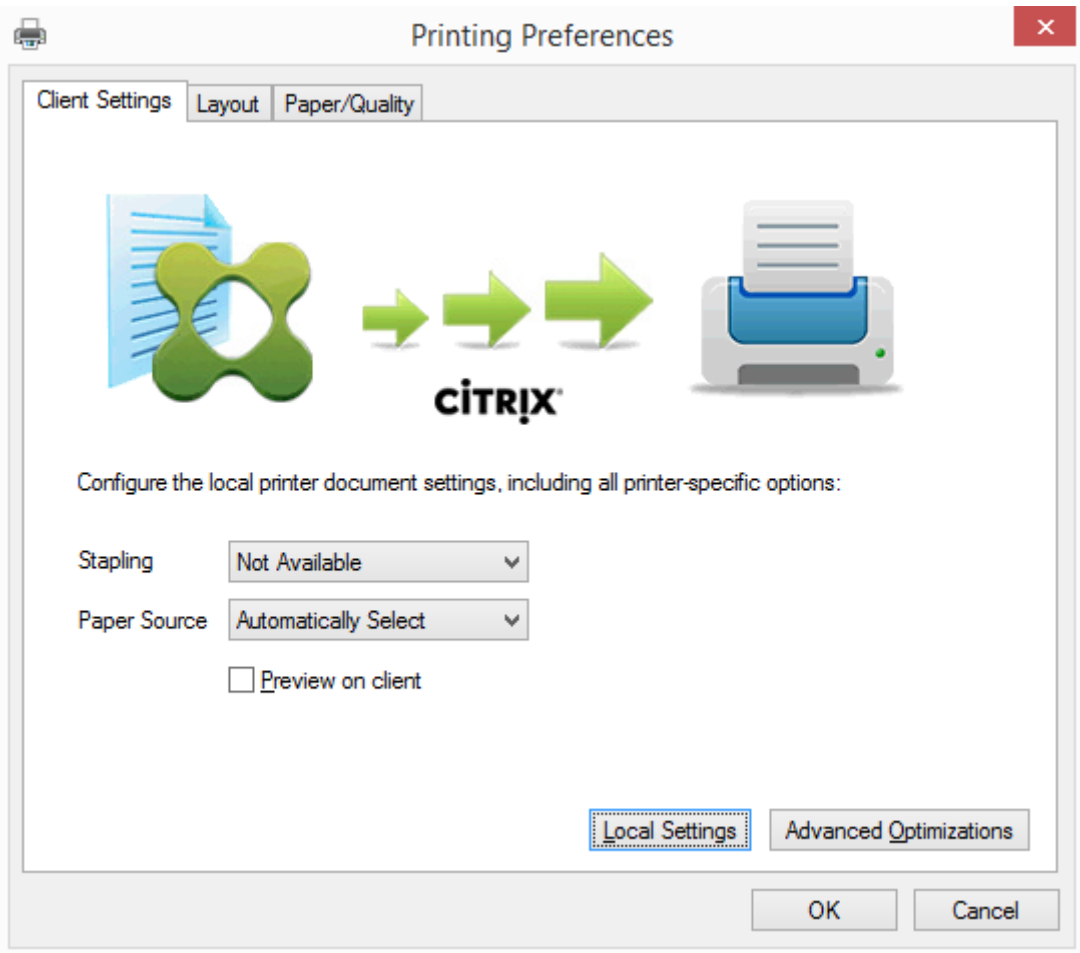
ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターを自動作成する	ユニバーサルプリントサーバーが有効な場合、ネイティブドライバーの代わりにユニバーサルプリンタードライバーを使ってクライアントネットワークプリンターが作成されます。ユーザー側には、同じプリンター名が表示されます。
セッションプリンター	Citrix ユニバーサルプリントサーバーソリューションを使用する場合、ユニバーサルプリンタードライバー関連のポリシー設定によりセッションプリンターが構成されます。
プリントサーバーへの直接接続	ユニバーサルプリントサーバーが有効で、［ユニバーサル印刷の使用］ポリシー設定で［ユニバーサル印刷のみを使用する］が構成されている場合、ユニバーサルプリンタードライバーでプリントサーバーに直接ネットワークプリンターの接続を作成できます。

ポリシー設定	相互作用
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 — ユニバーサルプリントサーバーにより使用される Citrix ユニバーサルプリンタードライバーにより、以下のユーザーインターフェイスコントロールが無効になります。

- ［プリンターのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタン
- ［ドキュメントのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタンおよび［クライアントでのプレビュー］ボタン

Citrix ユニバーサルプリンタードライバー（EMF および XPS ドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリ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。



ホチキス留めや安全な PIN などの非標準のプリンター設定を設定するには、Citrix UPD EMF または XPS ドライバーを使用するあらゆるクライアントマッピングされたプリンターに対して、カスタムの UPD 印刷ダイアログで［ロ

ーカル設定］を選択します。マップされたプリンターの［プリンターの設定］ダイアログがクライアント上のセッションの外部に表示されるので、ユーザーはあらゆるプリンターオプションを変更でき、アクティブなセッションでそのドキュメントを印刷する場合、変更されたプリンター設定が使用されます。

これらの機能は、ネイティブドライバーが Microsoft の印刷機能テクノロジを使用して利用可能としている場合にのみ、利用できます。ネイティブドライバーでは、印刷機能 XML で、標準化された印刷スキーマキーワードを使用する必要があります。標準化されていないキーワードを使用すると、Citrix のユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

ユニバーサルプリントサーバーを使用するときの Citrix 印刷プロバイダーのプリンターの追加ウィザードは、Windows 印刷プロバイダーのプリンターのものとほぼ同じです。ただし、以下の違いがあります。

- 名前またはアドレスを指定してプリンターを追加する場合、プリントサーバーの HTTP/SOAP ポート番号を指定できます。このポート番号は、プリンター名の一部として表示されます。
- Citrix ユニバーサルプリンタードライバーに関するポリシーでユニバーサル印刷が常に使用されるように設定すると、プリンターを選択するときにユニバーサルプリンタードライバー名が表示されます。Windows 印刷プロバイダーはユニバーサルプリンタードライバーを使用できません。

Citrix 印刷プロバイダーはクライアント側でのレンダリングをサポートしません。

ユニバーサルプリントサーバーについて詳しくは、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、リソース負荷が軽減され、ユーザーが高速にログオンできるようになります。ユニバーサルプリンターでは、クライアント側のあらゆる印刷装置を使用できます。

  Citrix ユニバーサルプリンターは、ユーザーが使用するユーザーデバイスや Citrix Receiver によっては正しく動作しない場合があります。Citrix ユニバーサルプリンターは Windows 環境で動作し、Citrix Offline Plug-in や、クライアント上にストリーム配信されるアプリケーションをサポートしません。このような環境では、クライアントプリンターの自動作成機能とユニバーサルプリンタードライバーの使用を検討してください。

  非 Windows Citrix Receiver のユーザーにユニバーサル印刷ソリューションを提供するには、自動的にインストールされる PostScript/PCL ベースのユニバーサルプリンタードライバーを使用してください。

- **Citrix** ユニバーサルプリンタードライバー - デバイスに依存しないプリンタードライバー。Citrix ユニバーサルプリンタードライバーを構成すると、デフォルトで EMF ベースのユニバーサルプリンタードライバーが使用されます。

  Citrix ユニバーサルプリンタードライバーによる印刷ジョブのサイズは、古いバージョンなどのプリンタードライバーのものよりも小さい場合があります。ただし、特殊なプリンターでの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 — 以下の Citrix ポリシー設定を使用してユニバーサル印刷を構成します。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。

- ユニバーサル印刷の使用：ユニバーサル印刷を使用する条件を指定します。
- 汎用ユニバーサルプリンターを自動作成する：ユニバーサル印刷と互換性があるユーザーデバイスが使用されたセッションで、汎用的な Citrix ユニバーサルプリンターオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。
- ユニバーサルドライバーの優先度：ユニバーサルプリンタードライバーの使用優先順位を指定します。一覧の上位にあるドライバーから順に使用されます。この一覧では、ドライバーを追加、編集、または削除したり、優先順位を変更したりできます。
- ユニバーサル印刷プレビューの設定：自動作成プリンターおよび汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷 EMF 処理モード：Windows ユーザーデバイス上での EMF スプールファイルの処理方法を制御します。デフォルトでは、EMF スプールファイルがクライアント上のスプールキューに直接挿入されます。これにより、EMF 形式の印刷を高速に実行でき、CPU リソースの消費も少なくなります。

ポリシーについて詳しくは、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色設定、両面印刷、部数などのデフォルト設定を変更する方法については、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最小限にするために、各セッションで特定のネットワークプリンターだけが作成されるように構成することができます。このようなプリンターをセッションプリンターと呼びます。

IP アドレスによりセッションプリンターポリシーをフィルターして、近接プリンター機能を提供できます。この機能を使用すると、ユーザーの IP アドレスの範囲に応じて、特定のネットワークプリンターが自動的に割り当てられるよ

うになります。近接プリンター機能は Citrix ユニバーサルプリントサーバーにより提供され、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 ユニバーサルプリントサーバーでは、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

August 24, 2021

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詳細にテストすることをお勧めします。

ユーザーがログオンすると、クライアントプリンタードライバーの互換性一覧がチェックされ、その後でクライアントプリンターがセットアップされます。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、ユニバーサルプリントサーバーとユニバーサルプリンタードライバーを使用します。以下のポリシー設定を構成して、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷最適化デフォルト：セッションで作成されるユニバーサルプリンターに適用されるデフォルト設定を指定します。
  - ［必要なイメージ品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを印刷できます。
  - ［ヘビーウェイト圧縮を有効にする］では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。デフォルトでは、ヘビーウェイト圧縮は無効になっています。

  - ［イメージおよびフォントのキャッシュ］では、印刷ストリームで使用されているイメージやフォントをキャッシュするかどうかを指定します。キャッシュを有効にすると、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。デフォルトでは、埋め込みイメージおよびフォントがキャッシュされます。
  - ［非管理者によるこれらの設定の変更を許可する］では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。デフォルトでは、禁止されています。
- ユニバーサル印刷イメージ圧縮制限：ユニバーサルプリンタードライバーでのイメージ印刷で使用できる品質レベルの上限を指定します。デフォルトでは、イメージ品質の上限が［最高品質（無損失圧縮）］に設定されています。
- ユニバーサル印刷品質制限：セッションでの印刷出力で使用できる最大 DPI 値（インチあたりのドット数）を指定します。デフォルトでは、DPI 値に上限はありません。

デフォルトでは、サーバー OS マシンからのすべての印刷ジョブがネットワークを介してプリントサーバーに直接転送されます。ネットワークで遅延が発生したり帯域幅に制限があったりする場合は、ICA 仮想チャネルでの印刷ジョブの送信を検討します。これを行うには、Citrix ポリシー設定の［プリントサーバーへの直接接続］設定で［無効］を選択します。ICA 仮想チャネルで送信されるデータは圧縮されるため、データが WAN を横断するときに消費される帯域幅が少なくなります。

印刷帯域幅を制限してセッションのパフォーマンスを改善する — サーバー OS マシンからユーザープリンターで印刷すると、帯域幅消費によりビデオなどほかの仮想チャネルのパフォーマンスが低下することがあります。この問題は、ユーザーが低速のネットワークを介してサーバーにアクセスする場合に顕著です。このような低下を防ぐために、ユーザープリンターでの印刷に使用される帯域幅を制限できます。転送される印刷データの量を制限すると、ビデオ、キーストローク、およびマウスデータ転送のため HDX データストリームで使用できる帯域幅が大きくなります。

重要：プリンター帯域幅の制限設定は、ほかのチャネルが使用されていない場合でも常に適用されます。

セッションでの印刷帯域幅制限を構成するには、
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ます。サイトでの制限を設定するには、Studio を使ってポリシーを構成します。個々のサーバーでの制限を設定するには、各サーバー OS マシン上でローカルの Windows グループポリシー管理コンソールを使ってポリシーを構成します。

- ［プリンターリダイレクトの最大帯域幅（Kbps）］設定で、印刷に使用される最大帯域幅をキロビット/秒（Kbps）で指定します。
- ［プリンターリダイレクトの最大帯域幅（%）］設定で、印刷に使用される最大帯域幅を、セッション全体に対する割合で指定します。

  注：［プリンターリダイレクトの最大帯域幅（%）］設定を使って帯域幅をパーセンテージで指定す る場合は、［セッション全体の最大帯域幅］設定で、セッション全体で使用可能な総帯域幅の最大 値をキロビット/秒（Kbps）
  で指定します。

  最大帯域幅を Kbps およびセッション全体に対する割合（%）で指定した場合、より高い制限（より低い値）の設定が適用されます。

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。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、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	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UAC が有効な場合、Microsoft 管理コンソール内にある［印刷の管理］スナップイン。UAC が無効な場合は、Windows 8 以前では［コントロールパネル］、Windows 8 では［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	UAC が有効な場合は Microsoft 管理コンソール内の［プリントサーバー］>［印刷の管理］スナップイン。UAC が無効な場合は［プリントサーバー］>［コントロールパネル］。

	印刷経路	場所
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	UAC が有効な場合、Microsoft 管理コンソール内にある［プリントサーバー］>［印刷の管理］スナップイン。UAC が無効な場合は、Windows 8 以前では［コントロールパネル］、Windows 8 では［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	UAC が有効な場合は［プリントサーバー］>［コントロールパネル］、UAC が無効な場合は［プリントサーバー］>［コントロールパネル］

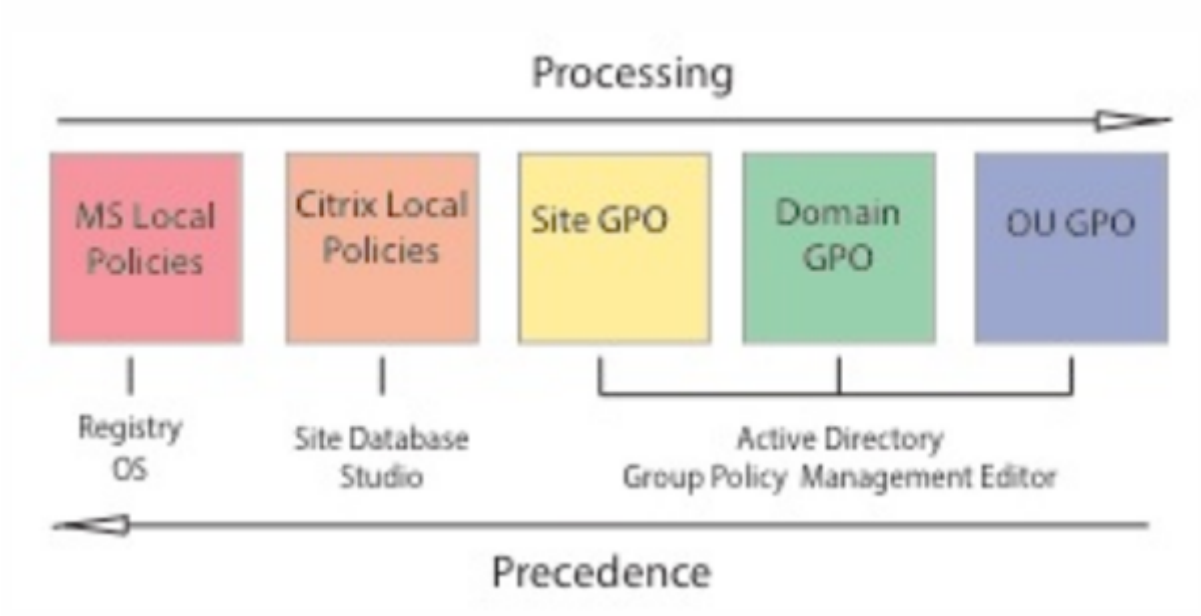
> 注:
>
> ネットワーク印刷経路で実行されたネットワークプリンターへの印刷キューは「プライベート」であり、システムで管理することはできません。

ポリシー

August 24, 2021

ポリシーは構成可能な設定項目をグループ化したもので、特定のユーザー、デバイス、または接続の種類に対して特定のセッション、帯域幅、およびセキュリティ構成が適用されるように制御する目的で使用します。

これらのポリシーは、特定の物理マシン、仮想マシン、またはユーザーに割り当てることができます。ユーザーに適用する場合、ローカルレベルのアカウントを指定したり Active Directory のセキュリティグループを指定したりできます。この構成では、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 コンソールで作成および管理され、サイトデータベースに格納されます。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）を使用して作成および管理され、Active Directory に格納されます。Microsoft ローカルポリシーは Windows 上で作成され、レジストリ内に格納されます。

Studio のモデル作成ウィザードを使用すると、複数のテンプレートやポリシーの設定項目とその構成内容を比較してポリシーの競合や重複を避けることができます。また、GPMC を使用して GPO を設定して、ネットワークのさまざまなレベルのユーザーにそれらを適用できます。

これらの GPO は Active Directory 内に保存され、セキュリティ上の理由から、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る。
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、グループの一部のメンバーで要件が異なるために一部の設定項目で例外が必要になることがあります。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。

ポリシーの使用

August 24, 2021

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、右側に次のタブが表示されます：［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）、［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）。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、右側に次のタブが表示されます：［説明］タブ（テンプレートの使用目的）、［設定］タブ（構成済みの設定項目の一覧）。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。

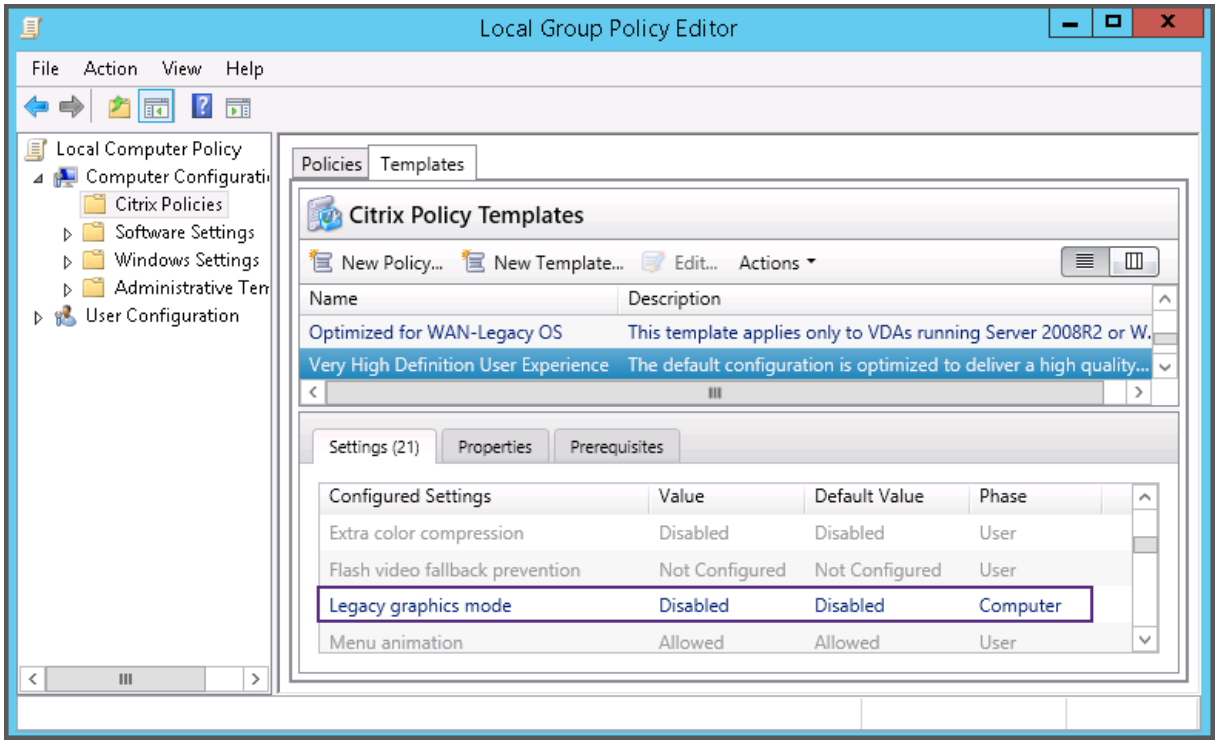
特定の製品バージョンや設定項目のカテゴリを選択することで、検索範囲を限定できます。すべての設定項目を検索対象にするには、［すべての設定］を選択します。

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

August 24, 2021

テンプレートは、事前定義された開始ポイントからポリシーを作成するためのソースです。組み込み Citrix テンプレートは、特定の環境またはネットワーク状況に対して最適化され、次のように使用できます。

- サイト間で共有する自分のポリシーおよびテンプレートを作成するためのソース。
- 結果を引用できるようになるため、展開環境間で結果をより簡単に比較するためのリファレンス。例: ””..when using Citrix template x or y..”
- テンプレートをインポートまたはエクスポートすることにより、Citrix サポートまたは信頼するサードパーティとポリシーを通信するための手段。

ポリシーテンプレートをインポートまたはエクスポートできます。追加のテンプレートと組み込みテンプレートの更新については、Citrix Knowledge Center のCTX202000を参照してください。

ポリシーの作成にテンプレートを使用するときの考慮事項については、CTX202330を参照してください。

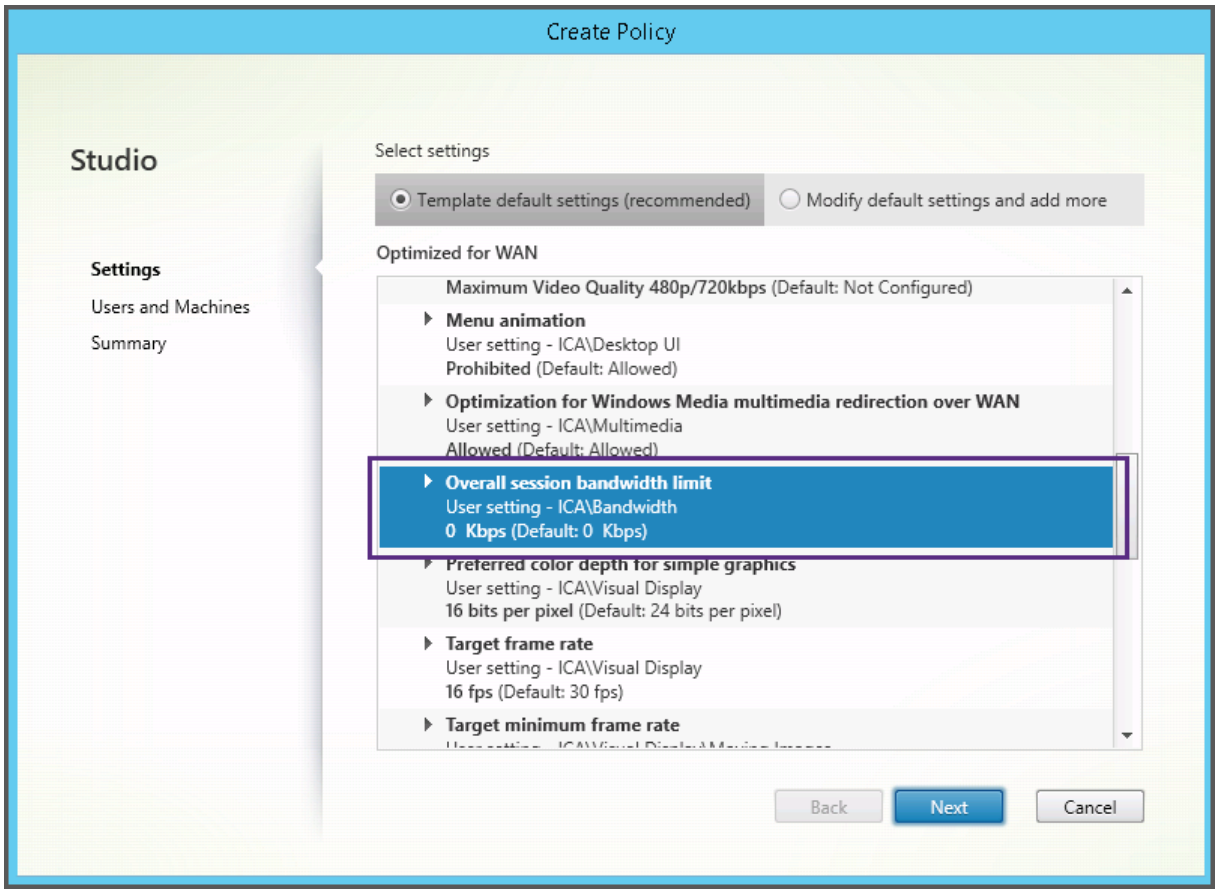
組み込みの **Citrix** テンプレート

使用できるポリシーテンプレートは以下のとおりです。

- 最高品位ユーザーエクスペリエンス。このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。
- 高サーバースケーラビリティ。サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増大させながら、良質のユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防ぎます。
- 高サーバースケーラビリティ **-** レガシ **OS**。この高サーバースケーラビリティテンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **NetScaler SD-WAN** に最適化。これは、NetScaler SD-WAN が展開されたブランチオフィスユーザーに適用して XenDesktop の配信を最適化するテンプレートです。(NetScaler SD-WAN は、CloudBridge の新しい名前です)。
- **WAN** の最適化。このテンプレートは、共有 WAN 接続を使用しているブランチオフィスや、低帯域幅接続を実行する遠隔地にいて、マルチメディアコンテンツがほとんどない視覚的に簡素なユーザーインターフェイスのアプリケーションにアクセスするタスクワーカーを対象としたものです。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。
- **WAN** の最適化 **-** レガシ **OS**。この WAN の最適化テンプレートは、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。
- 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。



XenApp および XenDesktop 7.6 FP3 より前のバージョン（ポリシー管理および VDA）を使用していて、高サーバースケーラビリティおよび WAN の最適化テンプレートを必要とする場合、これらのテンプレートを適用するときはそのレガシ OS バージョンを使用してください。

> 注
>
> 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で、［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。

タスク	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］を選択します。
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］をクリックします。
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］をクリックします。
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］の順に選択します。

タスク	手順
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］の順に選択します。
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］タブをクリックします。
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］タブをクリックします。
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［前提条件］タブをクリックします。

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

August 24, 2021

ポリシーを作成する前に、そのポリシーの適用先となるユーザーまたはデバイスのグループを決定します。ユーザーの担当業務、接続の種類、ユーザーデバイス、または作業場所に応じてポリシーを適用できます。または、Windows の Active Directory のグループポリシーと同じ基準を使用できます。

グループに適用するポリシーを作成済みの場合は、別のポリシーを作成するのではなく、既存のポリシーの設定内容を編集することを検討してください。特定の設定内容を変更するため、または特定のユーザーを適用対象から除外するためだけに新しいポリシーを作成することは避けてください。

既存のポリシーテンプレートを基に新しいポリシーを作成し、必要に応じて設定項目をカスタマイズします。または、テンプレートを使用せずにポリシーを作成して、必要な設定項目を選択して構成します。

Citrix Studio では、新しいポリシーを作成すると、［ポリシーの有効化］チェックボックスが明示的にオンになっていない限り［無効］に設定されます。

ポリシー設定

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のリダイレクト］設定で［禁止］を選択すると、［クライアント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 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 の場合：12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6 の場合：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。完全一致の場合、ClientABCName。使用するワイルドカード：Client*Name
デリバリーグループ	所属するデリバリーグループ。
デリバリーグループの種類	実行されるデスクトップまたはアプリケーションの種類。プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーションから選択します。
組織単位（OU）	組織単位。
タグ	マシンのタグ。注：タグを使用する場合にポリシーを確実に正しく適用するには、CTX142439から Hotfix を入手してインストールしてください。
ユーザーまたはグループ	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

は優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。たとえば、優先度の高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーの同じ設定で［有効］が選択されていても、その設定には［無効］が適用されます。構成されていないポリシー設定は無視されます。

重要：グループポリシー管理コンソールを使って Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当ておよび設定が意図したとおりに適用されない場合があります。詳しくは、CTX127461を参照してください。

「Unfiltered」という名前のポリシーはデフォルトで提供されています。

- Studio を使用して Citrix ポリシーを管理する場合は、Unfiltered ポリシーに追加する設定がそのサイトのすべてのサーバー、仮想デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合は、そのポリシーのグループポリシーオブジェクト（GPO）スコープに属するすべてのサイトおよび接続に Unfiltered ポリシーの設定が適用されます。たとえば、営業部署の組織単位に大阪支社のすべての営業メンバーを含んでいる Sales-OSK という GPO がある場合に、いくつかのユーザーポリシー設定を追加した Unfiltered ポリシーを Sales-OSK に設定します。ここで大阪支社の営業部長がサイトにログオンすると、この部長は Sales-OSK GPO のメンバーなので、Unfiltered ポリシーのすべての設定がセッションに適用されます。

割り当ての［モード］によっても、そのポリシーの適用先が異なります。割り当てのモードとして
［許可］（デフォルト）が設定されている場合、その割り当て条件にマッチした接続にのみポリシーが適用されます。割り当てのモードとして
［拒否］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 2 つ追加し、一方を［許可］にしてもう一方を［拒否］にした場合、［拒否］を設定した割り当てが優先されます。例：

  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、［拒否］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［拒否］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。例：

  Policy 2 に以下の割り当てを追加します：

  - Assignment C は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てで、［許可］を設定します。
  - Assignment D は 10.8.169.*（企業ネットワーク）を指定するクライアント IP アドレス割り当てです。モードは［許可］に設定されます。

ここで営業部長が社内のオフィスからログオンした場合、上記 2 つの割り当てに合致するので、この Policy 2 が適用されます。

Policy 3 に以下の割り当てを追加します:

- Assignment E は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てで、［許可］を設定します。
- Assignment F は特定の NetScaler Gateway 接続に適用される［アクセス制御］割り当てで、［許可］を設定します。

ここで営業部長が社内のオフィスからログオンした場合、Assignment F に合致しないので、この Policy 3 は適用されません。

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で、［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。

タスク	手順
新しいポリシーの作成	［ポリシー］タブの［新規］をクリックします。
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］をクリックします。
既存のポリシーの優先度を変更する	［ポリシー］タブでポリシーを選択して［上げる］または［下げる］をクリックします。
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］タブをクリックします。
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］タブをクリックします。
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］タブをクリックします。
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］の順に選択します。
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］をクリックします。

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

August 24, 2021

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、［Secure ICA の最低暗号化レベル］設定やアプリケーションやデスクトップごとに指定されている配信設定は無視されます。

たとえば、デリバリーグループを作成するときに指定する暗号化レベルは、その環境全体に対して設定されているレベルと同じである必要があります。

注：ダブルホップ環境における 2 つ目のホップにおいて、デスクトップ OS の VDA がサーバー OS の VDA に接続すると、デスクトップ OS の VDA 上の Citrix ポリシーがユーザーデバイスのように機能します。たとえば、ユーザーデバイス上のイメージをキャッシュするようポリシーが設定されると、ダブルホップ環境における 2 つ目のホップに対してキャッシュされたイメージはデスクトップ OS の VDA マシンでキャッシュされます。

ポリシーおよびテンプレートの比較

Studio では、複数のポリシーやポリシーテンプレートの設定項目を比較することができます。たとえば、環境に適した設定項目が構成されているかどうかを確認するときに、この機能を使用できます。また、そのポリシーやテンプレートの各設定項目の設定値を、デフォルトの値と比較することもできます。

1. Studio のナビゲーションペインで［ポリシー］を選択します。

2. ［比較］タブをクリックし、［選択］をクリックします。
3. 比較するポリシーまたはテンプレートのチェックボックスをオンにします。［設定項目のデフォルト値と比較する］チェックボックスをオンにすると、各設定項目のデフォルト値が比較結果に追加されます。
4. ［比較］をクリックすると、構成された設定項目とその設定値が一覧表示されます。
5. すべての設定項目を表示するには、［すべての設定項目を表示］を選択します。元の表示に戻るには、［共通の設定項目を表示］を選択します。

ポリシーの優先度

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［拒否］を選択します。

割り当てのモードとして［拒否］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［拒否］モードを選択

この 2 つのフィルターが設定されたポリシーは、Assignment A で指定した範囲の IP アドレスを持つサイトにログオンするすべてのユーザーに適用されます。ただし、Assignment B で指定したユーザーアカウントを使用してこの

サイトにログオンするユーザーには、IP アドレスが Assignment A で指定した範囲内であってもこのポリシーは適用されません。

接続に適用されるポリシーの確認

複数のポリシーが適用されるために、意図した設定が接続に反映されないことがあります。作成したポリシーよりも優先度の高いポリシーがあると、意図した設定内容が上書きされてしまいます。管理者は、ポリシーの優先度や追加されている設定項目を基に、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

August 24, 2021

次の表は、ポリシーの各設定項目のデフォルト設定と、適用される Virtual Delivery Agent（VDA）のバージョンの一覧です。

ICA

名前	デフォルト設定	VDA
クライアントクリップボードリダイレクト	許可	すべてのバージョンの VDA
デスクトップの起動	禁止	VDA for Server OS 7 以降
EDT	無効	VDA 7.13。「アダプティブトランスポート」を参照してください。
ICA リスナー接続タイムアウト	120,000 ミリ秒	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
ICA リスナーポートの番号	1494	すべてのバージョンの VDA
クライアント接続での非公開アプリケーションの起動	禁止	VDA for Server OS 7 以降

名前	デフォルト設定	VDA
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

名前	デフォルト設定	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	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。
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	0Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、および VDA for Desktop OS 7 以降

名前	デフォルト設定	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（%）	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
デスクトップコンポジションリダイレクトの画質	Medium	VDA 5.6、VDA for Desktop OS 7 以降
デスクトップの壁紙	許可	すべてのバージョンの VDA
メニューをアニメーション化する	許可	すべてのバージョンの VDA
ドラッグ中にウィンドウの内容を表示する	許可	すべてのバージョンの VDA

ICA/エンドユーザーモニタリング

名前	デフォルト設定	VDA
ICA 往復測定	有効	すべてのバージョンの VDA
ICA 往復測定間隔	15 秒	すべてのバージョンの VDA
アイドル接続の ICA 往復測定	無効	すべてのバージョンの VDA

ICA/デスクトップエクスペリエンス拡張

名前	デフォルト設定	VDA
拡張デスクトップエクスペリエンス	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

名前	デフォルト設定	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
クライアント側リムーバブルドライブ	許可	すべてのバージョンの VDA
ホストからクライアントへのリダイレクト	無効	VDA for Server OS 7 以降
クライアント側のドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
クライアント側ドライブへの読み取り専用アクセス	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
ユーザーフォルダーのリダイレクト	許可	Web Interface 環境でのみ。VDA for Server OS 7 以降
非同期書き込みを使用する	無効	すべてのバージョンの VDA

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的無損失の圧縮を使用する	無効	VDA 7.6 以降
表示メモリの制限	65536KB	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
メモリが不足したときの表示モード	色数を下げる	すべてのバージョンの VDA
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

名前	デフォルト設定	VDA
従来のグラフィックモード	無効	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	無効	VDA for Server OS 7 以降
キューイメージの破棄	有効	すべてのバージョンの VDA
圧縮にビデオコーデックを使用する	選択された場合ビデオコーデックを使用する	VDA 7.6 FP3 以降
ビデオコーデックにハードウェアエンコーディングを使用します	有効	VDA 7.11 以降

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
固定キャッシュしきい値	3000000bps	VDA for Server OS 7 以降

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawk ディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawk 表示チャネルポートの範囲	3224、3324	VDA 7.6 FP2 以降

ICA/Keep-Alive

名前	デフォルト設定	VDA
ICA Keep-Alive タイムアウト	60 秒	すべてのバージョンの VDA
ICA Keep-Alive	ICA Keep-Alive メッセージを送信しない	すべてのバージョンの VDA

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリ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。この設定は無効になっており、Windows 10 および Windows Server 2016 マシンでは使用できません。
コンボボックスをデバイス側で表示する	禁止	VDA 5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5 ビデオリダイレクト	禁止	VDA 7.12 以降
ビデオ品質の制限	未構成	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
マルチメディア会議	許可	すべてのバージョンの VDA

名前	デフォルト設定	VDA
WAN 接続での Windows Media マルチメディアリダイレクトの最適化	許可	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
WAN 接続での Windows Media マルチメディアリダイレクトでの GPU の使用	禁止	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
Windows メディアフォールバック防止	未構成	VDA 7.6 FP3 以降
Windows Media のクライアント側でのコンテンツ取得	許可	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
Windows Media リダイレクト	許可	すべてのバージョンの VDA
Windows Media リダイレクトのバッファーサイズ	5 秒	VDA 5、5.5、5.6 FP1
Windows Media リダイレクトのバッファーサイズ使用	無効	VDA 5、5.5、5.6 FP1

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP を使用したオーディオ	許可	VDA for Server OS 7 以降
オーディオ UDP ポートの範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
マルチポートポリシー	プライマリポート（2598）に優先度［高］	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアント COM ポートを自動接続する	無効	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
クライアント LPT ポートを自動接続する	無効	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
クライアント COM ポートリダイレクト	禁止	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
クライアント LPT ポートリダイレクト	禁止	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのバージョンの VDA
デフォルトプリンター	クライアントのメインプリンターをデフォルトに設定する	すべてのバージョンの VDA
プリンター割り当て	ユーザーの現在のプリンター	すべてのバージョンの VDA
プリンター自動作成イベントログの設定	エラーおよび警告をログに記録する	すべてのバージョンの VDA
セッションプリンター	プリンターの指定なし	すべてのバージョンの VDA
プリンターの自動作成を待機する (デスクトップ)	無効	すべてのバージョンの VDA

ICA/印刷**/**クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成する	すべてのクライアントプリンターを自動作成する	すべてのバージョンの VDA
汎用ユニバーサルプリンターを自動作成する	無効	すべてのバージョンの VDA
クライアントプリンター名	標準のプリンター名	すべてのバージョンの VDA
プリントサーバーへの直接接続	有効	すべてのバージョンの VDA
プリンタードライバーのマッピングと互換性	規則の指定なし	すべてのバージョンの VDA
プリンタープロパティの保存	クライアントに保存できない場合にのみユーザープロファイルに保存する	すべてのバージョンの VDA
クライアントプリンターの保持と復元	許可	VDA 5、5,5、5.6 FP1

ICA/印刷/ドライバー

名前	デフォルト設定	VDA
付属のプリンタードライバーの自動インストール	有効	すべてのバージョンの VDA
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/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーの有効化	無効	すべてのバージョンの VDA
ユニバーサルプリントサーバー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

名前	デフォルト設定	VDA
ユニバーサルプリントサーバー入力データストリームの最大帯域幅（Kpbs）	0	すべてのバージョンの VDA
ユニバーサルプリントサーバー 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、ヘビーウエイト圧縮を有効にする =False。画像と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 =True、埋め込みフォントのキャッシュを許可する =True。非管理者によるこれらの設定の変更を許可する =False。	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の VDA

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICA の最低暗号化レベル	基本	VDA for Server OS 7 以降

ICA/サーバーの制限

名前	デフォルト設定	VDA
サーバーのアイドルタイマーの間隔	0 ミリ秒	VDA for Server OS 7 以降

ICA/セッションの制限

名前	デフォルト設定	VDA
切断セッションタイマー	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
切断セッションタイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
セッション接続タイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降
セッションアイドルタイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 以降

ICA/セッション画面の保持

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

名前	デフォルト設定	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	Medium	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

ICA/USB デバイス

名前	デフォルト設定	VDA
クライアント USB デバイス最適化規則	有効（VDA 7.6 FP3 以降）、無効（VDA 7.11 以降）デフォルトでは、規則は指定されていません。	VDA 7.6 FP3 以降
クライアント USB デバイスリダイレクト	禁止	すべてのバージョンの VDA
クライアント USB デバイスリダイレクト規則	規則の指定なし	すべてのバージョンの VDA

名前	デフォルト設定	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
単純なグラフィックスの優先色深度	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	Medium	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	Normal	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
動画圧縮	有効	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
プログレッシブ圧縮のレベル	なし	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
プログレッシブ圧縮のしきい値	2147483647Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
保持する最低フレーム数	10fps	VDA 5.5、5.6 FP1、VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

ICA/視覚表示**/**静止画

名前	デフォルト設定	VDA
エクストラ色圧縮	無効	すべてのバージョンの VDA
エクストラ色圧縮しきい値	8192Kbps	すべてのバージョンの VDA
ヘビーウェイト圧縮	無効	すべてのバージョンの VDA
非可逆圧縮のレベル	Medium	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	無効	VDA for Server OS 7 以降
CPU 使用率から除外するプロセスの優先順位	通常以下および低	VDA for Server OS 7 以降
ディスク使用率	無効	VDA for Server OS 7 以降
最大セッション数	250	VDA for Server OS 7 以降
メモリ使用率	無効	VDA for Server OS 7 以降
基本メモリ使用量	負荷なし：768MB	VDA for Server OS 7 以降

Profile Management/上級設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのバージョンの VDA
問題が発生する場合にユーザーをログオフ	無効	すべてのバージョンの VDA
ロックされたファイルにアクセスする場合の試行数	5	すべてのバージョンの VDA
ログオフ時にインターネット Cookie ファイルを処理	無効	すべてのバージョンの VDA

Profile Management/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのバージョンの VDA
Profile Management の有効化	無効	すべてのバージョンの VDA
除外グループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA
オフラインプロファイルサポート	無効	すべてのバージョンの VDA
ユーザーストアへのパス	Windows	すべてのバージョンの VDA
ローカル管理者のログオン処理	無効	すべてのバージョンの VDA
処理済みグループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA

Profile Management/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。[処理済みグループ] で指定したすべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA
クロスプラットフォーム設定の有効化	無効	すべてのバージョンの VDA
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのバージョンの VDA

名前	デフォルト設定	VDA
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CM が使用されます。	すべてのバージョンの VDA
クロスプラットフォーム設定を作成するためのソース	無効	すべてのバージョンの VDA

Profile Management/ファイルシステム**/**除外

名前	デフォルト設定	VDA
除外の一覧 - ディレクトリ	無効。ユーザープロファイルのすべてのフォルダーが同期されます。	すべてのバージョンの VDA
除外の一覧 - ファイル	無効。ユーザープロファイルのすべてのファイルが同期されます。	すべてのバージョンの VDA

Profile Management/ファイルシステム**/**同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのバージョンの VDA
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのバージョンの VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可	無効	すべてのバージョンの VDA
ドメイン名を包含	無効	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/AppData**（**Roaming**）

名前	デフォルト設定	VDA
AppData（Roaming）パス	無効。パスは指定されていません。	すべてのバージョンの VDA
AppData(Roaming) のリダイレクト設定	[AppData（Roaming）パス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**アドレス帳

名前	デフォルト設定	VDA
アドレス帳パス	無効。パスは指定されていません。	すべてのバージョンの VDA
アドレス帳のリダイレクト設定	［アドレス帳パス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**デスクトップ

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

名前	デフォルト設定	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

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	無効	すべてのバージョンの VDA
一般的な情報	無効	すべてのバージョンの VDA
一般的な警告	無効	すべてのバージョンの VDA
ログの有効化	無効	すべてのバージョンの VDA
ファイルシステム操作	無効	すべてのバージョンの VDA
ファイルシステム通知	無効	すべてのバージョンの VDA
ログオフ	無効	すべてのバージョンの VDA
ログオン	無効	すべてのバージョンの VDA
ログファイルの最大サイズ	1048576	すべてのバージョンの VDA
ログファイルへのパス	無効。%System-Root%\System32\Logfiles\UserProfileManager に生成されます	すべてのバージョンの VDA
個人用ユーザー情報	無効	すべてのバージョンの VDA
ログオンおよびログオフ時のポリシー値	無効	すべてのバージョンの VDA
レジストリ操作	無効	すべてのバージョンの VDA
ログオフ時のレジストリ差分	無効	すべてのバージョンの VDA

Profile Management/プロファイル制御

名前	デフォルト設定	VDA
キャッシュしたプロファイルを削除する前の待ち時間	0	すべてのバージョンの VDA
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	すべてのバージョンの VDA
ローカルプロファイル競合の制御	ローカルプロファイルを使用	すべてのバージョンの VDA
既存のプロファイルの移行	ローカルおよび移動	すべてのバージョンの VDA

名前	デフォルト設定	VDA
テンプレートプロファイルへのパス	無効。ユーザーが最初にログオンするコンピューター上のデフォルトのユーザープロファイルから新しいユーザープロファイルが作成されます。	すべてのバージョンの VDA
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのバージョンの VDA
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのバージョンの VDA
すべてのログオンで Citrix 固定プロファイルとして使用されるテンプレートプロファイル	無効	すべてのバージョンの VDA

Profile Management/レジストリ

名前	デフォルト設定	VDA
除外の一覧	無効。HKEY_CURRENT_USER ハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンの VDA
包含の一覧	無効。HKEY_CURRENT_USER ハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンの VDA

Profile Management/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常時キャッシュ	無効	すべてのバージョンの VDA
常時キャッシュサイズ	0Mb	すべてのバージョンの VDA
プロファイルストリーミング	無効	すべてのバージョンの VDA
ストリーム配信ユーザープロファイルグループ	無効。OU 内のすべてのユーザープロファイルが処理されます。	すべてのバージョンの VDA

名前	デフォルト設定	VDA
待機領域のロックファイルのタイムアウト（日数）	1 日	すべてのバージョンの VDA

Receiver

名前	デフォルト設定	VDA
StoreFront アカウント一覧	ストアの指定なし	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降

Virtual Delivery Agent

名前	デフォルト設定	VDA
コントローラー登録の IPv6 ネットマスク	ネットマスクの指定なし	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
コントローラー登録ポート	80	すべてのバージョンの VDA
コントローラー SID	SID の指定なし	すべてのバージョンの VDA
コントローラー	Controller の指定なし	すべてのバージョンの VDA
コントローラーの自動更新を有効にする	有効	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
IPv6 コントローラー登録のみを使用する	無効	VDA for Server OS 7 以降、VDA for Desktop OS 7 以降
サイト GUID	GUID の指定なし	すべてのバージョンの VDA

Virtual Delivery Agent/HDX 3D Pro

名前	デフォルト設定	VDA
無損失を有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro 品質レベル		VDA 5.5、5.6 FP1

Virtual Delivery Agent/Monitoring

名前	デフォルト設定	**VDA**
プロセスの監視を有効にします	無効	VDA 7.11 以降
リソースの監視を有効にします	有効	VDA 7.11 以降

仮想 **IP**

名前	デフォルト設定	VDA
仮想 IP ループバックサポート	無効	VDA 7.6 以降
仮想 IP ループバックプログラム一覧	なし	VDA 7.6 以降

ポリシー設定リファレンス

August 24, 2021

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］または［HDX MediaStream マルチメディアアクセラレーションの最大帯域幅（%)］
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	[USB デバイスリダイレクトの最大帯域幅］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]

目的	使用するポリシー設定
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] および [TWAIN 圧縮リダイレクト]
クライアント側 USB デバイスの使用を制御する	[クライアント USB デバイスリダイレクト] および [クライアント USB デバイスリダイレクト規則]
WAN を介した接続でのクライアント側ドライブへの書き込み速度を改善する	非同期書き込みを使用する

コンテンツリダイレクト

目的	使用するポリシー設定
サーバーからユーザーデバイス側にコンテンツをリダイレクトするかどうかを制御する	ホストからクライアントへのリダイレクト

デスクトップ **UI**

目的	使用するポリシー設定
セッションでの壁紙の表示を制御する	デスクトップの壁紙
ウィンドウの内容を表示したままドラッグする機能を制御する	ドラッグ中にウィンドウの内容を表示する

グラフィック/マルチメディア

目的	使用するポリシー設定
仮想デスクトップがクライアント側に送信されるときの、1 秒あたりのフレームの最大数を設定する	ターゲットフレーム数
ユーザーデバイス側に表示されるイメージの表示品質を制御する	表示品質

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	Flash アクセラレーションのデフォルトの動作
セッションで特定の Web ページ上の Flash コンテンツを表示するかどうかを制御する	[Flash サーバー側でのコンテンツ取得 URL リスト]、[Flash URL 互換性リスト]、[Flash ビデオフォールバック防止］ポリシー設定、[Flash ビデオフォールバック防止エラー *.swf]
サーバー側でレンダリングするビデオの圧縮の制御	[圧縮にビデオコーデックを使用する]、[ビデオコーデックにハードウェアエンコーディングを使用します]
HTML5 マルチメディア Web コンテンツのユーザーへの配信の制御	HTML5 ビデオリダイレクト

マルチストリームネットワークトラフィックの優先度

目的	使用するポリシー設定
マルチストリーム接続の ICA トラフィックのポートを指定して、各ポートのネットワーク優先度を定義する	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にする	マルチストリーム（コンピューターポリシーおよびユーザーポリシー）

印刷

目的	使用するポリシー設定
ログオン時のクライアントプリンターの自動作成を制御する	[クライアントプリンターを自動作成する］および［クライアントプリンターリダイレクト]
プリンタープロパティの保存先を制御する	プリンタープロパティの保存
印刷ジョブをサーバーから直接プリンターに送信するか、クライアント経由で送信するかを制御する	プリントサーバーへの直接接続
クライアント側プリンターの使用を制御する	クライアントプリンターリダイレクト
クライアントプリンターおよびネットワークプリンターの自動作成時に、Windows に付属のプリンタードライバーを自動的にインストールするかどうかを制御する	付属のプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーの使用を制御する	ユニバーサル印刷の使用

目的	使用するポリシー設定
ローミングユーザーの接続方法に応じて自動作成されるプリンターを制御する	デフォルトプリンター
負荷を分散し、Universal Print Server のフェールオーバーしきい値を設定する	[負荷分散のためのユニバーサルプリントサーバー]、[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:
>
> デスクトップセッションおよび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

August 24, 2021

[ICA] カテゴリには、ICA リスナーの接続とクリップボードのマッピングに関する設定項目が含まれています。

アダプティブトランスポート

この設定では、EDT 上のデータトランスポートをプライマリとし、TCP にフォールバックすることを許可または禁止します。

デフォルトでは、アダプティブトランスポートは無効（[オフ]）になっており、常に TCP が使用されます。

1. Studio で、ポリシー設定「HDX アダプティブトランスポート」を有効にします（デフォルトでは無効）。また、この機能を、サイト内にあるすべてのオブジェクトのユニバーサルポリシーとすることは推奨しません。
2. ポリシー設定を有効にするには、値を ［優先］に設定し、[**OK**] をクリックします。

優先。可能な場合、Adaptive transport over EDT が使用され、TCP にフォールバックします。

診断モード。EDT が強制的にオンになり、TCP へのフォールバックは無効になります。この設定はトラブルシューティングでのみお勧めします。

オフ。TCP が強制的にオンになり、EDT が無効になります。

詳しくは、「アダプティブトランスポート」を参照してください。

アプリケーションの起動待機タイムアウト

この設定では、セッションで最初のアプリケーションの起動を待機する待機タイムアウトの値をミリ秒単位で指定します。この時間を超えた後にアプリケーションが起動されると、セッションは終了します。

デフォルトの時間（1 万ミリ秒）を選択するか、数値をミリ秒単位で指定できます。

クライアントクリップボードリダイレクト

この設定項目では、クライアント側のクリップボードをサーバーのクリップボードにマップすることを許可または禁止します。

デフォルトでは許可されます。

セッションとローカルのクリップボード間でデータを転送できなくするには、［禁止］を選択します。ただし、セッション内で動作するアプリケーション間でのクリップボードを介したデータ転送は無効になりません。

この設定を許可したら、［クリップボードリダイレクトの最大帯域幅（Kbps）］設定または［クリップボードリダイレクトの最大帯域幅（%）］設定を使用して、クライアント接続でクリップボードが使用できる帯域幅の上限を設定します。

クライアントクリップボードに書き込みを許可する形式

［クライアントクリップボードの書き込み制限］が［有効］に設定されている場合、ホスト側のクリップボードデータは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
- CF_HTML

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、［**CF_HTML**］（およびサポートを希望するほかの形式）のエントリを追加します。

注：HTML 形式のクリップボードコピーのサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースのあらゆるスクリプト（存在する場合）が、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルを HTML ファイルとして保存して実行する場合に限り、ライブになります。

カスタム定義のデータ形式を追加することもできます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

［クライアントクリップボードリダイレクト］または［クライアントクリップボードの書き込み制限］で［禁止］が設定されている場合、この設定項目は無視されます。

デスクトップの起動

この設定により、VDA の Direct Access Users グループの非管理者ユーザーによる ICA コネクションを使った VDA 上のセッションへの接続を許可または禁止します。

デフォルトでは、管理者以外のユーザーはこれらのセッションに接続できません。

この設定は、RDP 接続を使用している VDA の Direct Access Users グループの非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっているかに関わらず VDA に接続できます。この設定は、VDA の Direct Access Users グループではない非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっているかに関わらず VDA に接続できません。

ICA リスナー接続タイムアウト

注：この設定は、Virtual Delivery Agent 5.0、5.5、および 5.6 Feature Pack 1 にのみ適用されます。

この設定では、ICA プロトコルによる接続が完了するまでの最大待機時間を指定します。

デフォルトの最大待機時間は、120000 ミリ秒（2 分）です。

ICA リスナーポートの番号

この設定では、サーバー上の ICA プロトコルで使用される TCP/IP ポートを指定します。

デフォルトのポート番号は、1494 に設定されています。

ほかのポートを指定する場合は、0 から 65535 の範囲で、ほかのウェルノウンポート番号と競合しない番号を使用してください。変更したポート番号を有効にするには、サーバーを再起動する必要があります。サーバー上のポート番号を変更した場合は、そのサーバーに接続する Citrix Receiver やプラグインソフトウェア側でもポート番号を変更する必要があります。

クライアント接続での非公開アプリケーションの起動

この設定項目では、サーバー上のリモートデスクトップを介した開始アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上のリモートデスクトップを介した開始アプリケーションの起動は許可されません。

ログオフチェッカー起動遅延

この設定では、ログオフチェッカー起動の遅延時間を指定します。このポリシーを使用して、クライアントセッションがセッション切断を待機する時間（秒単位）を設定します。

この設定により、ユーザーがサーバーからログオフするのにかかる時間を長くすることもできます。

クライアントクリップボードの書き込み制限

この設定項目を［許可］に設定すると、ホスト側のクリップボードデータがクライアントエンドポイント側に共有されなくなります。この場合、特定のデータの共有を許可するには、［クライアントクリップボードに書き込みを許可する形式］設定を使用します。

デフォルトでは、禁止に設定されています。

セッションクリップボードの書き込み制限

この設定項目を［許可］に設定すると、クライアント側のクリップボードデータがユーザーセッション側に共有されなくなります。この場合、特定のデータの共有を許可するには、［セッションクリップボードに書き込みを許可する形式］設定を使用します。

デフォルトでは、禁止に設定されています。

セッションクリップボードに書き込みを許可する形式

［セッションクリップボードの書き込み制限］設定が［許可］の場合、クライアント側のクリップボードデータはセッション内のアプリケーション側に共有されません。この［セッションクリップボードに書き込みを許可する形式］設定では、特定の種類のクリップボードデータの共有を許可します。

以下のシステム定義のクリップボードデータ形式を追加できます。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

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、［**CF_HTML**］（およびサポートを希望するほかの形式）のエントリを追加します。

注：HTML 形式のクリップボードコピーのサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースのあらゆるスクリプト（存在する場合）が、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルを HTML ファイルとして保存して実行する場合に限り、ライブになります。

カスタム定義のデータ形式を追加することもできます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

［クライアントクリップボードリダイレクト］設定または［セッションクリップボードの書き込み制限］設定で［禁止］が設定されている場合、この設定項目は無視されます。

クライアントの自動再接続のポリシー設定

January 22, 2019

［クライアントの自動再接続］カテゴリには、セッションの自動再接続の制御に関する設定項目が含まれています。

クライアントの自動再接続

この設定では、接続が中断した後で同じクライアントから自動再接続することを許可または禁止します。

Citrix Receiver for Windows 4.7 以降のクライアントの自動再接続では、Citrix Studio からのポリシー設定のみを使用します。Studio でこれらのポリシーを更新すると、サーバーからクライアントにクライアントの自動再接続が同期されます。以前のバージョンの Citrix Receiver for Windows では、クライアントの自動再接続を構成するのには、Studio ポリシーを使用してレジストリまたは default.ica ファイルを変更します。

クライアントの自動再接続を許可すると、ユーザーは接続が切断された時点の状態に戻って作業を再開できます。自動再接続機能では、切断された接続が検出されてそのセッションにユーザーが再接続されます。

セッション ID と資格情報のキーが含まれている Citrix Receiver の Cookie を使用していない場合は、自動再接続によって新しいセッションが開始されることがあります。つまり、既存のセッションに再接続されるのではありません。再接続に時間がかかって Cookie の有効期限が切れた場合や、ユーザーが資格情報を入力する必要がある場合には、Cookie は使用されません。また、ユーザーが自分で切断した場合、クライアントの自動再接続はトリガーされません。

再接続中は、セッションウィンドウが灰色になります。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。セッションがタイムアウトになると、接続は切断されます。

アプリケーションセッションで自動再接続が許可されている場合は、セッションが再接続するまでの残り時間を指定するカウントダウンタイマーが通知領域に表示されます。Citrix Receiver による再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。

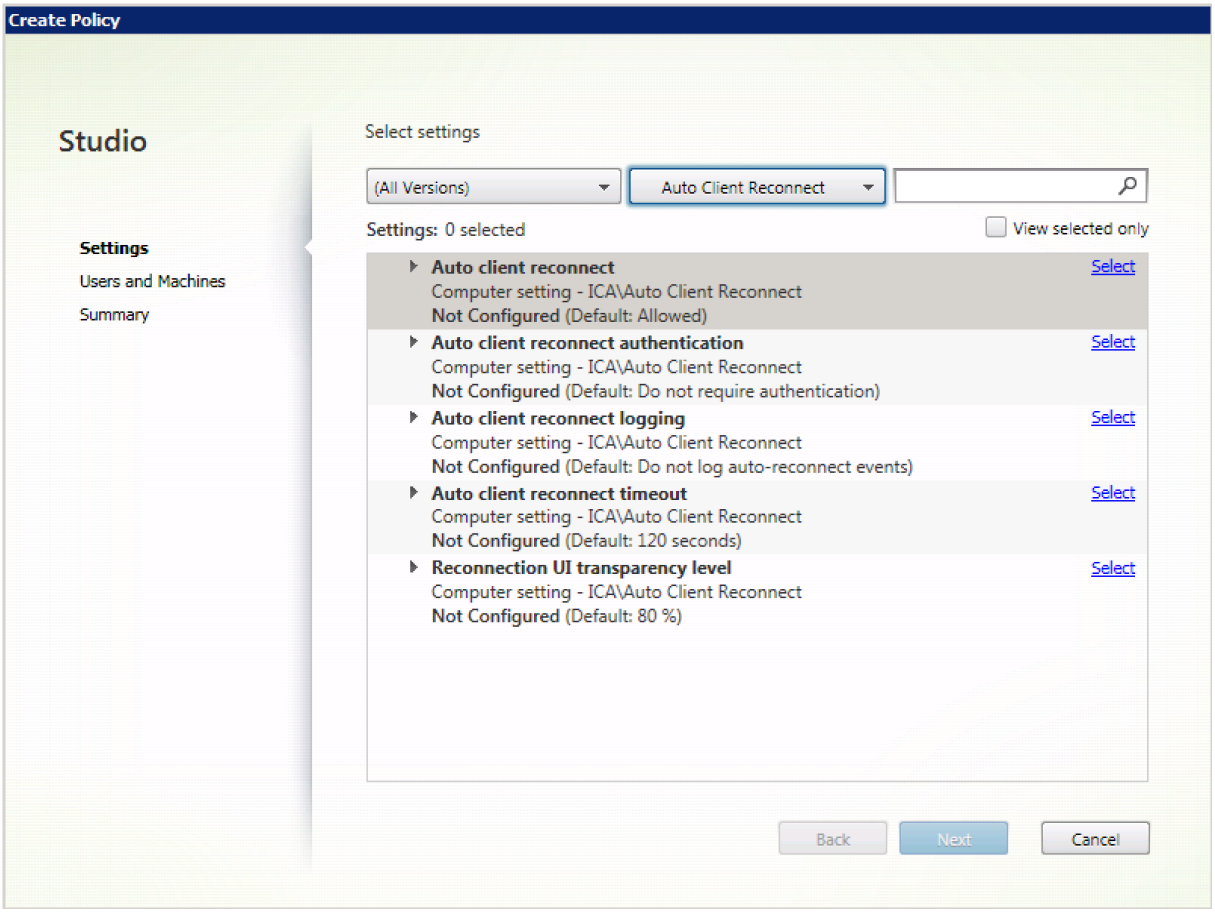
ユーザーセッションでは、自動再接続が許可されている場合、Citrix Receiver は、指定された時間、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。デフォルトでは、この時間は 2 分です。この期間を

変更するには、ポリシーを編集します。

デフォルトでは、クライアントの自動再接続が許可されます。

クライアントの自動再接続を無効にするには

1. Citrix Studio を開始します。
2. ［クライアントの自動再接続］ポリシーを開きます。
3. ポリシーを ［禁止］に設定します。



クライアントの自動再接続時の認証

この設定では、自動再接続時に認証処理を必要とするかどうかを制御します。［認証を必要とする］を選択すると、クライアントの自動再接続時に認証のためのダイアログボックスが開きます。

ユーザーが最初にログオンすると、そのユーザーの資格情報は暗号化されてメモリに格納され、その暗号キーを含んだ Cookie が作成されます。この Cookie は、Citrix Receiver に送信されます。この設定項目を構成して［認証を必要とする］を選択すると、Cookie は使用されなくなります。その代わりに、切断セッションへの再接続時に、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

デフォルトでは、認証は要求されません。

クライアントの自動再接続時の認証を変更するには

1. Citrix Studio を開始します。
2. ［クライアントの自動再接続時の認証］ポリシーを開きます。
3. 認証を有効または無効にします。
4. ［**OK**］をクリックします。

クライアントの自動再接続のログ

この設定では、クライアントの自動再接続イベントをログに記録するかどうかを制御します。

ログを有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。これらのイベントは、そのイベントが発生した個々のサーバーのシステムログに記録されます。

デフォルトでは、ログは無効になっています。

クライアントの自動再接続時のロギングを変更するには

1. Citrix Studio を開始します。
2. ［クライアントの自動再接続のログ］ポリシーを開きます。
3. ロギングを有効または無効にします。
4. ［**OK**］をクリックします。

クライアントの自動再接続のタイムアウト

デフォルトでは、クライアントの自動再接続タイムアウトは 120 秒に設定されます。自動クライアント接続の構成可能なタイムアウトの最大値は 300 秒です。

クライアントの自動再接続のタイムアウトを変更するには

1. Citrix Studio を開始します。
2. ［クライアントの自動再接続のタイムアウト］ポリシーを開きます。
3. タイムアウト値を編集します。
4. ［**OK**］をクリックします。

再接続 **UI** の透過レベル

Studio ポリシーを使用すると、セッション画面の保持の再接続時に、XenApp または XenDesktop のセッションウィンドウに適用される不透明度レベルを構成できます。

デフォルトでは、再接続 UI の透明度は、80 に設定されています。

再接続ユーザーインターフェイスの不透明度レベルを変更するには

1. Citrix Studio を開始します。
2. ［再接続 **UI** の透明度レベル］ポリシーを開きます。

3. 値を編集します。
4. [**OK**] をクリックします。

オーディオのポリシー設定

August 24, 2021

[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。

現在、この音質が設定されている場合のみ、UDP 上のリアルタイムトランスポート（RTP）がサポートされています。この音質は、非常に低速なネットワーク接続（512Kbps 未満）や、ネットワークで輻輳やパケット損失などが生じる環境で使用します。

- 帯域幅が十分で、サウンドの音質が重要である場合は、［高 - 高品位オーディオ］を選択します。この設定では、ネイティブのサウンドデータを再生または録音できます。サウンドデータは、CD レベルの音質が維持される 112Kbps の高品質レベルで圧縮されます。ただし、大量のネットワークデータ転送が要求されるため、CPU およびネットワークに負担がかかる場合があります。

録音と再生を同時に行った場合、消費帯域幅は 2 倍になります。

帯域幅の上限を指定するには、［オーディオリダイレクトの最大帯域幅（Kbps）］設定または［オーディオリダイレクトの最大帯域幅（%）］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用できる帯域幅の上限を設定します。これにより、アプリケーションのパフォーマンスが向上しますが、音質が低下することがあります。録音と再生を同時に行った場合、消費帯域幅は 2 倍になります。帯域幅の上限を指定するには、［オーディオリダイレクトの最大帯域幅（Kbps）］設定または［オーディオリダイレクトの最大帯域幅（%）］設定を使用します。

Windows サーバー OS マシンで複数のオーディオデバイスをサポートするには、［オーディオプラグアンドプレイ］設定で［有効］が選択されていることも確認してください。

重要:［クライアントオーディオリダイレクト］設定で［禁止］を選択すると、すべての HDX オーディオ機能が無効になります。

クライアントマイクリダイレクト

この設定では、クライアント側のマイクのリダイレクトを有効または無効にします。この設定を有効にすると、セッション内でクライアント側のマイクを使ってオーディオを録音できるようになります。

デフォルトでは許可されます。

セキュリティの設定により、ユーザーデバイスに信頼されていないサーバーからユーザーデバイス側のマイクにアクセスしたときに、警告メッセージが表示されます。ユーザーは、このメッセージに対してアクセスを許可したり拒否したりできます。この警告は、ユーザーが Citrix Receiver 側で無効にできます。

Windows サーバー OS マシンで複数のオーディオデバイスをサポートするには、［オーディオプラグアンドプレイ］設定で［有効］が選択されていることも確認してください。

ユーザーデバイス側で［クライアントオーディオリダイレクト］設定が無効になっている場合、この設定は無視されます。

帯域幅のポリシー設定

February 3, 2020

［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

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

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。

双方向のコンテンツリダイレクトのポリシー設定

August 24, 2021

双方向のコンテンツリダイレクトの設定セクションには、クライアントからホスト（およびホストからクライアント）への URL リダイレクトを有効にするか無効にするかのポリシー設定が含まれています。サーバーポリシーは Citrix Studio で設定し、クライアントポリシーは、Citrix Receiver グループポリシーオブジェクト管理用テンプレートで設定します。

URL リダイレクトに関しては、Citrix ではホストからクライアントへのリダイレクトおよびクライアント用のローカルアプリケーションアクセスが利用可能ですが、ドメインに参加している Windows クライアントに関しては、双方向のコンテンツリダイレクトを使用することをお勧めします。

双方向のコンテンツリダイレクトを利用するには、XenApp または XenDesktop 7.13 以降に加えて、Citrix Receiver for Windows 4.7 以降が必要です。

> 重要
>
> - リダイレクト規則によってループが構成されないように注意してください。たとえば、VDA のクライアント規則で「https://www.citrix.com」に設定され、クライアントの VDA 規則で同じ URL が設定されていると無限ループになる可能性があります。
> - サポート対象は、ドメイン参加のエンドポイントのみです。
> - 明示的な URL リダイレクトのみがサポートされます（Web ブラウザーのアドレスバーに表示される URL や、ブラウザーによっては、ブラウザー内ナビゲーションで発見できる URL だけが正しくリダイレクトされます）。短縮 URL はサポートされていません。
> - 双方向のコンテンツリダイレクトに対応しているのは、Internet Explorer 8 から 11 のみです。Internet Explorer は、ユーザーデバイスと VDA の双方で使用する必要があります。
> - 双方向のコンテンツリダイレクトには、Internet Explorer ブラウザー用のアドオンが必要です。詳しくは、「Web ブラウザーアドオンの登録」を参照してください。
> - セッションの起動に関する問題でリダイレクトが失敗した場合のフォールバックメカニズムはありませ

ん。
- 2 つのアプリケーションが複数の StoreFront アカウントで同じ表示名に設定されていた場合、プライマリ StoreFront アカウントの表示名が起動に使用されます。
- Citrix Receiver for Windows のみがサポートされます。
- 新しい Web ブラウザーのウィンドウが表示されるのは、URL がクライアントにリダイレクトされた場合だけです。Web ブラウザーを開いている状態で URL が VDA にリダイレクトされると、リダイレクトされた URL が新しいタブで開かれます。
- ドキュメント、メール、PDF などのファイルの埋め込みリンクをサポートしています。
- この機能は、デスクトップセッションでもアプリケーションセッションでも使用できますが、これとは異なり、ローカルアプリケーションアクセスの URL リダイレクトは、デスクトップセッションでしか使用できません。
- URL リダイレクトでローカルアプリケーションアクセスが有効になっている場合（VDA またはクライアントにおいて）、双方向のコンテンツリダイレクトは無効です。

ホストからクライアントおよびホストからホストへのリダイレクト

Citrix Studio を使用して、ホストからクライアント（クライアント側）とホストからホスト（VDA 側）のリダイレクトポリシーを構成します。

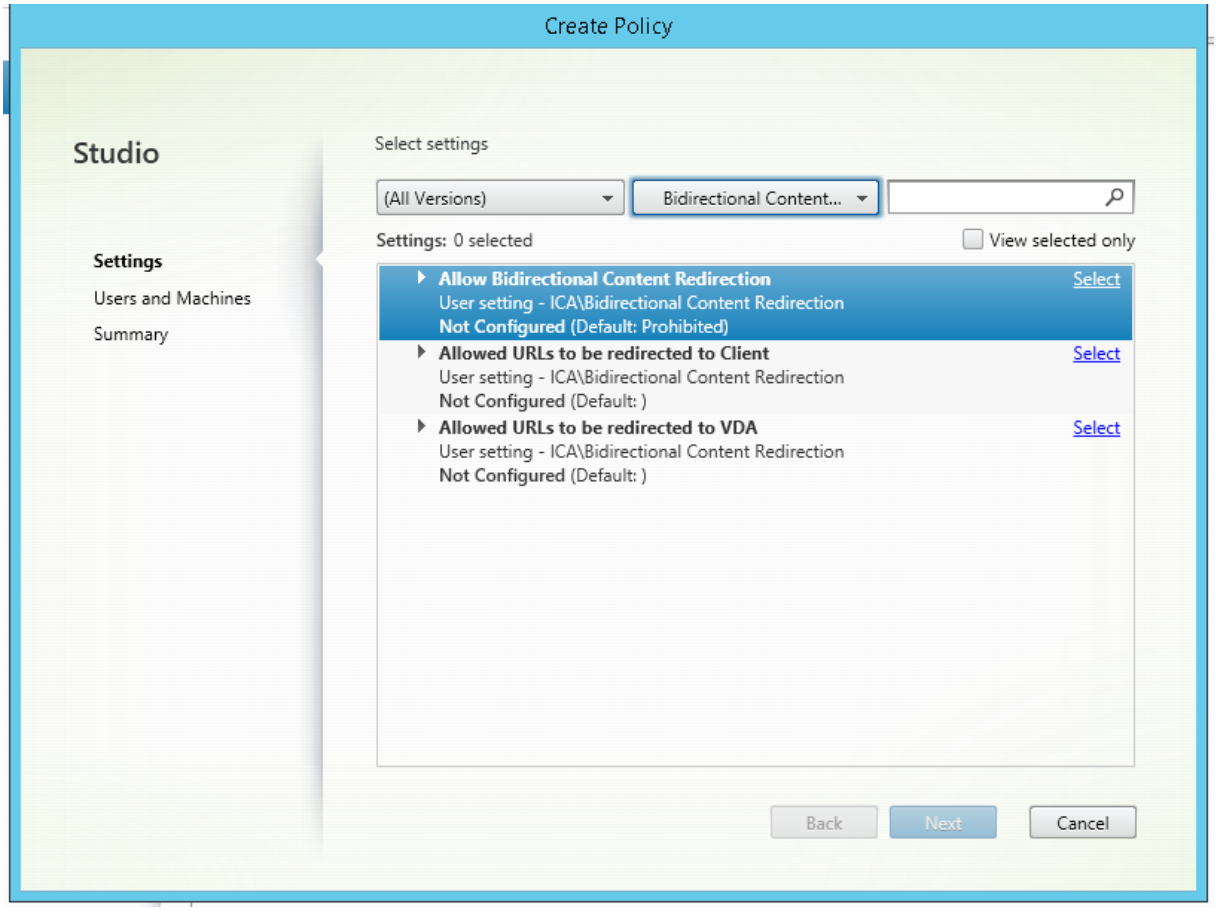
デフォルトでは、双方向のコンテンツリダイレクトは禁止されています。

双方向のコンテンツリダイレクトを有効化するには

URL が複数ある場合、URL を 1 つずつ指定することもできますが、セミコロンで区切った URL の一覧で指定しても構いません。ワイルドカード文字としてアスタリスク（*）をドメイン名に使用できます。例：

`https://*.citrix.com`、`https://www.google.com`

1. Citrix Studio を開始します。
2. ［双方向のコンテンツリダイレクト］ポリシーを開きます。
3. ［双方向のコンテンツリダイレクトを許可する］を選択し、［許可］を選んで、［**OK**］をクリックします。このオプションを許可しないと、この手順を完了できません。
4. ［クライアントへのリダイレクトを許可する **URL**］を選択し、URL または URL の一覧を指定するか、またはデフォルト値から選択します。
5. ［**VDA** へのリダイレクトを許可する **URL**］を選択し、URL または URL の一覧を指定するか、またはデフォルト値から選択します。

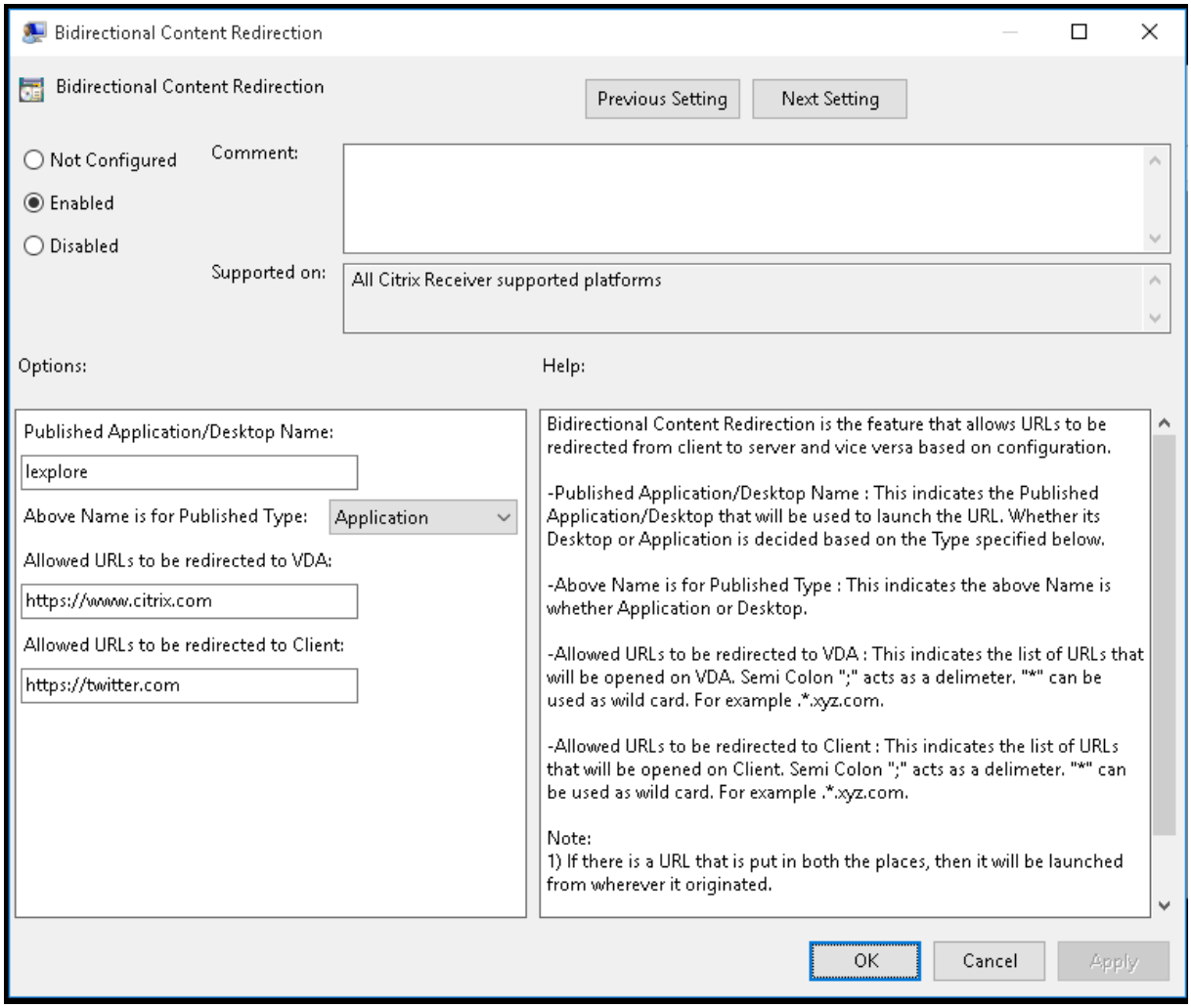


クライアントからホスト（**VDA**）およびクライアントからクライアントへのリダイレクト

Citrix Receiver グループポリシーオブジェクト管理テンプレートを使って、クライアントからホスト（VDA 側）およびクライアントからクライアント（クライアント側）へのリダイレクトを構成します。

双方向のコンテンツリダイレクトを有効化するには

URL が複数ある場合、URL を 1 つずつ指定することもできますが、セミコロンで区切った URL の一覧で指定しても構いません。ワイルドカード文字としてアスタリスク（*）を使用できます。



Web ブラウザーアドオンの登録

双方向のコンテンツリダイレクトには、Internet Explorer ブラウザー用のアドオンが必要です。

以下のコマンドを実行して、Internet Explorer 用のアドオンを登録したり登録解除したりできます:

- クライアントデバイス上でアドオンを登録する場合: <client-installation-folder>\redirector.exe /regIE
- クライアントデバイス上でアドオンの登録を解除する場合: <client-installation-folder>\redirector.exe /unregIE
- VDA 上でアドオンを登録する場合: <VDAinstallation-folder>\VDARedirector.exe /regIE
- VDA 上でアドオンの登録を解除する場合: <VDAinstallation-folder>\VDARedirector.exe /unregIE

たとえば、Citrix Receiver を実行するデバイス上で Internet Explorer 用のアドオンを登録するには、次のコマンドを実行します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

また、VDA for Windows Server OS が動作するサーバー上で Internet Explorer 用のアドオンを登録するには、次のコマンドを実行します。

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regIE

クライアントセンサーのポリシー設定

March 1, 2019

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

August 24, 2021

［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、［デスクトップコンポジションリダイレクト］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リダイレクトの画質

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のアニメーション化が有効で、またメニューのアニメーション化 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

March 25, 2020

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

November 28, 2018

この設定項目では、ローカルで Windows 7 デスクトップを実行しているユーザーに対して、サーバーオペレーティングシステム上のセッションに Windows 7 デスクトップテーマを適用するかどうかを構成します。

デフォルトでは、この設定は許可されています。

Windows クラシックテーマが選択されたユーザープロファイルが存在する仮想デスクトップでは、この設定を有効にしてもデスクトップエクスペリエンス拡張が提供されません。この設定項目が未構成または無効の場合、Windows 7 テーマのユーザーが Windows Server 2012 上の仮想デスクトップにログオンすると、テーマの適用に失敗したことを示すエラーメッセージが表示されます。

これらの問題は、ユーザープロファイルをリセットすることで解決されます。

実行中のユーザーセッションが存在する仮想デスクトップでこの設定項目を有効から無効に変更すると、Windows 7 テーマおよび Windows クラシックテーマでの表示に問題が発生します。この問題を避けるには、この設定項目の構成を変更した後で仮想デスクトップを再起動してください。また、管理者は仮想デスクトップの移動プロファイルを削除する必要もあります。さらに、プロファイル間の一貫性の問題を避けるため、仮想デスクトップの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

November 28, 2018

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

August 24, 2021

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 背景色の一覧

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：`https://citrix.com 000003`。

指定される URL は Flash コンテンツの URL である必要があります。これは Web サイトの URL とは異なることがあります。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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] “Force-HDXFlashEnabled”=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。

- Flash アクセラレーションを有効にする：Flash リダイレクトが使用されます。
- Flash Player をブロックする：Flash リダイレクトおよびサーバー側でのレンダリングが行われません。これにより、ユーザーは Flash コンテンツを表示できなくなります。
- アクセラレーションを無効にする：Flash リダイレクトは使用されません。適切なバージョンの Flash Player for Windows Internet Explorer がサーバーにインストールされている場合、ユーザーはサーバー側で処理された Flash コンテンツを表示できます。

この設定は、［Flash URL 互換性リスト］設定に追加した特定の Web ページや Flash インスタンスでは無視されます。また、Flash リダイレクト機能を使用するには、ユーザーデバイス側でも［このユーザーデバイスでの HDX MediaStream Flash リダイレクトを有効にする］を有効にする必要があります。

Flash イベントのログ

この設定では、Flash イベントを Windows のアプリケーションイベントログに記録するかどうかを指定します。

デフォルトでは、ログは有効になっています。

Windows 7 または Windows Vista が動作するコンピューターでは、Flash リダイレクトのログは［アプリケーションとサービスログ］ノードに記録されます。

Flash インテリジェントフォールバック

この設定は、Flash コンテンツのクライアント側でのレンダリングが不要または低速な場合に、サーバー側でのレンダリングに自動的に切り替える機能を有効または無効にします。

デフォルトでは、有効になっています。

Flash 遅延しきい値

この設定では、Flash コンテンツのレンダリングをサーバー側で行うかどうかを決定する遅延時間のしきい値を、0〜30 ミリ秒で指定します。

デフォルトのしきい値は、30 ミリ秒です。

HDX MediaStream for Flash では、起動時にサーバーとクライアント間の遅延時間が計測されます。計測値がしきい値未満の場合、HDX MediaStream for Flash 機能によりクライアント側で Flash コンテンツがレンダリングされます。遅延がしきい値を超える場合は、サーバー側で Flash コンテンツがレンダリングされます（そのサーバー上に Adobe Flash Player がインストールされている場合）。

この設定を有効にするときは、［Flash アクセラレーションの後方互換］設定で［有効］が選択されていることを確認してください。

注：HDX MediaStream Flash リダイレクトを従来モードで使用する場合のみ適用されます。

Flash ビデオフォールバック防止

この設定は、「小さな」Flash コンテンツがレンダリングされてユーザーに表示されるのかどうか、されるならどのようにされるのかを指定します。

デフォルトでは、この設定は構成されていません。

この設定を構成するには、次のいずれかのオプションを選択します。

- 小さなコンテンツのみ。サーバー上でインテリジェントフォールバックコンテンツのみレンダリングされます。ほかの Flash コンテンツはエラー *.swf と置き換えられます。
- サポートされたクライアントがある小さなコンテンツのみ。クライアントが現在 Flash リダイレクトを使用している場合に、サーバー上でインテリジェントフォールバックコンテンツのみレンダリングされます。ほかの Flash コンテンツはエラー *.swf と置き換えられます。
- サーバー側コンテンツなし。サーバー上のすべてのコンテンツは、エラー *swf と置き換えられます。

このポリシー設定を使用するには、エラー*.swf* ファイルを指定する必要があります。このエラー.swf は、VDA 上でレンダリングしない任意のコンテンツを置き換えます。

Flash ビデオフォールバック防止エラー *.swf

この設定は、サーバー負荷管理ポリシーが使用されている場合に Flash インスタンスを置き換えるためユーザーに表示されるエラーメッセージの URL を指定します。例:

```
http://domainName.tld/sample/path/error.swf
```

Flash サーバー側でのコンテンツ取得 URL リスト

この設定のリストに追加した Web サイトの Flash コンテンツは、サーバーにより取得され、ユーザーデバイスに転送されます。

デフォルトでは、サイトは指定されていません。

サーバー側でのコンテンツ取得は、インターネットに直接アクセスできないユーザーデバイスに対して有効にします。また、ユーザーデバイス側でも［サーバー側のコンテンツの取得を有効にする］設定を有効にする必要があります。

第 2 世代の Flash リダイレクトには、Flash の SWF ファイルをサーバー側でダウンロードするフォールバック機能が含まれています。ユーザーデバイスが Web サイトから Flash コンテンツを取得できず、Web サイトが Flash サーバー側コンテンツ取得 URL 一覧で指定されている場合、サーバー側コンテンツの取得は自動的に発生します。

対象の URL をリストに追加する場合、以下の点に注意してください。

- Flash Player を開始する上位レベルの HTML ページの URL ではなく、Flash コンテンツの URL を追加します。
- URL の最初または最後にワイルドカード文字としてアスタリスク（*）を使用できます。
- URL の最後にワイルドカード文字を使うと、すべての子 URL を指定できます（`http://www.citrix.com/*`など）。

- 冒頭の「http://」や「https://」は正しく認識されますが、省略することもできます。

Flash URL 互換性一覧

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（https://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

August 24, 2021

グラフィックセクションには、ユーザーセッションでの画像処理の制御に関するポリシー設定が含まれています。

視覚的無損失の圧縮を使用する

この設定により、グラフィックに対して、真の無損失圧縮の代わりに視覚的に無損失の圧縮を使用できるようになります。視覚的無損失では、真の無損失よりもパフォーマンスは向上しますが、見た目にはわからない程度の軽微な損失が発生します。この設定によって、表示品質設定の値の使用方法が変更されます。

デフォルトでは、無効になっています。

表示メモリの制限

この設定では、セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。

デフォルトの表示メモリ制限は、65536 キロバイトに設定されます。

セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。キロバイト単位の容量指定は、128 から 4,194,303 です。最大値 4,194,303 によって表示メモリが制限されることはありません。デフォルトでは、65536 キロバイトに設定されます。表示色数を多くしたり解像度を上げたりすると、必要なメモリの量が増えます。従来の

グラフィックモードでは、この最大値に達すると、［メモリが不足したときの表示モード］設定に基づいて色数または解像度が低下します。

高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は、次の式で算出できます。

必要とされるメモリ（バイト単位）＝（1 ピクセルあたりのビット数を 8 で割った色数）*（垂直方向のピクセル単位の解像度）*（水平方向のピクセル単位の解像度）

たとえば、ウィンドウの高さが 600、ウィンドウの幅が 800、色数が 32 ビットの場合、必要なメモリの最大量は（32÷8）*（600 ピクセル）*（800 ピクセル）＝ 1920000 バイトであるため、［表示メモリの制限］設定で 1920KB を指定します。

32 ビット以外の色数は、［従来のグラフィックモード］設定が有効な場合のみ使用できます。

HDX では、各セッションで必要な表示メモリ量だけが割り当てられます。このため、デフォルト値よりも多くのメモリが必要なユーザーが一部だけの場合にこの設定項目で表示メモリの制限を増やしても、スケーラビリティは低下しません。

メモリが不足したときの表示モード

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、セッション表示用のメモリが上限に達したときに、色数と解像度のどちらを下げるかを指定します。

デフォルトでは、最初に色数が低下します。

セッション表示用のメモリが上限に達したときに、表示品質を下げることでメモリ不足による問題の発生を防ぐことができます。色数を下げることを選択すると、表示用のメモリが上限に達したときに、まずより少ない色でのイメージ表示に切り替わります。解像度を下げることを選択すると、まず 1 インチあたりのピクセル数が少なくなります。

色数または解像度の低下をユーザーに通知するには、［メモリ不足による表示品質の低下をユーザーに通知する］設定を使用します。

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。

Windows Aero プレビューオプション	説明
ピークウィンドウプレビュー	Windows タスクバー上に開いた縮小版上にマウスポインターを合わせると、そのウィンドウがフルサイズで表示されます。
フリップ	Alt+Tab キーを押すと、開いているすべてのウィンドウの縮小版が一覧表示されます。
フリップ 3D	Tab+Windows ロゴキーを押すと、開いているすべてのウィンドウが立体的に重なって一覧表示されます。

デフォルトでは、有効になっています。

イメージキャッシュ

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定項目では、セッション内のイメージのセクションキャッシュおよび取得を有効または無効にします。必要な場合にセクションのイメージをキャッシュし、そのセクションを取得すると、スクロールがよりスムーズになり、ネットワーク上のデータ伝送量が減少して、ユーザーデバイス上で必要とされる処理が少なくなります。

デフォルトでは、イメージのキャッシュ設定は有効になっています。

注：イメージのキャッシュ設定は、イメージがどのようにキャッシュおよび取得されるかを制御します。イメージがキャッシュされるかどうかについては制御しません。従来のグラフィックモード設定が有効な場合は、イメージがキャッシュされます。

従来のグラフィックモード

この設定では、リッチなグラフィック表示が無効になります。この設定を使用すると、従来のグラフィック表示が取り消され、WAN やモバイル接続での帯域幅の使用量が削減されます。XenApp および XenDesktop 7.13 に導入された帯域幅の削減によって、このモードは廃止されます。

この設定はデフォルトで無効になっており、リッチなグラフィック表示が提供されます。

Windows 7 および Windows Server 2008 R2 VDA では、従来のグラフィックモードがサポートされます。

Windows 8.x、10、または Windows Server 2012、2012 R2、2016 では、従来のグラフィックモードはサポートされていません。

XenApp および XenDesktop 7.6 FP3 以降でのグラフィックモードおよびポリシーの最適化について詳しくは、Knowledge Center の記事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のレスポンスが向上します。ただし、中間フレームが脱落するため、アニメーションの動きがスムーズでなくなる場合があります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオのデコードを使用できる場合は、グラフィックの圧縮にビデオコーデック（H.264）を使用できます。［画面全体］が選択された場合、ビデオコーデックにはすべてのデフォルトコーデックが適用されます。［アクティブに変化する領域］が選択された場合、画面上に変更が定期的にある領域にビデオコーデックが使用され、他

のデータでは静止画圧縮およびビットマップのキャッシュが使用されます。エンドポイントでビデオのデコードを使用できない、または使用しないように指定すると、静止画像圧縮とビットマックキャッシュの組み合わせが使用されます。［選択された場合ビデオコーデックを使用する］が指定されている場合、選択はさまざまな要素に基づいて行われます。選択方法が拡張されているため、結果はバージョンによって異なる場合があります。

現在のシナリオに最適な設定が自動的に選択されるようにするには、［選択された場合ビデオコーデックを使用する］を選択します。

ユーザーエクスペリエンスと帯域幅の改善のために最適化する場合、特にサーバー側でレンダリングするビデオや 3D グラフィックを多用する場合は、［画面全体］を選択します。

ビデオパフォーマンス、特に低帯域幅が改善されるように最適化しつつ、コンテンツが静的かつ徐々に変更されるようにするためにスケーラビリティを維持するには［領域をアクティブに変更］を選択します。この設定は、マルチモニターの展開でサポートされます。

サーバー CPU の負荷を最適化する場合、およびサーバー側でレンダリングするビデオやその他の画像処理に多くのリソースを消費するアプリケーションがほとんどない場合は、［ビデオコーデックを使用しない］を選択します。

デフォルトでは、［選択された場合ビデオコーデックを使用する］に設定されています。

ビデオのハードウェアエンコーディングの使用

この設定によりグラフィックハードウェア（搭載している場合）を利用して、画面要素を H.264 ビデオコーデックで圧縮できます。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して CPU ベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトのオプションは ［有効］です。

複数のモニターがサポートされます。

H.264 デコーディングをサポートする Citrix Receiver は、NVENC ハードウェアエンコーディングで使用できます。

非可逆圧縮（4:2:0）と視覚的無損失圧縮（4:4:4）がサポートされます。視覚的無損失（グラフィックポリシー設定［視覚的無損失圧縮を使用する］）には、Receiver for Windows 4.5 以降が必要です。

NVIDIA

NVIDIA GRID GPU の場合、ハードウェアエンコーディングは、HDX 3D Pro モードの VDA for Desktop OS でサポートされています。

NVIDIA GPU は、NVENC ハードウェアエンコーディングをサポートする必要があります。サポートされている GPU の一覧については、「NVIDIA ビデオコーデック SDK」を参照してください。

NVIDIA GRID には、ドライバーのバージョン 3.1 以降が必要です。NVIDIA Quadro には、ドライバーのバージョン 362.56 以降が必要です。NVIDIA リリース R361 ブランチからのドライバーをお勧めします。

VDA が（HDX 3D Pro ではなく）標準モードで構成された場合の機能である無損失テキストには、NVENC ハードウェアエンコーディングとの互換性はありません。HDX 3D Pro モードで有効になっている場合、無損失テキストは NVENC ハードウェアエンコーディングよりも優先されます。

アクティブに変化する領域に対する H.264 ハードウェアコーデックの選択的使用はサポートされません。

Intel

Intel Iris Pro グラフィックプロセッサの場合、ハードウェアエンコーディングは、VDAs for Desktop OS（標準モードまたは HDX 3D Pro モード）および VDA for Server OS でサポートされています。

サポート対象は、Intel Broadwell プロセッサファミリの Intel Iris Pro グラフィックプロセッサ以降です。Intel Remote Displays SDK バージョン 1.0 は必須であり、Intel の Web サイト「Remote Displays SDK」からダウンロードできます。

無損失テキストがサポートされています。

［領域をアクティブに変更］に対する H.264 ハードウェアコーデックの選択的使用がサポートされています。

対応は、Windows 10 および Windows Server 2012 以降です。

3D Pro モードの VDA で、Intel エンコーダーは最大で 8 つのエンコーディングセッションを可能にする優れたユーザーエクスペリエンスをもたらします（たとえば、1 人のユーザーが 8 つのモニターを使ったり、8 人のユーザーが各自モニターを使用するなど）。8 つ以上のエンコーディングセッションが必要な場合は、仮想マシンが接続するモニター数を確認してください。優れたユーザーエクスペリエンスを維持するために、管理者はこのポリシー設定をユーザー単位またはマシン単位に構成できます。

キャッシュのポリシー設定

August 24, 2021

［キャッシュ］カテゴリには、狭帯域幅のクライアント接続でイメージデータをユーザーデバイス上にキャッシュする機能を有効にするための設定項目が含まれています。

固定キャッシュしきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、ビットマップをユーザーデバイスのハードドライブ上にキャッシュするときの帯域幅しきい値を指定します。この機能により、サイズの大きな、頻繁に使用されるイメージがキャッシュされ、以降のセッションで再使用されます。

デフォルトのしきい値は、3000000bps です。

帯域幅がこのしきい値を下回る場合、固定キャッシュ機能が有効になります。つまり、デフォルトの設定では、接続帯域幅が 3,000,000bps を下回る場合に、ビットマップがユーザーデバイスのハードドライブ上にキャッシュされます。

Framehawk のポリシー設定

November 28, 2018

Framehawk セクションには、サーバーで Framehawk ディスプレイチャネルを有効化し、構成するためのポリシー設定が含まれます。

Framehawk ディスプレイチャネル

この機能を有効にすると、サーバーは Framehawk ディスプレイチャネルを使用して、ユーザーのグラフィックスおよび入力リモート処理を試行します。この表示チャネルは、UDP を使用して、高い損失および遅延特性を示すネットワークにより快適なユーザーエクスペリエンスを提供します。ただし、使用するサーバーのリソースや帯域幅は他のグラフィックモードよりも多くなります。

デフォルトでは、Framehawk ディスプレイチャネルは無効になっています。

Framehawk 表示チャネルポートの範囲

このポリシー設定項目では、VDA でユーザーデバイスとの Framehawk ディスプレイチャネルデータの送受信に使用される UDP ポート番号の範囲を「*<lowest port number>,<highest port number>*」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

November 28, 2018

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

October 31, 2019

［ローカルアプリアクセス］カテゴリには、ホストされるデスクトップ環境で、ユーザーデバイス上にインストールされたローカルアプリケーションとホスト上のアプリケーションをシームレスに使用できるようにするための設定項目が含まれています。

ローカルアプリアクセスを許可する

この設定では、ホストされるデスクトップ環境で、ローカルアプリケーションとホスト上のアプリケーションの統合を許可または禁止します。

ユーザーがローカルのアプリケーションを起動すると、そのアプリケーションが仮想デスクトップ上で動作しているかのように表示されます。

デフォルトでは、ローカルアプリケーションへのアクセスは禁止されます。

URL リダイレクトのブラックリスト

この設定では、ユーザーデバイス上のローカルの Web ブラウザーで開く Web サイトを指定します。通常、ユーザーの現在位置の情報を使用する Web サイト（msn.com や newsgoogle.com など）や、クライアント側で処理した

方が効率的なマルチメディアコンテンツサイトなどの URL を指定します。

デフォルトでは、サイトは指定されていません。

URL リダイレクトのホワイトリスト

この設定では、ユーザーデバイス側にリダイレクトしない Web サイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルデバイスでの動作のポリシー設定

November 28, 2018

モバイルデバイスでの動作セクションには、Citrix Mobility Pack の動作を制御するためのポリシー設定が含まれています。

キーボードの自動表示

この設定では、モバイルデバイス画面上におけるキーボードの自動表示を有効または無効にします。

デフォルトでは、無効になっています。

タッチパネルでの操作に最適化されたデスクトップ

この設定は無効になっており、Windows 10 または Windows Server 2016 マシンでは使用できません。

この設定では、タッチパネルでの操作に最適化されたデスクトップの起動を許可または禁止して、全体的な Citrix Receiver インターフェイスの動作を指定します。

デフォルトでは、タッチパネルでの操作に最適化されたデスクトップが起動します。

通常の Windows インターフェイスのデスクトップを起動する場合は、［禁止］を選択します。

コンボボックスをデバイス側で表示する

この設定では、モバイルデバイスでのセッションで表示するコンボボックスの種類を指定します。モバイルデバイス側のコンボボックスコントロールを表示するには、［許可］を選択します。管理者がこの設定で許可を選択しても、Citrix Receiver for iOS のユーザーは、セッション設定で通常の Windows コンボボックスの表示を選択できます。

デフォルトでは、コンボボックスをデバイス側で表示する機能は禁止されています。

マルチメディアのポリシー設定

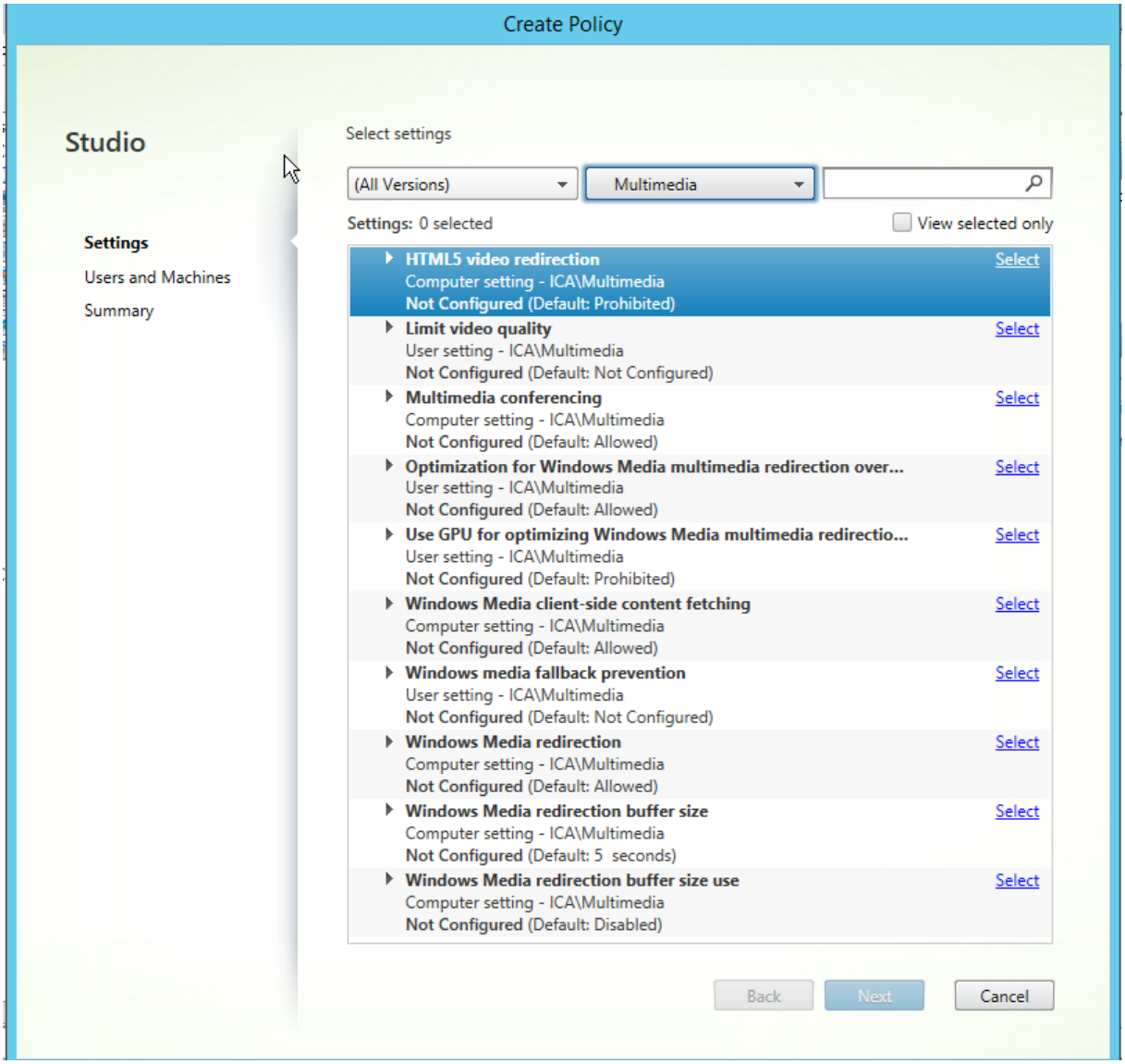
October 22, 2021

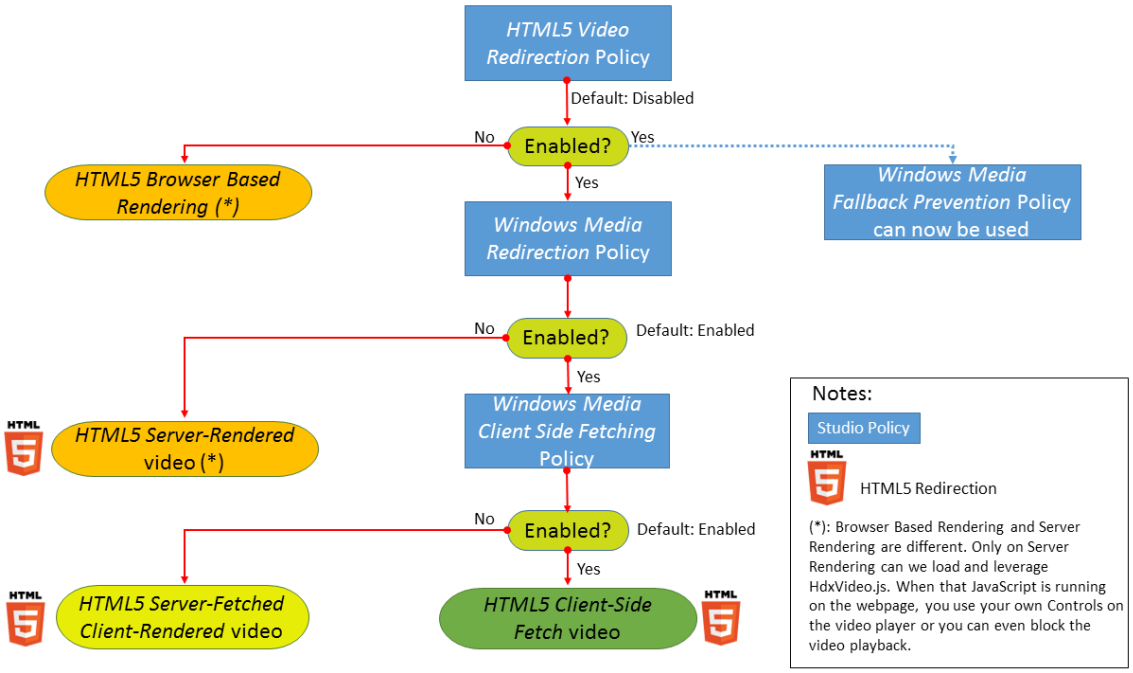
［マルチメディア］セクションには、ユーザーセッションでの HTML5 および Windows のオーディオとビデオのストリーム配信の管理に関するポリシー設定があります。

HTML5 ビデオリダイレクト

XenApp および XenDesktop サーバーがユーザーに HTML5 マルチメディア Web コンテンツを提供する方法を制御、最適化します。

デフォルトでは、この設定は無効になっています。





このリリースでは、この機能は管理対象 Web ページでのみ利用できます。HTML5 マルチメディアコンテンツが利用できる Web ページ（たとえば、社内研修サイトのビデオ）に JavaScript を追加する必要があります。

HTML5 ビデオリダイレクションを構成するには:

1. **HdxVideo.js** ファイルを、VDA のインストール先の%Program Files%/Citrix/ICA Service/HTML5 Video Redirection から、社内 Web ページの場所にコピーします。
2. 次の行を Web ページに挿入します（Web ページに別のスクリプトが設定されている場合は、**HdxVideo.js** をこのスクリプトの前に追加します）:
   `<script src="HdxVideo.js"type="text/javascript"></script>`

注: HdxVideo.js が Web ページと同じ場所にない場合は、**src** 属性を使って HdxVideo.js へのフルパスを指定します。

管理対象の Web ページに JavaScript が追加されていない場合、ユーザーが HTML5 ビデオを再生すると、XenApp および XenDesktop はサーバー側レンダリングにデフォルト設定されます。

Windows Media リダイレクトを許可しないと、HTML5 ビデオリダイレクションは機能しません。このポリシーは、サーバー側フェッチ/クライアント側レンダリングでは必須であり、クライアント側フェッチでも必要とされます（この場合、［*Windows Media* のクライアント側でのコンテンツ取得］を［許可］に設定する必要があります）。

Microsoft Edge ではこの機能はサポートされていません。

HdxVideo.js により、ブラウザーの HTML5 プレーヤーのコントローラーが独自のものに置き換えられます。特定の Web サイトで HTML5 ビデオリダイレクションが有効であるかどうかを確認するには、プレーヤーのコントローラーを ［***HTML5*** ビデオリダイレクション］ポリシーが［禁止］に設定されている場合のシナリオと比較します:

（このポリシーが［許可］に設定されている場合の Citrix のカスタムコントローラー）

（このポリシーが［禁止］に設定されているか未構成の場合のネイティブの Web ページコントローラー）

次のビデオコントロールがサポートされます。

- 再生
- 一時停止
- シーク
- リピート
- オーディオ
- 全画面

HTML5 ビデオリダイレクションのテストページがhttps://www.citrix.com/virtualization/hdx/html5-redirect.htmlにあります。

TLS および **HTML5** ビデオリダイレクション

HTML5 ビデオリダイレクションを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で動作する Citrix HDX HTML5 ビデオリダイレクションサービス（WebSocketService.exe）への TLS 接続を確立する必要があります。このリダイレクションを実現し、Web ページの TLS 整合性を維持するために、Citrix HDX HTML5 ビデオリダイレクションサービスは VDA の証明書ストアで 2 つのカスタム証明書を生成します。

HdxVideo.js は、セキュア WebSocket を使用して VDA で動作する WebSocketService.exe と通信します。このプロセスはローカルシステムで動作し、SSL の終了とユーザーセッションマッピングを実行します。

WebSocketService.exe は 127.0.0.1 ポート 9001 でリスンします。

ビデオ品質の制限

この設定は Windows Media にのみ適用され、HTML5 には適用されません。この設定を使用するには、［*WAN* 接続での *Windows Media* マルチメディアリダイレクトの最適化］を有効化する必要があります。

この設定では、HDX 接続で許可される最大ビデオ品質レベルを指定します。最大ビデオ品質を指定すると、マルチメディアコンテンツに対する一定レベルの QoS（Quality of Service）を保証できます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを指定するには、次のいずれかのオプションを選択します。

- 1080p/8.5mbps
- 720p/4.0mbps

- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

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による最適化された Web カメラリダイレクションテクノロジの使用を許可または禁止します。

デフォルトでは、許可されます。

この設定をポリシーに追加するときは、[Windows Media リダイレクト] 設定で［許可］（デフォルト）が選択されていることを確認してください。

マルチメディア会議を使用する場合、次の条件を満たしていることを確認してください：

- マルチメディア会議に使用する Web カメラの製造元が提供するドライバーが、クライアントにインストール済みである。
- ビデオ会議セッションの開始前に Web カメラをユーザーデバイスに接続している。サーバーで、複数の Web カメラを同時に使用することはできません。ユーザーデバイス上に複数の Web カメラが装着されている場合、サーバーでは、最初に検出されたものから接続が試行されます。

このポリシーは、汎用 USB リダイレクトを使用して Web カメラをリダイレクトする場合は必要ありません。その場合は、VDA に Web カメラドライバーをインストールします。

WAN 接続での **Windows Media** マルチメディアリダイレクトの最適化

この設定は Windows Media にのみ適用され、HTML5 には適用されません。この設定によりリアルタイムマルチメディアトランスコードが有効になります。これにより、オーディオやビデオのメディアコンテンツを劣化ネットワーク経由でモバイルデバイスにストリーム配信することができるようになり、また WAN 通信経由での Windows Media コンテンツの配信方法を改善することでユーザーエクスペリエンスが向上します。

デフォルトでは、WAN を介した Windows Media コンテンツの配信が最適化されます。

この設定をポリシーに追加するときは、[**Windows Media** リダイレクト］設定で ［許可］が選択されていることを確認してください。

この設定を有効にすると、メディアのストリーム配信を有効にするリアルタイムマルチメディアトランスコードが必要に応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

この設定は Windows Media にのみ適用され、Virtual Delivery Agent（VDA）上のグラフィック処理ユニット（GPU）でリアルタイムマルチメディアトランスコード処理を行うことができるようになります。これにより、サーバースケーラビリティが改善されます。GPU でのトランスコード処理は、VDA 側にハードウェアアクセラレーションをサポートする GPU が搭載されて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。

Windows メディアフォールバック防止

この設定は HTML5 と Windows Media の両方に適用されます。この設定を HTML5 で使用するには、［***HTML5*** ビデオリダイレクション］ポリシーを ［許可］に設定します。

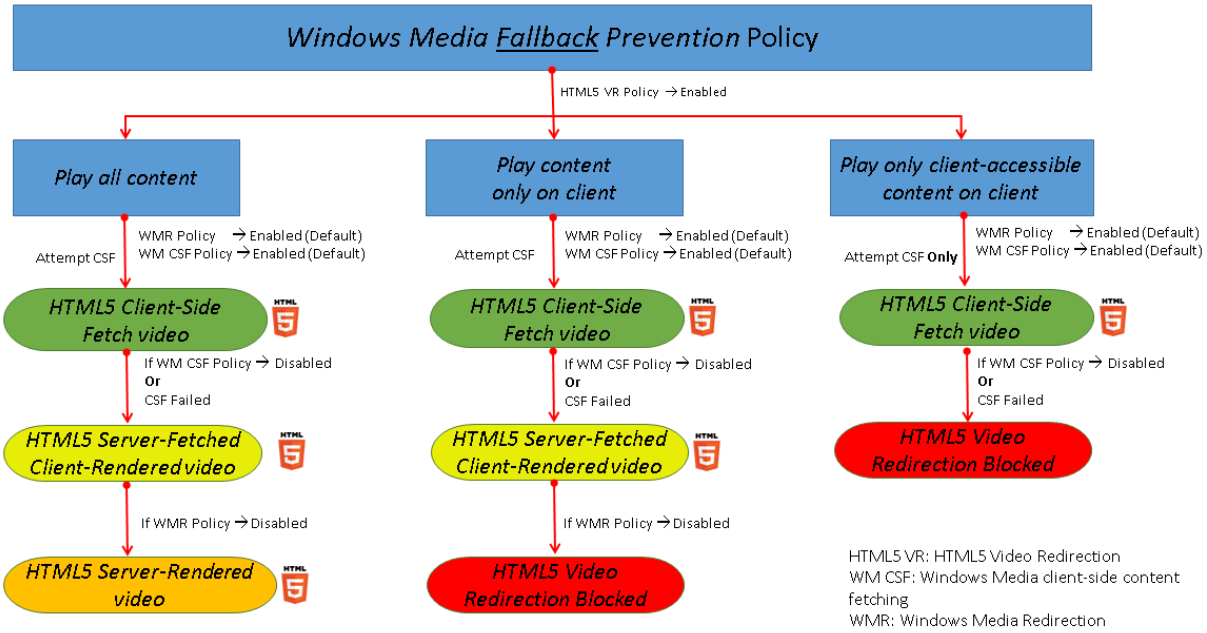
管理者はこの Windows メディアバック防止ポリシー設定を使って、ユーザーへのストリーム配信コンテンツの配信方法を指定できます。

デフォルトでは、この設定は構成されていません。この設定が［未構成］に設定されている場合の動作は、［すべてのコンテンツを再生］のものと同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- すべてのコンテンツを再生：クライアント側でのコンテンツ取得、Windows Media リダイレクトの順に試行します。失敗した場合、サーバー上でコンテンツを再生します。
- クライアントにあるすべてのコンテンツのみを再生：クライアント側でのフェッチ、Windows Media リダイレクトの順に試行します。失敗した場合、コンテンツは再生されません。
- クライアント上のクライアントがアクセスできるコンテンツのみを再生：クライアント側でのフェッチのみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツを再生しない場合、プレーヤーのウィンドウにエラーメッセージ「Company has blocked video because of lack of resources」が表示されます（デフォルトの期間は 5 秒間）。



エラーメッセージが表示される期間は、VDA の次のレジストリキーでカスタマイズできます。レジストリにエントリがない場合は、期間はデフォルトで 5 秒間になります。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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。

レジストリパスは、VDA のアーキテクチャによって異なります。

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー:

値の名前:VideoLoadManagementErrDuration

種類:DWORD

範囲:1 から DWORD 制限まで(デフォルト = 5)

単位:秒

Windows Media のクライアント側でのコンテンツ取得

この設定は HTML5 と Windows Media の両方に適用されます。この設定では、インターネットまたはイントラネット上のマルチメディアファイルを、XenApp や XenDesktop のホストサーバーを介さずにソースプロバイダーか

らユーザーデバイスへ直接ストリーム配信することを許可または禁止します。

デフォルトでは、［許可］に設定されています。この設定を許可すると、マルチメディアファイルがホストサーバーではなくユーザーデバイス上で処理されるため、ネットワーク消費が効率化され、サーバースケーラビリティが向上します。また、ユーザーデバイス上に Microsoft DirectShow や Media Foundation などの高度なマルチメディアフレームワークをインストールする必要もなくなり、ユーザーデバイスでは URL からファイルを再生することだけできればよくなります。

この設定をポリシーに追加するときは、［**Windows Media** リダイレクト］設定で ［許可］が選択されていることを確認してください。［**Windows Media** リダイレクト］設定を無効にすると、Windows Media のクライアント側でのコンテンツ取得機能も無効になります。

Windows Media リダイレクト

この設定は HTML5 と Windows Media の両方に適用され、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。

デフォルトでは、［許可］に設定されています。HTML5 の場合、［***HTML5*** ビデオリダイレクション］ポリシーが ［禁止］に設定されているとこの設定は適用されません。

この設定を許可すると、セッション内で再生されるオーディオおよびビデオの品質が向上して、ユーザーデバイス上のファイルを再生しているときの品質に近くなります。マルチメディアデータはサーバーからユーザーデバイスに、元の圧縮されたままの形で配信され、ユーザーデバイス側でメディアの展開およびレンダリングが行われます。

Windows Media ダイレクトでは、Microsoft 社の DirectShow、DirectX Media Objects（DMO）、および Media Foundation 規格に準拠するコーデックでエンコードされたマルチメディアファイルが最適化されます。ユーザーデバイス側でメディアファイルの展開およびレンダリングを行うため、そのファイルのエンコーディング形式をサポートするコーデックがユーザーデバイス上にインストールされている必要があります。

デフォルトでは、Citrix Receiver でオーディオポリシーの構成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 メディアリダイレクトによるメディアの再生品質が、基本的な ICA 圧縮および通常のオーディオ機能での品質よりも悪い場合は、［禁止］を選択します。キーフレームの周波数が著しく低いメディアデータを狭帯域幅接続で再生する場合などで、この機能による問題がまれに生じることがあります。

Windows Media リダイレクトのバッファーサイズ

この設定は古いものであり、HTML5 には適用されません。

この設定では、マルチメディアアクセラレーションのバッファーサイズを 1〜10 秒の間で指定します。

デフォルトのバッファーサイズは 5 秒です。

Windows Media リダイレクトのバッファーサイズ使用

この設定は古いものであり、HTML5 には適用されません。

この設定では、[**Windows Media** リダイレクトバッファーサイズ] 設定で指定したバッファーサイズを有効または無効にします。

デフォルトでは、指定されているデフォルトバッファーサイズが使用されません。

この設定が無効の場合、または Windows Media リダイレクトバッファーサイズ設定が構成されていない場合、サーバーではデフォルトのバッファーサイズ値（5 秒）が使用されます。

マルチストリーム接続のポリシー設定

August 24, 2021

マルチストリーム接続セクションには、セッションでの複数 ICA 接続の QoS（Quality of Service）優先度の管理に関するポリシー設定が含まれます。

UDP を使用したオーディオ

この設定では、サーバーの UDP を使用したオーディオを許可または禁止します。

デフォルトでは許可されます。

この機能を有効にすると、サーバー上の UDP ポートが開き、[UDP でのオーディオリアルタイムトランスポート] 設定が有効なすべての接続でそのポートが使用されます。

オーディオ **UDP** ポートの範囲

この設定項目では、Virtual Delivery Agent（VDA）でユーザーデバイスとのオーディオパケットデータの送受信に使用されるポート番号の範囲を「<lowest port number>,<highest port number>」形式で指定します。VDA では、オーディオデータの送受信に各 UDP ポートペアの使用が試行されます。まず最小のポート番号が使用され、以降の試行では 2 ずつ番号を増やしていきます。各ポートは、受信トラフィックと送信トラフィックの両方に使用されます。

デフォルトでは、「16500,16509」に設定されています。

マルチポートポリシー

この設定では、ICA トラフィックで使用される TCP ポートおよび各ポートのネットワーク優先度を指定します。

デフォルトでは、プライマリポート（2598）に優先度［高］が設定されています。

ポートには、以下の優先度を設定できます。

- 最高 - Web カメラを使ったビデオ会議など、リアルタイムプロセスに適しています。
- 高 - 画面、キーボード、マウスなど、インタラクティブなトラフィックに適しています。
- 中 - クライアント側ドライブのマッピング機能など、バルクプロセスに適しています。
- 低 - 印刷など、バックグラウンドプロセスに適しています。

各ポートには異なる優先度を設定する必要があります。つまり、CGP ポート 1 と CGP ポート 3 の両方で優先度に［最高］を設定することはできません。

ポートの優先度設定を削除するには、ポート番号として「0」を入力します。プライマリポートの優先度設定を削除したり変更したりすることはできません。

この設定項目をポリシーに追加したら、サーバーを再起動します。この設定は、［マルチストリームコンピューター］設定の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 SD-WAN でマルチストリーム機能をサポートする場合は、この設定項目を使用する必要はありません。このポリシー設定は、サードパーティ製のルーターや従来の Branch Repeater を使用する環境で QoS（Quality of Service）優先度を指定するときに使用できます。

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］設定の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、予期しない動作が発生する可能性があります。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

August 24, 2021

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

August 24, 2021

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］>［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］>［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

August 24, 2021

クライアントプリンターセクションには、クライアントプリンターに関するポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保存、およびプリントサーバーへの接続のための設定が含まれています。

クライアントプリンターを自動作成する

この設定では、自動作成するクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定より優先されます。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、［クライアントプリンターリダイレクト］設定で［許可］が選択されている場合にのみ適用されます。

この設定では、次のオプションを選択します。

- ［すべてのクライアントプリンターを自動作成する］では、ユーザーデバイス上のすべてのプリンターが自動作成されます。
- ［デフォルトのクライアントプリンターのみを自動作成する］では、ユーザーデバイス上のデフォルトプリンターのみが自動作成されます。
- ［ローカル（ネットワークを介さない）クライアントプリンターのみを自動作成する］では、ユーザーデバイスのローカルポート（LPT ポート、COM ポート、USB ポート、TCP/IP ポートなど）に直接接続されているプリンターのみが自動作成されます。
- ［クライアントプリンターを自動作成しない］では、ユーザーがログオンするときのすべてのクライアントプリンターの自動作成が無効になります。リモートデスクトップサービス（RDS）で設定されているクライアントプリンターの自動作成オプションが適用されるようにするには、このオプションを選択して、そのポリシーの優先度をほかのポリシーよりも高くします。

汎用ユニバーサルプリンターを自動作成する

注：このポリシー設定問題を解決するための Hotfix が Citrix Knowledge Center の CTX141565 および CTX141566 で提供されています。

この設定では、UDP をサポートするクライアントのセッションで Citrix ユニバーサルプリンターの汎用印刷オブジェクトを自動作成する機能を有効または無効にします。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連する設定項目は以下のとおりです。

- ユニバーサル印刷の使用
- ユニバーサルドライバーの優先度

クライアントプリンター名

この設定では、自動作成されるクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

[標準のプリンター名］を選択すると、「セッション 3 のクライアント名の HP LaserJet 4」などのプリンター名が作成されます。

MetaFrame Presentation Server 3.0 またはそれ以前のバージョンと互換性のある命名規則でクライアントプリンターを作成するには、［従来のプリンター名］を選択します。
この場合、「Client/clientname#/HPLaserJet 4」などの名前が使用されます。このオプションは安全性に欠けます。

注：このオプションは、以前のバージョンの XenApp や XenDesktop との互換性を保持する場合に使用します。

プリントサーバーへの直接接続

この設定では、ネットワーク共有上のクライアントプリンターを使用するときに、クライアントを経由せずに仮想デスクトップやホストサーバーからプリントサーバーに直接接続することを有効または無効にします。

デフォルトでは有効になっています。

仮想デスクトップやホストサーバーとネットワークプリントサーバーが同一 LAN 上にあり、WAN で隔たれていない場合に直接接続を有効にします。この場合、仮想デスクトップやホストサーバーから LAN を介してプリントサーバーに直接印刷データが転送されるため、処理が高速になります。

仮想デスクトップやホストサーバーとネットワークプリントサーバーが WAN で隔たれていたり、遅延や帯域幅の問題が生じたりする場合は、直接接続を無効にできます。直接接続を無効にすると、印刷ジョブがユーザーデバイスに送信され、そこからネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、データが WAN を横断するときに消費される帯域幅が少なくなります。

同じ名前を持つネットワークプリンターが 2 つ存在する場合は、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定では、自動作成されるクライアントプリンターのドライバー置換規則を指定します。

この設定は、自動作成されるクライアントプリンターの一覧から Microsoft OneNote と XPS Document Writer を除外して構成されます。

ドライバー置換規則を定義すると、プリンターの自動作成時に特定のドライバーの使用を許可したり、ユニバーサル印刷の使用を指定したりできます。ドライバーの置換規則では、サーバーとクライアント間でドライバー名をマップして、ユーザーデバイスから提供されるプリンタードライバーではなくサーバー上のドライバーが使用されるように設定します。これにより、サーバー側のドライバーとクライアント側のドライバーの名前が異なっていても、サーバー上のアプリケーションからクライアントプリンターに出力できるようになります。

ドライバー置換規則の一覧では、ドライバーマッピングの追加、既存のマッピングの編集、マッピングに対するカスタム設定の上書き、マッピングの削除、および一覧のドライバーエントリの順序の変更を実行できます。マッピングを追加するには、クライアント側プリンタードライバーの名前を入力し、それを置換するサーバー側プリンタードライバーを選択します。

プリンタープロパティの保存

この設定では、ユーザーが変更したクライアントプリンターのプロパティをどこに保存するかを指定します。

デフォルトでは、システムの判定により、クライアントデバイスに保存できない場合にのみユーザープロファイルにプリンタープロパティが保存されます。

この設定では、次のオプションを選択します。

- [クライアントデバイスにのみ保存する] は、更新されないユーザープロファイル（固定プロファイルや移動プロファイル）を使用する環境で選択します。このオプションは、サーバーファーム内のすべてのサーバーで XenApp 5 以降が動作しており、ユーザーが Citrix Online Plug-in Versions 9〜12.x、または Citrix Receiver 3.x を使用する場合にのみ選択してください。
- [ユーザープロファイルにのみ保存する] は、使用帯域幅とログオン速度に制限があるユーザーデバイス（このオプションではネットワークトラフィックが軽減されます）、または古いプラグインソフトウェアを使用するユーザーのためのオプションです。このオプションでは、サーバー上のユーザープロファイルにプリンタープロパティを保存し、ユーザーデバイス上のプロパティを使用しません。このオプションは、Presentation Server 3.0 またはそれ以前のバージョンと、Presentation Server クライアント 8.x 以前が使用される環境で選択してください。ただし、このオプションはリモートデスクトップサービス（RDS）の移動プロファイルにのみ適用されます。
- [クライアントに保存できない場合にのみユーザープロファイルに保存する] では、システムによりプリンタープロパティの保存先が決定されます。ユーザーデバイスに保存できない場合にのみ、ユーザープロファイルにプリンタープロパティが保存されます。さまざまな環境やクライアントの条件に対応できるオプションですが、システムチェック処理が行われるため、ログオン時に遅延が生じたり使用帯域幅が増えたりすることがあります。
- [プリンタープロパティを保持しない] を選択した場合、プリンタープロパティは保持されません。

クライアントプリンターの保持と復元

この設定では、ユーザーデバイス上のプリンターをセッション間で保持および再作成する機能を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

「保持されるプリンター」とは、ユーザーが作成し次回セッションの開始時に再作成されるプリンターを指します。保持されるプリンターが XenApp により再作成されるときは、［クライアントプリンターを自動作成する］設定以外のすべてのポリシー設定が考慮されます。

「復元されるプリンター」とは、管理者がカスタマイズしクライアントポートに永続的に接続された状態で保存されるプリンターを指します。

ドライバーのポリシー設定

February 3, 2020

ドライバーセクションには、プリンタードライバーに関するポリシー設定が含まれています。

付属のプリンタードライバーの自動インストール

この設定項目では、Windows に付属のドライバーセットや、pnputil.exe /a によりホスト上にステージングされたドライバーパッケージから、プリンタードライバーを必要に応じて自動的にインストールする機能を有効または無効にします。

デフォルトでは、自動インストールが有効になっています。

ユニバーサルドライバーの優先度

この設定項目では、ユニバーサルプリンタードライバーの使用優先順位を指定します。一覧の上位にあるドライバーから順に使用されます。

デフォルトの優先順位は以下のとおりです。

- EMF
- XPS
- PCL5c
- PCL4
- PS

この一覧では、ドライバーを追加、編集、または削除したり、優先順位を変更したりできます。

ユニバーサル印刷の使用

この設定では、どのような状況でユニバーサル印刷を使用するかを指定します。

デフォルトでは、要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用します。

ユニバーサル印刷では、プリンター固有の標準ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理がシンプルになります。ユニバーサルプリンタードライバーを使用できるかどうかは、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアにより決定されます。構成によっては、ユニバーサル印刷を使用できない場合があります。

この設定では、次のオプションを選択します。

- ［プリンター固有のドライバーのみを使用する］では、クライアントプリンターの自動作成時に、そのプリンター固有の標準プリンタードライバーが使用されます。必要なプリンタードライバーがサーバーにない場合、そのクライアントプリンターは自動作成されません。
- ［ユニバーサル印刷のみを使用する］を有効にすると、プリンター固有の標準ドライバーは使用されません。ユニバーサルプリンタードライバーのみを使用してプリンターが作成されます。
- ［要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する］では、可能な場合はプリンター固有の標準ドライバーが使用されます。プリンター固有のドライバーがサーバーにない場合は、最適なユニバーサルドライバーを使用してクライアントプリンターが自動作成されます。
- ［ユニバーサル印刷を使用できない場合にのみプリンター固有のドライバーを使用する］では、可能な場合はユニバーサルプリンタードライバーが使用されます。ユニバーサルプリンタードライバーがサーバーにない場合は、適切なプリンター固有の標準ドライバーを使用してクライアントプリンターが自動作成されます。

Universal Print Server のポリシー設定

February 3, 2020

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。

ユニバーサルプリントサーバーの有効化

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。

ユニバーサルプリントサーバー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。

ユニバーサルプリントサーバー入力データストリームの最大帯域幅（**Kpbs**）

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。

ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）ポート

この設定では、Universal Print Server の Web サービス（HTTP/SOAP）リスナーで使用される TCP ポート番号を指定します。ユニバーサルプリントサーバーはオプションコンポーネントで、ネットワークプリンターでの Citrix ユニバーサルプリントドライバーの使用を有効にします。ユニバーサルプリントサーバーが使用されると、印刷コマンドが SOAP over HTTP 上の SOAP を経由して XenApp および XenDesktop ホストからユニバーサルプリントサーバーに送信されます。この設定は、ユニバーサルプリントサーバーが 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ユニバーサルプリントサーバーに接続しません。この設定は、XenApp および XenDesktop 上の VDA を変更します。また、ユニバーサルプリントサーバーのデフォルトのポートを変更する必要があります。

デフォルトのポート番号は、8080 に設定されています。

ほかのポートを指定する場合は、0 から 65535 の番号を使用してください。

負荷分散のためのユニバーサルプリントサーバー

この設定には、Citrix のほかの印刷ポリシー設定を評価した後、セッション起動時に確立されるプリンター接続の負荷分散に使用するユニバーサルプリントサーバー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。

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

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

February 3, 2020

ユニバーサル印刷セクションには、ユニバーサル印刷の管理に関するポリシー設定が含まれています。

ユニバーサル印刷 **EMF** 処理モード

この設定では、Windows ユーザーデバイス上での EMF スプールファイルの処理方法を制御します。

デフォルトでは、EMF スプールファイルがクライアント上のスプールキューに直接挿入されます。

この設定では、次のオプションを選択します。

- ［EMF スプールファイルを再処理する］を有効にすると、EMF スプールファイルが再処理され、ユーザーデバイス上の GDI サブシステム経由で送信されます。通常、EMF 再処理を必要とするドライバーは自動的に検出

され、適切な印刷経路が使用されますが、セッションで正しく検出されない場合があります。そのような場合にこのオプションを選択します。

- Citrix ユニバーサルプリンタードライバーで［EMF スプールファイルを直接挿入する］を有効にすると、EMF レコードがホスト上でスプールされ、その EMF スプールファイルがユーザーデバイス側に送信され処理されます。通常、この EMF スプールファイルはクライアント上のスプールキューに直接挿入されます。EMF 形式を処理できるプリンターおよびドライバーでは、この方法により印刷を高速に実行できます。

ユニバーサル印刷イメージ圧縮制限

この設定では、Citrix ユニバーサルプリンタードライバーでのイメージ印刷で使用できる品質レベルの上限を指定します。

デフォルトでは、イメージ品質の上限が［最高品質（無損失圧縮）］に設定されています。

［非圧縮］を選択すると、EMF 印刷では圧縮が無効になります。

この設定では、次のオプションを選択します。

- 圧縮なし
- 最高品質（無損失圧縮）
- 高品質
- 標準品質
- 低品質（最大圧縮）

この設定項目を［ユニバーサル印刷最適化デフォルト］と同じポリシーに追加する場合は、次の点に注意してください。

- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベルが［ユニバーサル印刷最適化デフォルト］での設定よりも低い場合は、［ユニバーサル印刷イメージ圧縮制限］の圧縮レベルが適用されます。
- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、［ユニバーサル印刷最適化デフォルト］の［必要なイメージ品質］および［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル印刷最適化デフォルト

この設定では、セッションで作成されるユニバーサルプリンタードライバーのデフォルトの印刷最適化オプションを指定します。

- ［必要なイメージ品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを印刷できます。
- ［ヘビーウェイト圧縮を有効にする］では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。デフォルトでは、ヘビーウェイト圧縮は無効になっています。

- ［イメージおよびフォントのキャッシュ］では、印刷ストリームで使用されているイメージやフォントをキャッシュするかどうかを指定します。キャッシュを有効にすると、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。デフォルトでは、埋め込みイメージおよびフォントがキャッシュされます。これらの設定は、ユーザーデバイスでその機能をサポートしている場合にのみ適用されます。
- ［非管理者によるこれらの設定の変更を許可する］では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。デフォルトでは、禁止されています。

注：これらのすべてのオプションは、EMF 印刷に対してのみ適用されます。XPS 印刷では、［必要なイメージ品質］オプションのみがサポートされます。

この設定項目を［ユニバーサル印刷イメージ圧縮制限］と同じポリシーに追加する場合は、次の点に注意してください。

- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベルが［ユニバーサル印刷最適化デフォルト］での設定よりも低い場合は、［ユニバーサル印刷イメージ圧縮制限］の圧縮レベルが適用されます。
- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、［ユニバーサル印刷最適化デフォルト］の［必要なイメージ品質］および［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル印刷プレビューの設定

この設定では、自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューは使用できません。

この設定では、次のオプションを選択します。

- 自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューを使用しない
- 自動作成プリンターの印刷プレビューのみを使用する
- 汎用ユニバーサルプリンターの印刷プレビューのみを使用する
- 自動作成プリンターおよび汎用ユニバーサルプリンターの印刷プレビューを使用する

ユニバーサル印刷品質制限

この設定では、セッションでの印刷出力で使用できる最大 DPI 値（インチあたりのドット数）を指定します。

デフォルトでは［制限なし］が選択されており、ユーザーは接続しているプリンターで許可されている最高印刷品質を選択できます。

そのほかの値を選択すると、ユーザーが使用できる出力解像度が制限されます。この設定では、印刷品質自体と、ユーザーが接続するプリンターの印刷能力の両方が制限されます。たとえば、［中解像度（600dpi）］を選択した場合、ユーザーの印刷出力の最高品質は 600DPI に制限され、ユニバーサルプリンターの［詳細設定］タブの印刷品質設定には、中品質（600DPI）を超える解像度オプションが表示されなくなります。

この設定では、次のオプションを選択します。

- ドラフト（150 dpi）
- 低解像度（300 dpi）
- 中解像度（600 dpi）
- 高解像度（1200 dpi）
- 制限なし

セキュリティのポリシー設定

November 28, 2018

セキュリティセクションには、セッションの暗号化とログオンデータの暗号化の構成に関するポリシー設定が含まれています。

SecureICA の最低暗号化レベル

この設定では、サーバーとユーザーデバイスの間で送信するセッションデータの暗号化に必要な最低限の暗号化レベルを指定します。

重要：Virtual Delivery Agent 7.x の場合、この設定を RC5 128 ビット暗号化によるログオンデータの暗号化を有効にするためだけに使用できます。ほかの暗号化レベルは、以前のバージョンの XenApp や XenDesktop との互換性を保持する場合に使用します。

VDA 7.x の場合、セッションデータの暗号化は VDA のデリバリーグループの基本設定を使って設定されます。デリバリーグループに対して［Secure ICA を有効にする］がオンになっている場合、セッションデータは RC5（128 ビット）暗号化で暗号化されます。デリバリーグループに対して［Secure ICA を有効にする］がオフになっている場合、セッションデータは基本レベルの暗号化で暗号化されます。

この設定では、次のオプションを選択します。

- ［基本］では、非 RC5 のアルゴリズムを使ってクライアント接続を暗号化します。この暗号化レベルでは、データストリームが直接読み取られることはありませんが、解読される恐れがあります。デフォルトでは、クライアントとサーバーの間のトラフィックには基本レベルの暗号化が使用されます。
- ［RC5（128 ビット、ログオンのみ）］では、RC5 128 ビット暗号化を使ってログオンデータを暗号化し、基本レベルの暗号化を使ってクライアント接続を暗号化します。
- ［RC5（40 ビット）］では、RC5 40 ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（56 ビット）］では、RC5 56 ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（128 ビット）］では、RC5 128 ビット暗号化を使ってクライアント接続を暗号化します。

クライアントとサーバー間の実際の通信では、Citrix 製品や Windows オペレーティングシステムでの暗号化設定も考慮されます。サーバーやユーザーデバイスでより高い暗号化レベルが設定されている場合は、その設定が優先されます。

機密データを使用するユーザーなど、特定のユーザーの通信データを保護してメッセージの整合性を保証するために、より高度な暗号化レベルを設定することもできます。ポリシーでより高度な暗号化レベルを指定すると、そのレベルよりも低い暗号化機能を使用する Citrix Receiver は、サーバーに接続できなくなります。

SecureICA では認証の実行またはデータの整合性のチェックはされません。エンドツーエンドの暗号化を提供するには、SecureICA を TLS と共に使用します。

SecureICA では FIPS 準拠のアルゴリズムは使用されません。このことが問題になる場合は、SecureICA を使用しないようにサーバーと Citrix Receiver を設定します。

SecureICA は、秘密保持のために RFC 2040 で説明されているように RC5 ブロック暗号を使用します。ブロックサイズは、64 ビット（32 ビットワード単位の倍数）です。キーの長さは、128 ビットです。ラウンド数は、12 です。

サーバーの制限のポリシー設定

August 24, 2021

[サーバーの制限] カテゴリには、アイドル状態の接続の制御に関する設定項目が含まれています。

サーバーのアイドルタイマーの間隔

この設定では、アイドル状態のセッション（ユーザーからの入力がない連続セッション）を自動的に切断するまでの時間をミリ秒単位で指定します。

デフォルトでは、アイドル状態の接続は切断されません。つまり、サーバーのアイドルタイマーの間隔は 0 です。この値を 60000 ミリ秒（60 秒）以上に設定することをお勧めします。

> 注
>
> このポリシー設定が使用される場合、セッションが指定した時間アイドル状態になると、「アイドルタイマーが切れました」ということを示すダイアログボックスがユーザーに表示されることがあります。このメッセージは Microsoft のダイアログボックスであり、Citrix ポリシー設定によって制御されるものではありません。詳しくは、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

August 24, 2021

[セッションの制限] セクションには、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ポリシー設定が含まれています。

> 重要:
>
> この記事で説明する設定は、Windows Server VDA には適用されません。サーバー VDA のセッション時間制限の構成の詳細については、「マイクロソフト KB -セッション時間制限」を参照してください。

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。このタイマーが有効な場合、タイマーが期限切れになると、切断されたセッションはログオフします。

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。このタイマーが有効な場合、タイマーが期限切れになると、セッションが切断されるかログオフします。Microsoft の制限時間に達したらセッションを終了する設定によって次のセッションの状態が決定します。

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。タイマーが期限切れになると、セッションは切断状態になり、［切断セッションタイマー］が適用されます。［切断セッションタイマー］が無効になると、セッションはログオフします。

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

March 1, 2019

セッション画面の保持セクションには、セッション画面の保持の管理に関するポリシー設定が含まれています。

セッション画面の保持

この設定では、セッション画面の保持機能を許可または禁止します。セッション画面の保持およびクライアントの自動再接続によって、ネットワークの中断からの回復後、ユーザーは Citrix Receiver セッションに自動的に再接続できます。デフォルトでは、セッション画面の保持が許可されます。

Citrix Receiver for Windows 4.7 以降では、Studio の設定がクライアントに適用されます。クライアントの Citrix Receiver グループポリシーオブジェクトは、Studio ポリシーによって上書きされます。Studio でこれらのポリシーを更新すると、サーバーからクライアントにセッション画面の保持が同期されます。

> 注:
>
> - Citrix Receiver for Windows 4.7 以降、および Windows 向け Citrix Workspace アプリの場合、Studio でポリシーを設定します。
> - バージョン 4.7 より古い Citrix Receiver for Windows の場合、Studio でポリシーを設定し、クライアントで Citrix Receiver グループポリシーオブジェクトテンプレートを設定することで動作を安定させます。

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。接続が失われると、ユーザーの表示は不透明になります。中断中、ユーザーにはセッションが停止しているように見えることがあり、ネットワーク接続が回復するとアプリケーションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

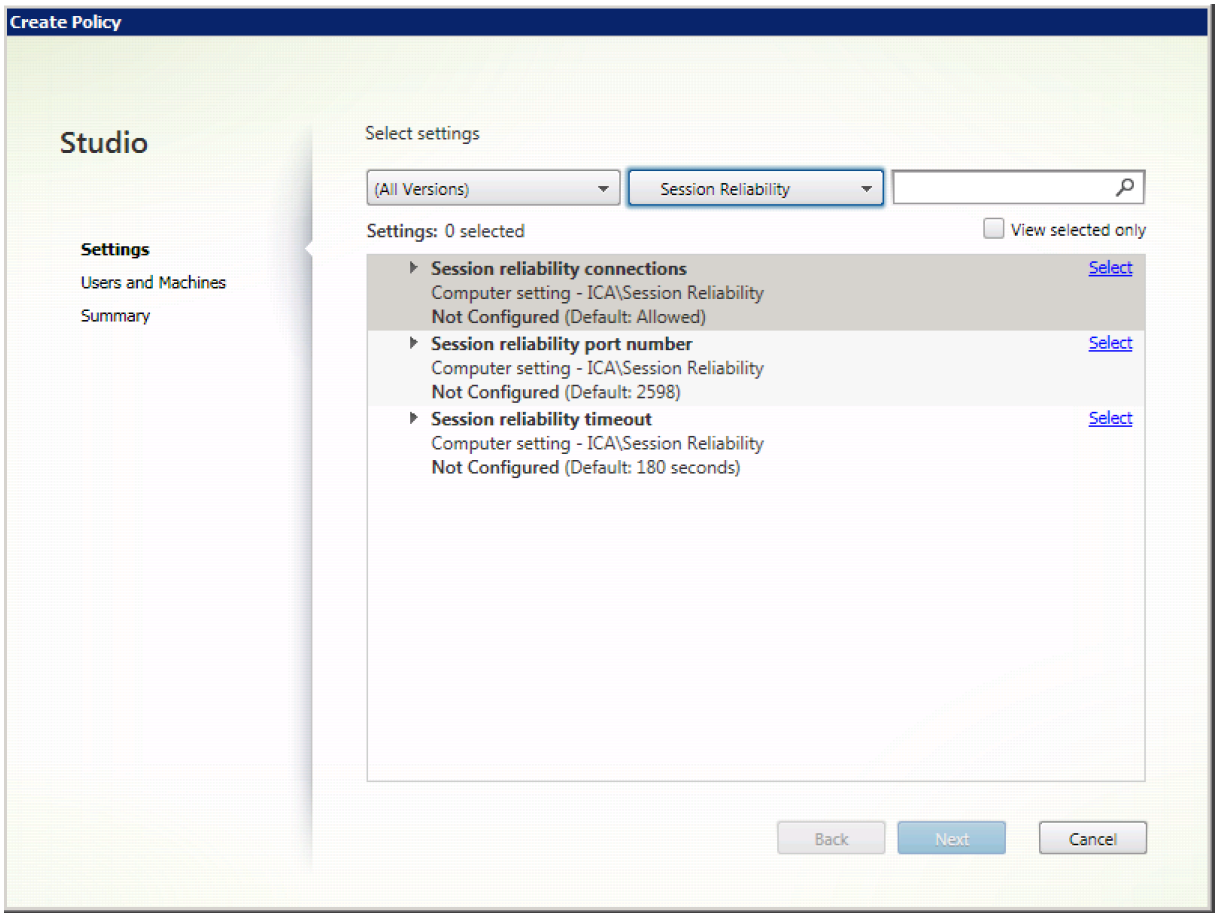
セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッション

が終了または切断されます。この後でクライアントの自動再接続のポリシー設定により、切断セッションへの再接続が行われます。

デフォルトでは、セッション画面の保持が許可されます。

セッション画面の保持を無効にするには:

1. Citrix Studio を開始します。
2. [セッション画面の保持] ポリシーを開きます。
3. ポリシーを [禁止] に設定します。



セッション画面の保持のポート番号

この設定では、セッション画面の保持機能で使用される、受信 TCP ポートを指定します。

デフォルトでは、ポート番号は、2598 に設定されます。

セッション画面の保持のポート番号を変更するには:

1. Citrix Studio を開始します。
2. [セッション画面の保持のポート番号] ポリシーを開きます。
3. ポート番号を編集します。

4. [**OK**] をクリックします。

セッション画面の保持のタイムアウト

この設定では、セッション画面の保持機能でセッションをアクティブのままサーバー上に保持する時間を秒単位で指定します。ここで指定した時間が経過しても再接続されないセッションは、「切断セッション」として処理されます。

セッションの持続時間を長く設定することもできますが、この機能は利便性が高く、ユーザーに再認証を求めるメッセージを表示することもありません。セッションの持続時間を長くすると、ユーザーがデバイスを置き去りして承認されていないユーザーに利用される可能性が高まります。

デフォルトでは、タイムアウトは 180 秒（3 分）に設定されています。

セッション画面の保持のタイムアウトを変更するには

1. Citrix Studio を開始します。
2. [セッション画面の保持のタイムアウト] ポリシーを開きます。
3. タイムアウト値を編集します。
4. [**OK**] をクリックします。

タイムゾーン制御のポリシー設定

November 28, 2018

タイムゾーン制御セクションには、セッションでのローカルタイムの使用に関するポリシー設定が含まれています。

レガシークライアントのローカルタイムゾーンを検出する

この設定では、クライアント側のローカルタイムゾーンの検出を有効または無効にします。クライアントによっては、正確なタイムゾーン情報がサーバーに送信されない場合があります。

デフォルトでは、必要に応じてクライアント側のタイムゾーンが検出されます。

この設定は、詳しいタイムゾーン情報をサーバーに送信しない、従来の Citrix Receiver または ICA クライアントでの使用を前提にしています。Windows でサポートされているバージョンの Citrix Receiver など、サーバーに詳しいタイムゾーン情報を送信する Citrix Receiver で使用する場合、この設定は何の影響も及ぼしません。

クライアントのローカルタイムゾーンを使用する

この設定では、ユーザーセッションに適用されるタイムゾーンを指定します。ユーザーセッションにサーバー側のタイムゾーンを適用したり、ユーザーデバイス側のタイムゾーンを適用したりできます。

デフォルトでは、ユーザーセッションのタイムゾーンが適用されます。

この機能を使用するには、グループポリシーエディターの［タイムゾーンリダイレクトを許可する］設定（[ユーザーの構成］>［管理用テンプレート］>［Windows コンポーネント］>［リモートデスクトップサービス］>［リモートデスクトップセッションホスト］>［デバイスとリソースのリダイレクト]）を有効にしてください。

TWAIN デバイスのポリシー設定

August 24, 2021

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
>
> Citrix Receiver for Windows 4.5 では、TWAIN 2.0 がサポートされています。

クライアント TWAIN デバイスリダイレクト

この設定では、サーバー上でホストされる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、TWAIN デバイスリダイレクトは許可されています。

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（%）

> 注:
>
> 64 ビットアプリケーションを使用する場合、TWAIN リダイレクトはサポートされません。

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

August 24, 2021

［USB デバイス］セクションには、USB デバイスのファイルリダイレクトの管理に関するポリシー設定が含まれています。

クライアント **USB** デバイス最適化規則

クライアント USB デバイス最適化規則をデバイスに適用して最適化を無効にしたり、最適化モードを変更したりできます。

ユーザーが USB 入力デバイスを接続すると、デバイスが USB ポリシー設定で許可されているかどうかホストがチェックします。デバイスが許可されている場合は、次にホストはデバイスのクライアント **USB** デバイス最適化規則をチェックします。規則が指定されていない場合は、デバイスは最適化されません。キャプチャモード（04）は署名デバイスに対する推奨モードです。長い遅延のためにパフォーマンスが低下しているその他のデバイスに対して、管理者は対話モード（02）を有効にできます。使用できるモードについては、以下の説明を参照してください。

ヒント

- Wacom 署名パッドおよびタブレットを使用する場合、スクリーンセーバーを無効にすることをお勧めします。その実行方法については、このセクションの最後で説明します。
- Wacom STU 署名パッドおよびタブレット製品シリーズの最適化のサポートは、XenApp および XenDesktop ポリシーのインストールで事前構成されています。
- 署名デバイスは XenApp および XenDesktop で動作し、署名デバイスとして使用するためのドライバーは必要ありません。Wacom には、デバイスをよりカスタマイズするためインストールできる追加のソフトウェアがあります。「https://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
Mode	最適化モードは、class=03 の入力デバイスでサポートされます。サポートされているモードは次のとおりです：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（4 桁の 16 進数値）
PID	デバイス記述子の製品 ID（4 桁の 16 進数値）
REV	デバイス記述子のリビジョン ID（4 桁の 16 進数値）

タグ名	説明
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

例

Mode=00000004 VID=067B PID=1230 class=03 # キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 # 対話モードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 # 最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 # 最適化が無効に設定されているデバイス（デフォルト）

Mode=00000200 VID=067B PID=1230 # 最適化が有効に設定されているデバイス

Wacom 署名パッドデバイスのスクリーンセーバーの無効化

Wacom 署名パッドおよびタブレットを使用する場合、次の手順に従ってスクリーンセーバーを無効にすることをお勧めします。

1. デバイスのリダイレクト後に **Wacom-STU-Driver** をインストールします。
2. **Wacom-STU-Display MSI** をインストールして、署名パッドコントロールパネルへのアクセスを有効にします。
3. ［コントロールパネル］**>** ［**Wacom STU Display**］**>** ［**STU430**］または ［**STU530**］の順に選択し、使用しているモデルのタブを選択します。
4. UAC セキュリティウィンドウがポップアップ表示されたら ［**Change**］をクリックしてから ［**Yes**］をクリックします。
5. ［**Disable slideshow**］を選択して、［**Apply**］をクリックします。

1 つの署名パッドモデルに対しての設定が完了したら、それがすべてのモデルに適用されます。

クライアント **USB** デバイスリダイレクト

この設定では、USB デバイスのクライアント側へのリダイレクトおよびクライアント側からのリダイレクトを許可または禁止します。

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がチェックされます。最初の一致が Allow 規則の場合、USB デバイスは仮想デスクトップにリモートで接続されます。最初の一致が Deny 規則の場合、その USB デバイスはローカルデスクトップでのみ使用可能になります。一致する規則がない場合、デフォルトの規則が使用されます。

ポリシー規則は、{Allow: | Deny:} の後に、「tag=value」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（4 桁の 16 進数値）
PID	デバイス記述子の製品 ID（4 桁の 16 進数値）
REL	デバイス記述子のリリース ID（4 桁の 16 進数値）。
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

新しいポリシー規則を作成する場合、以下の点に注意してください:

- 大文字と小文字は区別されません。
- 規則の末尾に、# で始まる任意のコメントを追加できます。
- 空白行およびコメントのみの行は無視されます。
- タグには等号（=）を使用する必要があります（例：VID=067B）。
- 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=067B 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拒否する場合は、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

August 24, 2021

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。

単純なグラフィックスの優先色深度

このポリシー設定は VDA バージョン 7.6 FP3 以降で使用できます。8 ビットオプションは VDA バージョン 7.12 以降で使用できます。

この設定により、単純なグラフィックがネットワーク経由で送信される際の色数を低下させることができます。ピクセルあたり 8 ビットまたは 16 ビットに色数を低下させると、画質をわずかに犠牲して、低帯域幅接続での応答性を潜在的に向上させることができます。［圧縮にビデオコーデックを使用する］ポリシー設定が［画面全体］に設定されている場合、8 ビット色数はサポートされません。

デフォルトの優先色数は、ピクセルあたり 24 ビットです。

8 ビット設定が VDA バージョン 7.11 以前に適用されている場合、VDA は 24 ビット（デフォルト）色数にフォールバックします。

ターゲットフレーム数

この設定項目では、仮想デスクトップからユーザーデバイスに送信されるイメージの 1 秒あたりの最大フレーム数（fps）を指定します。

デフォルトの最大フレーム数は、30fps です。

1 秒あたりのフレーム数を高く（30 など）すると、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1 秒あたりのフレーム数を低く（10 など）すると、ユーザーエクスペリエンスは低下しますが、サーバーのスケーラビリティが向上します。CPU が低速なユーザーデバイスに対しては、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。

サポートされている 1 秒あたりの最大フレームレートは 60 です。

表示品質

この設定では、ユーザーデバイス側に表示されるイメージの表示品質を指定します。

デフォルトでは、［中］に設定されています。

イメージの表示品質を指定するには、次のいずれかのオプションを選択します。

- 低 - 対話操作性のために表示品質を低下させてもよい、帯域幅が制限されたネットワークに適しています。
- 中 - 一般的に最良のパフォーマンスおよび帯域幅効率が提供されます。
- 高 - 視覚的に無損失なイメージ品質が提供されます。
- 操作時は低品質 - 多くのネットワークトラフィックが発生している間は非可逆イメージが送信され、ネットワークトラフィックが減少したときに高品質な無損失イメージが送信されます。この設定により、帯域幅を制限されたネットワーク接続でのパフォーマンスが向上します。
- 常に無損失 - X 線写真を表示するなど、イメージの画質が優先される場合には、［常に無損失］を選択して、非可逆イメージデータがユーザーデバイスに送信されないようにします。

［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

August 24, 2021

動画セクションには、動画の圧縮機能を無効にしたり変更したりするためのポリシー設定が含まれています。

画質の下限レベル

注: Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、アダプティブ表示の最低レベルの画質を指定します。圧縮率が小さいほど、画質は高くなります。超最高、最高、高、通常、または低から選択します。

デフォルトでは、［通常］に設定されています。

動画圧縮

この設定では、アダプティブ表示を有効または無効にします。アダプティブ表示機能では、ビデオやスライドショーのスライド切り替え時の画質が、使用可能な帯域幅に基づいて自動的に調節します。アダプティブ表示を有効にすると、表示品質を劣化させることなくプレゼンテーションをスムーズに実行できます。

デフォルトでは、アダプティブ表示が有効になっています。

VDA 7.0～7.6 では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA Version 7.6 FP1 以降については、従来のグラフィックモードが有効の場合、または従来のグラフィックモードが無効でグラフィックの圧縮にビデオコーデックが使用されていない場合、この設定が適用されます。

従来のグラフィックモードが有効な場合、ポリシーの変更を適用する前にセッションを再起動する必要があります。アダプティブ表示とプログレッシブ表示は相互に排他的です。アダプティブ表示を有効にすると、プログレッシブ表示は無効になり、その逆の場合も同じです。ただし、プログレッシブ表示とアダプティブ表示の両方を同時に無効にすることは可能です。従来からの機能であるプログレッシブ表示は XenApp または XenDesktop にはお勧めしません。プログレッシブしきい値レベルを設定するとアダプティブ表示は無効になります。

プログレッシブ圧縮のレベル

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、最初にダウンロードされるイメージの品質を落として、初期表示のパフォーマンスを向上させる機能を制御します。

デフォルトでは、プログレッシブ圧縮は適用されません。

プログレッシブ圧縮では、初期表示の後で、より詳細なイメージデータがダウンロードされます（そのイメージの圧縮レベルは非可逆圧縮設定で制御されます）。［最高］または［超最高］を選択すると、写真など帯域幅に負荷のかかるグラフィックの表示パフォーマンスが向上します。

プログレッシブ圧縮による効果を得るには、
［非可逆圧縮のレベル］よりも高い圧縮レベルを指定する必要があります。

注：プログレッシブ表示の圧縮レベルを高くすると、セッションでの動的イメージの対話操作性が向上します。この機能を有効にすると、3D モデルを回転させる場合など、イメージを動かしている間の表示品質は一時的に低下します。イメージを停止させると、非可逆圧縮のレベルで制御される画質が適用されます。

関連する設定項目は以下のとおりです。

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮のしきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、プログレッシブ圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。この帯域幅に達しないクライアント接続にのみ圧縮が適用されます。

デフォルトのしきい値は、2147483647KB/秒です。

関連する設定項目は以下のとおりです。

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

保持する最低フレーム数

この設定では、低帯域幅接続時に確保される動的イメージの最低フレーム数を、フレーム数/秒（fps）単位で指定します。

デフォルトでは、10fps に設定されています。

VDA 7.0～7.6 では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA 7.6 FP1 以降では、［従来のグラフィックモード］が有効であるか無効であるかにかかわらず、この設定が適用されます。

静止画のポリシー設定

August 24, 2021

静止画セクションには、静止画の圧縮機能を無効にしたり変更したりするための設定が含まれています。

エクストラ色圧縮

この設定では、狭帯域幅接続でのイメージ配信で使用されるエクストラ色圧縮機能を有効または無効にします。この機能を有効にすると、イメージ品質が低下しますが狭帯域幅接続におけるセッションの応答性が向上します。

デフォルトでは、エクストラ色圧縮は無効になっています。

エクストラ色圧縮を有効にした場合、［エクストラ色圧縮しきい値］の設定値を下回るクライアント接続でのみこの圧縮機能が適用されます。クライアント接続の帯域幅がしきい値を上回る場合、または［エクストラ色圧縮］設定で［無効］が選択されている場合、この圧縮機能は適用されません。

エクストラ色圧縮しきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、エクストラ色圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。クライアント接続帯域幅がこの値を下回る場合、エクストラ色圧縮が適用されます（［エクストラ色圧縮］設定で［有効］が選択されている場合）。

デフォルトのしきい値は、8192KB/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、プログレッシブ圧縮よりもさらに消費帯域幅を節約する機能を有効または無効にします。ヘビーウェイト圧縮では、CPU 要求度の高いグラフィックアルゴリズムが使用され、画質を損なわずにイメージデータで使用される帯域幅を抑えることができます。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

この圧縮機能を有効にすると、すべての非可逆圧縮設定に適用されます。この機能は Citrix Receiver でサポートされ、ほかのプラグインソフトウェアでは無視されます。

関連する設定項目は以下のとおりです。

- プログレッシブ圧縮のレベル
- プログレッシブ圧縮のしきい値

非可逆圧縮のレベル

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、狭帯域幅接続でのイメージ配信で使用される非可逆圧縮のレベルを指定します。狭帯域幅接続では、ICA セッション内での非圧縮イメージの表示に時間がかかる場合があります。

デフォルトでは、中レベルの圧縮が選択されています。

イメージ表示のパフォーマンスを改善させるには、高い圧縮レベルを使用します。逆に、X 線写真を表示するなどイメージの画質が優先される場合では、非可逆圧縮を無効にします。

関連する設定項目：非可逆圧縮のしきい値

非可逆圧縮のしきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、非可逆圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。

デフォルトのしきい値は、2147483647KB/秒です。

非可逆圧縮のしきい値を指定せずに［非可逆圧縮のレベル］設定をポリシーに追加すると、LAN 環境での高精細ビットマップ（写真など）の表示速度が向上する場合があります。

関連する設定項目：非可逆圧縮のレベル

WebSocket のポリシー設定

August 24, 2021

WebSocket セクションには、Citrix Receiver for HTML5 を使用した仮想デスクトップおよびホストアプリケーションへのアクセスに関するポリシー設定が含まれています。WebSocket 機能により、Web ブラウザーアプリケーションとサーバー間の双方向通信が有効になります。複数の HTTP 接続を確立する必要がないため、セキュリティが向上し、サーバーのオーバーヘッドが軽減されます。

WebSocket 接続

この設定では、WebSocket プロトコルによる接続を許可または禁止します。

デフォルトでは、無効になっています。

WebSocket ポート番号

この設定では、WebSocket 接続の着信ポートの番号を指定します。

デフォルトでは、値は 8008 です。

WebSocket 信頼される接続元サーバー一覧

この設定では、信頼される接続元サーバー（通常 Citrix Receiver for Web）の URL をコンマ区切りの一覧で指定します。この一覧に追加したサーバーからの WebSocket 接続のみが受け入れられます。

デフォルトでは、ワイルドカード文字「*」が設定されています。これにより、すべての Citrix Receiver for Web サイト URL が信頼され、アクセスが許可されます。

この設定では、URL を以下の形式で指定します。

```
<protocol>://<Fully qualified domain name of host>:[port]
```

ここで、<protocol> は HTTP または HTTPS です。<port> 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

August 24, 2021

負荷管理セクションには、Windows サーバーマシン間の負荷を管理するためのポリシー設定が含まれています。

負荷評価基準インデックスの計算については、CTX202150を参照してください。

同時ログオントレランス

この設定では、サーバーが許容できる同時ログオンの最大数を指定します。

デフォルトでは、「2」に設定されています。

この設定が有効になっているときは、サーバー VDA 上のアクティブな同時ログオン数が指定された数を超えないように負荷分散されます。ただし、上限は厳密に制限されていません。上限を制限する（指定された数値を超える同時ログインを失敗させる）には、次のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
種類：DWORD
値：1

CPU 使用率

この設定では、サーバーを「負荷限界」とみなす CPU 使用率をパーセンテージで指定します。この設定を有効にすると、デフォルトで 90% になったときにそのサーバーが負荷限界として認識されます。

デフォルトでは無効になっており、CPU 使用率が負荷計算から除外されます。

CPU 使用率から除外するプロセスの優先順位

この設定では、特定の優先度レベル以下のプロセスを CPU 使用率の負荷計算から除外できます。

デフォルトでは、［通常以下］または［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、768MB に設定されています。

Profile Management のポリシー設定

August 24, 2021

[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

August 24, 2021

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。

自動構成機能は、ランタイムの環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーのようなものです。これによって、設定を手動で構成する必要がなくなります。ランタイム環境には、以下の要素が含まれます:

- Windows OS
- Windows OS バージョン
- Citrix Virtual Desktops がある
- Personal vDisk がある

環境が変更されると、自動構成により次のポリシーが変更される場合があります:

- アクティブライトバック
- 常時キャッシュ
- 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
- キャッシュしたプロファイルを削除する前の待ち時間
- プロファイルストリーミング

上記のポリシーに関して OS ごとのデフォルトの状態については、次の表を参照してください:

	サーバー OS	デスクトップ OS
アクティブライトバック	有効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。
常時キャッシュ	無効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。
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	有効	無効。Personal vDisk が使用されている場合、Citrix Virtual Desktops が割り当てられている場合、または Citrix Virtual Desktops がインストールされていない場合。それ以外の場合は有効。
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 秒	ユーザーの変更が永続的でない場合は 60 秒。それ以外の場合は 0 秒。
プロファイルストリーミング	有効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。

ただし、自動構成機能を無効にすると、上記のすべてのポリシーがデフォルトで無効になります。

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。

ログオフ時にインターネット **Cookie** ファイルを処理

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

March 25, 2020

基本設定セクションには、Profile Management の基本構成に関するポリシー設定が含まれています。

アクティブライトバック

この設定では、更新されたファイルやフォルダー（レジストリ設定は除く）をセッション中、つまりユーザーがログオフする前にユーザーストアに同期する機能を有効または無効にします。

デフォルトでは、無効になっています。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、有効になります。

Profile Management の有効化

この設定では、Profile Management によるログオンおよびログオフのプロファイル処理を有効または無効にします。

デフォルトでは、展開を容易にするために無効になっています。

重要：Profile Management を有効にする前に、ほかのすべてのセットアップタスクを実行し、Citrix ユーザープロファイルの動作をテストすることをお勧めします。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここでまたは INI ファイルで構成しない場合、Profile Management はいかなる方法でも Windows ユーザープロファイルを処理しません。

除外グループ

この設定では、Profile Management でのプロファイル処理から除外するコンピューターのローカルグループおよびドメイングループ（ローカル、グローバル、およびユニバーサル）を指定します。

この設定を有効にすると、指定したユーザーグループのプロファイルが Profile Management で処理されなくなります。

この設定はデフォルトで無効になっており、すべてのユーザーグループのプロファイルが処理されます。

ドメイングループは、「ドメイン名\グループ名」の形式で指定します。

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。
- 無効または未構成。この場合、#homeDirectory#\Windows の値が使用されます。

このポリシー設定を構成する場合、以下の変数を使用します。

- パーセントで囲まれたシステム環境変数（%ProfVer% など）。ただし、システム環境変数が正しくセットアップされている必要があります。
- ハッシュで囲まれた Active Directory ユーザーオブジェクトの属性（#sAMAccountName# など）。
- Profile Management の変数。詳しくは、Profile Management のドキュメントを参照してください。

%username% や%userdomain% などのユーザー環境変数を使用したり、location や users などの組織の変数を完全に定義するカスタム属性を作成したりすることもできます。属性では大文字と小文字が区別されます。

例：

- 「\\server\share#sAMAccountName#」と指定した場合、UNC パス\server\share\JohnSmith にユーザー設定が格納されます（現在のユーザーの #sAMAccountName# 属性が JohnSmith である場合）。
- 「\\server\profiles$%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS!」と指定した場合、「\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64」などに格納されます。

重要：属性や変数を使用する場合は、NTUSER.DAT があるフォルダーの 1 つ上のフォルダーを指定していることを確認してください。たとえば、NTUSER.DAT が\\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile にある場合は、ユーザーストアのパスとして「\\server\profiles$\JohnSmith.Finance\v2x64」を指定します。UPM_Profile サブフォルダーを含める必要はありません。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、ホームドライブの Windows ディレクトリが使用されます。

ローカル管理者のログオン処理

この設定では、BUILTIN\Administrators グループのメンバーのログオンを処理するかどうかを指定します。これにより、ローカルの管理者権限があるドメインユーザー（通常、仮想デスクトップが割り当てられているユーザー）がログオン時のプロファイル処理をバイパスして、Profile Management で問題が生じているデスクトップのトラブルシューティングを行えるようになります。

この設定が無効または構成しない場合、サーバーオペレーティングシステムではドメインユーザーのログオンは処理されますが、ローカル管理者のログオンは処理されません。デスクトップオペレーティングシステムでは、ローカル管理者のログオンも処理されます。

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、「ドメイン名\グループ名」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

March 25, 2020

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

November 28, 2018

［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

November 28, 2018

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

October 22, 2021

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との間で同期する、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ディレクトリを指定します。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

November 28, 2018

［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

August 24, 2021

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の場所を指定します。

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

August 24, 2021

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、Contacts フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Contacts 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

August 24, 2021

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

この設定では、Desktop フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Desktop 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

August 24, 2021

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、Documents フォルダーのリダイレクト先のネットワークの場所を指定します。

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 Documents フォルダーにリダイレクトするだけではなく、Music、Pictures、Videos 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、Documents 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。

Documents フォルダーの内容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

August 24, 2021

［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、Downloads フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Downloads 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

August 24, 2021

［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、Favorites フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Favorites 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

August 24, 2021

［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、Links フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Links 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

August 24, 2021

［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、Music フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Music 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。

Music 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。
- Documents フォルダーに相対的リダイレクト: Documents 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 Documents フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定を構成しない場合、このフォルダーは Profile Management によりリダイレクトされません。

ピクチャのポリシー設定

August 24, 2021

［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、Pictures フォルダーのリダイレクト先のネットワークの場所を指定します。

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、Pictures 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。

Pictures 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。
- Documents フォルダーに相対的リダイレクト： Documents 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 Documents フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定を構成しない場合、このフォルダーは Profile Management によりリダイレクトされません。

保存したゲームのポリシー設定

August 24, 2021

［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、Saved Games 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、Saved Games フォルダーのリダイレクト先のネットワークの場所を指定します。

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

August 24, 2021

［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、Start Menu 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、Start Menu フォルダーのリダイレクト先のネットワークの場所を指定します。

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

August 24, 2021

［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、Searches 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、Searches フォルダーのリダイレクト先のネットワークの場所を指定します。

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

August 24, 2021

［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、Video 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。

Video 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。
- Documents フォルダーに相対的リダイレクト: Documents 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 Documents フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定を構成しない場合、このフォルダーは Profile Management によりリダイレクトされません。

ビデオパス

この設定では、Video フォルダーのリダイレクト先のネットワークの場所を指定します。

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

August 24, 2021

［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、この設定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、この設定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、この設定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、この設定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、この設定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、この設定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

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、この設定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\UserProfileMa
にログファイルが生成されます。

保存フォルダーのパスとして、ローカルドライブ、リモートドライブ、またはネットワークドライブ（UNC パス）を指定できます。リモートドライブは大規模な分散環境では便利ですが、大量のネットワークトラフィックが発生するためログファイルには不適切である場合があります。プロビジョニングした仮想マシンに永続的なハードドライブがある場合は、そのドライブ上のローカルパスを指定します。これにより、仮想マシンを再起動してもログファイルが保持されます。永続的なハードドライブがない仮想マシンの場合、UNC パスを指定するとログファイルを保持できますが、この仮想マシンのシステムアカウントにはその UNC パスに対する書き込みアクセス権が必要です。オフラインプロファイル機能で管理するラップトップコンピューターの場合は、ローカルパスを使用します。

ログファイルを UNC パス上のフォルダーに保存する場合は、そのフォルダーに適切なアクセス制御リストを適用して、認証されたユーザーやコンピューターのみがログファイルにアクセスできるようすることをお勧めします。

この設定をここで構成しない場合、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\UserProfi
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、この設定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、この設定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、この設定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、この設定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

August 24, 2021

［プロファイル制御］カテゴリには、Profile Management でのユーザープロファイル管理機能を制御するための設定項目が含まれています。

キャッシュしたプロファイルを削除する前の待ち時間

この設定では、ローカルにキャッシュされたプロファイルをそのユーザーのログオフ後に Profile Management が削除するまでの待機時間を指定します。

0 を指定すると、ログオフ処理が完了した後でプロファイルが直ちに削除されます。Profile Management では、1 分ごとにログオフの状態がチェックされます。このため、この設定項目で 60 を指定すると、ユーザーのログオフ後 1〜2 分後にプロファイルが削除されます。ログオフ時にファイルやレジストリハイブにアクセスするプロセスがある場合は、ここで待機時間を延長できます。また、プロファイルのサイズが大きい場合、待機時間を延長することでログオフ時間が短縮されることがあります。

デフォルトでは 0 が指定されており、ローカルにキャッシュされたプロファイルがログオフ後に直ちに削除されます。

この設定を有効にするときは、［ログオフ時にローカルでキャッシュしたプロファイルの削除］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、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
- ローカル
- ローミング
- 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ほかのフォルダーやファイルを格納しているフォルダーのものである必要があります。

注：パスに「NTUSER.DAT」を含めないでください。たとえば、「\\myservername\myprofiles\template\ntuser.dat」ではなく「\\myservername\myprofiles\template」を指定します。

UNC パスやローカルマシン上のパスなどの絶対パスを使用します。たとえば、Citrix Provisioning Services イメージ上のテンプレートプロファイルを永続的に指定するにはローカルマシン上のパスを指定します。相対パスは使用できません。

注：Active Directory 属性の拡張、システム環境変数、および%USERNAME% や%USERDOMAIN% 変数を使用することはできません。

この設定はデフォルトで無効になっており、最初にログオンしたデバイス上のデフォルトのユーザープロファイルを基にそのユーザーのプロファイルが作成されます。

この設定をここで構成しない場合、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

March 25, 2020

［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

October 22, 2021

［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ミング］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ミング

この設定では、Profile Management によるユーザープロファイルのストリーム配信機能を有効または無効にします。この設定を有効にすると、プロファイルに含まれるファイルやフォルダーが、ログオンしたユーザーがアクセスした時点でユーザーストアからローカルコンピューターに取得されます。待機領域内のレジストリエントリやファイルは、直ちに取得されます。

デフォルトでは、無効になっています。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定では、ストリーム配信する組織単位のユーザープロファイルを Windows ユーザーグループで指定します。

この設定を有効にすると、指定したユーザーグループのユーザープロファイルのみがストリーム配信されます。ほかのユーザープロファイルは、通常どおりに処理されます。

この設定はデフォルトで無効になっており、組織単位のすべてのユーザープロファイルが通常どおりに処理されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミングの除外機能を有効にするには

プロファイルストリーム配信除外機能を有効にすると、ユーザーがログオンしたときに、Profile Management はログオン除外一覧に指定されたフォルダーを配信せず、すべてのフォルダーはユーザーストアからローカルコンピューターに直ちには同期されません。

詳しくは、「プロファイルストリーム配信除外機能を有効にするには」を参照してください。

待機領域のロックファイルのタイムアウト

この設定項目では、サーバーが応答不能になってユーザーストアのロックが解除されない場合に、待機領域のファイルをユーザーストアに同期するまでの日数を指定します。これにより、待機領域が膨張することを防いで、ユーザーストアに常に最新のファイルが同期されるようになります。

デフォルトでは、1 日に設定されています。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定および INI ファイルをここで構成しない場合、デフォルト値が使用されます。

Receiver のポリシー設定

January 22, 2019

注：特に明記されていない限り、「Receiver」は Citrix Receiver を指します。

[Receiver] カテゴリには、仮想デスクトップ上の Citrix Receiver for Windows で使用される StoreFront アドレスの一覧を指定するための設定項目が含まれています。

StoreFront アカウント一覧

この設定では、仮想デスクトップ上で実行される Citrix Receiver for Windows に設定する StoreFront ストアの一覧を指定します。デリバリーグループを作成するときに、管理者はこの一覧からストアを選択して、そのデリバリーグループの仮想デスクトップ上で動作する Citrix Receiver for Windows に適用できます。

デフォルトでは、ストアは指定されていません。

一覧にストアを追加するときは、以下の情報をセミコロンで区切って入力します。

- ストア名：ユーザーに表示されるストア名です。
- ストア URL：ストアの URL です。
- ストアの有効/無効：そのストアをユーザーが使用できるかどうかを「On」または「Off」で指定します。
- ストアの説明：ユーザーに表示される説明です。

例：Sales Store;`https://sales.mycompany.com/Citrix/Store/discovery;On;Store` for Sales staff

Virtual Delivery Agent のポリシー設定

October 31, 2019

[Virtual Delivery Agent 設定］カテゴリには、Virtual Delivery Agent（VDA）と Controller 間の通信を制御するための設定項目が含まれています。

重要：重要：VDA を Delivery Controller に登録するときに、これらの設定項目で提供される情報が必要になります（自動更新機能を使用しない場合）。これらの情報は登録に必要であるため、グループポリシーエディターを使って以下の設定項目を構成する必要があります（VDA のインストール時にこれらの情報を指定する場合を除く）。

- コントローラー登録の IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用する
- サイト GUID

コントローラー登録の **IPv6** ネットマスク

このポリシー設定では、VDA で使用されるサブネットを指定できます。この場合、グローバル IP は使用されません。これにより、指定した IPv6 アドレスおよびネットワークでのみ VDA が登録されます。VDA は、指定されたネットマスクに最初にマッチしたアドレスでのみ登録されます。この設定を使用する場合は、［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。

コントローラー登録ポート

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定で［禁止］が選択されていることを確認してください。

この設定項目では、VDA の Controller 登録をレジストリで行うときに使用される TCP/IP ポート番号を指定します。

デフォルトのポート番号は、80 に設定されています。

コントローラー **SID**

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定で［禁止］が選択されていることを確認してください。

この設定項目では、VDA の Controller 登録をレジストリで行うときに使用される Controller のセキュリティ識別子（SID）をスペース区切りの一覧で指定します。これはオプションの設定項目で、［Controller］設定と一緒に使用して、登録に使用される Controller の一覧を制限できます。

デフォルトでは、空白になっています。

コントローラー

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。

コントローラーの自動更新を有効にする

この設定項目では、インストール後の VDA を Controller に自動的に登録する機能を許可または禁止します。

VDA を Controller に登録すると、登録先の Controller により環境内の Controller の FQDN および SID の一覧が VDA に送信されます。この一覧の内容は、VDA により永続的なストレージに書き込まれます。また、各 Controller は 90 分ごとにサイトのデータベースにアクセスして、Controller の追加や削除、およびポリシーの変更内容について確認し、登録した VDA に更新情報を送信します。VDA は、受信した最新の一覧に基づいてすべての Controller からの接続を受け入れます。

デフォルトでは、有効になっています。

IPv6 コントローラー登録のみを使用する

この設定項目では、Controller への登録時に VDA で使用されるアドレスの形式を指定します。

- この設定項目を有効にすると、そのマシンの IPv6 アドレスを使用して VDA が Controller と登録および通信を行います。VDA が Controller と通信するときに、グローバル IP アドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（ほかの IPv6 アドレスを使用できない場合のみ）の順で IPv6 アドレスが選択されます。
- この設定が無効な場合、そのマシンの IPv4 アドレスを使用して VDA が Controller と登録および通信を行います。

デフォルトでは、無効になっています。

サイト **GUID**

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定で［禁止］が選択されていることを確認してください。

この設定項目では、VDA の Controller 登録を Active Directory ベースで行うときに使用される、サイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、空白になっています。

HDX 3D Pro のポリシー設定

August 24, 2021

[HDX 3D Pro] カテゴリには、ユーザーの画質構成ツールを有効にして構成するための設定項目が含まれています。ユーザーがこのツールを使用すると、画質と応答性間のバランスをリアルタイムで調整して、帯域幅の使用を最適化できます。

無損失を有効にする

この設定では、ユーザーが画質構成ツールで無損失圧縮を有効にしたり無効にしたりすることを許可するかどうかを指定します。デフォルトでは、ユーザーは無損失圧縮を有効にできません。

ユーザーが無損失圧縮を有効にすると、自動的に画質構成ツールで設定可能な最高画質に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの能力に応じて、GPU または CPU ベースの圧縮が使用されます。

HDX 3D Pro 品質レベル

この設定では、ユーザーが画質構成ツールで設定できる画質調整範囲の最小値および最大値を指定します。

画質は 0～100 の値で指定します。最大値には、最小値を超える値を設定する必要があります。

監視のポリシー設定

August 24, 2021

監視セクションには、プロセスとリソースの監視、およびアプリケーション障害の監視に関するポリシー設定が含まれています。

これらのポリシーのスコープは、サイト、デリバリーグループ、デリバリーグループの種類、組織単位、およびタグによって定義されます。

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントは VDA から収集され、監視データベースに格納されます。VDA からデータポイントを送信するとネットワーク帯域幅が消費され、これを保存すると監視データベースで大幅に容量が消費されます。特定のスコープ（特定のデリバリーグループや組織単位など）でリソースデータとプロセスデータのいずれか、または両方とも監視しない場合は、ポリシーを無効にすることをお勧めします。

プロセスの監視を有効にします

この設定を有効にすると、VDA がインストールされているマシンでのプロセスの監視が許可されます。CPU やメモリ使用量などの統計が監視サービスに送信されます。統計は、Director でのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は無効になっています。

リソースの監視を有効にします

この設定を有効にすると、VDA がインストールされているマシンでのクリティカルパフォーマンスカウンターの監視が許可されます。統計（CPU やメモリ使用量、IOPS、ディスク遅延などのデータ）が監視サービスに送信されます。統計は、Director でのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は有効になっています。

スケーラビリティ

CPU およびメモリデータは、各 VDA からデータベースに 5 分間隔で適用されます。プロセスデータ（有効な場合）は、データベースに 10 分間隔で適用されます。IOPS およびディスク遅延データは、データベースに 1 時間間隔で適用されます。

CPU とメモリデータ

CPU とメモリデータは、デフォルトで ［有効］に設定されています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
5 分データ	1 日
10 分データ	7 日間
時間単位のデータ	30 日間
日単位のデータ	90 日間

IOPS およびディスク遅延データ

IOPS およびディスク遅延データは、デフォルトで有効になっています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
時間単位のデータ	3 日
日単位のデータ	90 日間

上記のデータ保持設定では、1 つの VDA の CPU、メモリ、IOPS、およびディスク遅延のデータを 1 年間格納するのに約 276KB の容量が必要です。

マシン数	必要なストレージ
1	276KB
1K	270MB
40K	10.6GB

プロセスデータ

デフォルトでは、プロセスデータは無効になっています。プロセスデータは、必要に応じてマシンのサブセットで有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データの粒度	日数
10 分のデータ	1 日
時間単位のデータ	7 日間

プロセスデータがデフォルトの保持設定で有効な場合、プロセスデータは 1 年間で VDA あたり約 1.5MB、ターミナルサービス VDA（TS VDA）あたり約 3MB 消費します。

マシン数	必要なストレージ（VDA）	必要なストレージ（TS VDA）
1	1.5MB	3MB
1,000	1.5GB	3GB

> 注
>
> 上記の数値には、インデックス領域は含まれません。上記の計算は概算であり、展開によって異なる可能性があります。

オプションの構成

デフォルトの保持設定をニーズに合わせて変更できます。ただし、これはストレージを余分に消費します。以下の設定を有効にすると、プロセス使用率データがより正確になります。有効にできる構成は次のとおりです。

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

これらの構成は、監視 Powershell コマンドレットSet-MonitorConfigurationで有効にできます。

アプリケーション障害の監視ポリシー

デフォルトでは、［アプリケーション障害］タブは、サーバー OS の VDA からのアプリケーション障害のみが表示されます。アプリケーション障害の監視の設定は、以下の監視ポリシーによって変更できます。

アプリケーション障害の監視を有効にする

アプリケーション障害の監視を、アプリケーションのエラーまたは障害（クラッシュと未処理例外）のいずれか、または両方を監視するように構成するには、以下の設定を行ってください。
［値］を ［なし］に設定して、アプリケーション障害の監視を無効にしてください。
デフォルトでは、この設定はアプリケーション障害のみになっています。

デスクトップ **OS VDA** でアプリケーション障害の監視を有効にする

デフォルトでは、サーバー OS の VDA でホストされたアプリケーションの障害のみが監視されています。デスクトップ OS の VDA を監視するには、このポリシーを ［許可］に設定します。
デフォルトでは、この設定は ［禁止］になっています。

障害の監視から除外するアプリケーション一覧

障害を監視しないアプリケーションの一覧を指定します。
デフォルトでは、この一覧は空です。

ストレージ計画のヒント

グループポリシーリソースデータやプロセスデータを監視しない場合は、グループポリシーを使用してどちらかまたは両方をオフにできます。詳しくは、「ポリシーの作成」の「グループポリシー」セクションを参照してください。

データのグルーミングデフォルトのデータ保持設定を変更して、データを早くグルーミングし、ストレージ領域を開放できます。グルーミングの設定について詳しくは、「API を使ったデータアクセス」の「データの粒度と保持」を参照してください。

仮想 IP のポリシー設定

March 25, 2020

［仮想 IP］カテゴリには、セッションの仮想ループバックアドレスの使用を制御するための設定項目が含まれています。

仮想 IP ループバックサポート

この設定項目では、各セッション固有の仮想ループバックアドレスの使用を有効にするかどうかを指定します。無効にすると、セッション固有の仮想ループバックアドレスは使用されません。

デフォルトでは、この設定は無効になっています。

仮想 IP ループバックプログラム一覧

この設定項目では、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。一覧にプログラムを追加するときは、実行可能ファイルの名前のみを指定します。パス全体を入力する必要はありません。

複数の実行可能ファイルを追加するには、各ファイルを別々の行に追加します。

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

August 24, 2021

VDA バージョン 7.0～7.8 では、COM ポートおよび LPT ポートの設定はレジストリを使用した場合にのみ構成できます。7.0 より前のバージョンの VDA、および VDA バージョン 7.9 以降では、これらの設定は Studio で構成できます。詳しくは、「ポートリダイレクトのポリシー設定」および「帯域幅のポリシー設定」を参照してください。

COM ポートおよび LPT ポートのリダイレクト設定は、VDA イメージまたはマシンのレジストリ HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\Deprecated で構成します。

COM ポートおよび LPT ポートリダイレクトを有効にするには、以下のレジストリキーを追加して REG_DWORD 値を設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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

October 31, 2019

［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。

警告表示間隔

この設定項目では、警告メッセージを表示する間隔を定義します。

間隔は、ddd.hh:mm:ss 形式で設定します。

- ddd はオプションのパラメーターで、日数を 0～999 で指定します。
- hh は時間で、0～23 で指定します。
- mm は分で、0～59 で指定します。
- ss は秒で、0～59 で指定します。

デフォルトでは、01:00:00（1 時間）が設定されています。

警告メッセージの内容

この設定項目では、予定されているソフトウェア更新、またはログオフが必要となるメンテナンスをユーザーに通知するためのメッセージを入力します。

デフォルトでは、「{TIMESTAMP} 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。

警告メッセージのタイトル

この設定項目では、警告メッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「Upcoming Maintenance」というタイトルが設定されています。

警告表示期間

この設定項目では、ソフトウェアの更新またはメンテナンスについての警告メッセージを表示する期間を定義します。

期間は、ddd.hh:mm:ss 形式で設定します。

- 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。

最終的な強制ログオフメッセージの内容

この設定項目では、強制ログオフ処理が開始されたことをユーザーに通知するためのメッセージを入力します。

デフォルトでは、「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。

最終的な強制ログオフメッセージのタイトル

この設定項目では、最終的な強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「Notification From IT Staff」というタイトルが設定されています。

強制ログオフの猶予期間

この設定項目では、ソフトウェアの更新またはメンテナンスのために、ユーザーにログオフを警告してから実際に強制ログオフ処理を開始するまでの待機期間を定義します。

期間は、ddd.hh:mm:ss 形式で設定します。

- 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。

強制ログオフメッセージの内容

この設定項目では、強制ログオフが開始される前に作業を保存してログオフするようにユーザーに通知するためのメッセージを入力します。

デフォルトでは、「{TIMESTAMP} 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。

強制ログオフメッセージのタイトル

この設定項目では、強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「Notification From IT Staff」というタイトルが設定されています。

Image Provider 統合の有効化

Connector エージェントでは、Provisioning Services または MCS で管理されるマシンのクローン上で動作しているかどうかが自動的に検出されます。これらのイメージ管理されたクローン上では、Configuration Manager に

よるアップデートが Connector エージェントによってブロックされ、カタログのマスターイメージ上にアップデートが自動的にインストールされます。

マスターイメージのアップデートが完了したら、Studio で MCS カタログクローンの再起動をオーケストレーションします。Connector エージェントは、Configuration Manager のメンテナンスウィンドウで PVS カタログクローンの再起動を自動的にオーケストレーションします。この動作を無効にして、Configuration Manager によってソフトウェアがカタログクローンにインストールされるように設定するには、イメージ管理モードを［無効］に変更します。

再起動メッセージの内容

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。

定期的なエージェントタスクの実行間隔

この設定項目では、Citrix Connector エージェントタスクの実行間隔を指定します。

期間は、ddd.hh:mm:ss 形式で設定します。

- 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。

管理

August 24, 2021

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

サイトを作成するときには、Citrix ライセンスサーバー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。接続のストレージとネットワークの詳細が、その接続のリソースになります。後でその接続やリソースを変更したり、新しい接続を作成したりできます。また、構成された接続を使用するマシンの管理も可能です。

ローカルホストキャッシュ

ローカルホストキャッシュを使用すると、Delivery Controller とサイトデータベースの間の接続が失敗しても、サイト内の接続仲介操作を続行できます。XenApp および XenDesktop に提供される、最も包括的な高可用性機能です。

接続リース

接続リースでなく、ローカルホストキャッシュをお勧めします。ローカルホストキャッシュは、より強力な代替選択肢です。

仮想 IP と仮想ループバック

Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

Delivery Controller

この記事では、Controller をサイトに追加およびサイトから削除する場合の考慮事項と手順を説明します。また、Controller を別のゾーンやサイトに移動する方法、および VDA を別のサイトに移動する方法についても説明します。

Delivery Controller による VDA 登録

VDA でアプリケーションやデスクトップの配信を支援できるようにするには、まず、Controller に登録（接続を確立）する必要があります。Controller のアドレスを指定するいくつかの方法については、この記事で説明します。Controller をサイトに追加、移動、または削除すると同時に、VDA が最新情報を受け取ることが重要です。

セッション

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。中には、セッションの信頼性を最適化し、不便さやダウンタイム、生産性の損失を軽減できる機能もあります。

- セッション画面の保持
- クライアントの自動再接続
- ICA Keep-Alive
- ワークスペースコントロール
- セッションローミング

Studio での検索の使用

Studio で、マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、柔軟な検索機能を使用します。

タグ

タグは、マシン、アプリケーション、グループ、ポリシーなどの項目を識別するために使用します。タグを使用すると、特定の操作が指定したタグの項目のみに適用されるように調整できます。

IPv4 または IPv6

XenApp および XenDesktop では、IPv4 のみまたは IPv6 のみ（ピュア IPv4 またはピュア IPv6）の環境がサポートされ、重複する IPv4 と IPv6 のネットワークを使用した「デュアルスタック」環境がサポートされます。ここでは、これらの展開について説明します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると、Citrix Profile Management も自動的にインストールされます。このプロファイルソリューションを使用する場合は、この記事で一般情報を確認し、完全な詳細については、Profile Management のドキュメントを参照してください。

Citrix Insight Services

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrix が提供するプラットフォームです。

ライセンス

February 12, 2021

> 注
>
> Studio と Director で Citrix ライセンスサーバー VPX がサポートされません。Citrix ライセンスサーバー VPX について詳しくは、Citrix ライセンスのドキュメントを参照してください。

管理者は、Studio を使用してライセンスを管理したり監視したりできます（ライセンスサーバーが Studio と同じドメインまたは信頼されたドメインで動作する場合）。そのほかのライセンス関連のタスクについては、ライセンスのドキュメントおよび「マルチタイプのライセンス」を参照してください。

以下で説明するタスクを実行するには、すべての管理作業を実行できるライセンス管理者である必要があります。Studio でライセンス情報を表示するには、［ライセンスの表示］以上の管理者権限が必要です。組み込みのすべての管理権限を実行できる管理者と読み取り専用管理者の役割には、この権限が含まれています。

以下の表に、サポートされるエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
XenApp	Platinum、Enterprise、Advanced	同時使用
XenDesktop	Platinum、Enterprise、App、VDI	ユーザー/デバイス、同時使用

> 重要:
>
> Citrix License Server for Windows のサポートされる最小バージョンは、11.15.0.0 ビルド 26000（MSI インストーラーバージョン 15.6.0.26000）です。
>
> バージョン 11.14.0.1 ビルド 22103（MSI インストーラーバージョン 14.2.0.22103）より古い License Server for Windows はサポートされなくなりました。

以下の表に、XenApp および XenDesktop の長期サービスリリースでサポートされる最小ライセンスバージョンを示します。

長期サービスリリース	サポートされる最小ライセンスサーバーバージョン	MSI インストーラーのバージョン
7.15 LTSR	11.14.0.1 ビルド 22103	14.2.0.22103
7.15 LTSR CU1 および CU2	11.14.0.1 ビルド 22103	14.2.0.22103
7.15 LTSR CU3 以降	11.15.0.0 ビルド 24100	15.4.0.24100
7.6 LTSR	11.14.0.1 ビルド 22103	14.2.0.22103

ライセンス情報を表示するには:

Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。指定したライセンスサーバーにインストールされているすべてのライセンスの一覧と、それらのライセンスの使用状況およびサイトのライセンス設定の概要が表示されます。

Citrix からライセンスをダウンロードするには、次の手順に従います。

1. Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。
2. ［操作］ペインで ［ライセンスの割り当て］を選択します。
3. ライセンスアクセスコードを入力します。このコードは、Citrix からメールで送信されます。

4. 製品を選択して、［ライセンスの割り当て］をクリックします。その製品について使用できるすべてのライセンスが割り当てられダウンロードされます。ライセンスアクセスコードを入力してすべてのライセンスを割り当ておよびダウンロードすると、そのライセンスアクセスコードは使用できなくなります。そのコードで追加のライセンス処理が必要な場合は、My Account にログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスファイルを追加するには、次の手順に従います。

1. Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。
2. ［操作］ペインで ［ライセンスの追加］を選択します。
3. ライセンスファイルを参照して、ライセンスサーバーに追加します。

ライセンスサーバーを変更するには、次の手順に従います。

1. Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。
2. ［操作］ペインで ［ライセンスサーバーの変更］を選択します。
3. ライセンスサーバーのアドレスを「name:port」形式で入力します。name はライセンスサーバーの DNS、NetBIOS、または IP アドレスです。ポート番号（<port>）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］ペインで ［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］ペインで ［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］ペインで ［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、目的の管理者を選択します。

3. ［操作］ペインで ［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］ペインで ［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:

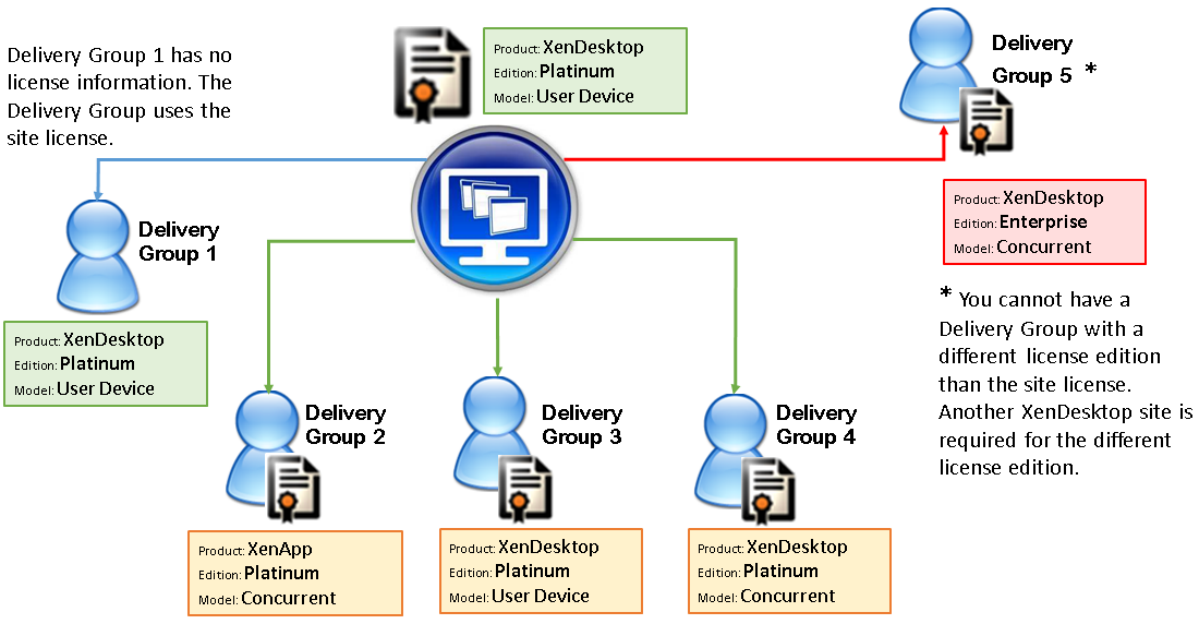
1. Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択し、目的の管理者グループを選択します。
3. ［操作］ペインで、［ライセンス管理者グループの編集］または ［ライセンス管理者グループの削除］を選択します。

マルチタイプのライセンス

July 3, 2019

マルチタイプのライセンスでは、単一の XenApp または XenDesktop サイト上にある複数のデリバリーグループでそれぞれ異なる種類のライセンスを使用できます。種類とは、製品 ID（XDT、MPS）とモデル（ユーザーデバイス、同時使用）の組み合わせのことです。デリバリーグループでは、サイトの製品エディションを使用する必要があります。

マルチタイプのライセンスが構成されていない場合は、完全に分割されているサイト上で構成されるときのみ異なる種類のライセンスを使用できます。デリバリーグループではサイトのライセンスが使用されます。



各種類のライセンスを使用するデリバリーグループを指定するには、次の Broker PowerShell コマンドレットを使用します:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには次を使用します。

- Citrix Studio
- Citrix Licensing Manager
- ライセンス管理コンソール
- citrix.com

Subscription Advantage の有効期間は、各ライセンスファイルおよび各製品とモデルに固有です。デリバリーグループ間の Subscription Advantage 有効期間は異なる場合があります。

Broker PowerShell SDK

DesktopGroup オブジェクトには次の 2 つのプロパティがあり、関連する New-BrokerDesktopGroup コマンドレットおよび Set-BrokerDesktopGroup コマンドレットを使用して操作することができます。

名前	値	制限事項
LicenseModel	グループのライセンスモデルを指定する列挙値です（Concurrent または UserDevice）。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。
ProductCode	グループのライセンス製品 ID を指定するテキスト文字列であり、XDT（XenDesktop の場合）または MPS（XenApp の場合）を設定します。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。

New-BrokerDesktopGroup

デスクトップのグループの仲介を管理するデスクトップグループを作成します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループの有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

Get-BrokerDesktopGroup

指定した条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroup コマンドレットの出力には、グループの ProductCode プロパティと LicenseModel プロパティが含まれます。これらのプロパティが New- BrokerDesktopGroup または Set-BrokerDesktopGroup により設定されていない場合、null 値が返されます。null の場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

1. 管理者権限で PowerShell を開き、Citrix スナップインを追加します。
2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して最新のライセンス構成を表示します。パラメーター **LicenseModel** および **ProductCode** を参照します。これらのパラメーターを以前に構成してない場合、空白の可能性があります。

   > 注:
   >
   > デリバリーグループにライセンス情報が設定されていない場合、**Site level Site license** を適用します。

3. ライセンスモデルを変更するには、コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行します。
4. ライセンス製品を変更するには、コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode** を実行します。
5. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力して変更を確認します。

   > 注:
   >
   > Premium ライセンスや Advanced ライセンスなどのエディションを混在させて一致させることはできません。

6. ライセンス構成を削除するには、前述と同じ **Set-BrokerDesktopGroup** コマンドを実行して、値を **$null** に設定します。

   > 注:
   >
   > Studio はデリバリーグループごとにライセンス構成を表示しません。PowerShell を使用して最新の

> 構成を表示します。

例

次の PowerShell コマンドレットサンプルでは、2 つの既存のデリバリーグループに対してマルチタイプのライセンスを設定し、3 番目のデリバリーグループを設定する方法について説明します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、PowerShell コマンドレット **Get-BrokerDesktopGroup** を使用します。

1. 1 番目のデリバリーグループを XenApp および Concurrent に設定します。
   Set-BrokerDesktopGroup -Name “Delivery Group for XenApp Platinum Concurrent” -ProductCode MPS -LicenseModel Concurrent
2. 2 番目のデリバリーグループを XenDesktop および Concurrent に設定します。
   Set-BrokerDesktopGroup -Name “Delivery Group for XenDesktop Platinum Concurrent” -ProductCode XDT -LicenseModel Concurrent
3. 3 番目のデリバリーグループを作成し、XenDesktop および UserDevice に設定します。
   New-BrokerDesktopGroup -Name “Delivery Group for XenDesktop Platinum UserDevice” -PublishedName “MyDesktop” -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

特殊考慮事項

マルチタイプのライセンスの機能は、通常の XenApp および XenDesktop のライセンスとは異なります。

Director または Studio からアラートや通知が行われることはありません。

- ライセンスの上限に近づいた場合、もしくは追加猶予期間のトリガーまたは有効期限に近づいた場合でも情報は提供されません。
- 特定のグループに問題が発生しても、通知はされません。

アプリケーション

August 24, 2021

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］ウィザードでは、デリバリーグループを 1 つ以上か、またはアプリケーショングループを 1 つ以上選択できますが、両方は選択できません。アプリケーションのグループ関連付けは後で変更できますが（アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは複雑度が増えないようにします。アプリケーションは、どちらかの種類のグループのみに含めます。

アプリケーションを複数のデリバリーグループまたはアプリケーショングループに関連付ける場合、そのすべてのグループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションが関連付けられているグループをすべて含めるようにします。

2 つのアプリケーションを（おそらくは異なるグループから）同じ名前で同じユーザーに公開する場合は、Studio で［アプリケーション名（ユーザー用）］ボックスに別の名前を入力します。これを行わないと、ユーザーの Citrix Receiver に同じ名前が 2 つ表示されます。

アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。アプリケーションの追加時、またはその後で、アプリケーションを配置するアプリケーションフォルダーを変更することもできます。

以下の情報を参照してください：

- デリバリーグループについて詳しくは、「デリバリーグループの作成」を参照してください。
- アプリケーショングループについて詳しくは、「アプリケーショングループの作成」を参照してください。
- アプリケーションに追加できるタグについて詳しくは、「タグ」を参照してください。

アプリケーションの追加

アプリケーションは、デリバリーグループまたはアプリケーショングループの作成時に追加できます。手順について詳しくは、「デリバリーグループの作成」と「アプリケーショングループの作成」で説明しています。次の手順で、グループ作成後にアプリケーションを追加する方法について説明します。

ヒント：

- リモート PC アクセスのデリバリーグループにアプリケーションを追加することはできません。
- デリバリーグループまたはアプリケーショングループからアプリケーションを削除するために、アプリケーションの追加ウィザードを使用することはできません。これは、別の処理になります。

1 つまたは複数のアプリケーションを追加するには、以下の手順に従います。

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. ［アプリケーショングループの追加］ウィザードが起動され、［はじめに］ページが表示されます。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。

- 1 つのデリバリーグループのみにアプリケーションを追加する場合は、手順 1 において Studio のナビゲーションペインで ［デリバリーグループ］を選択してから、中央ペインでデリバリーグループを 1 つ選択し、［操作］ペインで ［アプリケーションの追加］を選択します。ウィザードに ［グループ］ページは表示されません。
- 1 つのアプリケーショングループのみにアプリケーションを追加する場合は、手順 1 において Studio のナビゲーションペインで ［アプリケーション］を選択してから、中央ペインでアプリケーショングループを 1 つ選択し、［操作］ペインで選択したアプリケーショングループ名の下にある ［アプリケーションの追加］を選択します。ウィザードに ［グループ］ページは表示されません。

グループ

このページには、サイトのすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成してある場合は、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を選択できますが、両方のグループは選択できません。言い換えると、アプリケーションを同時にアプリケーショングループとデリバリーグループに追加することはできません。通常は、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加する必要があります。

すべてのアプリケーションは常に少なくとも 1 つのグループに関連付ける必要があるため、アプリケーションを追加するときには、少なくとも 1 つのデリバリーグループ（または、使用できる場合はアプリケーショングループ）の横にあるチェックボックスをオンにする必要があります。

アプリケーション

［追加］ボックスをクリックして、アプリケーションのソースを表示します。

- ［スタートから］メニュー：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。

割り当て済みの AppDisk からアプリケーションを追加するには、[[スタート] メニューから] を選択します。ここにアプリケーションがない場合、[手動で定義] を選択して詳細を入力します。フォルダーアクセスエラーが発生した場合は、フォルダーを「共有」用に構成し、[手動で定義] からアプリケーションを再度追加してください。

アプリケーションのプロパティ (設定) は、このページから、または後で変更できます。

アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。アプリケーションは、このページから、または後で変更できます。アプリケーションの追加時に、同じフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された新しい名前を受け入れるか、または拒否してアプリケーションの名前を変更するか別のフォルダーを選択できます。たとえば、アプリケーションフォルダーに既に「app」が存在する場合に、このフォルダーに「app」という名前の別のアプリケーションを追加しようとすると、新しい名前「app_1」が提案されます。

概要

追加するアプリケーションが 10 個以下の場合、[追加するアプリケーション] のリストにそれらの名前が表示されます。追加するアプリケーションが 10 個より多い場合は、合計数が示されます。

概要の情報を確認し、[完了] をクリックします。

アプリケーションのグループ関連付けの変更

アプリケーションの追加後、アプリケーションを関連付けるデリバリーグループやアプリケーショングループを変更できます。

ドラッグアンドドロップを使用して、アプリケーションを追加のグループに関連付することができます。ドラッグアンドドロップする代わりに、[操作] ペインのコマンドを使用することもできます。

アプリケーションを複数のデリバリーグループまたは複数のアプリケーショングループに関連付けた場合、グループの優先度を使用して、アプリケーションを検索するときに複数のグループを確認する順序を指定できます。デフォルトでは、すべてのグループの優先度は 0（最高）です。同じ優先度のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、(1) デリバリーグループに共有マシンが含まれていてこのグループが XenDesktop 7.x バージョンで作成されており、かつ (2)［デリバリーグループの編集］権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれるデリバリーグループを選択することもできます。［プロパティ］ダイアログボックスをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

1. Studio のナビゲーションペインで ［アプリケーション］を選択し、中央ペインでアプリケーションを選択します。
2. ［操作］ペインで ［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場合は、［追加］ドロップダウンリストをクリックし、［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場合は、グループを 1 つまたは複数選択して ［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場合は、グループを選択して ［優先度の編集］をクリックします。優先度の値を選択し、［**OK**］をクリックします。
7. 作業が完了したら、変更を適用してウィンドウを開いたままにする場合は ［適用］を、変更を適用してウィンドウを閉じる場合は ［**OK**］をクリックします。

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や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からは削除されますが、元々アプリケーションを追加するときに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。下部中央のペインで ［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. 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場合は ［適用］を、変更を適用してウィンドウを閉じる場合は ［**OK**］をクリックします。

以下の一覧では、ページはカッコ内に示しています。

- Receiver でアプリケーションを表示するカテゴリーまたはフォルダー（デリバリー）
- コマンドライン引数（「公開アプリケーションにパラメーターを渡す」セクションを参照）（場所）
- 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（ID）
- 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 のキーワード（ID）
- 制限（「アプリケーション制限の構成」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（ID）
- 実行可能ファイルへのパス（「公開アプリケーションにパラメーターを渡す」セクションを参照）（場所）
- ユーザーのデスクトップにショートカットを表示するかどうか：有効化または無効化（デリバリー）
- 表示：Citrix Receiver でアプリケーションを表示できるユーザーを制限します（非表示のアプリケーションでも開始できます。非表示にすると同時に開始できないようにするには、別のグループに追加します）（表示の制限）
- 作業ディレクトリ（場所）

使用中のアプリケーションに変更内容を反映させるには、ユーザーがそのセッションからログオフする必要があります。

アプリケーション制限の設定

アプリケーションの使用を管理するため、アプリケーション制限を設定します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理することができます。同様に、アプリケーション制限を使用して、リソースの消費量が大きいアプリケーションの同時インスタンスの数を管理することもできます。これによってサーバーパフォーマンスを維持し、サービスの質の低下を防ぐことができます。

この機能により、（Citrix Receiver や StoreFront などからの）Controller を介したアプリケーション起動数が制限されます。これ以外の方法で起動されて実行されるアプリケーションの数は制限されません。すなわち、アプリケーション制限は、同時使用を管理する管理者をサポートし、あらゆるシナリオに適用されるわけではありません。たとえば、Controller がリース接続モードである場合は、アプリケーション制限を適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。以下の 2 つのアプリケーション制限設定があり、そのいずれかまたは両方を設定できます：

- デリバリーグループのすべてのユーザーによるアプリケーションの最大同時インスタンス数
- デリバリーグループの 1 人のユーザーにつき 1 つのアプリケーションインスタンス

制限が設定されている場合、設定された制限を超過するアプリケーションインスタンスをユーザーが起動しようとすると、エラーメッセージが生成されます。

アプリケーション制限の使用例

- 同時インスタンスの最大数の制限。デリバリーグループで、アプリケーション Alpha の同時インスタンスの最大数を 15 に設定しました。その後、このデリバリーグループのユーザーが、このアプリケーションの 15 インスタンスを同時に実行しています。このデリバリーグループのユーザーが Alpha を起動しようとすると、エラーメッセージが生成され、Alpha は起動しません。起動すると、先に設定した、アプリケーションの同時インスタンス数の制限値（15）を超過することになるためです。
- **1** ユーザーにつき **1** インスタンスのアプリケーション制限。別のデリバリーグループで、1 ユーザーにつき 1 インスタンスのオプションをアプリケーション Beta に対して有効にしました。ユーザー Tony が、アプリケーション Beta を正常に起動しました。当日のその後、このアプリケーションは Tony のセッションで引き続き実行中でしたが、Tony は Beta の別のインスタンスを起動しようとしました。しかし、起動すると 1 ユーザーにつき 1 インスタンスの制限を超過することになるため、エラーメッセージが生成され、Beta は起動しません。
- 同時インスタンスの最大数および **1** ユーザーにつき **1** インスタンスの制限。別のデリバリーグループで、同時インスタンスの最大数を 10 に設定し、1 ユーザーにつき 1 インスタンスのオプションをアプリケーション Delta に対して有効にしました。その後、このデリバリーグループの 10 人のユーザーがそれぞれ Delta のインスタンスを実行している場合、このデリバリーグループの別のユーザーが Delta を起動しようとすると、エラーメッセージが生成され、Delta は起動しません。現在の 10 人の Delta ユーザーのいずれかがこのアプリケーションの 2 つ目のインスタンスを起動しようとしても、エラーメッセージが生成され、2 つ目のインスタンスは起動しません。

アプリケーションインスタンスが Controller を介さない方法（Controller がリース接続モードの場合など）でも起動し、設定された制限を超過している場合、アプリケーションを使用中のユーザーがインスタンスを終了し、実行中のインスタンス数が制限を超過しなくなるまで、追加のインスタンスを起動することはできません。制限を超過した分のインスタンスが強制的にシャットダウンされることはなく、ユーザーがインスタンスを終了するまで継続できます。

セッションローミングを無効にする場合、1 ユーザーにつき 1 インスタンスのアプリケーション制限も無効にしてください。1 ユーザーにつき 1 インスタンスのアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する 2 つの値は、どちらも設定しないでください。ローミングについて詳しくは、「セッション」を参照してください。

アプリケーション制限を設定するには、以下の手順に従います:

1. Studio のナビゲーションペインで ［アプリケーション］を選択し、アプリケーションを選択します。
2. ［操作］ペインで ［アプリケーションプロパティの編集］を選択します。
3. ［デリバリー］ページで、次のいずれかのオプションを選択します。操作が終了したら、［**OK**］または ［適用］をクリックします。（［**OK**］をクリックすると、変更が適用され、［アプリケーションプロパティの編集］ダイアログボックスは閉じます。［適用］をクリックすると、変更が適用され、ダイアログボックスは閉じずに開い

たままとなります)。

- アプリケーションの無制限使用を許可します。インスタンスの同時実行数に制限はありません。これがデフォルトの設定です。
- アプリケーションの制限を設定します。以下の 2 種類の制限があります。いずれかまたは両方を指定します。
  - 同時に実行できるインスタンスの最大数の指定
  - 1 ユーザーにつき 1 アプリケーションインスタンスの制限

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの［場所］ページで、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルタイプに関連付けると、その公開アプリケーションのコマンドライン（実行可能ファイルのパス）の後に”%*“（二重引用符で囲んだパーセントとアスタリスク記号）が追加されます。これらの記号は、ユーザーデバイス側に渡されるパラメーターのプレースホルダーとして機能します。

ファイルタイプに関連付けられている公開アプリケーションが起動しない場合は、記号が正しくコマンドラインに含まれていることを確認してください。“%*” 記号が追加されている場合は、ユーザーデバイスから渡されるパラメーターがデフォルトで検証されます。特殊なパラメーターを必要とする公開アプリケーションでは、コマンドラインに”%**“（二重引用符で囲んだパーセントと 2 個のアスタリスク記号）が追加されています。これによりコマンドライン検証が無効になります。コマンドラインにこれらの記号が含まれていない場合は、手作業で追加できます。

実行可能ファイルのパスに、「C:\Program Files」のようなスペースを使ったフォルダー名が含まれている場合は、アプリケーションのコマンドラインを二重引用符で囲み、このスペースがコマンドラインに属していることを示します。それには、パスの前後に二重引用符を追加し、%* 記号の前後にもう 1 組の二重引用符を追加します。このとき、パスの末尾の二重引用符と、%* 記号の前の二重引用符の間に、必ずスペースを 1 つ入力してください。

たとえば、公開アプリケーション Windows Media Player のコマンドラインは次のようになります:

“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”

アプリケーションフォルダーの管理

デリバリーグループに新しく追加したアプリケーションは、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フォルダーを配置するには、その既存のフォルダーを選択します。次に、［操作］ペインで ［フォルダーの作成］を選択します。名前を入力してください。
- 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。名前を入力してください。
- フォルダーを削除するには、削除するフォルダーを選択し、［操作］ペインの ［フォルダーの削除］を選択します。アプリケーションやサブフォルダーを含んでいるフォルダーを削除すると、それらのアプリケーションやサブフォルダーも削除されます。アプリケーションを削除すると、そのアプリケーションの割り当てがデリバリーグループから削除されます。マシンからアンインストールされることはありません。
- アプリケーションをフォルダーに移動するには、1 つまたは複数のアプリケーションを選択します。次に、［操作］ペインで ［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

また、［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、追加するアプリケーションを特定のフォルダー（新規フォルダーも可）に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。）

ユニバーサル **Windows** プラットフォームアプリ

October 22, 2021

XenApp および XenDesktop では、VDA がインストールされているユニバーサル Windows プラットフォーム（UWP）アプリの Windows 10 および Windows Server 2016 マシンでの使用がサポートされます。UWP アプリについて詳しくは、以下の Microsoft 社のドキュメントを参照してください。

- What is a Universal Windows Platform (UWP) app?
- オフラインアプリの配布
- ユニバーサル Windows プラットフォーム（UWP）アプリのガイド

この記事全体で、UWP アプリを意味する用語として「ユニバーサルアプリ」を使用します。

要件および制限事項

ユニバーサルアプリは Windows10 および Windows Server 2016 マシン上の VDA でサポートされています。

VDA のバージョンは 7.11 以上である必要があります。

以下の XenApp および XenDesktop 機能は、ユニバーサルアプリの使用時にはサポートされないか、または制限されます:

- ファイルタイプの関連付けはサポートされません。
- ローカルアプリケーションアクセスはサポートされません。
- 動的プレビュー：セッションで実行中のアプリが重複している場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、ユニバーサルアプリではサポートされません。
- アクションセンターリモート：ユニバーサルアプリでは、アクションセンターを使用して、セッションでメッセージを表示することができます。メッセージをユーザーに表示するには、これらのメッセージをエンドポイントにリダイレクトします。

同じサーバーからのユニバーサルアプリと非ユニバーサルアプリの起動は Windows 10 VDA ではサポートされません。Windows Server 2016 では、ユニバーサルアプリと非ユニバーサルアプリは別のデリバリーグループまたはアプリケーショングループに属する必要があります。

マシンにインストールされるユニバーサルアプリはすべて列挙されるため、Windows ストアへのユーザーアクセスを無効にすることを Citrix ではお勧めします。これにより、1 人のユーザーによってインストールされたユニバーサルアプリが他のユーザーによってアクセスされるのを防ぐことができます。

サイドローディングの実行中に、ユニバーサルアプリはマシンにインストールされ、他のユーザーが使用できるようになります。他のユーザーがアプリを起動すると、アプリがインストールされます。その後 OS によって AppX データベースが更新され、アプリを起動しているユーザーには「インストール時の状態」と表示されます。

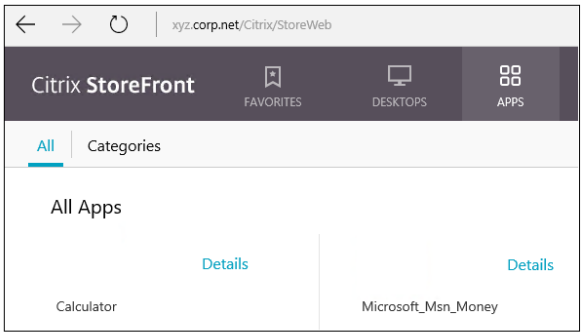
シームレスウィンドウまたは固定ウィンドウで起動された公開ユニバーサルアプリから正常にログオフすると、セッションが終了せずにユーザーがログオフしている状態になることがあります。このような場合は、セッションに残っ

ているいくつかのプロセスが、セッションの適切な終了を阻止しています。これを解決するには、CTX891671のガイダンスに従って、セッションの修了を阻止しているプロセスを特定し、そのプロセスを「LogoffCheckSysModules」レジストリキーの値に追加します。

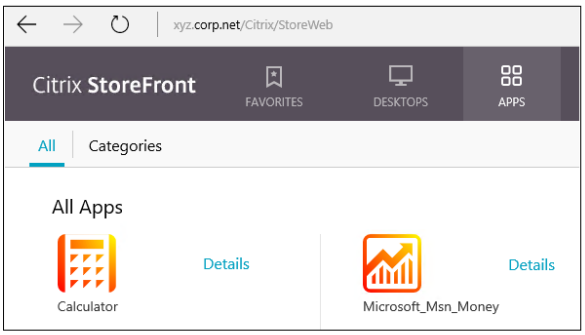
ユニバーサルアプリのアプリケーション表示名や説明の名前が正しくないことがあります。アプリケーションをデリバリーグループに追加するときに、これらのプロパティを編集および修正してください。

その他の問題については、「既知の問題」を参照してください。

現時点では、複数のユニバーサルアプリに透過性が有効になった白いアイコンがありますが、これによって StoreFront のディスプレイの白い背景でアイコンが見えなくなるという問題があります。これを回避するために、背景の色を変更できます。たとえば、StoreFront マシンで、ファイル C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css を編集します。このファイルの末尾に、**.storeapp-icon {background-image: radial-gradient(circle at top right, yellow, red); }** を追加します。以下の図は、この例の編集前と編集後を示しています。



Before



After

Windows Server 2016 では、ユニバーサルアプリを起動するとサーバーマネージャーも起動されることがあるという問題がありました。この問題の発生を回避するには、HKEY_LOCAL_MACHINE\SOFTWARE\Software\Microsoft\ServerMan レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効します。詳しくは、「https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/」を参照してください。

ユニバーサルアプリのインストールと公開

ユニバーサルアプリのサポートは、デフォルトで有効になっています。

VDA でユニバーサルアプリを使用できないようにするには、HKEY_LOCAL_MACHINE\SOFTWARE\Software\Citrix\VirtualDe に、**EnableUWASeamlessSupport** レジストリキーを追加して［**0**］に設定します。

1 つまたは複数のユニバーサルアプリを VDA（またはマスターイメージ）にインストールするには、以下のいずれかの方法を使用します。

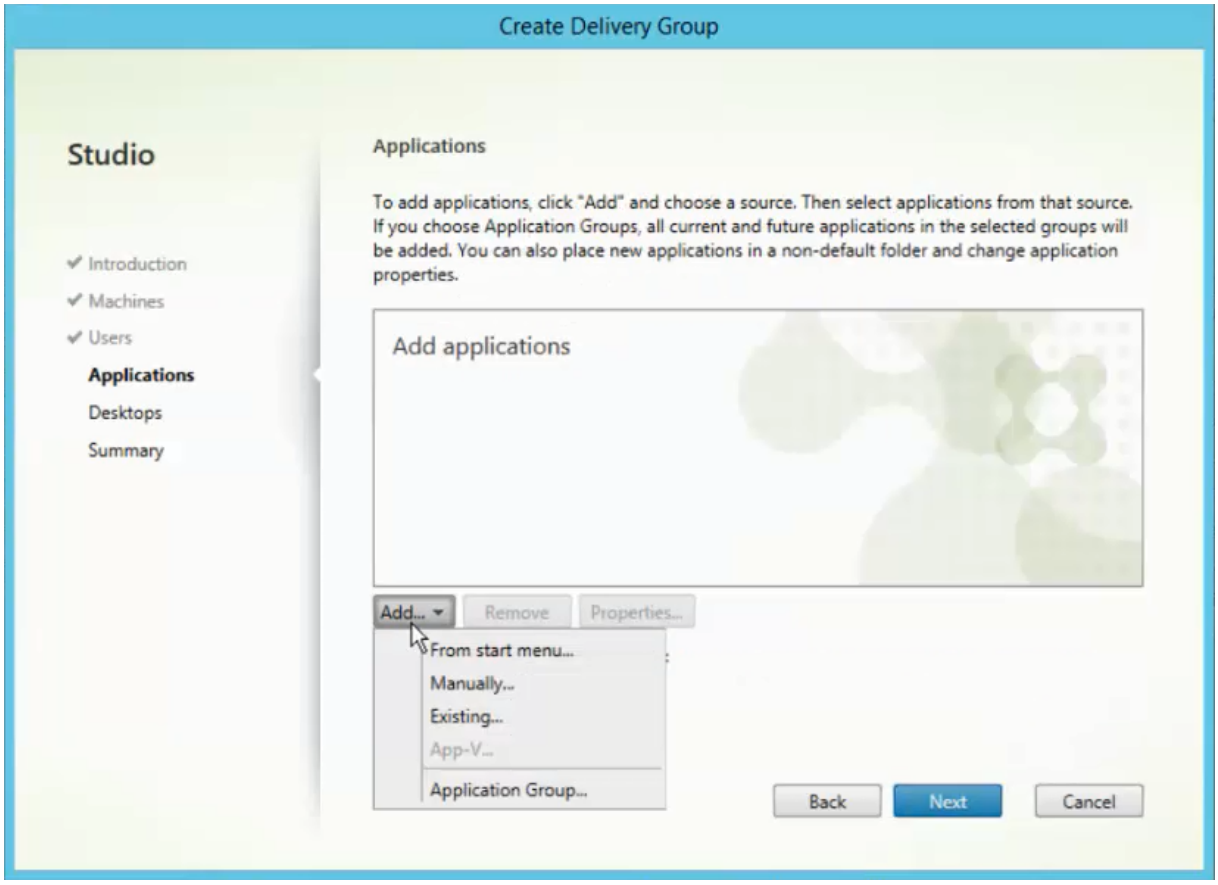
- ビジネス向け Windows ストアからのオフラインインストールの完了、Deployment Image Servicing and Management（DISM）などのツールを使用した、アプリのデスクトップイメージへの展開。詳しくは、「https://

docs.microsoft.com/en-us/microsoft-store/distribute-offline-apps?redirectedfrom=MSDN」を参照してください。

- アプリのサイドロード。詳しくは、「https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10?redirectedfrom=MSDN」を参照してください。

1 つまたは複数のユニバーサルアプリを XenApp または XenDesktop に追加するには、以下の手順に従います:

ユニバーサルアプリがマシンにインストールされたら、ユニバーサルアプリをデリバリーグループまたはアプリケーショングループに追加します。この処理は、グループの作成時、またはその後に行うことができます。ウィザードの［アプリケーション］ページで、［[スタート］メニューから］ソースを選択します。



アプリケーションの一覧が表示されたら、公開するユニバーサルアプリのチェックボックスをオンにします。［次へ］をクリックします。

ユニバーサルアプリのアンインストール

ユニバーサルアプリを Remove-AppXPackage などのコマンドでアンインストールする場合、アイテムは管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行する必要があります。すべてのユーザーのマシンから 1 つのコマンドで AppX パッケージをアンインストールすることはできません。

ゾーン

August 24, 2021

展開が WAN で接続された広範な場所に分散している場合、ネットワークの遅延と信頼性に関する問題が発生することがあります。このような問題の影響を軽減するには、次の 2 つの方法があります:

- それぞれに独自の SQL Server サイトデータベースを持つ複数のサイトの展開

このオプションは、大規模な環境で推奨されます。複数サイトは個別に管理され、各サイトに独自の SQL Server サイトデータベースが必要です。各サイトが個別の XenApp 展開です。

- 単一サイト内に複数のゾーンを構成します。

ゾーンを構成することにより、リモートのユーザーが、WAN の大規模セグメントを経由する接続を必ずしも必要とせず、リソースに接続できるようにサポートできます。ゾーンを使用することにより、単一の Citrix Studio コンソール、Citrix Director、およびサイトデータベースからの効果的なサイト管理が実現します。これにより、リモートの場所への追加サイト（個別のデータベースを含む）の展開、それに要する人員の配置、ライセンス取得、および運用のコストが削減されます。

ゾーンは、あらゆる規模の展開で有用です。ゾーンを使用して、アプリケーションおよびデスクトップとエンドユーザーの距離を縮めることにより、パフォーマンスを改善することができます。1 つのゾーンにおいて、1 つまたは複数の Controller をローカルでインストールして冗長性と回復性を確保することができますが、これは必須ではありません。

サイトで多数の Controller を構成すると、サイト自体への Controller の新規追加など一部の操作のパフォーマンスが低下する可能性があります。こうした事態を回避するため、XenApp または XenDesktop サイトのゾーンの数は 50 以下に制限することをお勧めします。

> 注:
>
> ゾーンのネットワーク待機時間が 250 ミリ秒（RTT）を超える場合は、ゾーンではなくサイトを複数展開することをお勧めします。

このアーティクルを通じ、「ローカル」という用語は、対象となるゾーンを指しています。たとえば、「VDA はローカル Controller に登録されます」という場合、VDA が存在するゾーンの Controller に登録されることを意味します。

このリリースでのゾーンは、XenApp Version 6.5 以前と大きな違いはありませんが、同一ではありません。たとえば、このゾーン実装では、データコレクターが存在しません。サイトのすべての Controller が、プライマリゾーンの 1 つのサイトデータベースと通信します。また、このリリースではフェールオーバーおよび優先ゾーンの機能が異なります。

ゾーンの種類

1 つのサイトには、必ず 1 つのプライマリゾーンがあります。また、サイトにはオプションで 1 つまたは複数のサテライトゾーンを含めることもできます。サテライトゾーンは、障害回復、地理的に離れたデータセンター、ブランチ

オフィス、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。

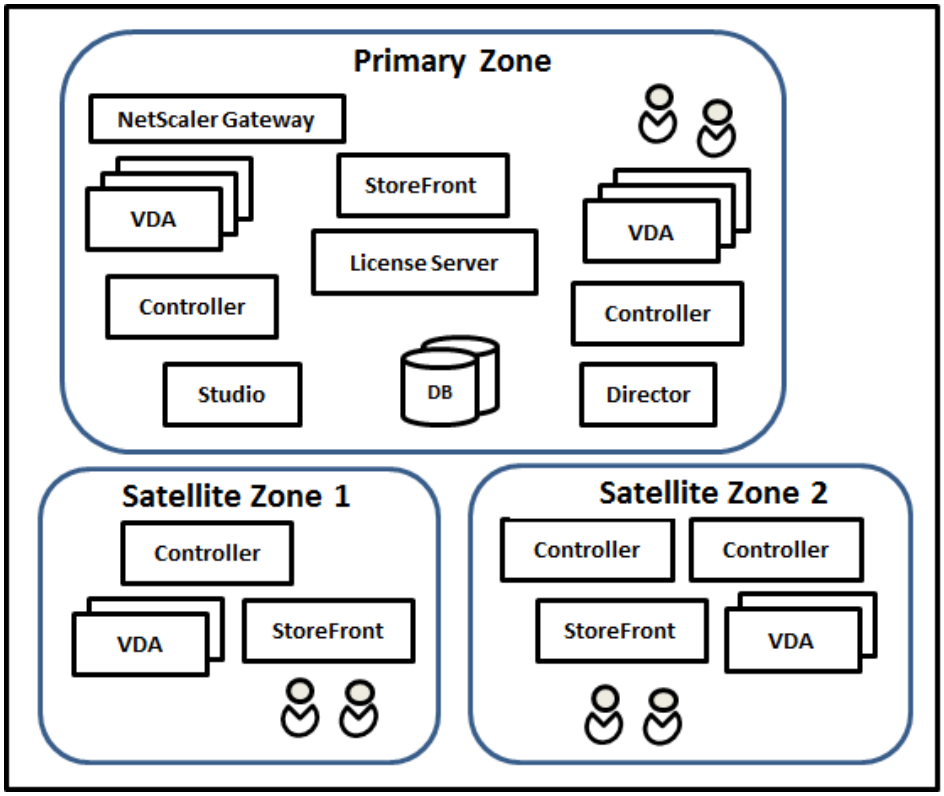
また、プライマリゾーンには、冗長性確保のために少なくとも 2 つの Controller が含まれている必要があります。また、データベースおよびインフラストラクチャと密結合されたアプリケーションを含む 1 つまたは複数の VDA が含まれる場合があります。

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）。

ニーズと環境に応じて、1 つのサイトに異なる構成のサテライトゾーンを含めることができます。次の図は、1 つのプライマリゾーンと、複数のサテライトゾーンの例を示しています。



- プライマリゾーンには、2 つの Controller、Studio、Director、StoreFront、ライセンスサーバー、サイトデータベース（および高可用性 SQL Server 展開）が含まれています。また、プライマリゾーンには複数の VDA および NetScaler Gateway も含まれています。
- サテライトゾーン 1 - VDA（Controller あり）

サテライトゾーン 1 には、Controller、VDA、および StoreFront サーバーが含まれています。このサテライトゾーンの VDA は、ローカル Controller に登録されます。ローカル Controller は、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

WAN で障害が発生した場合、接続リース機能を使用して、サテライトゾーンの Controller がそのゾーンの VDA への接続を引き続き仲介することができます。このような展開は、オフィスを社内ネットワークに接続する WAN リンクで障害が発生しても、作業者がローカル StoreFront サイトおよびローカル Controller を使用してローカルリソースにアクセスするオ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や、ローカル Controller で障害が発生している場合など）、VDA ではプライマリゾーンの Controller への登録が試行されます。この場合、サテライトゾーンの Controller が再び利用可能になっても、VDA はプライマリゾーンで登録されたままになります。サテライトゾーンの VDA では、別のサテライトゾーンの Controller への登録が試行されることはありません。
- Controller の VDA 検出で自動更新が有効になっており、VDA のインストール時に Controller アドレスの一覧を指定した場合、初回登録では、（Controller が含まれるゾーンに関係なく）その一覧からランダムに Controller が選択されます。その VDA が含まれるマシンが再起動された後、そのローカルゾーン内の Controller が VDA 登録の優先 Controller になります。
- サテライトゾーンの Controller で障害が発生した場合、可能であれば別のローカル Controller へのフェールオーバーが実行されます。ローカル Controller を利用できない場合は、プライマリゾーンの Controller へのフェールオーバーが実行されます。
- Controller をゾーン内またはゾーン外に移動し、自動更新が有効である場合、両方のゾーンの VDA に対し、ローカルの Controller とプライマリゾーンの Controller を示す更新された一覧が送信されます。これにより、登録および接続の受け入れが可能な Controller が VDA で認識されます。
- マシンカタログを別のゾーンに移動すると、そのカタログの VDA が、カタログを移動したゾーンの Controller に再登録されます（現在のゾーンに適切に接続されていないゾーンにカタログを移動する場合（遅延が大きいネットワークやまたは低帯域幅ネットワークなど）は、関連付けられているすべてのホスト接続も同じゾーンに移動してください）。
- プライマリゾーンの Controller には、すべてのゾーンの接続リース機能データが保持されます。サテライトゾーンの Controller には、そのゾーンおよびプライマリゾーンの接続リース機能データが保持されますが、ほかのサテライトゾーンのデータは保持されません。

プライマリゾーンですべての Controller が失敗すると、以下の状態になります。

- Studio がサイトに接続できない。
- プライマリゾーンで VDA に接続できない。
- プライマリゾーンの Controller が使用できるようになるまで、サイトのパフォーマンスが低下し続ける。

Version 7.7 よりも前の VDA バージョンが含まれるサイトでは、以下のルールが適用されます。

- サテライトゾーンの VDA では、そのローカルゾーンおよびプライマリゾーンの Controller からの要求が受け入れられます（Version 7.7 以降の VDA では、ほかのセカンダリゾーンからの Controller 要求を受け入れることができます）。
- サテライトゾーンの VDA は、プライマリゾーンまたはローカルゾーンの Controller にランダムに登録され

ます（Version 7.7 以降の VDA では、ローカルゾーンが優先されます）。

ゾーン優先度

> 重要:
>
> ゾーンの優先度機能を使用するには、StoreFront 3.7 以上および NetScaler Gateway 11.0-65.x 以上を使用している必要があります。

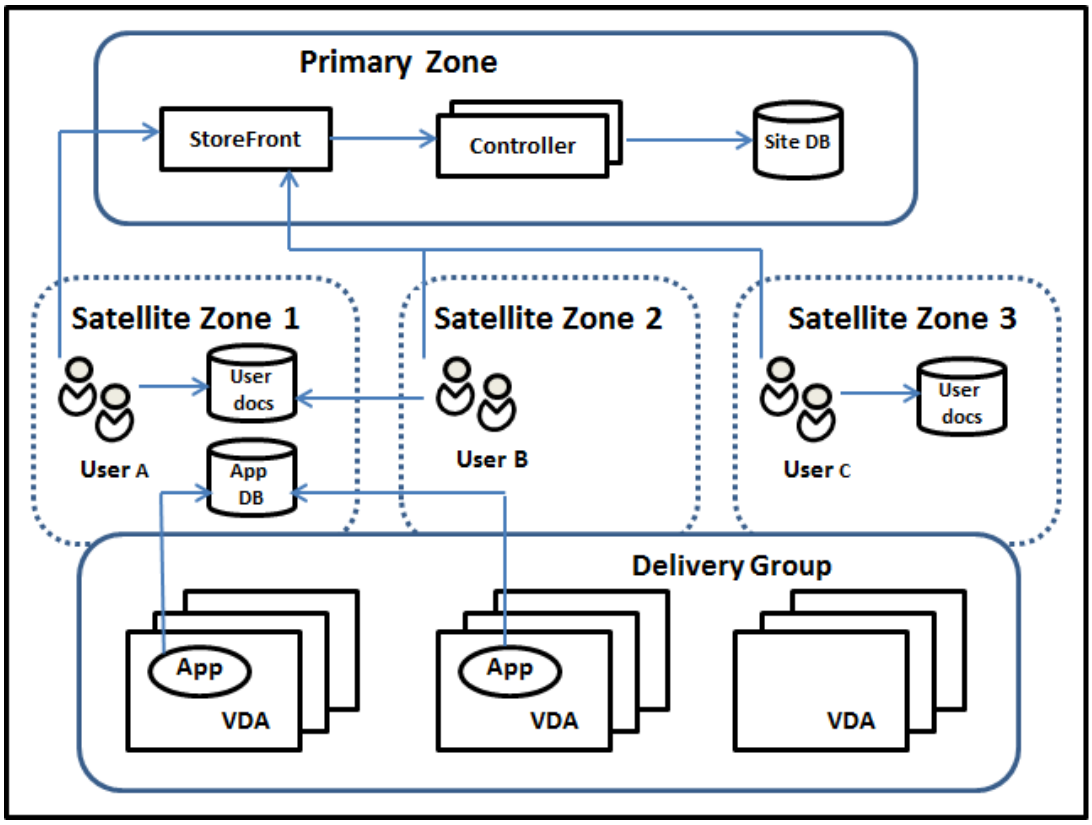
複数のゾーンがあるサイトでは、管理者は、アプリケーションやデスクトップの起動にどの VDA が使用されるかを、ゾーンの優先度機能によってより柔軟に制御できます。

ゾーンの優先度のしくみ

ゾーンの優先度には以下の 3 つの形式があります。以下によっては、特定のゾーンに VDA を使用するのが好ましい場合があります。

- アプリケーションのデータの保存先。これを「アプリケーションホーム」と呼びます。
- プロファイルやホームシェアなどの、ユーザーのホームデータの場所。これを「ユーザーホーム」と呼びます。
- （Citrix Receiver が実行されている）ユーザーの現在位置。これを「ユーザーの場所」と呼びます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDA は 3 つのサテライトゾーンにまたがっていますが、同じデリバリーグループに属しています。その

ため、ブローカーはユーザーの起動依頼にどの VDA を使用するかを選択できる場合があります。この例では、ユーザーが Citrix Receiver エンドポイントを実行できる場所が多数存在しています。ユーザー A はサテライトゾーン 1 で、Citrix Receiver でデバイスを使用しています。ユーザー B はサテライトゾーン 2 でデバイスを使用しています。1 人のユーザーのドキュメントをさまざまな場所に格納できます。ユーザー A と B は、サテライトゾーン 1 をベースに共有を使用します。ユーザー C はサテライトゾーン C からの共有を使用します。また、公開アプリケーションのいずれかによって、サテライトゾーン 1 にあるデータベースが使用されます。

ユーザーまたはアプリケーションにホームゾーンを構成して、ユーザーまたはアプリケーションをゾーンと関連付けることができます。すると、Delivery Controller のブローカーがこれらの関連付けを使用して、セッションが開始されるゾーンを選択します（リソースが利用可能な場合）。以下を実行します：

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションに構成できるホームゾーンは 1 回あたり 1 つのみです（ユーザーについては、複数のゾーンメンバーシップがある場合は例外となることがあります。「そのほかの考慮事項」セクションを参照してください。ただし、その場合においても、ブローカーが使うホームゾーンは 1 つのみです）。

ユーザーおよびアプリケーションのゾーン優先度を構成できますが、ブローカーは起動する優先ゾーンを 1 つだけ選択します。優先ゾーンの選択におけるデフォルトの優先順位は、アプリケーションホーム、ユーザーホーム、ユーザーの場所の順になります。（この順序は制限できます（次のセクション参照））。ユーザーがアプリケーションを起動したとき：

- アプリケーションに構成済みのゾーンの関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンとなります。
- アプリケーションには構成済みのゾーンの関連付けがなく、ユーザーには構成されたゾーンの関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンとなります。
- アプリケーションにもユーザーにもゾーンの関連付けが構成されていない場合、優先ゾーンはユーザーが Citrix Receiver インスタンスを実行しているゾーン（ユーザーの場所）となります。このゾーンが定義されていない場合は、VDA およびゾーンのランダム選択が使用されます。負荷分散は、優先ゾーン内のすべての VDA に適用されます。優先ゾーンがない場合、負荷分散はデリバリーグループ内のすべての VDA に適用されます。

ゾーン優先度の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）すると、ゾーン優先度がどのように使われるか（または使われないか）をさらに制限できます。

- ユーザーのホームゾーンの使用必須：デリバリーグループで、セッションをユーザーのホームゾーンで開始し（ユーザーのホームゾーンがある場合）、ホームゾーンでリソースが利用可能でない場合には別のゾーンにフェールオーバーしないように指定できます。この制限は、大きなプロファイルやデータファイルがゾーン間でコピーされないようにする必要がある場合に有用です。つまり、他のゾーンでセッションを開始するのではなく、他のゾーンではセッションが開始されないようにします。
- アプリケーションのホームゾーンの使用必須：同様に、アプリケーションのホームゾーンを構成する際に、アプリケーションをそのゾーンでのみ起動し、アプリケーションのホームゾーンでリソースが利用可能でない場

合には他のゾーンにフェールオーバーしないように指定できます。

- アプリケーションのホームゾーンなし、構成済みのユーザーホームゾーンは無視：アプリケーションのホームゾーンを指定しない場合は、アプリケーションを起動するときに構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、ユーザーの場所ゾーン優先度を使用して、ユーザーに他のホームゾーンがある場合でも、ユーザーが使用している（Citrix Receiver 実行中の）マシンの近くにある VDA で特定のアプリケーションが実行されるようにできます。

優先ゾーンによるセッション使用への影響

ユーザーがアプリケーションやデスクトップを起動すると、ブローカーは既存のセッションよりも優先ゾーンを使用しようとします。

アプリケーションまたはデスクトップを起動しているユーザーに、起動中のリソースに最適なセッション（アプリケーションのセッション共有を使用できるセッション、または起動中のリソースをすでに実行しているセッションなど）があるにもかかわらず、セッションがユーザーまたはアプリケーションの優先ゾーン以外のゾーンの VDA で実行されている場合、新しいセッションが作成されることがあります。これにより、セッションは、ユーザーのセッション要件に対して優先度の低いゾーンに再接続される前に、正しいゾーンで開始されます（そのゾーンに使用可能な容量がある場合）。

操作できなくなる孤立セッションが発生しないようにするため、優先ではないゾーンにあっても、再接続は既存の切断されたセッションにのみ許可されます。

セッション開始の望ましさの順は、以下のとおりです。

1. 優先ゾーンにある既存セッションに再接続する。
2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある接続中の既存セッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

ゾーン優先度に関するそのほかの考慮事項

- ユーザーグループ（セキュリティグループなど）のホームゾーンを構成する場合、（直接または間接メンバーシップによる）そのグループのユーザーは、指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができるため、他のグループのメンバーシップで他のホームゾーンが構成されている可能性があります。そのような場合は、そのユーザーのホームゾーンの特定があいまいになる可能性があります。

ユーザーに、グループメンバーシップで取得されなかった構成済みのホームゾーンがある場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップで取得されたゾーンの関連付けはすべて無視されます。

ユーザーに、グループメンバーシップのみで取得された複数の異なるゾーンの関連付けがある場合、ブローカーはそれらのゾーンの中からランダムに選択します。ブローカーがゾーンを選択すると、そのゾーンはユーザーのグループメンバーシップが変更されるまで、後続のセッションの開始に使用されます。

- ユーザーの場所ゾーン優先度には、デバイスの接続を経由している Citrix NetScaler Gateway によるエンドポイントデバイス上の Citrix Receiver の検出が必要になります。NetScaler は、IP アドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンの ID は、StoreFront から Controller に渡される必要があります。

ゾーン優先度について詳しくは、「Zone Preference Internals」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置することができます。マシンカタログでホスト接続を使用する場合は、カタログと接続の両方が同じゾーンに含まれており、遅延が少なく、高帯域幅の接続である必要があります。
- サテライトゾーンにアイテムを配置すると、これらのアイテムおよびこれらに関連する他のオブジェクトとサイトとの通信方法に影響します。
  - Controller マシンがサテライトゾーンに配置されている場合、これらのマシンは同一のサテライトゾーンにあるハイパーバイザーおよび VDA マシンと良好に（ローカルに）接続できるものとみなされます。そのため、サテライトゾーンにあるハイパーバイザーや VDA マシンを処理する場合、プライマリゾーンの Controller ではなく同じサテライトゾーンにある Controller が使用されます。
  - ハイパーバイザー接続がサテライトゾーンに配置されている場合、このハイパーバイザー接続で管理されているすべてのハイパーバイザーも同じサテライトゾーン内に存在するものとみなされます。そのため、サテライトゾーンにあるハイパーバイザー接続を使用して通信する場合、プライマリゾーンの Controller ではなく同じサテライトゾーンにある Controller が使用されます。
  - マシンカタログがサテライトゾーンに配置されている場合、このカタログ内のすべての VDA マシンも同じサテライトゾーンにあるとみなされます。このため、各 VDA の初回登録後に Controller リストの自動更新メカニズムが有効になると、サイトへの登録時にはプライマリゾーンの Controller ではなくローカルの Controller が使用されます。
  - NetScaler Gateway インスタンスもゾーンに関連付けることができます。この関連付けはこの記事で説明する他の要素と同様に、XenApp または XenDesktop のサイト構成ではなく StoreFront の最適な HDX ルーティング構成の一環として行います。ゾーンに関連付けられた NetScaler Gateway は、そのゾーンにある VDA マシンへの HDX 接続で優先して使用されます。
- 実稼働サイトを作成してから、最初のマシンカタログおよびデリバリーグループを作成した場合、すべてのアイテムがプライマリゾーンに含まれます。初期セットアップを完了するまで、サテライトゾーンは作成できません（空のサイトを作成した場合、プライマリゾーンには初期状態では Controller のみが含まれています。サテライトゾーンは、マシンカタログおよびデリバリーグループの作成前または作成後に作成できます）。
- 1 つまたは複数のアイテムが含まれる最初のサテライトゾーンを作成する場合、サイトのそのほかすべてのアイテムはプライマリゾーンに残ります。
- プライマリゾーンのデフォルト名は「プライマリ」です。この名前は変更できます。Studio 表示ではどのゾーンがプライマリゾーンかが示されますが、プライマリゾーンには容易に特定できる名前を使用するのがベストプラクティスです。プライマリゾーンは再割り当てする（すなわち、別のゾーンをプライマリゾーンにする）ことができます。ただし、プライマリゾーンには必ずサイトデータベースと高可用性サーバーが含まれている

必要があります。

- サイトデータベースは、必ずプライマリゾーンに含まれている必要があります。
- ゾーンを作成した後、アイテムをゾーン間で移動できます。この柔軟性により、近くに配置することによって最適に機能する複数のアイテムを別々のゾーンに配置してしまう可能性があります。たとえば、マシンカタログを、カタログ内のマシンを作成する接続（ホスト）とは別のゾーンに移動すると、パフォーマンスが低下する場合があります。そのため、アイテムをゾーン間で移動する前に、意図しない影響が出る可能性を考慮してください。カタログとホスト接続（同じゾーンまたは適切に接続されているゾーン（遅延が少なく高帯域幅のネットワーク経由など）でカタログが使用するもの）を維持します。
- パフォーマンスを最適化するため、Studio と Director はプライマリゾーンのみにインストールします。サテライトゾーンに追加の Studio インスタンスが必要な場合（Controller が含まれるサテライトゾーンが、プライマリゾーンにアクセスできなくなった場合のフェールオーバーとして使用されている場合など）、Studio をローカル公開アプリケーションとして実行します。Director は Web アプリケーションであるため、サテライトゾーンからもアクセスできます。
- サテライトゾーンの NetScaler Gateway はゾーン内の接続に使用できますが、ほかのゾーンまたは外部からそのゾーンへのユーザー接続に使用するのが理想的です。
- 注意：ゾーンの優先度機能を使用するには、StoreFront 3.7 以上および NetScaler Gateway 11.0-65.x 以上を使用している必要があります。

接続の質の制限

サテライトゾーンの Controller は、サイトデータベースに対して SQL 操作を直接実行します。このため、サテライトゾーンと、サイトデータベースが含まれるプライマリゾーンとのリンクの質はある程度制限されます。一部の制限は、サテライトゾーンに展開されている VDA の数とこれらの VDA 上のユーザーセッションの数に関係します。このため、VDA とセッションの数が少ないサテライトゾーンでは、VDA とセッションの数が多いサテライトゾーンよりもデータベースへの接続の質が低下します。

詳しくは、「遅延および SQL ブロッキングクエリの向上」を参照してください。

仲介のパフォーマンスに対する遅延時間の影響

ゾーンではリンクの遅延時間が大きくなりますが、ローカルブローカーが存在する場合、エンドユーザーのエクスペリエンスではさらに遅延が生じることになります。こうしたユーザーが行う作業のほとんどで、サテライトゾーンの Controller とサイトデータベース間での往復時間による遅れが生じます。

アプリケーションを起動する場合、セッションの仲介プロセスでセッション開始の要求を送信するのに適した VDA が見つかるまで、さらに遅れが生じます。

ゾーンの作成と管理

すべての管理権限を実行できる管理者は、ゾーンの作成および管理に関するすべてのタスクを実行できます。ただし、ゾーンを作成、編集、または削除できるカスタムの役割を作成することもできます。アイテムをゾーン間で移動する

ために、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありません。ただし、移動するアイテムの編集権限は必要になります。たとえば、マシンカタログをゾーン間で移動するには、そのマシンカタログの編集権限が必要です。詳しくは、「委任管理」を参照してください。

Provisioning Services を使用する場合：このリリースに付属する Provisioning Services コンソールではゾーンが認識されないため、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場合は、Studio を使用することをお勧めします。Studio ウィザードを使用してカタログを作成し、適切なサテライトゾーンを指定します。その後、Provisioning Services コンソールを使用して、そのカタログのマシンをプロビジョニングします（Provisioning Services ウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でサテライトゾーンに移動するには Studio を使用する必要があります）。

ゾーンの作成

1. Studio のナビゲーションペインで、［構成］**>**［ゾーン］の順に選択します。
2. ［操作］ペインで ［ゾーンの作成］を選択します。
3. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意にする必要があります。
4. 新しいゾーンに配置するアイテムを選択します。選択できるアイテムの一覧では、フィルターまたは検索を実行できます。また、アイテムを選択せずに空のゾーンを作成することもできます。
5. ［保存］をクリックします。

この方法とは別に、Studio でアイテムを 1 つ以上選択してから、［操作］ペインで ［ゾーンの作成］を選択することもできます。

ゾーンの名前または説明の変更

1. Studio のナビゲーションペインで、［構成］**>**［ゾーン］の順に選択します。
2. 中央ペインでゾーンを選択し、［操作］ペインで ［ゾーンの編集］を選択します。
3. ゾーンの名前または説明（もしくはその両方）を変更します。プライマリゾーンの名前を変更する場合、そのゾーンをプライマリゾーンとして容易に特定できるようにしてください。
4. ［**OK**］または ［適用］をクリックします。

アイテムのゾーン間移動

1. Studio のナビゲーションペインで、［構成］**>**［ゾーン］の順に選択します。
2. 中央ペインでゾーンを選択し、1 つまたは複数のアイテムを選択します。
3. アイテムを移動先ゾーンにドラッグするか、または［操作］ペインで ［アイテムを移動］を選択してから移動先ゾーンを指定します。

選択したアイテムが確認メッセージで一覧にされ、それらすべてのアイテムを移動するかどうかが確認されます。

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を使用している場合、そのカタログと接続はともに同じゾーンに含める必要があります。同じゾーンに含まれていない場合、パフォーマンスが低下する可能性があります。どちらかのアイテムを移動したら、もう 1 つのアイテムも移動してください。

ゾーンの削除

ゾーンは、削除する前に空にする必要があります。プライマリゾーンは削除できません。

1. Studio のナビゲーションペインで、［構成］**>**［ゾーン］の順に選択します。
2. 中央ペインでゾーンを選択します。
3. ［操作］ペインで ［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。

ユーザーのホームゾーンの追加

ユーザーにホームゾーンを構成することは、ゾーンへのユーザーの追加とも言います。

1. Studio のナビゲーションペインで ［構成］**>**［ゾーン］の順に選択し、中央ペインでゾーンを選択します。
2. ［操作］ペインで ［ゾーンにユーザーを追加します］を選択します。
3. ［ゾーンへのユーザーの追加］ダイアログボックスで、［追加］をクリックしてからゾーンに追加するユーザーおよびユーザーグループを選択します。すでにホームゾーンがあるユーザーを指定すると、2 つの選択肢を提供するメッセージが表示されます。［はい］を選択すると、指定したユーザーのうち、ホームゾーンのないユーザーのみが追加されます。［いいえ］を選択すると、ユーザー選択ダイアログに戻ります。
4. ［**OK**］をクリックします。

構成済みのホームゾーンがあるユーザーについては、ユーザーのホームゾーンからのセッション開始のみ要求できます。

1. デリバリーグループを作成または編集します。
2. ［ユーザー］ページで、［セッションはユーザーのホームゾーンで開始（構成済みの場合）］チェックボックスを選択します。

そのデリバリーグループ内のユーザーによって開始されたすべてのセッションは、そのユーザーのホームゾーンから開始される必要があります。そのデリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は有効になりません。

ユーザーのホームゾーンの削除

この手順は、ゾーンからのユーザーの削除とも言います。

1. Studio のナビゲーションペインで ［構成］**>**［ゾーン］の順に選択し、中央ペインでゾーンを選択します。
2. ［操作］ペインで ［ゾーンからユーザーを削除します］を選択します。
3. ［ゾーンへのユーザーの追加］ダイアログボックスで、［削除］をクリックして、ゾーンから削除するユーザーおよびグループを選択します。このアクションにより、ユーザーがゾーンからのみ削除されます。これらのユーザーは、属してい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には残ったままとなります。
4. 確認のメッセージが表示されたら、削除を確定します。

アプリケーションのホームゾーンの管理

アプリケーションにホームゾーンを構成することは、ゾーンへのアプリケーションの追加とも言います。デフォルトで、マルチゾーン環境では、アプリケーションにはホームゾーンがありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、またはその後に、Studio でアプリケーションを選択して、そのプロパティを編集することによって構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、またはアプリケーションを既存のグループに追加するときに、ウィザードの［アプリケーション］ページで［プロパティ］を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、Studio のナビゲーションペインで ［アプリケーション］を選択します。アプリケーションを選択し、［操作］ペインで ［アプリケーションプロパティの編集］を選択します。

アプリケーションのプロパティまたは設定の ［ゾーン］ページで以下の操作を行います:

- アプリケーションにホームゾーンを追加する場合は、
  - ［選択したゾーンを決定に使用］ラジオボタンを選択し、ドロップダウンからゾーンを選択します。
  - アプリケーションを選択したゾーンからのみ起動する（他のゾーンからは起動しないようにする）には、ゾーン選択の下にあるチェックボックスを選択します。
- アプリケーションにホームゾーンを設定しない場合は、
  - ［ホームゾーンを構成しない］ラジオボタンを選択します。
  - このアプリケーションを起動するときに、ブローカーによって構成済みのユーザーのゾーンが考慮されないようにするには、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションのホームゾーンまたはユーザーのホームゾーンがこのアプリケーションを起動する場所の決定に使用されることはありません。

ゾーンの指定が含まれるそのほかの操作

サテライトゾーンを少なくとも 1 つ既に作成している場合、ホストの接続時またはマシンカタログの作成時（サイト作成時を除く）に、アイテムの割り当て先ゾーンを指定できます。

ほとんどの場合、プライマリゾーンがデフォルトで指定されます。Machine Creation Services を使用してマシンカタログを作成する場合、ホスト接続に対して構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合は、プライマリゾーンとして処理され、ゾーン選択ボックスは表示されません。

接続とリソース

August 24, 2021

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。その接続で使用するストレージとネットワークをリソースから選択します。

読み取り専用管理者は接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、すべての管理権限を実行できる管理者である必要があります。詳しくは、「委任管理」を参照してください。

接続の種類に関する情報の参照先

管理者は、サポートされている仮想化プラットフォームを使用して XenApp や XenDesktop の環境をホストおよび管理できます。サポートされる種類については、「システム要件」を参照してください。サポートされたクラウド展開ソリューションを使用して、製品コンポーネントをホストしたり仮想マシンをプロビジョニングしたりすることができます。これらのソリューションでは、コンピューティングリソースをプールしてパブリック、プライベート、およびハイブリッドの IaaS（Infrastructure as a Service）クラウドを構築できます。

詳しくは、以下の情報ソースを参照してください。

Microsoft Hyper-V

- 「Microsoft System Center Virtual Machine Manager 仮想化環境」
- Microsoft 社のドキュメント

Microsoft Azure

- Microsoft Azure 仮想化環境の記事
- Microsoft 社のドキュメント

Microsoft Azure Resource Manager

- 「Microsoft Azure Resource Manager 仮想化環境」
- Microsoft 社のドキュメント

Amazon Web Services（AWS）

- Citrix および 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。

- AWS 接続の専用ホストを指定するために使用される専用ホストおよび PowerShell パラメーター`tenancytype`は、このバージョンの XenApp および XenDesktop でサポートされません。専用ホストのサポートは、リリース 1811 で追加されました。詳しくは、「AWS クラウドを使用して MCS でマシンを作成する方法」を参照してください。

CloudPlatform

- CloudPlatform のドキュメント
- Studio での接続の作成時には、API キーおよび秘密キーの値を入力する必要があります。CloudPlatform でこれらの値を含んでいるキーファイルをエクスポートしてから、値を Studio にインポートすることができます。

Citrix XenServer

- Citrix XenServer のドキュメント
- 接続の作成時には、VM パワー管理者以上の権限を持つアカウントの資格情報を指定する必要があります。
- XenServer との通信を HTTPS で保護することをお勧めします。HTTPS を使用するには、XenServer にインストールされているデフォルトの SSL 証明書を置き換える必要があります（CTX128656を参照）。
- 高可用性機能で使用されるハイパーバイザーを選択することもできます（XenServer の高可用性が有効な場合）。プールマスターに障害が生じても XenServer との通信が中断されないように、（［Edit High Availability］から）プール内のすべてのサーバーを選択することをお勧めします。
- XenServer で vGPU がサポートされる場合は、GPU の種類およびグループ、または GPU パススルーを選択することができます。選択した項目で専用の GPU リソースが使用可能かどうか画面に表示されます。

Nutanix Acropolis

- 「Nutanix 仮想化環境」
- Nutanix のドキュメント

VMware

- 「VMware 仮想化環境」
- VMware 製品ドキュメント：

ホストストレージ

マシンのプロビジョニング時、データは種類別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。
- MCS でプロビジョニングされたマシンに書き込まれるすべての非永続データ、Windows ページファイル、ユーザープロファイルデータ、および ShareFile と同期されるすべてのデータを含む一時データ。このデータは、マシンの再起動のたびに破棄されます。
- Personal vDisk に保存された個人データ。

データの種類ごとに個別のストレージを用意することにより、各ストレージデバイスの負荷が軽減されて IOPS パフォーマンスが向上し、ホストで使用可能なリソースを最大限に活用できます。さらに、他のデータに比べて永続性と復元性がより重要なデータなど、データの種類に応じて適切なストレージを使用できるようになります。

ストレージは共有（中央に配置し、すべてのホストから分離して、すべてのホストで使用）することも、ハイパーバイザーのローカルに配置することもできます。中央共有ストレージの例として、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）や、ストレージベンダーからのアプライアンスなどがあります。中央ストレージには、ハイパーバイザーのストレージ制御パスやパートナープラグインからの直接アクセスなど、独自の最適化が備わっていることもあります。

一時データをローカルに保存することにより、共有ストレージへのアクセスでネットワークを経由する必要がなくなります。さらに、共有ストレージデバイスの負荷（IOPS）も軽減されます。共有ストレージは費用が高いため、ローカルにデータを保存することによってコストを抑えられます。こうした利点は、ハイパーバイザーサーバー上で十分なストレージを使用できることよりも重要になるでしょう。

接続の作成時、ストレージをハイパーバイザー間で共有するか、またはストレージをハイパーバイザーのローカルに配置する 2 つのストレージ管理方法からいずれかを選択してください。

> 注：
>
> 1 つまたは複数の XenServer ホスト上のローカルストレージを一時データストレージとして使用する場合は、プール内の各ストレージの場所に一意の名前が付いていることを確認してください。（XenCenter で名前を変更するには、ストレージを右クリックして名前のプロパティを編集します）。

ハイパーバイザー間で共有されるストレージ

ハイパーバイザー間でストレージを共有する方法では、長期間保持する必要のあるデータが保存され、バックアップおよび管理を一元的に行うことができます。このストレージでは、OS ディスクおよび Personal vDisk が保持されます。

この方法を選択する場合、永続性を必要としない一時マシンデータや、共有ストレージ内のデータほど復元性を必要としない一時マシンデータに（同じハイパーバイザープール内のサーバー上の）ローカルストレージを使用するかどうかを選択できます。これは一時データキャ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 で、ローカルストレージに一時データキャッシュディスクを作成することはできません。

接続を作成するときに一時データをローカルに保存するオプションを有効にすると、この接続を使用するマシンカタログを作成する際に、各 VM のキャッシュディスクサイズおよびメモリサイズにデフォルト以外の値を有効にして構成することができます。ただし、デフォルト値は接続の種類に適切な値に設定されており、ほとんどの場合はデフォルト値で十分です。詳しくは、「マシンカタログの作成」を参照してください。

また、ハイパーバイザーはディスクイメージのローカルな読み込みキャッシュによる最適化テクノロジを提供します（例：XenServer の IntelliCache）。これも、中央ストレージへのネットワークトラフィックを軽減します。

ハイパーバイザーのローカルに配置するストレージ

ストレージをハイパーバイザーのローカルに配置する方法では、データはハイパーバイザー上にローカルで保存されます。この方法を使用する場合、最初のマシン作成時およびその後のイメージ更新時に、マスターイメージおよびほかの OS データはサイトで使用されるすべてのハイパーバイザーに転送されます。これにより、管理ネットワークでかなりのトラフィックが生じます。イメージ転送も時間がかかる処理であり、各ホストでイメージを利用できるようになるタイミングも異なります。

この方法を選択した場合、バックアップおよび障害回復システムに復元性とサポートを提供するために Personal vDisk の共有ストレージを使用するかどうかを選択することができます。

接続とリソースの作成

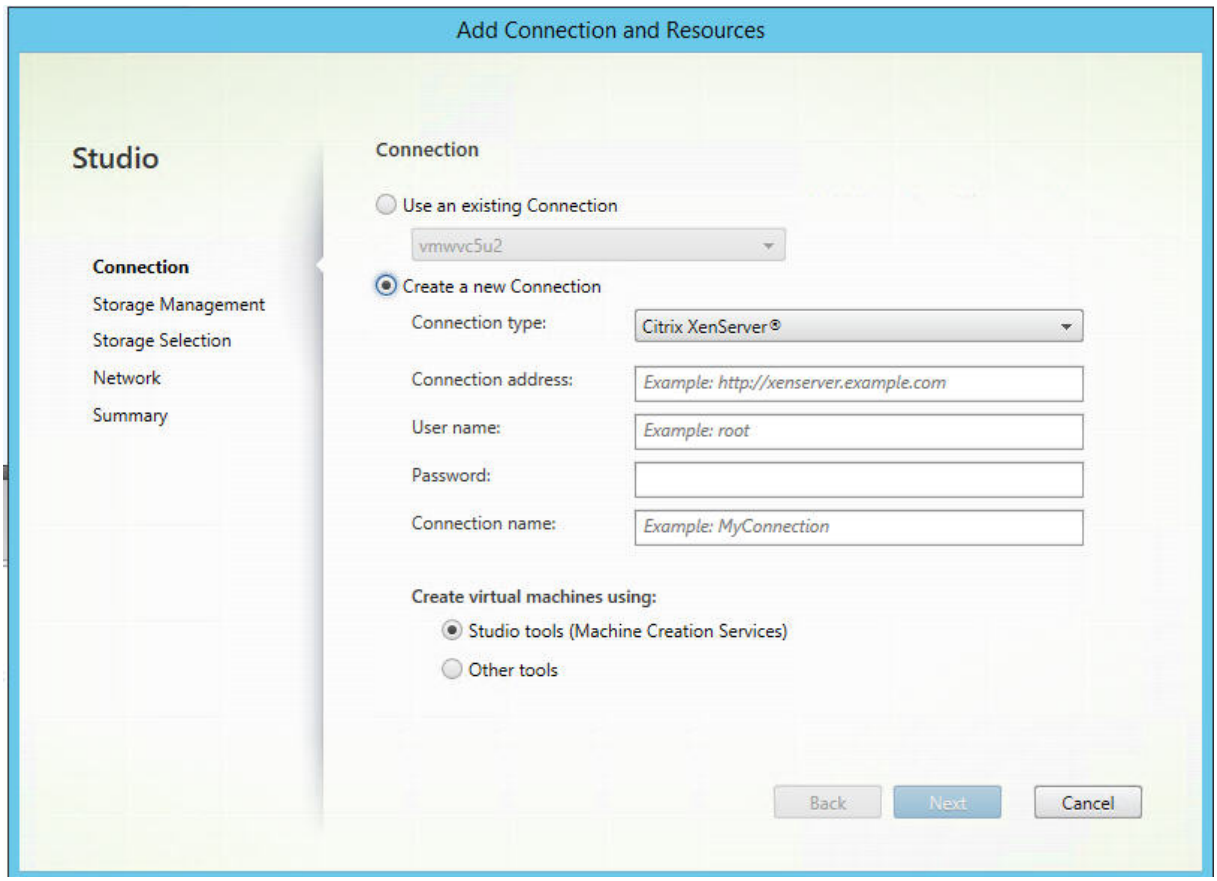
管理者は、サイトを作成するときに、オプションで最初の接続を作成できます。サイト作成ウィザードには、［接続］、［ストレージの管理］、［ストレージの選択］、［ネットワーク］といった接続関連のページがあります。

サイトの作成後に接続を作成する場合は、次の手順 1 から開始してください。

> 重要:
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が使用可能になっている必要があります。

- Studio の［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。
- ［操作］ペインの ［接続およびリソースの追加］を選択します。
- ウィザードの指示に従って、以下のページの操作を行います（具体的なページ内容は、選択した接続の種類に応じて異なります）。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。

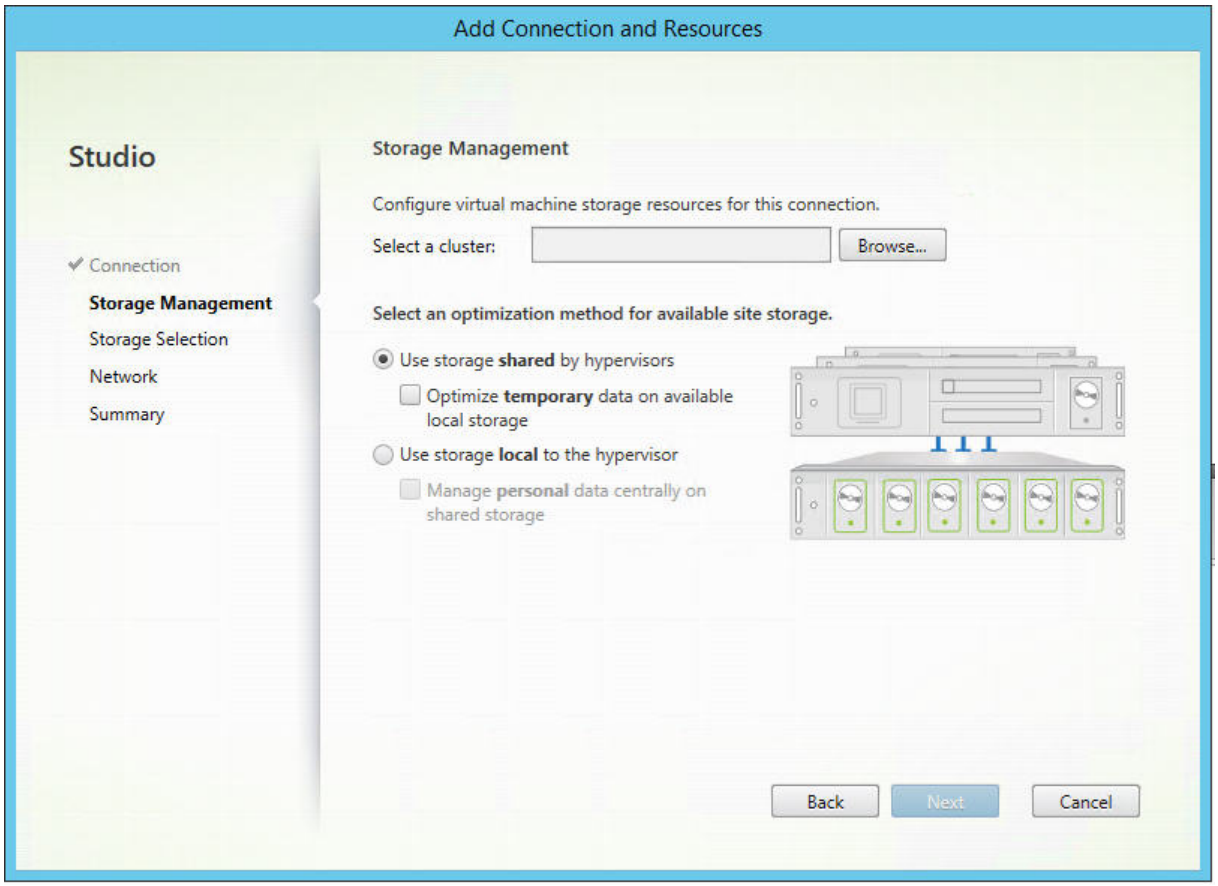
接続



［接続］ページで以下を実行します：

- 新しい接続を作成するには、［新しい接続を作成する］をクリックします。既存の接続と同じホスト構成に基づいて接続を作成する場合は、［既存の接続を使用する］を選択してから該当の接続を選択します。
- ［接続の種類］フィールドで、使用しているハイパーバイザーまたはクラウドサービスを選択します。
- 接続のアドレスおよび資格情報は、選択した接続の種類に応じて異なります。要求された情報を入力します。
- 接続名を入力します。この接続名は Studio で表示されます。
- 仮想マシンの作成に使用するツールを、Studio ツール（Machine Creation Services や Provisioning Services など）またはその他のツールから選択します。

ストレージ管理



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

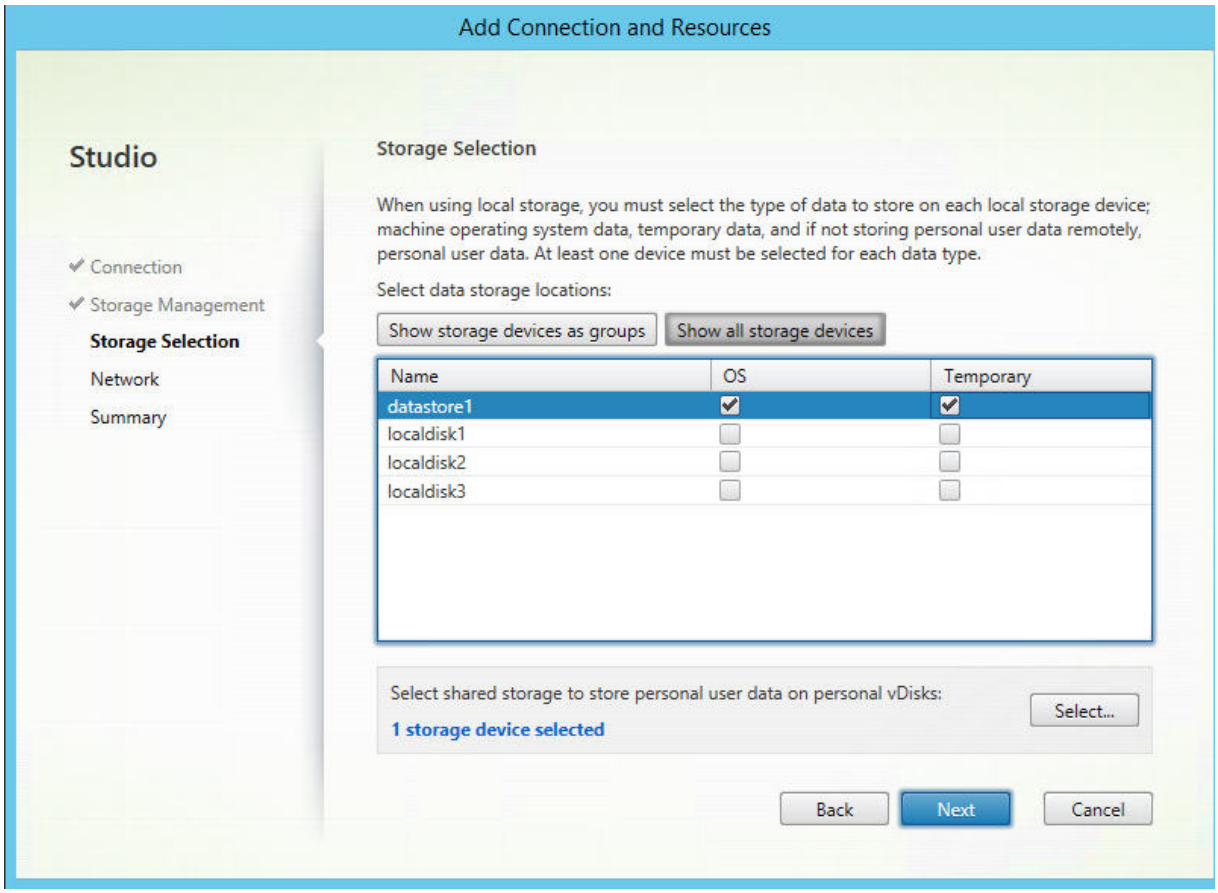
Hyper-V または VMware ホストに対する接続を構成している場合は、クラスター名を参照してから選択します。他の接続の種類では、クラスター名は要求されません。

ストレージ管理方法（ハイパーバイザー間で共有されるストレージまたはハイパーバイザーのローカルに配置するストレージ）を選択します。

- ハイパーバイザー間で共有されるストレージを選択する場合、一時データを使用可能なローカルストレージで保持するかどうかを指定します（この接続を使用するマシンカタログで、デフォルトではない一時ストレージのサイズを指定できます）。例外：クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Manager ではローカルストレージに一時データキャッシュディスクを作成できないため、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



ストレージの選択について詳しくは、「ホストストレージ」を参照してください。

使用可能なデータの種類ごとに 1 つ以上のストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータの種類は変化します。ウィザードの次のページに進むには、サポートされる各データの種類に対して 1 つ以上のストレージデバイスを選択する必要があります。

前のページで以下のいずれかを選択した場合、［ストレージの選択］ページ下部には追加の設定オプションが含まれます。

- ハイパーバイザー間で共有されるストレージを選択し、［利用可能なローカルストレージ上で一時データを最適化します］チェックボックスをオンにしている場合、（同じハイパーバイザープールで）一時データに使用するローカルストレージデバイスを選択できます。
- ハイパーバイザーのローカルに配置するストレージを選択し、［共有ストレージ上でパーソナルデータを一元的に管理します］チェックボックスをオンにしている場合、個人（PvD）データに使用する共有デバイスを選択できます。

現在選択中のストレージデバイスの数が表示されます（上図では「1 個のストレージデバイスが選択されました」）。このエントリの上にマウスを合わせると、選択したデバイスの名前が表示されます（構成されたデバイスがある場合のみ）。

1. 使用するストレージデバイスを変更するには［選択］をクリックします。

2. ［ストレージの選択］ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして［**OK**］をクリックします。

ネットワーク

リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別できるように、Studio に表示されます。

仮想マシンで使用するネットワークを 1 つまたは複数選択します。

概要

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以外の値を設定できます。「マシンカタログの作成」を参照してください。

接続の設定の編集

接続の名前の変更または新しい接続の作成のために、この手順を使用しないでください。これらの操作とは異なります。アドレスの変更は、現在のホストマシンに新しいアドレスがある場合にのみ行ってください。異なるマシンへのアドレスを入力すると、接続のマシンカタログが破損します。

接続の GPU 設定を変更することはできません。これは、そのリソースにアクセスするマシンカタログで、GPU 固有のマスターイメージを使用する必要があるためです。新しい接続を作成します。

1. Studio の［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。
2. 接続を選択し、［操作］ペインの ［接続の編集］を選択します。
3. 接続の編集時に可能な設定については、以下の手順に従います。
4. 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も XenServer との通信が中断されないように、プール内のすべてのサーバーを選択することをお勧めします。

［詳細設定］ページ：

接続の種類が、リモート PC アクセスで使用される Microsoft System Center Configuration Manager（ConfMgr）の Wake On LAN 接続の場合は、ConfMgr のウェイクアッププロキシ、マジックパケット、およびパケットの転送情報を入力します。

制限しきい値設定を使用して、接続に対して許可される電源操作の最大数を指定することができます。電源管理設定で同時に起動するマシンの数が多すぎたり少なすぎたりする場合に、この設定を行います。接続の種類のそれぞれには固有のデフォルト値が設定されています。これらの値は、ほとんどのケースに適切であり通常は変更する必要はありません。

[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で、すべてのマシンのうちこの接続を使用できる最大マシン数を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、実際に適用される上限値は、絶対値の 10 よりも小さい、34 の 10% を四捨五入した 3 になります。

[**1** 分あたりの最大新規操作] は、絶対値です。パーセンテージ値はありません。

注：[接続オプション] ボックスへの情報の入力は、Citrix サポート担当者からの指示があった場合のみ行ってください。

接続のメンテナンスモードのオン/オフの切り替え

接続のメンテナンスモードをオンにすると、その接続（ホスト）上に格納されているマシンに新規の電源操作が適用されるのを防ぐことができます。ユーザーは、メンテナンスモードになっているマシンには接続できません。ユーザーが既に接続している場合は、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場合は、[操作] ペインの [メンテナンスモードをオンにする] を選択します。メンテナンスモードをオフにするには、[メンテナンスモードをオフにする] を選択します。

個々のマシンのメンテナンスモードをオンまたはオフにすることもできます。マシンカタログ内またはデリバリーグループ内のマシンに対し、メンテナンスモードをオンまたはオフにすることもできます。

接続の削除

> 注意：
>
> 接続の削除は、多くのマシンおよびそのデータの損失が発生する可能性のある操作です。削除されるマシン上に重要なユーザーデータがないかどうかを確認し、重要なデータがある場合はバックアップを作成しておいてください。

接続を削除する前に、以下の点について確認してください。

- 接続上に格納されているマシンからすべてのユーザーがログオフしていること。
- 実行したまま切断されたユーザーセッションがないこと。
- プールおよび専用のマシンの場合は、メンテナンスモードになっていること。
- 接続で使用されている、マシンカタログ内のすべてのマシンの電源がオフになっていること。

マシンカタログで指定されている接続を削除すると、そのカタログを使用できなくなります。削除する接続がマシンカタログにより参照されている場合は、同時にそのカタログを削除することもできます。ただし、そのマシンカタログがほかの接続で使用されていないことを確認してから削除してください。

1. Studio の［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。
2. 接続を選択し、［操作］ペインで ［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］ペインで ［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］ペインで ［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、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. リソースを選択してから、［操作］ペインで次の適切なエントリを選択します：［リソースの削除］、［リソース名の変更］、または ［リソースのテスト］。

XenServer 接続での **IntelliCache** の使用

IntelliCache を使用すると、共有ストレージとローカルストレージを組み合わせて使用できるようになり、VDI 展開のコスト効率が向上します。これによってパフォーマンスが向上し、ネットワークトラフィックが減少します。この機能では、共有ストレージ上のマスターイメージがローカルストレージにキャッシュされ、共有ストレージでのデータ読み取りが減少します。共有デスクトップの場合、差分ディスクへの書き込みはホスト上のローカルストレージに書き込まれ、共有ストレージには書き込まれません。

- IntelliCache を使用する場合、共有ストレージは NFS である必要があります。
- パフォーマンスを向上させるため、高パフォーマンスのローカルストレージデバイスを使用することをお勧めします。

IntelliCache を使用するには、XenServer と Studio の両方でこの機能を有効にする必要があります。

- XenServer のインストール時に［**Enable thin provisioning (Optimized storage for XenDesktop)**］を選択します。IntelliCache が有効なサーバーと無効なサーバーを同一プールで混在させることはサポートされません。詳しくは、XenServer のドキュメントを参照してください。
- XenApp および XenDesktop では、IntelliCache はデフォルトで無効になっています。この機能は XenServer 接続の作成時にのみ有効にでき、これを後で無効にすることはできません。Studio で XenServer 接続を追加するときに、以下の手順に従います：
  - ストレージの種類として、［共有］を選択します。
  - ［**IntelliCache** を使用して共有ストレージデバイス上の負荷を軽減させる］チェックボックスをオンにします。

接続タイマー

ポリシー設定を使用すると、以下の 3 つの接続タイマーを構成できます。

- 最長接続タイマー：ユーザーデバイスと仮想デスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの［セッション接続タイマー］設定および［セッション接続タイマー間隔］設定を使用します。
- 接続アイドルタイマー：ユーザーからの入力がないユーザーデバイスと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仮想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。

ローカルホストキャッシュ

August 24, 2021

XenApp および XenDesktop サイトデータベースを常に使用可能状態にするために、Microsoft 社の高可用性ベストプラクティスに従って耐障害性の高い SQL Server 展開から開始することをお勧めします（「システム要件」の「データベース」に XenApp および XenDesktop でサポートされている SQL Server の高可用性機能が一覧にされています）。ただし、ネットワークの問題および中断によってユーザーがアプリケーションやデスクトップに接続できなくなる場合があります。

ローカルホストキャッシュ（LHC）機能を使用すると、停止状態が発生しても、XenApp または XenDesktop サイトの接続仲介操作を続行できます。Delivery Controller とサイト構成データベースとの間の接続が失敗すると、停止状態が発生します。ローカルホストキャッシュは、サイトデータベースに 90 秒間アクセスできない場合に使用されます。

ローカルホストキャッシュは、XenApp および XenDesktop の最も包括的な高可用性機能です。XenApp 7.6 で導入された接続リース機能のより強力な代替選択肢です。

このローカルホストキャッシュ実装は、XenApp 6.x 以前の XenApp リリースのローカルホストキャッシュ機能の名前を共有しますが、大幅に改善されています。この実装は、破損に対してより頑強で耐性もあります。定期的に dsmaint コマンドを実行する必要がないなど、メンテナンス要件が最小になります。このローカルホストキャッシュは技術的にはまったく異なる実装です。以下、その仕組みについて説明します。

> 注:
>
> バージョン 7.15 LTSR では接続リース機能はサポートされていますが、それ以降のリリースでは削除される予定です。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部として次の情報が格納されます:

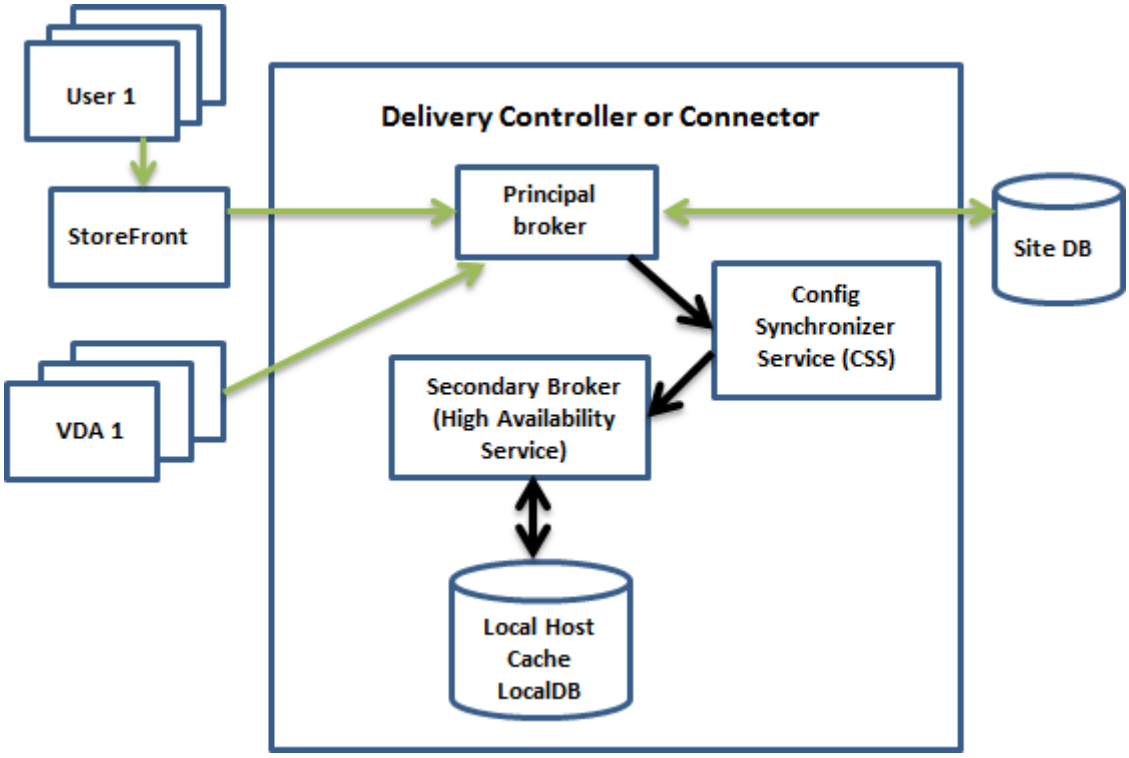
- サイトから公開されたリソースに対する特別な権限が割り当てられているユーザーおよびグループの ID
- サイトの公開リソースを現在使用しているか、最近使用したユーザーの ID
- サイトに構成されている VDA マシン（リモート PC アクセスマシンを含む）の ID
- 公開リソースへの接続で頻繁に使用されている Citrix Receiver クライアントマシンの ID（名前と IP アドレス）

また、メインデータベースが利用できなくなったときに確立され、現在アクティブな接続に関する情報も格納されています:

- Citrix Receiver で実行されたクライアントマシンのエンドポイント分析の結果
- サイトに関連するインフラストラクチャマシン（NetScaler Gateway や StoreFront サーバーなど）の ID
- ユーザによる最近のアクティビティの日時とタイプ

機能

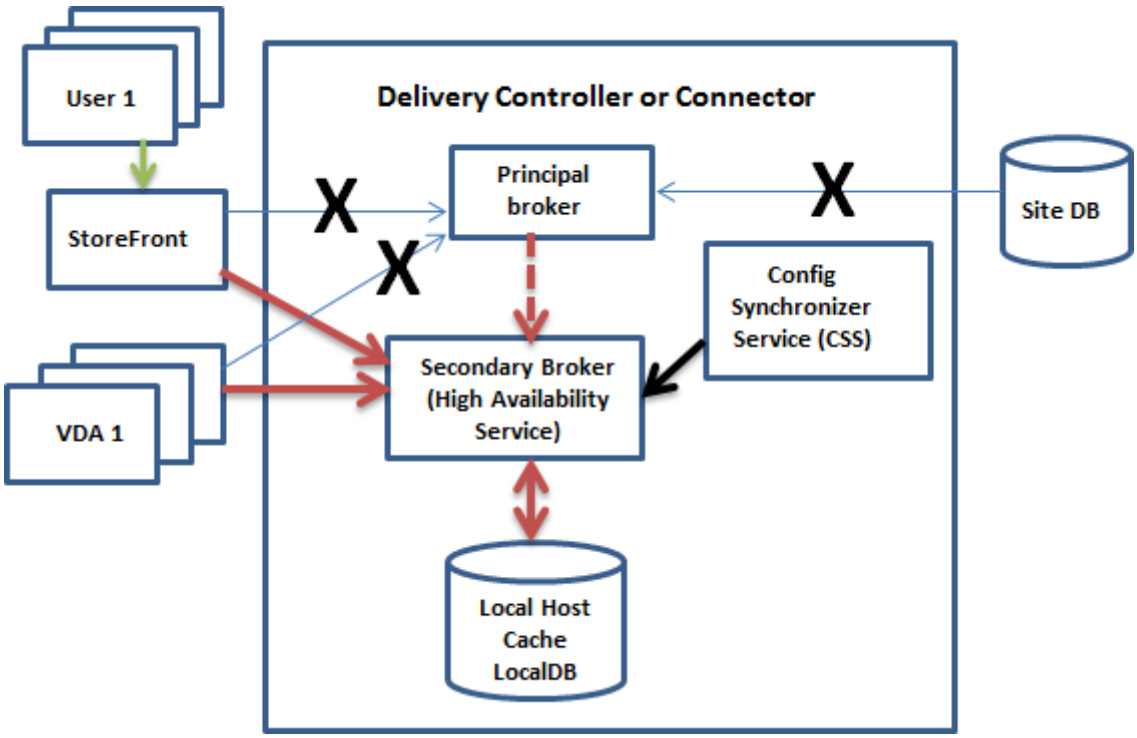
次の図は、通常の操作中のローカルホストキャッシュコンポーネントと通信経路を示しています。



通常の操作中:

- Controller 上のプリンシパルブローカー（Citrix Broker Service）は、StoreFront から接続要求を受け取り、サイトデータベースと通信して、Controller に登録されている VDA にユーザーを接続します。
- 2 分おきにチェックして、プリンシパルブローカーの構成が変更されたかどうか判断します。この変更は、PowerShell/Studio の操作（デリバリーグループプロパティの変更など）によっても、システム操作（マシン割り当てなど）によっても開始できます。
- 最後のチェック以降に変更されると、プリンシパルブローカーは、Citrix Config Synchronizer Service（CSS）を使用して Controller 上のセカンダリブローカー（Citrix High Availability Service）に情報を同期（コピー）します。前回のチェック以降に変更された項目だけでなく、すべてのブローカー構成データがコピーされます。セカンダリブローカーは、Controller 上の Microsoft SQL Server Express LocalDB データベースにデータをインポートします。CSS により、セカンダリブローカーの LocalDB データベースの情報がサイトデータベースの情報に一致することが保証されます。LocalDB データベースは、同期が発生するたびに再作成されます。
- 最後のチェック以降に変更が発生しなかった場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合の通信径路の変更を示しています（停止状態の開始）:



停止状態が開始された場合:

- プリンシパルブローカーはサイトデータベースと通信できなくなり、StoreFront および VDA 情報（図中の X 印）のリスニングを停止します。次に、プリンシパルブローカーは、接続要求（図中の赤い点線）のリスニングと処理を開始するように、セカンダリブローカー（High Availability Service）に指示します。
- 停止状態の開始時に、セカンダリブローカーにはその時点の VDA 登録データがありませんが、VDA との通信が始まるとすぐに再登録処理がトリガーされます。その処理中、セカンダリブローカーは、その VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理する間、プリンシパルブローカーはサイトデータベースへの接続の監視を続行します。接続が回復すると、プリンシパルブローカーはセカンダリブローカーに接続情報のリスニングを停止するように指示し、プリンシパルブローカーが操作の仲介を再開します。再登録処理は、VDA がプリンシパルブローカーと次に通信するときにトリガーされます。セカンダリブローカーは、前回の停止状態以降に残った VDA 登録があれば削除して、CSS から受け取った構成変更による LocalDB データベースの更新を再開します。

同期中に停止状態が開始されるという可能性の低い事象では、その時点のインポートは破棄され、最新の既知の構成が使用されます。

イベントログには、同期および停止に関する情報が含まれます。詳しくは、下の「モニター」セクションを参照してください。

また、停止状態を意図的にトリガーすることもできます。理由と方法について詳しくは「停止状態の強制」セクションを参照してください。

複数の **Controller** があるサイト

CSS は、他のタスク同様、ゾーン内のすべての Controller に関する情報を日常作業としてセカンダリブローカーに提供します（展開に複数のゾーンがない場合、この操作はサイト内のすべての Controller に影響します）。その情報により、各セカンダリブローカーは、同じ立場にあるすべてのセカンダリブローカーを認識します。

セカンダリブローカーは独立したチャネルで相互に通信します。実行しているマシンの FQDN 名のアルファベット順の一覧を使用して、停止状態が発生したときにどのセカンダリブローカーがゾーン内の仲介操作を担当するかを決定（選出）します。停止状態中、すべての VDA が、選出されたセカンダリブローカーに再登録します。選出されていないゾーン内のセカンダリブローカーは、着信接続と VDA 登録要求を能動的に拒否します。

停止状態中に、選出されたセカンダリブローカーに障害が発生した場合、別のセカンダリブローカーが選出されて引き継ぎ、VDA は選出されたセカンダリブローカーに新しく再登録します。

停止状態中に Controller を再起動した場合：

- この Controller をプライマリブローカーに選出していない場合は、再起動しても影響はありません。
- この Controller をプライマリブローカーに選出している場合は、別の Controller が選出されて VDA はそちらに再登録します。再起動した Controller の電源がオンになると、この Controller が自動的にブローカーを引き継ぐため、VDA はもう一度再登録します。このシナリオでは、再登録中にパフォーマンスが影響を受けることがあります。

プライマリブローカーに選出した Controller を、通常の操作中に電源を切ってから停止状態中に電源を入れると、ローカルホストキャッシュをこの Controller 上で使用することはできません。

イベントログには、選出に関する情報が含まれます。後述の「モニター」セクションを参照してください。

設計に関する考慮事項および要件

ローカルホストキャッシュは、サーバーでホストされるアプリケーションおよびデスクトップと静的な（割り当て済み）デスクトップでサポートされます。プール型の VDI デスクトップ（MCS や PVS で作成）ではサポートされません。

停止モードでの操作に時間制限は適用されませんが、可能な限り速やかにサイトを通常操作に復元するようにします。

停止状態中にできなくなることと変更されること：

- 管理者は Studio や PowerShell コマンドレットを使用できません。
- ハイパーバイザー資格情報をホストサービスから取得できません。すべてのマシンの電力状態が不明で、電源操作を発行できません。ただし、電源が入っているホスト上の VM を接続要求のために使用することができます。
- 割り当てられたマシンは、通常の操作中に割り当てが発生した場合のみ使用できます。停止状態中は新しい割り当てはできません。
- リモート PC アクセスマシンの自動登録と構成はできません。ただし、通常の操作中に登録、構成されたマシンは使用できます。

- サーバーでホストされるアプリケーションとデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。
- ユーザーは、現在アクティブ/選択されている（セカンダリ）ブローカーを含むゾーン内の登録済み VDA からのみ、アプリケーションとデスクトップを起動できます。停止状態中は、ゾーン間での起動（あるゾーンのブローカーから別のゾーンの VDA へ）はサポートされません。

停止状態が発生した場合、ShutdownDesktopsAfterUseプロパティが有効なデリバリーグループにプールされている電源管理対象のデスクトップ VDA は、デフォルトで保守モードになります。このデフォルトの設定を変更して、停止状態中にこれらのデスクトップを使用できるようにすることができます。ただし、停止状態中は電源管理が機能しないことがあります。（通常の操作を開始すると電源管理が始まります）。また、これらのデスクトップは再起動していないため、前のユーザーのデータが含まれている可能性があります。

デフォルトの動作を上書きするには、サイト全体で、影響を受けるデリバリーグループごとに、これを有効にする必要があります。

サイトに対して次の PowerShell コマンドレットを実行します：

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

影響を受ける各デリバリーグループに対して、次の PowerShell コマンドレットを実行します：

```
Set-BrokerDesktopGroup -Name "\<*name*\>"-ReuseMachinesWithoutShutdownInOutage
 $true
```

この機能をサイトでデリバリーグループごとに有効にしても、構成済みの「ShutdownDesktopsAfterUse」プロパティの、通常操作時の動作には影響がありません。

RAM サイズ：

LocalDB サービスは、約 1.2GB の RAM（データベースキャッシュ用に最大 1GB、SQL Server Express LocalDB の実行用にさらに 200MB）を使用できます。High Availability Service は、停止状態が長時間続き、多数のログオンが発生した場合（たとえば 12 時間でユーザー数 1 万人）、最大 1GB の RAM を使用できます。これらのメモリ要件は Controller の通常の RAM 要件とは別なので、RAM の総容量を増やす必要がある場合があります。

サイトデータベースに SQL Server Express インストールを使用する場合、サーバーに 2 つの sqlserver.exe プロセスを持つ点に注意してください。

CPU コアとソケットの構成：

Controller の CPU 構成、特に SQL Server Express LocalDB が利用できるコア数は、メモリ割り当て以上に、ローカルホストキャッシュのパフォーマンスに直接影響を及ぼします。この CPU オーバーヘッドが発生するのは、データベースとの接続が失われ、High Availability Service がアクティブである停止状態の間だけです。

LocalDB は複数のコア（最大 4 つ）を使用できますが、単一のソケットだけに制限されます。ソケットを追加しても（たとえば、4 つのソケットにそれぞれ 1 つのコア）、パフォーマンスは向上しません。それよりも複数のコアを持つ複数のソケットの使用を Citrix ではお勧めします。Citrix のテストでは、2x3（2 つのソケット、3 つのコア）の構成が、4x1 および 6x1 の構成より良好なパフォーマンスを示しました。

ストレージ：

ユーザーが停止状態の間にリソースにアクセスすると、LocalDB は増大します。たとえば、1 秒に 10 回ログオンするログオン/ログオフテスト実行では、データベースは 2〜3 分に 1MB 増大しました。通常の操作が再開すると、ローカルデータベースが再作成され、容量は元に戻ります。ただし、停止状態中のデータベース増大を考慮に入れて、LocalDB がインストールされるドライブ上のブローカーは十分な容量を持つ必要があります。ローカルホストキャッシュを使用すると、停止状態中に追加の I/O が生じます（数十万の読み取りで、1 秒あたり約 3MB の書き込み）。

パフォーマンス：

停止状態中は 1 つのブローカーがすべての接続を処理するため、通常の操作時に複数の Controller に負荷を分散するサイト（あるいは、ゾーン）では、停止状態中に、選出されたブローカーが普通よりはるかに多くの要求を処理する必要があることがあります。このため、CPU への要求が高くなります。選出されたブローカーが停止状態中に変更される可能性があるため、サイト（ゾーン）内のすべてのブローカーが、LocalDB と影響を受けるすべての VDA によって課される追加の負荷を処理できる必要があります。

VDI の制限事項：

- 単一ゾーンに VDI を展開する場合、停止状態時には最大 10,000 の VDA を効果的に処理できます。
- 複数ゾーンに VDI を展開する場合、停止状態時には各ゾーンで最大 10,000 の VDA、サイト全体では最大 40,000 の VDA を効果的に処理できます。たとえば次のそれぞれのサイトが、停止状態時に効果的に処理されます。
  - 4 つのゾーンそれぞれに 10,000 の VDA が含まれるサイト。
  - 1 つのゾーンには 10,000 の VDA が含まれ、残り 6 つのゾーンにはそれぞれ 5,000 の VDA が含まれる、合計 7 つのゾーンからなるサイト。

停止状態中に、サイト内の負荷管理が影響を受ける可能性があります。負荷評価基準（特にセッション数規則）を超過する可能性があります。

すべての VDA がブローカーに再登録する間、そのブローカーには現在のセッションについての完全な情報がないことがあります。このため、その間の接続要求により、既存のセッションへの再接続が可能であっても、新しいセッションが起動される可能性があります。こうした時間（「新しい」ブローカーが再登録時にすべての VDA からセッション情報を取得する時間）が発生するのは避けられません。停止状態の開始時に接続していたセッションは移行期間に影響は受けませんが、新しいセッションおよびセッション再接続は影響を受ける可能性がある点に注意してください。

この期間は、VDA が異なるブローカーに再登録する必要があるときは常に発生します。

- 停止状態の開始：プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止状態中のブローカー障害：障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの回復：通常の操作が再開し、プリンシパルブローカーが制御を再開したとき。

Citrix Broker Protocol の HeartbeatPeriodMs レジストリ値（デフォルト = 600000ms（10 分））を小さくすることによって期間を短縮できます。このハートビート値は、VDA が ping に使用する間隔の 2 倍であるため、デフォルト値では 5 分ごとに ping が発生します。

たとえば、ハートビートを 5 分（300000ms）に変更するには、次のコマンドを実行します。このようにすると、ping は 2.5 分ごとに発生します：

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000

VDA の登録をどんなに早くしても、間隔を完全になくすことはできません。

ブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数により増加します。たとえば、5000 個の VDA を同期する場合には、10 分以上かかる可能性があります。イベントログの同期エントリについて詳しくは、後述の「モニター」セクションを参照してください。

ローカルホストキャッシュの管理

ローカルホストキャッシュを正常に動作させるには、各 Controller 上の PowerShell 実行ポリシーを、RemoteSigned、Unrestricted、または Bypass に設定する必要があります。

SQL Server Express LocalDB

ローカルホストキャッシュが使用する Microsoft SQL Server Express LocalDB は、Controller をインストールするか、Controller を 7.9 以前のバージョンからアップグレードするときに、自動的にインストールされます。LocalDB を管理者がメンテナンスする必要はありません。セカンダリブローカーだけがこのデータベースと通信します。PowerShell コマンドレットを使用してこのデータベースに関する変更を行うことはいっさいできません。LocalDB は、Controller 間で共有できません。

SQL Server Express LocalDB データベースソフトウェアは、ローカルホストキャッシュが有効かどうかに関係なくインストールされます。

このインストールを防止するには、Controller のインストールまたはアップグレード時に、XenDesktopServerSetup.exe コマンドで「/exclude “Local Host Cache Storage (LocalDB)”」オプションを使用します。ただし、ローカルホストキャッシュ機能はデータベースがないと機能しないことと、セカンダリブローカーでは異なるデータベースを使用できないことに注意してください。

この LocalDB データベースのインストールは、サイトデータベースとして使うために SQL Server Express をインストールするかどうかには影響しません。

XenApp または **XenDesktop** のインストールとアップグレード後のデフォルト設定

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

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

ローカルホストキャッシュの有効化と無効化

ローカルホストキャッシュを有効化するには、次のように入力します:

```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
$false
```

このコマンドレットは、接続リース機能も無効化します。ローカルホストキャッシュと接続リースの両方を有効化しないでください。

ローカルホストキャッシュが有効かどうかを判断するには、次のように入力します。

```
Get-BrokerSite
```

LocalHostCacheEnabled プロパティが True で、ConnectionLeasingEnabled プロパティが False であることを確認します。

ローカルホストキャッシュを無効化（および接続リースを有効化）するには、次のように入力します:

```
Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled
$true
```

ローカルホストキャッシュが動作していることを確認する

ローカルホストキャッシュが適切に設定され動作していることを確認するには:

- 同期のインポートが正常に完了していることを確認します。イベントログをチェックします。
- SQL Server Express LocalDB データベースが Delivery Controller ごとに作成されたことを確認します。これにより、必要に応じて High Availability Service が処理を引き継げるようになります。
- Delivery Controller サーバーで、C:\Windows\ServiceProfiles\NetworkService に移動します。
- HaDatabaseName.mdf および HaDatabaseName_log.ldf が作成されていることを確認します。
- Delivery Controller に停止状態を強制します。ローカルホストキャッシュが動作することを確認したら、すべての Controller を通常モードに戻します。この処理には、大量の VDA 登録を避けるために 15 分程度かかることがあります。

停止状態の強制

データベースの停止状態を意図的に強制することもできます。

- ネットワークが稼動と停止を繰り返している場合。ネットワークの問題が解決するまで停止状態を強制することにより、通常モードと停止状態モードの移行が繰り返されるのを防げます。
- 障害回復プランをテストするには:
- サイトデータベースサーバーの交換または修理中。

停止状態を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。

- HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\LHC で、[OutageModeForced] を [1] に設定します。この指示により、ブローカーはデータベースの状態に関係なく停止状態モードに入ります（値を 0 に設定すると、サーバーの停止状態モードが終了します）。
- Citrix Cloud のシナリオでは、コントロールプレーンやプライマリゾーンへの接続の状態に関係なく、コネクタが停止状態モードに入ります。

モニター

イベントログに、同期および停止状態が発生した時刻が示されます。

Config Synchronizer Service:

通常の操作中に、CSS がブローカー構成をコピーおよびエクスポートして、High Availability Service（セカンダリブローカー）を使用してそれを LocalDB にインポートするとき、次のイベントが発生することがあります。

- 503：プリンシパルブローカー構成に変更が見つかり、インポートが開始されます。
- 504：ブローカー構成がコピーおよびエクスポートされて、LocalDB に正常にインポートされました。
- 505：LocalDB へのインポートが失敗しました。詳しくは下記を参照してください。
- 510：プライマリ構成サービスから構成サービス構成データを受信していません。
- 517：プライマリブローカーとの通信に問題がありました。
- 518：セカンダリブローカー（High Availability Service）が実行されていないため、Config Sync スクリプトが中止されました。

High Availability Service:

- 3502：停止状態が発生し、セカンダリブローカー（High Availability Service）が操作の仲介を実行しています。
- 3503：停止状態が解決され、通常の操作が再開しました。
- 3504：どのセカンダリブローカーが選出されたかと、選出に関わった他のブローカーを示します。

トラブルシューティング

LocalDB への同期インポートが失敗し、505 イベントがポストされた場合、いくつかのトラブルシューティングツールを利用できます。

CDF トレーシング： ConfigSyncServer モジュールおよび BrokerLHC モジュール向けのオプションが用意されています。それらのオプションと他のブローカーモジュールの組み合わせで問題を識別できるはずです。

レポート：同期インポートが失敗した場合、レポートを生成できます。このレポートの最後に、エラーの原因となったオブジェクトが記載されています。このレポート機能は同期速度に影響するため、Citrix では使用しないときは無効にしておくことをお勧めします。

CSS トレースレポートを有効化および作成するには、次のコマンドを入力します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```


HTML レポートはC:\\Windows\\ServiceProfiles\\NetworkService\\AppData\\Local\\Temp\\CitrixBrokerConfigSyncReport.htmlに格納されます。

レポートが生成されたら、次のコマンドを入力してレポート機能を無効にします:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグのために正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File file-pathname
```

たとえば、`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`などです。

セキュリティキーの管理

October 22, 2021

> 注:
>
> この機能は、StoreFront 1912 LTSR CU2 以降とともに使用する必要があります。

この機能により、承認された StoreFront および Citrix Gateway マシンのみが Citrix Cloud と通信できるようになります。この機能を有効にすると、キーが含まれていないすべての要求がブロックされます。この機能を使用して、内部ネットワークの攻撃から保護するセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです:

1. PowerShell SDK を使用して、Studio でこの機能を有効にします。
2. Studio で設定を構成します（Studio コンソールまたは PowerShell を使用します）。
3. StoreFront で設定を構成します（PowerShell を使用します）。

セキュリティキー機能の有効化

デフォルトでは、この機能は無効になっています。これを有効にするには、Remote PowerShell SDK を使用します。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。

この機能を有効にするには、次の手順を実行します:

1. XenApp および XenDesktop リモート PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:
    - `Add-PSSnapIn Citrix*`。このコマンドは、Citrix スナップインを追加します。
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabl "-Value "True"`

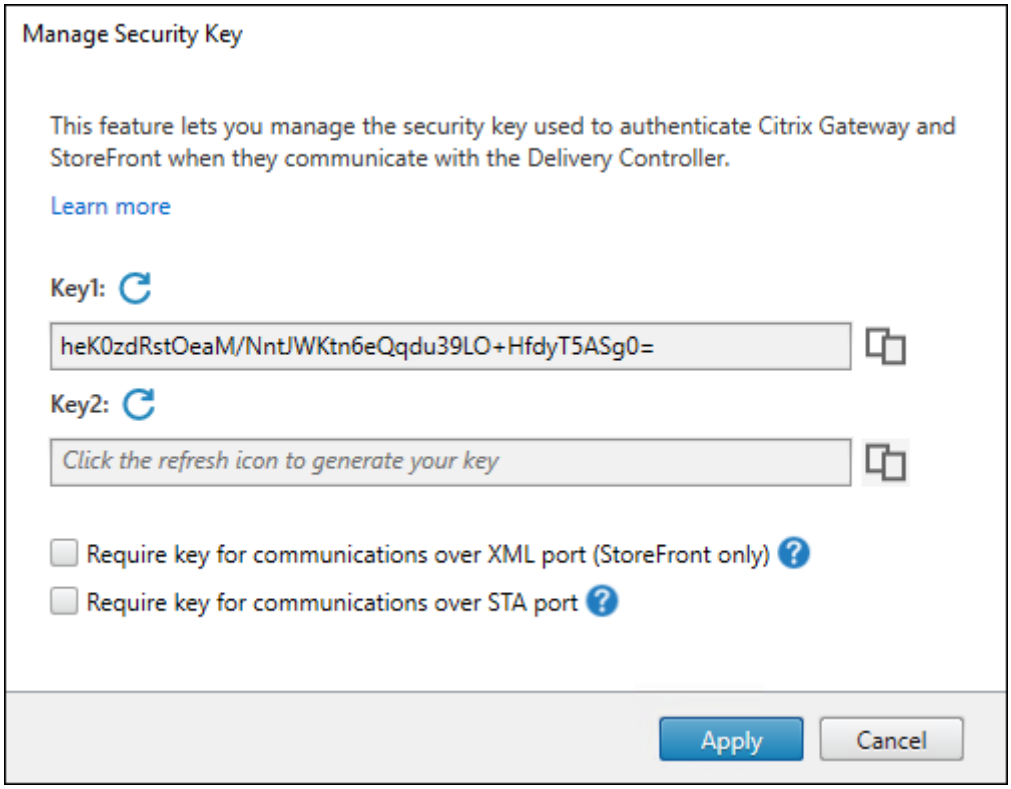
Studio での設定の構成

Studio コンソールまたは PowerShell を使用して、Studio で設定を構成できます。

Studio コンソールの使用

この機能を有効にした後、[**Studio**] **>** [構成] **>** [セキュリティキーの管理] に移動します。[セキュリティキーの管理] オプションを表示するには、[更新] のクリックが必要な場合があります。

[セキュリティキーの管理] をクリックすると、[セキュリティキーの管理] ウィンドウが表示されます。



> 重要:
>
> - 2 つのキーを使用できます。XML ポートと STA ポートを介した通信に、同じキーまたは異なるキーを使用できます。一度に 1 つのキーのみを使用することをお勧めします。未使用のキーは、キーの交換にのみ使用されます。
> - 既に使用中のキーを更新するために [更新] アイコンをクリックしないでください。クリックした場合、サービスが中断されます。

更新アイコンをクリックしてキーを生成します。

XML ポート経由の通信にキーが必須とする (**StoreFront** のみ)。選択されている場合、XML ポート経由での通信を認証するためにキーを必要とするかを示します。StoreFront は、このポートを介して Citrix Cloud と通信します。XML ポートの変更について詳しくは、Knowledge Center のCTX127945を参照してください。

STA ポート経由の通信にキーが必須とする。選択されている場合、STA ポート経由での通信を認証するためにキーを必要とするかを示します。Citrix Gateway および StoreFront は、このポートを介して Citrix Cloud と通信します。STA ポートの変更について詳しくは、Knowledge Center のCTX101988を参照してください。

変更を適用後、［閉じる］をクリックして ［セキュリティキーの管理］ウィンドウを終了します。

PowerShell の使用

以下は、Studio の操作に相当する PowerShell の手順です。

1. XenApp および XenDesktop リモート PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:
   - `Add-PSSnapIn Citrix*`
3. 次のコマンドを実行してキーを生成し、Key1 を設定します:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 次のコマンドを実行してキーを生成し、Key2 を設定します:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 次のコマンドのいずれかまたは両方を実行して、通信の認証でキーを使用できるようにします:
   - XML ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STA ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

StoreFront での設定の構成

Studio での構成が完了したら、PowerShell を使って StoreFront で関連する設定を構成する必要があります。

StoreFront サーバーで、次の PowerShell コマンドを実行します:

- XML ポート経由での通信のキーを構成するには、`Get-STFStoreServie`および `Set-STFStoreService`コマンドを使用します。次に例を示します:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnable $true -XMLValidationSecret <the key you generated in Studio>`
- STA ポート経由での通信のキーを設定するには、`New-STFSecureTicketAuthority`コマンドを使用します。次に例を示します:

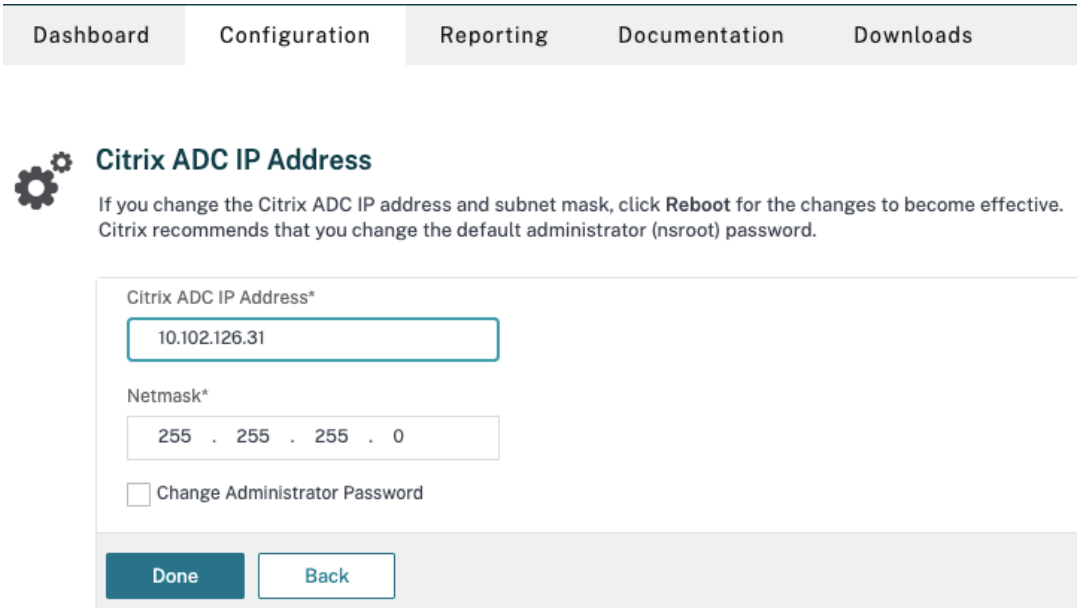
- `PS C:\> $sta = New-STFSecureTicketAuthority -StaUrl <STA URL> -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

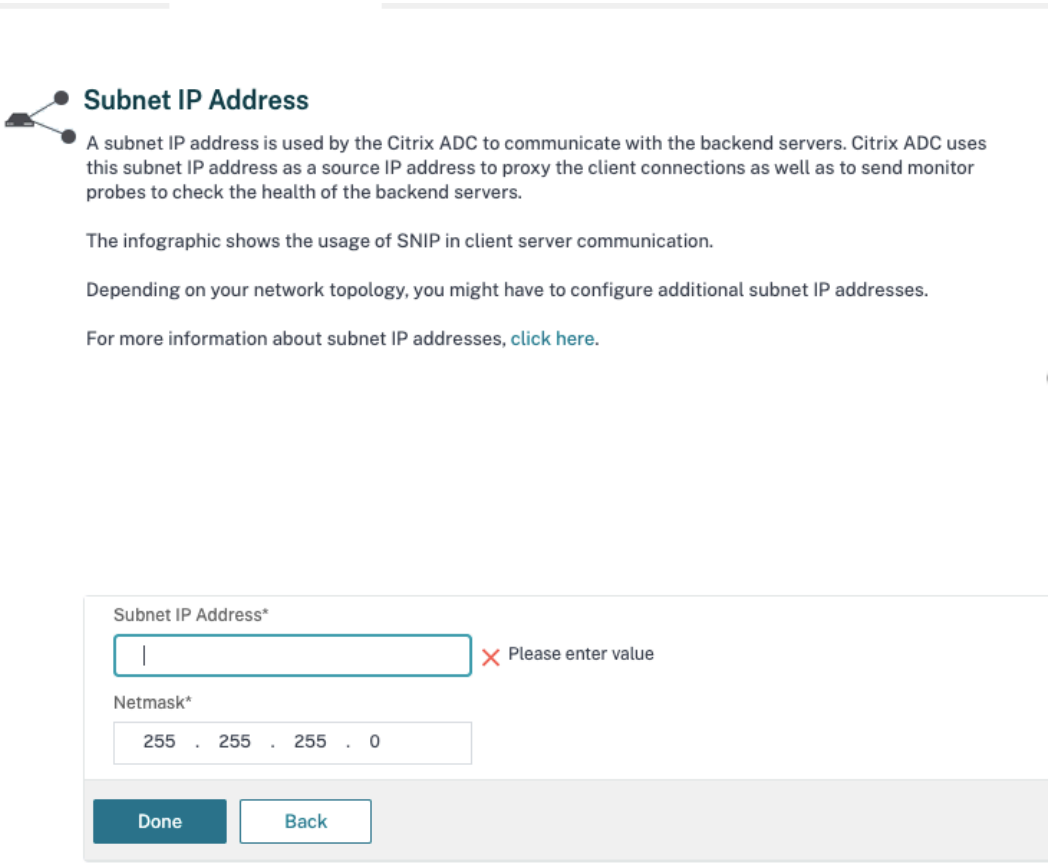
Citrix ADC での設定の構成

> 注:
>
> ゲートウェイとして Citrix ADC を使用しない限り、Citrix ADC でこの機能を構成する必要はありません。Citrix ADC を使用する場合は、以下の手順に従ってください。

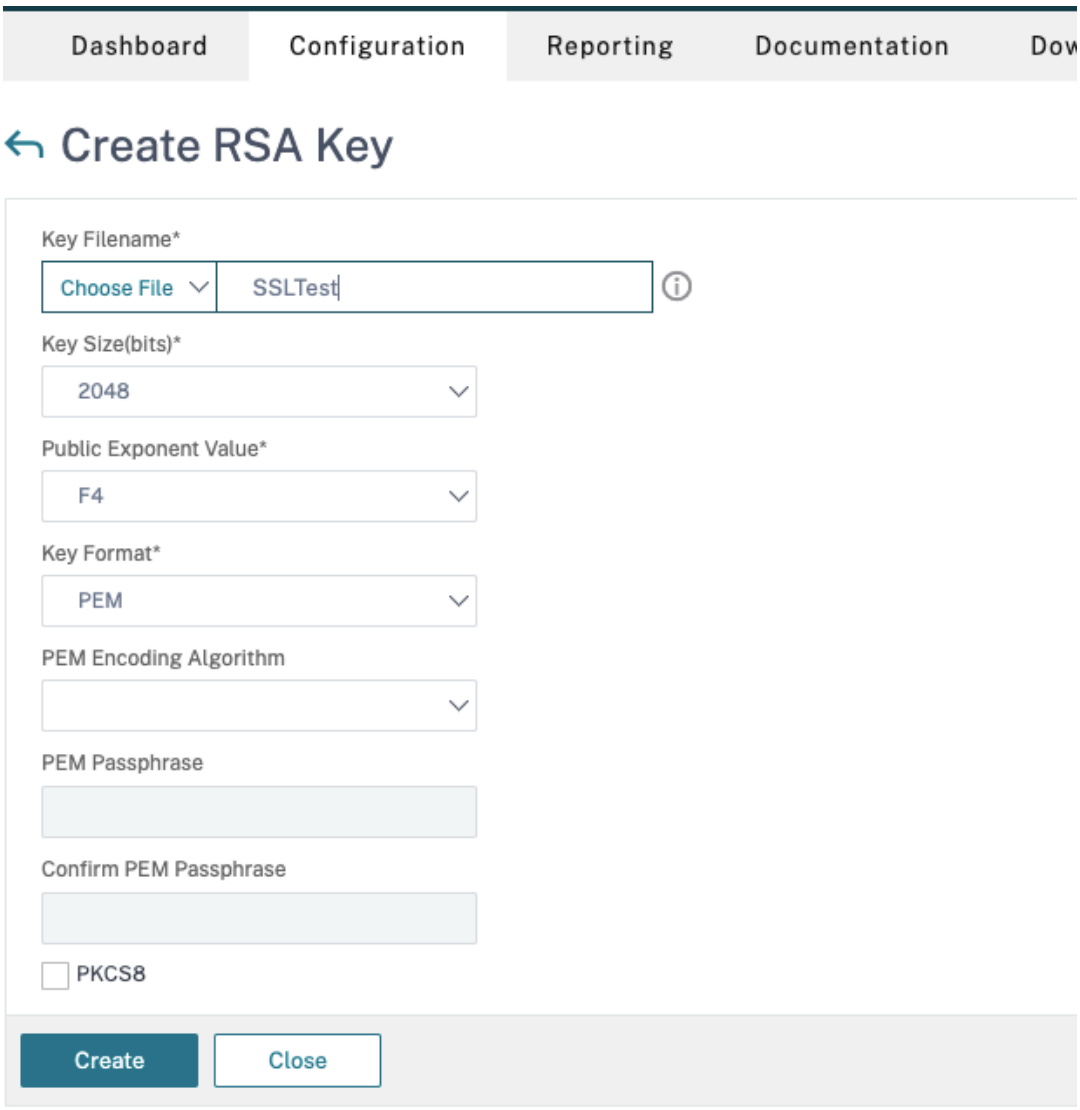
1. 以下の前提条件の構成が既に設定されていることを確認してください:
   - 以下の Citrix ADC 関連の IP アドレスが構成されている。
     - Citrix ADC コンソールにアクセスするための Citrix ADC 管理 IP（NSIP）アドレス。詳しくは、「NSIP アドレスの構成」を参照してください。



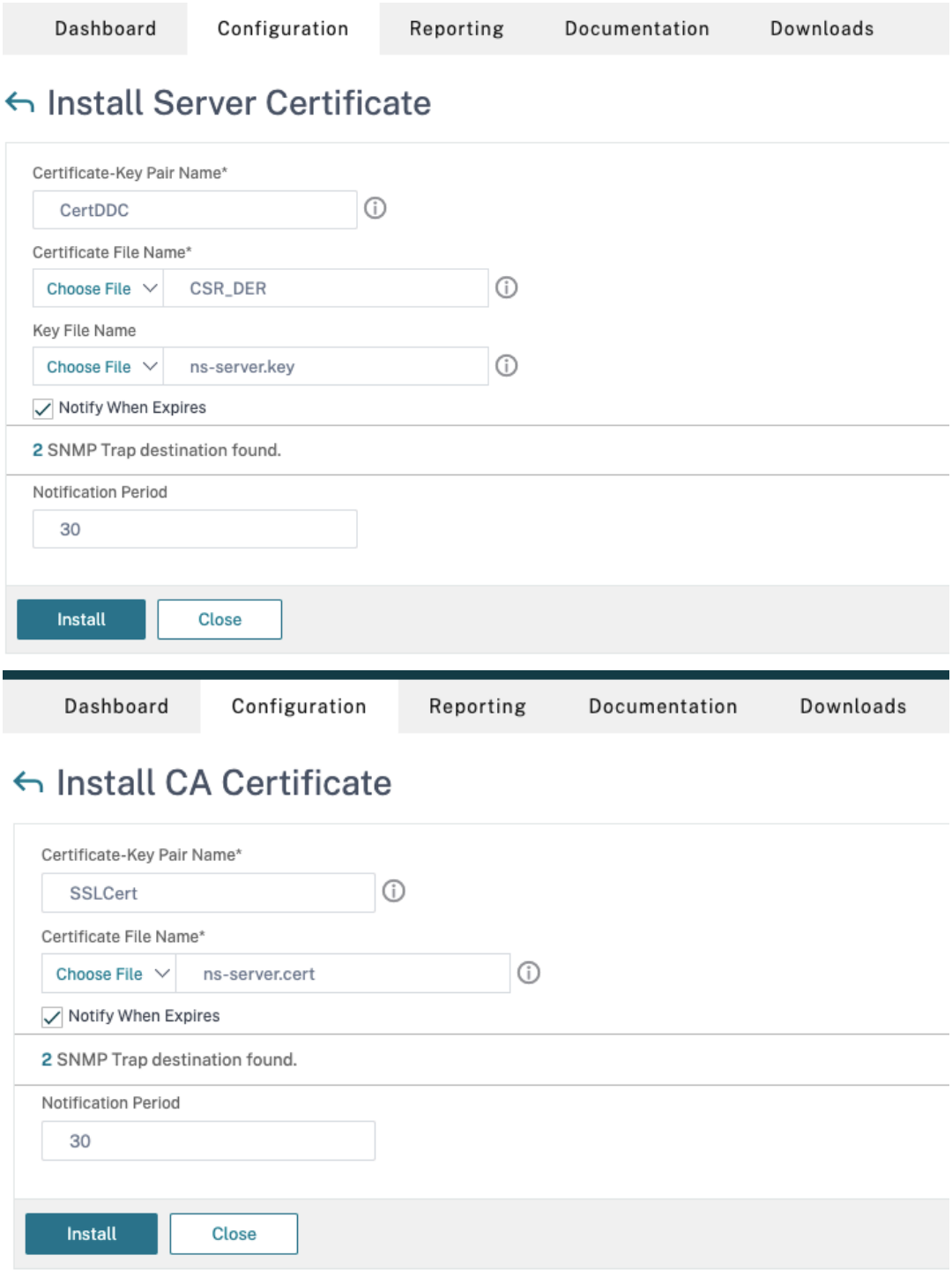
     - Citrix ADC アプライアンスとバックエンドサーバー間の通信を有効にするためのサブネット IP（SNIP）アドレス。詳しくは、「サブネット IP アドレスの構成」を参照してください。
     - ADC アプライアンスにログインしてセッションを起動するための Citrix Gateway 仮想 IP アドレスとロードバランサー仮想 IP アドレス。詳しくは、「仮想サーバーの作成」を参照してください。



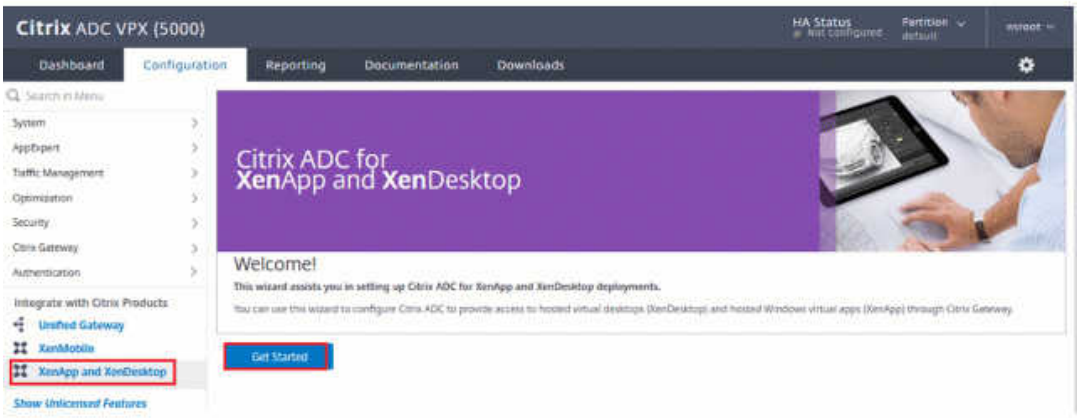
- Citrix ADC アプライアンスで必要なモードと機能が有効である。
  - モードを有効にするには、Citrix ADC GUI で［**System**］>［**Settings**］>［**Configure Mode**］の順に移動します。
  - 機能を有効にするには、Citrix ADC GUI で ［**System**］>［**Settings**］>［**Configure Basic Features**］の順に移動します。
- 証明書関連の構成が完了している。
  - 証明書署名要求（CSR：Certificate Signing Request）が作成されていること。詳しくは、「証明書の作成」を参照してください。



- サーバー証明書と CA 証明書およびルート証明書がインストールされていること。詳しくは、「インストール、リンク、および更新」を参照してください。



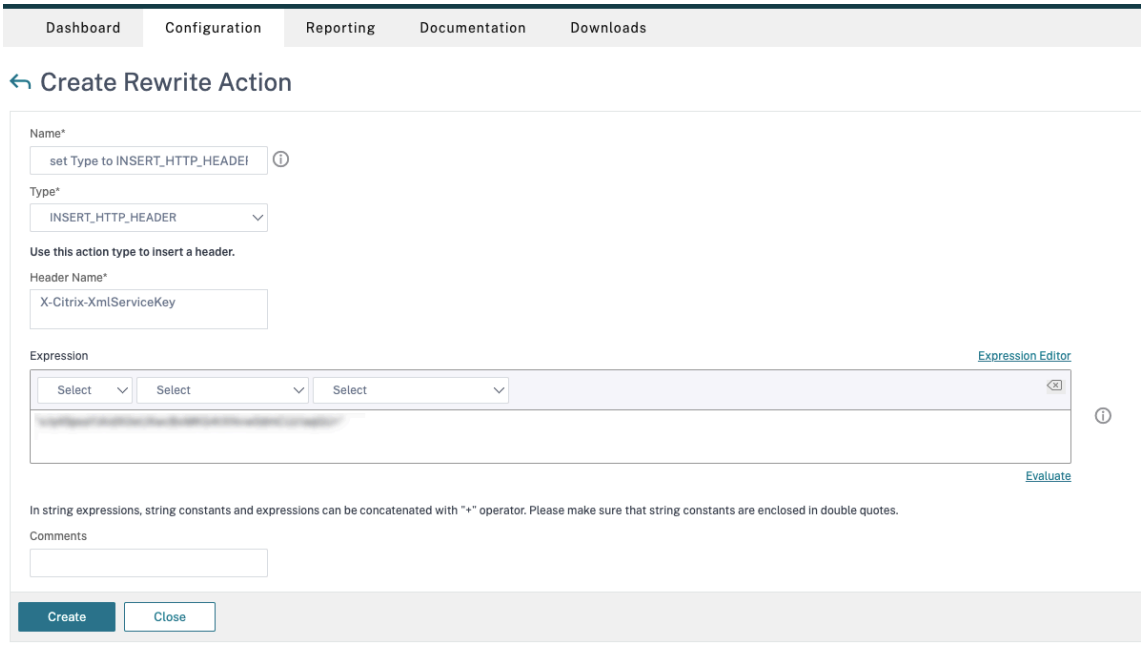
- Citrix Virtual Desktops 用に Citrix Gateway が作成されていること。[**Test STA Connectivity**] ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳しくは、「Citrix Virtual Apps and Desktops 用の Citrix ADC のセットアップ」を参照してください。



2. 書き換えアクションを追加します。詳しくは、「書き換えアクションの構成」を参照してください。

   a) [**AppExpert**] > [**Rewrite**] > [**Actions**] の順に移動します。

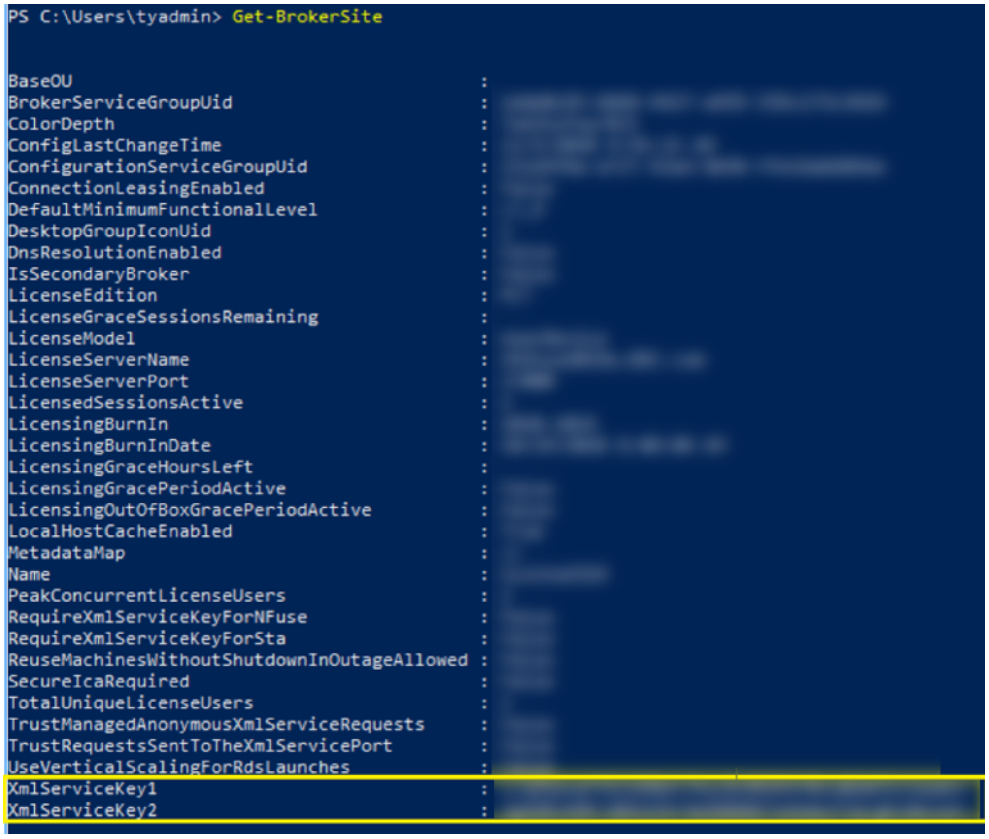
   b) [**Add**] をクリックして、新しい書き換えアクションを追加します。アクションに「set Type to INSERT_HTTP_HEADER」という名前を付けることができます。



   a) [**Type**] で、[**INSERT_HTTP_HEADER**] を選択します。

   b) [**Header Name**] に「X-Citrix-XmlServiceKey」と入力します。

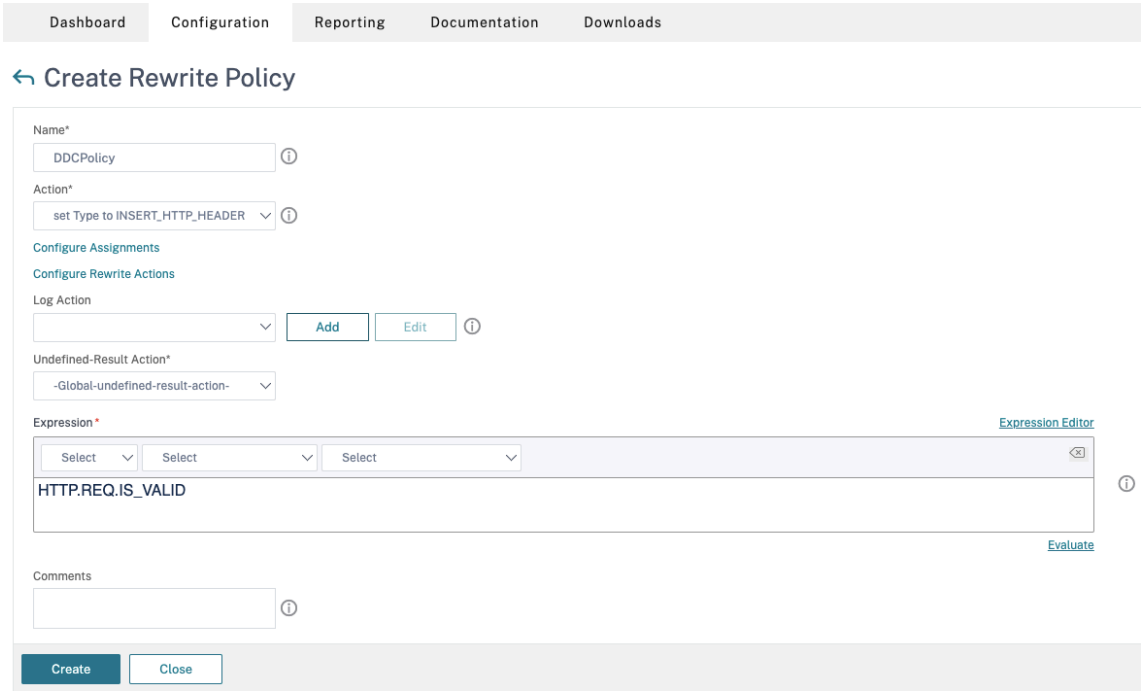
   c) [**Expression**] に、引用符付きで「<XmlServiceKey1 value>」を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller の構成からコピーできます。



3. 書き換えポリシーを追加します。詳しくは、「書き換えポリシーの構成」を参照してください。

   a) [**AppExpert**] > [**Rewrite**] > [**Policies**] の順に移動します。

   b) [**Add**] をクリックして、新しいポリシーを追加します。



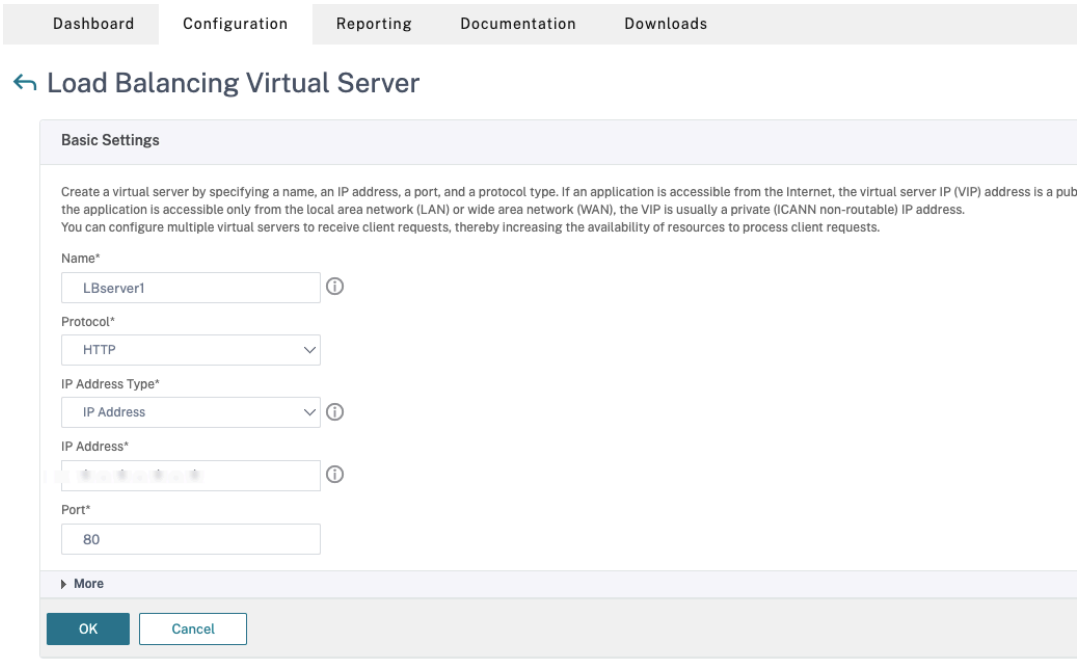
a) [**Action**] で、前の手順で作成したアクションを選択します。
b) [**Expression**] に、「HTTP.REQ.IS_VALID」を追加します。
c) [**OK**] をクリックします。

4. 負荷分散を設定します。STA サーバーごとに 1 つの負荷分散仮想サーバーを構成する必要があります。そうしない場合、セッションの起動が失敗します。

   詳しくは、「基本的な負荷分散の設定」を参照してください。

   a) 負荷分散仮想サーバーを作成します。

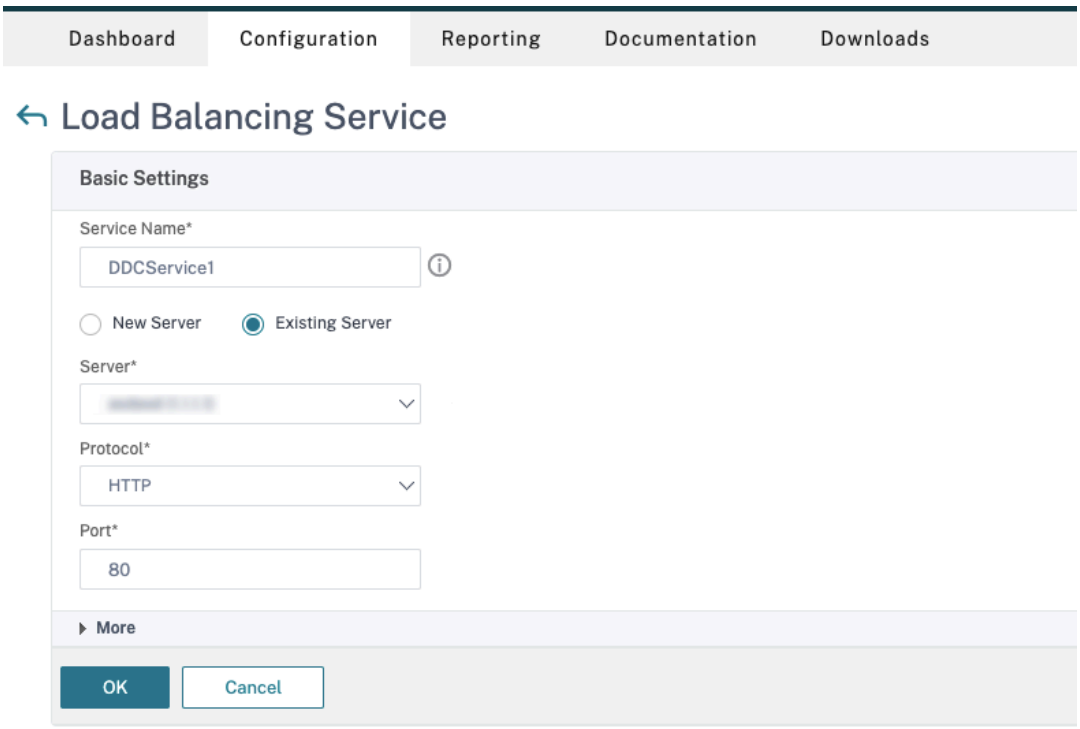
   - [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に移動します。
   - [**Virtual Servers**] ページで [**Add**] をクリックします。



   - [**Protocol**] で、[**HTTP**] を選択します。
   - 負荷分散仮想 IP アドレスを追加し、[**Port**] で [**80**] を選択します。
   - [**OK**] をクリックします。

   b) 負荷分散サービスを作成します。

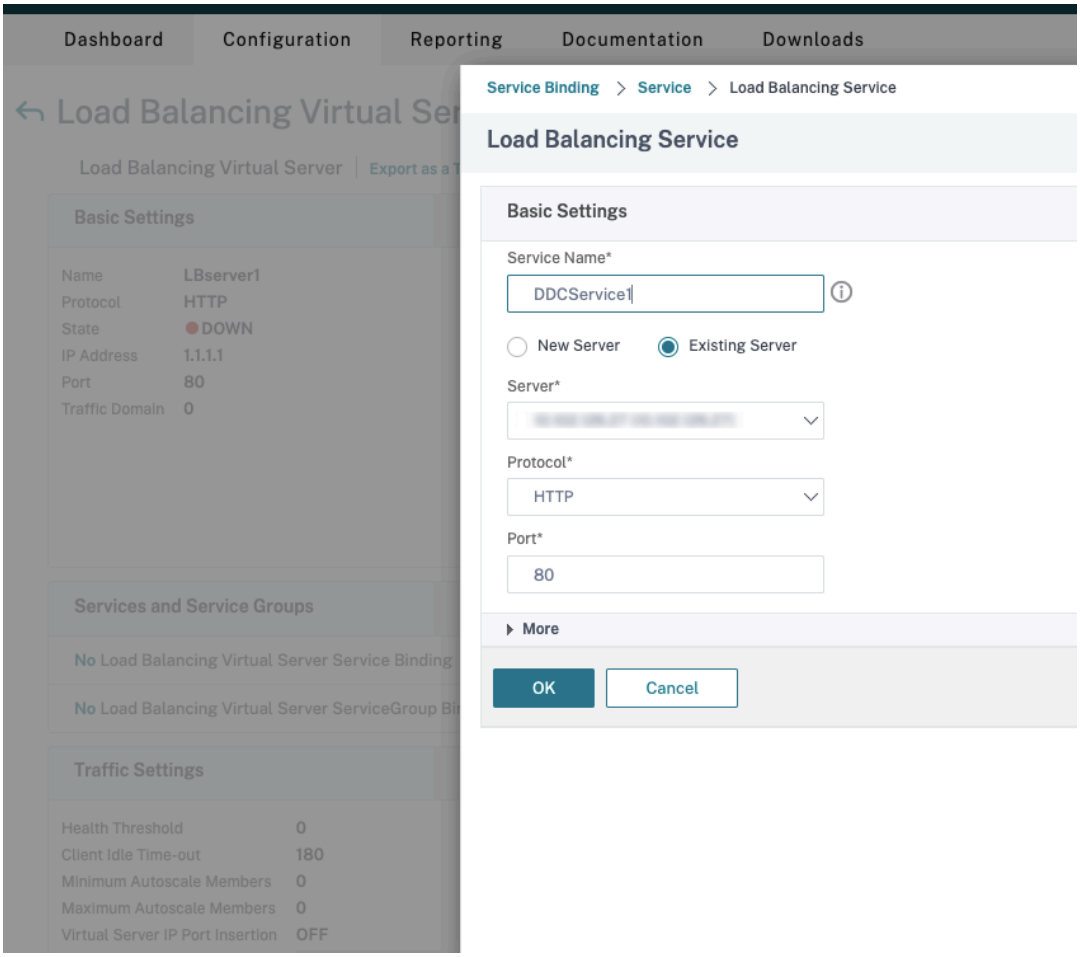
   - [**Traffic Management**] > [**Load Balancing**] > [**Services**] の順に移動します。



- [**Existing Server**] で、前の手順で作成した仮想サーバーを選択します。
- [**Protocol**] で [**HTTP**] を選択し、[**Port**] で [**80**] を選択します。
- [**OK**] をクリックし、[**Done**] をクリックします。

c) サービスを仮想サーバーにバインドします。

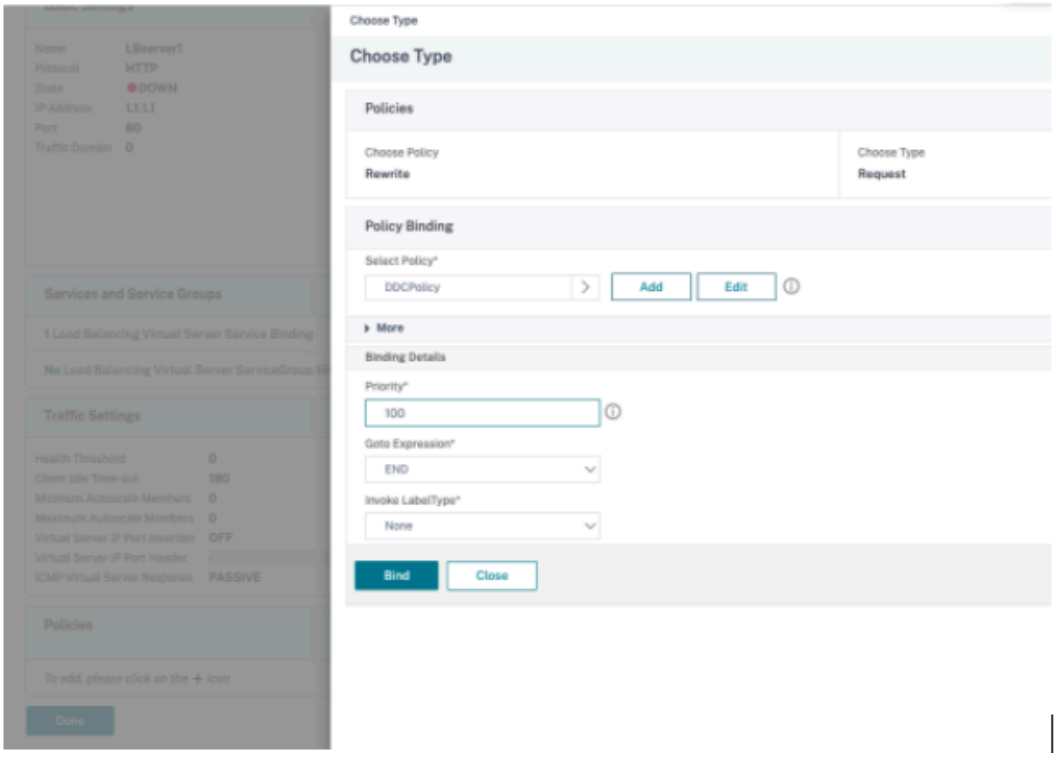
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Services and Service Groups**] の [**No Load Balancing Virtual Server Service Binding**] をクリックします。



- [**Service Binding**] で、前に作成したサービスを選択します。
- [バインド] をクリックします。

d) 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

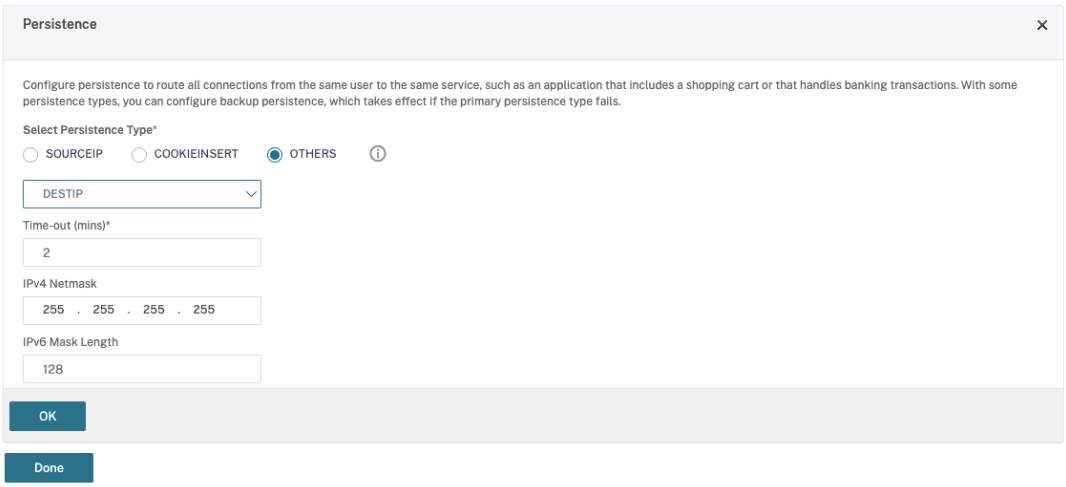
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で [**Policies**] をクリックし、[**Policies**] セクションで [**+**] をクリックします。



- [**Choose Policy**] で [**Rewrite**] を選択し、[**Choose Type**] で [**Request**] を選択します。
- [続行] をクリックします。
- [**Select Policy**] で、前に作成した書き換えポリシーを選択します。
- [バインド] をクリックします。
- [完了] をクリックします。

e) 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で、[**Persistence**] をクリックします。



- 永続性タイプを [**Others**] にします。

- 仮想サーバーによって選択されたサービスの IP アドレス（宛先 IP アドレス）に基づいて、永続セッションを作成するには、[**DESTIP**] を選択します。
- [**IPv4 Netmask**] で、DDC と同じネットワークマスクを追加します。
- [**OK**] をクリックします。

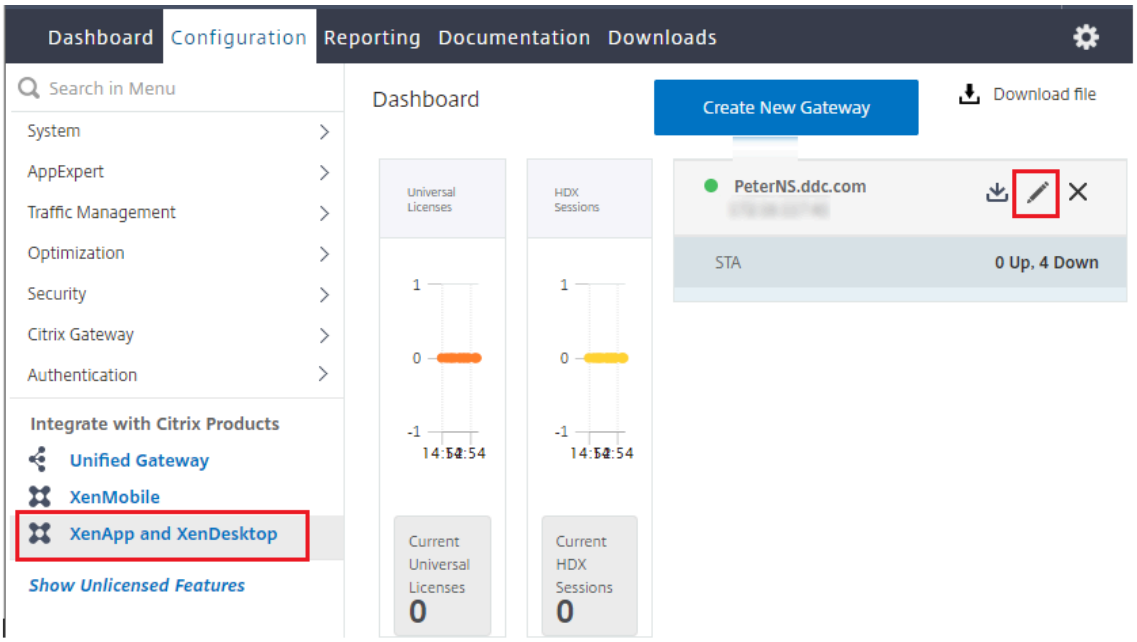
f) 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADC アプライアンスが既に **Citrix Virtual Desktops** により構成されている場合の構成の変更

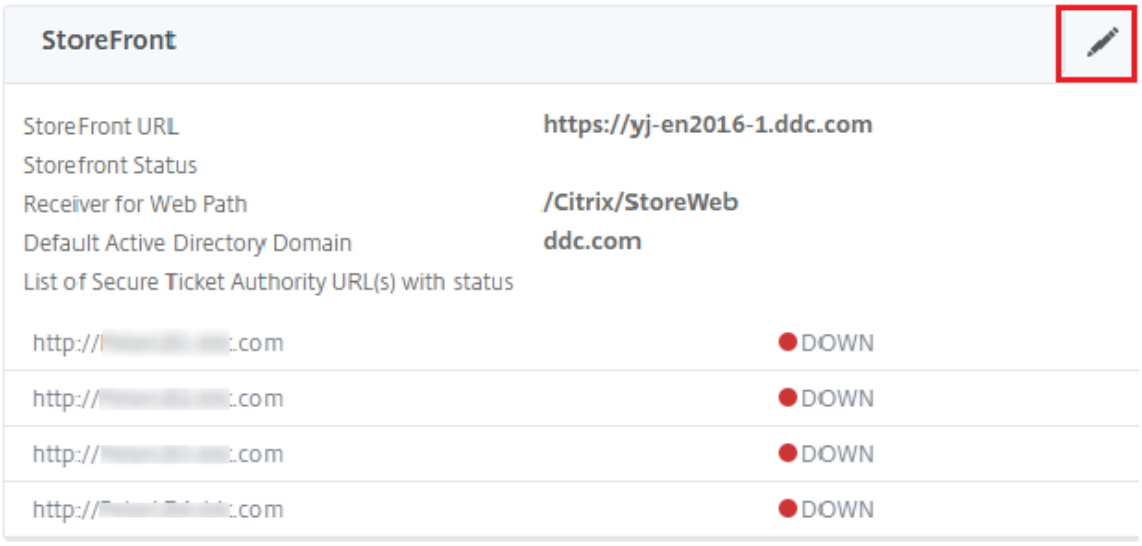
Citrix Virtual Desktops を使用して Citrix ADC アプライアンスを既に構成している場合、Secure XML 機能を使用するには、次の構成変更を行う必要があります。

- セッションを起動する前に、ゲートウェイの **Security Ticket Authority URL** を変更して、負荷分散仮想サーバーの FQDN（完全修飾ドメイン名）を使用します。
- `TrustRequestsSentToTheXmlServicePort`パラメーターが False に設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターは False に設定されています。ただし、顧客が Citrix Virtual Desktops 用に Citrix ADC を既に構成している場合は、`TrustRequestsSentToTheXmlServicePort`が True に設定されています。

1. Citrix ADC GUI で、[**Configuration**] > [**Integrate with Citrix Products**] の順に移動し、[**XenApp and XenDesktop**] をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

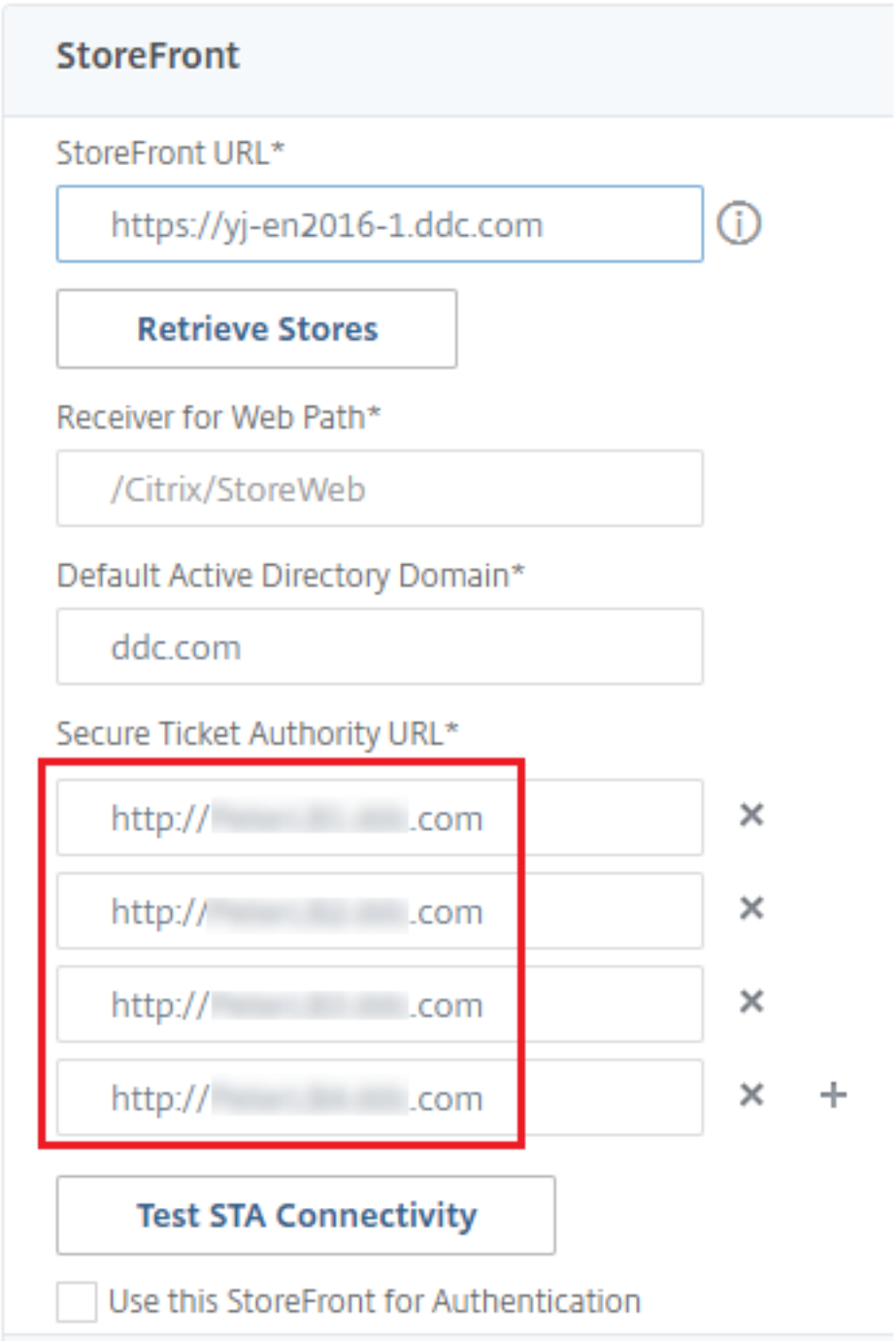


3. StoreFront ペインで、編集アイコンをクリックします。



4. [**Secure Ticket Authority URL**] を追加します。

   - Secure XML 機能が有効になっている場合、STA URL は負荷分散サービスの URL である必要があります。
   - Secure XML 機能が無効になっている場合、STA URL は STA の URL（DDC のアドレス）である必要があり、DDC の TrustRequestsSentToTheXmlServicePort パラメーターは True に設定されている必要があります。



接続リース

August 24, 2021

> 重要:
>
> ローカルホストキャッシュ（LHC）は、接続リースよりも望ましい XenApp および XenDesktop 高可用性ソリューションです。詳しくは、「ローカルホストキャッシュ」を参照してください。

- このリリースでは、XenApp と XenDesktop の新規インストールの間に、接続リース機能はデフォルトで無効になります。
- XenApp と XenDesktop 7.15 Long Term Service Release に続く最新のリリースでは、接続リース機能は提供されなくなる予定です。

サイトデータベースを常に使用可能状態にするために、Microsoft 社の高可用性ベストプラクティスに従って耐障害性の高い SQL Server 展開から開始することをお勧めします。ただし、ネットワークの問題および中断によって Delivery Controller がデータベースにアクセスできなくなり、その結果、ユーザーがアプリケーションやデスクトップに接続できなくなる場合があります。

SQL Server 高可用性ベストプラクティスを補完する接続リース機能を使用すると、サイトデータベースが使用不可の場合でも、ユーザーが直近で使用したアプリケーションやデスクトップに接続および再接続できるようになります。

通常、多くの公開リソースを使用できるユーザーでも、定期的に使用するのはその一部のみです。接続リース機能を有効にすると、通常時（データベースが使用可能なとき）に、最近使用されたアプリケーションやデスクトップのユーザー接続が各 Controller でキャッシュされます。

各 Controller 上でリースが生成され、それがサイトデータベースにアップロードされてほかの Controller と定期的に同期されます。各 Controller のキャッシュには、リースのほかにアプリケーション、デスクトップ、アイコン、ワーカーなどの情報が格納されます。リースとその関連情報は、各 Controller のローカルディスクに保存されます。データベースを使用できなくなると、Controller はリース接続モードになります。この場合、ユーザーが StoreFront から最近使用したアプリケーションやデスクトップへの接続を試みると、キャッシュされている操作が「再生」されます。

接続は、2 週間の「リース期間」をキャッシュされます。そのため、ユーザーが直前の 2 週間に起動したデスクトップとアプリケーションは、データベースが使用不可になった場合でも引き続き StoreFront 経由でアクセスできます。ただし、直前の 2 週間に起動しなかったデスクトップとアプリケーションは、データベースが使用不可になった場合にはアクセスできなくなります。たとえば、あるアプリケーションを最後に起動したのが 3 週間前である場合、そのアプリケーションのリース期限が切れているため、現時点でデータベースが使用不可になると起動できなくなります。長時間実行されているアプリケーションまたはデスクトップのアクティブセッションまたは切断セッションのリースは、期限切れと見なされないように延長されます。

デフォルトでは、接続リースはサイト全体に影響します。ただし、特定のユーザーのすべてのリースを取り消すことができます。これにより、Controller がリース接続モードのときに、そのユーザーはすべてのアプリケーションやデスクトップにアクセスできなくなります。そのほかのいくつかのレジストリ設定は Controller 単位で適用されます。

考慮事項と制限事項

接続リースを使用すると接続の回復性やユーザーの生産性を向上させることができますが、そのほかの機能のパフォーマンス、可用性、および操作に関連する注意事項があります。

接続リースは、サーバーでホストされるアプリケーションおよびデスクトップと静的な（割り当て済み）デスクトップでサポートされます。プール型の VDI デスクトップや、データベースが利用できなくなった時点でデスクトップが割り当てられていないユーザーはサポートされません。

リース接続モードの Controller では、以下の制限事項があります：

- 管理者は Studio、Director、または PowerShell コンソールを使用できません。
- 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。例：
  - Controller がリース接続モードになっていないときにユーザーがデバイス（NetScaler Gateway 経由で外部から接続しているデバイス）からセッションを起動し、Controller がリース接続モードになった後で LAN 上の別のデバイスから接続した場合、セッションがローミングされずに新しいセッションが作成されることがあります。
  - データベースが使用できなくなる直前にアプリケーションが起動した場合、セッションの再接続に失敗することがあります。この場合、新しいセッションとアプリケーションインスタンスが起動します。
- 静的な（割り当て済み）デスクトップでは、電源管理が行われません。Controller がリース接続モードになるときに電源がオフになった VDA は、管理者が手動で電源をオンにしない限り、データベース接続が回復するまで使用できません。
- セッションの事前起動とセッション残留が有効になっている場合、新しい事前起動セッションは開始されません。データベースが利用可能になるまでは、構成されたしきい値に従って事前起動セッションや残留セッションが自動終了することはありません。
- サイト内の負荷管理が影響を受ける可能性があります。サーバーベースの接続は直近に使用された VDA に割り当てられます。負荷評価基準（特にセッション数規則）を超過する可能性があります。
- SQL Server Management Studio と使ってデータベースをオフラインにすると、Controller がリース接続モードになりません。以下の Transact-SQL 文を使用してください：
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> 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。

構成と展開

接続リース機能を使用するには、環境を以下のように構成する必要があります:

- VDA は Version 7.6 以降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 以降である必要があります。
- サイトデータベースのサイズ要件が大きくなります。
- 各 Controller には、キャッシュされるリースファイル用の追加のディスクスペースが必要です。

接続リース機能の有効/無効は、PowerShell SDK、または Windows のレジストリで切り替えることができます。PowerShell SDK を使用する場合は、現在のリースを削除することもできます。接続リース機能を制御する PowerShell コマンドレットは以下のとおりです。詳しくは、コマンドレットのヘルプを参照してください。

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false - 接続リース機能のオン/オフを切り替えます。デフォルト値: $true
- Get-BrokerServiceAddedCapability - ローカルの Controller に「ConnectionLeasing」を出力します。
- 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** と仮想ループバック

August 24, 2021

注: これらの機能は、サポートされている Windows サーバーマシンでのみ有効です。Windows デスクトップ OS マシンでは使用できません。

Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

CRM（Customer Relationship Management）や CTI（Computer Telephony Integration）などの特定のアプリケーションでは、アドレス割り当て、ライセンス付与、識別、またはそのほかの目的で IP アドレスが使用されるため、セッションに固有の IP アドレスまたはループバックアドレスが必要です。また、一部のアプリケーションでは

静的なポートにバインドされるため、マルチユーザー環境でそのアプリケーションの追加インスタンスを起動しようとすると、そのポートが使用済みなので起動に失敗します。これらのアプリケーションが XenApp 環境で正しく動作するためには、クライアントデバイスごとに異なる IP アドレスが使用される必要があります。

仮想 IP と仮想ループバックは、それぞれ独立した機能です。これらの機能のいずれかまたは両方を使用できます。

使用する機能に応じて、管理者は以下の操作を行います。

- Microsoft 社の仮想 IP 機能を使用するには、Windows サーバー上で仮想 IP を有効にして構成します。(Citrix ポリシーの設定は必要ありません。)
- Citrix の仮想ループバック機能を使用するには、Citrix ポリシーで 2 つの設定項目を構成します。

仮想 **IP**

Windows サーバー上で仮想 IP 機能を有効にすると、セッション内で動作する各アプリケーションで固有のアドレスが使用されるように構成できます。ユーザーは、これらのアプリケーションを、ほかの公開アプリケーションと同じように使用することができます。以下のいずれかの動作をするプロセスでは、仮想 IP アドレスを設定します。

- ハードコードされた（固定された）TCP ポート番号を使用する。
- Windows ソケットを使用し、固有の IP アドレスまたは固定された TCP ポート番号を使用する。

アプリケーションで仮想 IP アドレスが必要かどうかを判断するには、次の手順に従います。

1. Microsoft 社の Web サイトから、TCPView ツールを入手します。このツールを使用すると、特定の IP アドレスおよびポートを使用しているすべてのアプリケーションを一覧表示できます。
2. TCPView の［Options］メニューで、［Resolve Addresses］を無効にします。これにより、一覧にホスト名ではなくアドレスが表示されるようになります。
3. 対象となるアプリケーションを起動して、使用されている IP アドレスとポート、およびそれらのポートを開いているプロセスの名前を TCPView で確認します。
4. サーバーの IP アドレス 0.0.0.0 または 127.0.0.1 を使用するプロセスを構成します。
5. そのアプリケーションの追加インスタンスを起動して、別のポート上で同じ IP アドレスが使用されないことを確認します。

Microsoft リモートデスクトップ（**RD**）の **IP** 仮想化のしくみ

- 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。このようにしてアプリケーションに渡された IP アドレスは、後続のソケットコール（bind や connect など）で使用されます。

アプリケーションでは、アドレス 0.0.0.0 で、リスナー用のポートのバインドが必要になる場合があります。このようなアプリケーションで静的なポート番号が使用されると、競合が発生するため、複数のインスタンスを起動できなくなります。仮想 IP アドレス機能では、0.0.0.0 へのファンクションコールが特定の仮想 IP アドレスに変換されます。これにより、セッションごとに異なるアドレス上のポートが使用されるため、同じポート番号を使用する複数のアプリケーションを実行できるようになります。このファンクションコールは、仮想 IP アドレス機能が有効な ICA セッションでのみ変換されます。たとえば、すべてのインターフェイス（0.0.0.0）と特定のポート（9000 など）にバインドするアプリケーションの 2 つのインスタンスが、それぞれ異なるセッションで実行される場合、VIPAddress1:9000 と VIPAddress2:9000 にバインドされるため、競合が起きません。

仮想ループバック

Citrix ポリシーで仮想 IP ループバック機能を有効にすると、各セッションで通信に独自のループバックアドレスが使用されるようになります。アプリケーションが Winsock 呼び出し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 を足したものです）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 Server 2008 R2 と Windows Server 2012 R2 でのみサポートされます。
- 仮想 IP アドレスと仮想ループバックの両方の機能を有効にする場合にのみ、優先ループバック機能を使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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\S
- 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、データ：プロセスの一覧 >

Delivery Controller

August 24, 2021

Delivery Controller は、ユーザーアクセスの管理や接続の仲介と最適化を行うためのサーバー側のコンポーネントです。また、Controller は、デスクトップおよびサーバーイメージを作成する Machine Creation Service も提供します。

サイトには、1 つ以上の Controller が必要です。1 つめの Controller のインストール後、サイトを作成するとき、または後日、さらに Controller を追加できます。サイトに複数の Controller があると、以下の 2 つの利点がもたらされます。

- 冗長性：ベストプラクティスとしては、実稼働サイトでは、常時 2 つ以上の Controller をそれぞれ異なる物理サーバー上に配置することをお勧めします。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加します。Controller を追加すると、より多くのユーザーやより多くのアプリケーションやデスクトップ要求を処理できるようになり、制御処理全体を向上させることができます。

各 Controller は、サイトデータベースと直接通信を行います。複数のゾーンを持つサイトでは、各ゾーンに存在する Controller が、プライマリゾーンにあるサイトデータベースと通信します。

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

Controller への VDA の登録方法

VDA を使用するには、そのサイトの Delivery Controller に登録（接続を確立）する必要があります。VDA の登録について詳しくは、「Delivery Controller への VDA の登録」を参照してください。

(XenApp および XenDesktop 7.x リリース以前の文書では、この文書に VDA の登録についての情報が含まれていました。この情報は増強され、現在は上記に関連した文書に含まれています)。

Controller の追加、削除、または移動

Controller の追加、削除、移動を行うには、データベースの記事に記載されているサーバーの役割とデータベースの役割の権限が必要です。

> 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、PowerShell コマンドレット **get-configdbconnection** 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 の追加

Controller は、サイトの作成時、または後日、追加できます。以前のバージョンがインストールされた Controller をこのバージョンのサイトに追加することはできません。

1. サポートされているオペレーティングシステムが稼動しているサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なコアコンポーネントをすべてインストールします。インストールウィザードを完了します。
2. サイトをまだ作成していない場合は、Studio を起動します。サイトの作成を促すメッセージが表示されます。サイトの作成ウィザードの［データベース］ページで［選択］ボタンをクリックし、追加する Controller がインストールされているサーバーのアドレスを追加します。重要：データベースの初期化スクリプトを生成する計画がある場合は、スクリプトを生成する前に、Controller を追加してください。
3. サイトの作成がすでに済んでいる場合は、Studio で、追加の Controller をインストールしたサーバーを指定します。［展開の変更］をクリックし、サイトのアドレスを入力します。

Controller の削除

Controller を削除すると、Citrix ソフトウェアやそのほかのコンポーネントはアンインストールされませんが、データベースからその Controller が削除されます。このため、この Controller では接続の仲介やそのほかのタスクを実行できなくなります。削除した Controller を、後で元のサイトや別のサイトに追加することができます。サイトには最低 1 つの Controller が必要なため、Studio の一覧に表示される最後の Controller を削除することはできません。

サイトから Controller 削除しても、データベースサーバーへの Controller ログオンは削除されません。これは、同じマシン上のほかの製品のサービスで使用されるログオンが削除されるのを防ぐためです。ログオンが必要ない場合には、手動で削除する必要があります。ログオンの削除には、securityadmin サーバーロール権限が必要です。

> 重要：
>
> サイトから Controller を削除するまでは、Active Directory でその Controller を削除しないでください。

1. Controller が動作しており、1 時間以内にその Controller が Studio にロードされることを確認してください。削除する Controller が Studio にロードされたら、メッセージに従って Controller をシャットダウンしてください。
2. Studio のナビゲーションペインで ［構成］**>**［**Controller**］の順に選択し、削除する Controller を選択します。
3. ［操作］ペインで ［**Controller** の削除］を選択します。適切なデータベースロールや権限がない場合は、Controller を削除するためのスクリプトを生成できます。そのスクリプトの実行をデータベース管理者に依頼してください。
4. データベースサーバーから Controller のマシンアカウントを削除しなければならない場合があります。これを行う前に、ほかのサービスがそのアカウントを使用していないことを確認してください。

Studio を使って Controller を削除した後、実行中のタスクを適切に完了させるためにその Controller へのトラフィックがしばらく残ることがあります。Controller を即座に削除するには、Controller がインストールされている

サーバーをシャットダウンするか、Active Directory からそのサーバーを削除することをお勧めします。その後で、サイト内のほかの Controller を再起動します。これにより、削除された Controller との通信が行われなくなります。

Controller の別のゾーンへの移動

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。VDA 登録やほかの操作に対するこの操作の影響については、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］ペインで ［移動］を選択します。
3. Controller の移動先ゾーンを指定します。

Controller の別のサイトへの移動

このソフトウェアの以前のバージョンで作成されたサイトには、Controller を移動できません。

1. Controller が現在配置されているサイト（移動元サイト）で Studio を開き、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］ペインで［**Controller** の削除］を選択します。データベースに対する適切な役割や権限がない場合は、Controller を削除するためのスクリプトを生成できます。そのスクリプトの実行をデータベース管理者など該当する権限を持つユーザーに依頼してください。サイトには最低 1 つの Controller が必要なため、Studio の一覧に表示される最後の Controller を削除することはできません。
3. 移動する Controller で Studio を開き、確認メッセージに応じてサービスをリセットします。さらに、［既存のサイトへ参加］を選択して、移動先サイトのアドレスを入力します。

VDA から別のサイトへの移動

VDA が Provisioning Services を使ってプロビジョニングされた場合、または既存のイメージの場合、アップグレード時、またはテストサイトで作成された VDA イメージを実務環境サイトに移動させる場合に、VDA をほかのサイトに移動（サイト 1 からサイト 2 へ）できます。MCS は ListOfDDCs の変更をサポートせず VDA は Controller への登録をチェックするため、Machine Creation Services（MCS）を使ってプロビジョニングされた VDA をあるサイトから別のサイトには移動できません。MCS を使ってプロビジョニングされる VDA は、作成されたサイトに割り当てられた ListOfDDCs をチェックします。

VDA をほかのサイトに移動するにはインストーラーを使用するか、Citrix ポリシーを使用します。

インストーラー：インストーラーを実行して、サイト 2 の Controller の FQDN（DNS エントリ）を指定してこの Controller を追加します。重要： Controller のポリシー設定を使用しない場合にのみ、インストーラーで Controller を指定します。

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 の完全修飾ドメイン名（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。

VDA 登録

August 24, 2021

はじめに

VDA を使用するには、そのサイトの 1 つまたは複数の Controller または Cloud Connector に登録（接続を確立）する必要があります。（オンプレミスの XenApp および XenDesktop 展開環境では、VDA は Controller に登録されます。XenApp および XenDesktop Service 展開環境では、VDA は Cloud Connector に登録されます。）VDA は ListofDDCs と呼ばれる一覧をチェックして、Controller またはコネクタを見つけます。VDA の ListOfDDCs には、その VDA をサイトの Controller または Cloud Connector にポイントする DNS エントリが含まれています。負荷分散のため、VDA は一覧のすべての Controller または Cloud Connector で接続を自動的に分散させます。

VDA 登録が重要な理由

- セキュリティの面で見ると、登録では Controller または Cloud Connector と VDA 間の接続を確立するため、デリケートな操作と言えます。このように注意が必要な操作では、不完全なものが 1 つでもあればその接続を拒否する必要があります。実際には、2 つの個別の通信チャネル（VDA から Controller または Cloud Connector、Controller または Cloud Connector から VDA）を確立することになります。接続では Kerberos が使用されるため、時刻の同期およびドメインへの参加に関する問題は見過ごせないものになります。Kerberos ではサービスプリンシパル名（SPN）が使用されるため、負荷分散された IP やホスト名は使用できません。
- Controller または Cloud Connector の追加および削除は、VDA に正確かつ最新の Controller または Cloud Connector の情報が設定されていないと、未登録の Controller または Cloud Connector により仲介されたセッションの起動が VDA により拒否される場合があります。また、無効なエントリにより、仮想デスクトップシステムソフトウェアの起動に遅延が生じることがあります。VDA では、信頼されていない不明な Controller または Cloud Connector からの接続は受け入れられません。

ListOfDDCs に加えて、ListOfSIDs（セキュリティ ID）により、ListOfDDCs に記載されているどのマシンを信頼するかが指定されます。ListOfSIDs は、Active Directory での負荷を軽減したり、改ざんされた DNS サーバーからのセキュリティ上の脅威を防いだりするために使用できます。詳しくは、「ListOfSIDs」を参照してください。

ListOfDDCs に複数の Controller または Cloud Connector が指定されている場合、VDA はランダムな順序で接続を試行します。オンプレミスの展開では、ListOfDDCs には Controller のグループを含めることもできます。VDA は、これらのグループ内の各 Controller への接続を試行し、その後で ListOfDDCs のほかのエントリを試行します。

XenApp と XenDesktop では、VDA のインストール中に構成済みの Controller または Cloud Connector に対する接続が自動でテストされます。Controller または Cloud Connector に接続できない場合は、エラーが表示されます。Controller または Cloud Connector に接続できないことを示す警告を無視した場合（または VDA のインストール中にアドレスを指定しなかった場合）は、メッセージが表示されます。

Controller または **Cloud Connector** のアドレスの構成方法

VDA の初めての登録時（初回登録と呼びます）に、管理者は使用する構成方法を選択します。初回登録中に、VDA 上に永続キャッシュが作成されます。以降の登録では、構成の変更が検出されない限り、VDA はこのローカルキャッシュから Controller または Cloud Connector のリストを取得します。

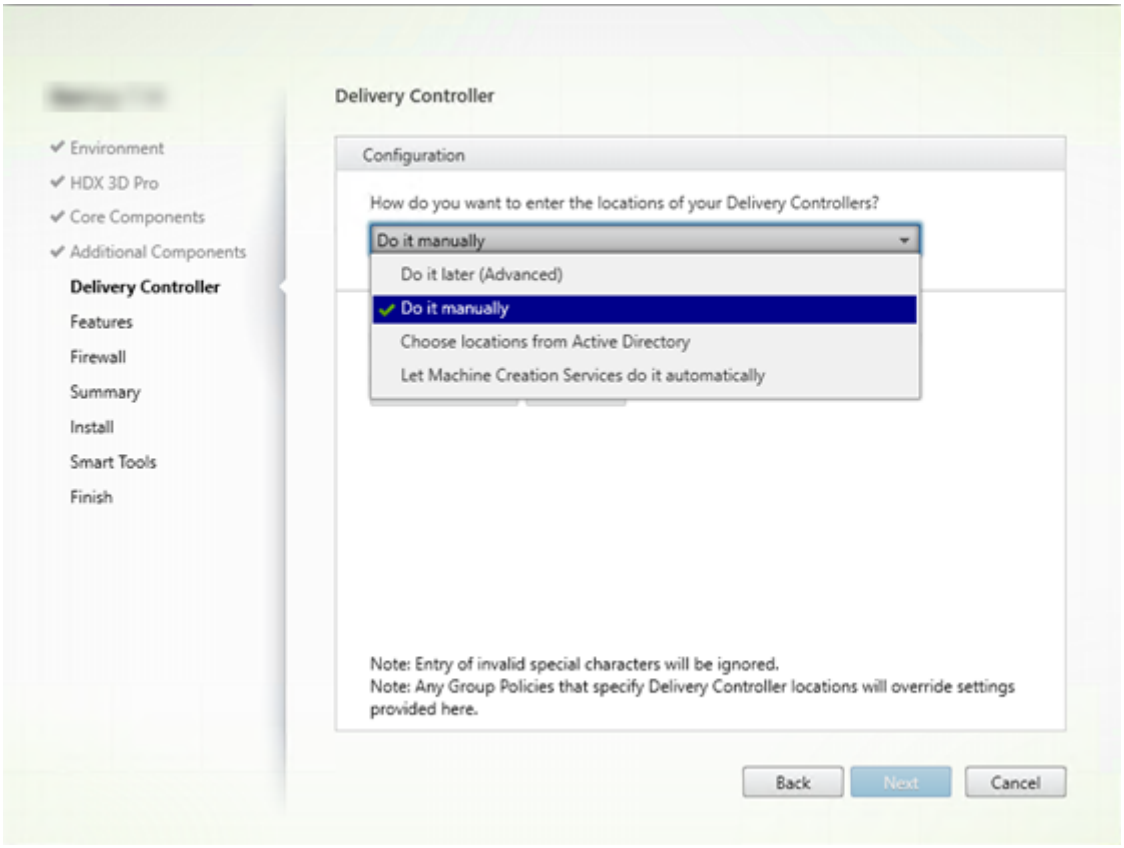
以降の登録時にこのリストを取得する一番簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳しくは、「自動更新」を参照してください。

VDA で Controller または Cloud Connector のアドレスを構成する方法は複数存在します。

- ポリシーベース（LGPO または GPO）
- レジストリベース（手動、GPP、VDA のインストール中に指定）
- Active Directory の OU ベース（旧 OU 検出）
- MCS ベース（personality.ini）

VDA をインストールするときに初回登録の方法を指定します（自動更新を無効にすると、初回以降の登録でも VDA のインストール時に選択した方法が使用されます）。

次の画像に、VDA インストールウィザードの ［**Delivery Controller**］ページを示します。



ポリシーベース（**LGPO** または **GPO**）

VDA の初回登録では GPO を使用することを Citrix ではお勧めします。この方法が最優先です（以前は自動更新が最優先となっていましたが、自動更新は初回登録後にのみ使用します）。ポリシーベースの登録には、構成にグループポリシーを使用できるという集中化のメリットがあります。

この方法を指定するには、次の手順の両方を実行します。

- VDA インストールウィザードの［**Delivery Controller**］ページで、［あとで実行（上級）］を選択します。VDA のインストール中に Controller のアドレスの指定は行いませんが、ウィザードからこれらのアドレスを指定するように複数回促されます（これは、VDA の登録が非常に重要なためです）。
- `Virtual Delivery Agent Settings > Controllers`設定で、Citrix ポリシーを使用してポリシーベースの VDA 登録を有効化または無効化します（セキュリティが最優先の場合、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します）。

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に格納されています。

レジストリベース

この方法を指定するには、次の手順のいずれかを実行します。

- VDA インストールウィザードの［**Delivery Controller**］ページで、［手動で指定する］を選択します。次に、インストール済みの Controller の完全修飾ドメイン名を入力し、［追加］をクリックします。追加の Controller をインストールした場合は、アドレスも追加します。
- コマンドラインでの VDA のインストールの場合は、/controllers オプションを使用してインストール済みの Controller または Cloud Connector の FQDN を指定します。

この情報は、通常レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`のレジストリ値 ListOfDDCs に格納されています。

また、このレジストリキーを手動で構成するか、グループポリシーの基本設定（GPP）を使用することもできます。この方法は、Controller または Cloud Connector 別に条件付きの処理を行う（例: コンピューター名が XDW-001-から始まる場合は XDC-001 を使用する）場合などは、ポリシーベースの方法よりも適しています。

サイトのすべての Controller または Cloud Connector の完全修飾ドメイン名の一覧が設定されている ListOfDDCs レジストリキーを更新します。（このキーは Active Directory サイト組織単位に相当します。）

`HKEY_LOCAL_MACHINE\Software\Citrix\\VirtualDesktopAgent\ListOfDDCs`（`REG_SZ`）

レジストリ`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`に ListOfDDCs と FarmGUID キーの両方がある場合は、ListOfDDCs が Controller または Cloud Connector の検出に使用されます。FarmGUID は、VDA のインストール時にサイト組織単位を指定した場合に作成されます（このキーは古い展開環境で使用する場合があります）。

オプションで、ListOfSIDs レジストリキーを更新します（詳しくは「ListOfSID」を参照してください）:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`（`REG_SZ`）

> 注意事項:
>
> Citrix ポリシーによりポリシーベースの VDA 登録も有効化している場合は、ポリシーベースの方法の方が優先度が高いため、VDA のインストール時に指定した設定がポリシーベースの設定で上書きされます。

Active Directory の OU ベース（旧）

この方法は主として後方互換性のためにサポートされているものであり、推奨されていません。現在もこの方法を使用している場合は、別の方法に変えることを Citrix ではお勧めします。

この方法を指定するには、次の手順の両方を実行します。

- VDA インストールウィザードの［**Delivery Controller**］ページで、［**Active Directory** から場所を選択する］を選択します。
- `Set-ADControllerDiscovery.ps1`スクリプトを使用します（各 Controller 上にあります）。また、各 VDA 上の FarmGuid レジストリを、適切な組織単位を指すように構成します。この設定はグループポリシーを使用して行うことができます。

詳しくは、「Active Directory の組織単位ベースの検出」を参照してください。

MCS ベース

VM のプロビジョニングに MCS のみを使用する予定の場合は、Controller または Cloud Connector のリストを設定するように MCS を構成することができます。この機能は自動更新と互換性があります。MCS は、初回プロビジョニング時（マシンカタログの作成時）に Controller または Cloud Connector のリストを`Personality.ini`ファイルに書き込みます。自動更新により、このリストが最新に保たれます。

大規模な環境では、この方法の使用は推奨されていません。この方法は次の場合に使用することをお勧めします。

- 環境が小規模である
- サイト間で VDA を移動させない
- VM のプロビジョニングに MCS のみを使用する
- グループポリシーを使用しない

この方法を指定するには次の手順を実行します。

- VDA インストールウィザードの［**Delivery Controller**］ページで、［**Machine Creation Services** で指定する］を選択します。

推奨事項

ベストプラクティス：

- 初回登録にはグループポリシーによる登録方法を使用します。
- 自動更新（デフォルトで有効化されています）を使用して Controller のリストを最新に保ちます。
- マルチゾーン展開（Controller または Cloud Connector が 2 つ以上）では、初回構成にグループポリシーを使用します。各ゾーンにローカルの Controller または Cloud Connector に対して VDA をポイントします。自動更新を使用して、VDA を最新の状態に保ちます。自動更新により、サテライトゾーンにある VDA の ListOfDDCs が自動で最適化されます。

自動更新

自動更新（XenApp および XenDesktop 7.6 で導入）は、デフォルトで有効化されています。これは、VDA 登録を最新の状態に保つ最も効率的な方法です。初回登録では自動更新は使用しませんが、自動更新ソフトウェアにより、初回登録を行うときに ListOfDDCs がダウンロードされ、永続キャッシュに格納されます。これは VDA ごとに行われます（このキャッシュには、マシンポリシーの情報も格納されます。これにより、再起動後もポリシー設定が保持されます）。

MCS または PVS を使用してマシンをプロビジョニングする場合、自動更新がサポートされます。PVS サーバーのキャッシュは除外されます（自動更新キャッシュ用の永続的なストレージがないためです）。

この方法を指定するには次の手順を実行します。

- 次の設定が含まれる Citrix ポリシーで自動更新を有効または無効にします：`Virtual Delivery Agent Settings > Enable auto update of Controllers`。この設定項目は、デフォルトで有効になっています。

自動更新の仕組みは次のとおりです。

- VDA の再登録の度（マシンの再起動後など）にキャッシュが更新されます。また、各 Controller または Cloud Connector も 90 分ごとにサイトのデータベースをチェックします。最後のチェック以降に Controller または Cloud Connector が追加または削除されていた場合、または VDA 登録に影響するポリシー変更が行われていた場合、Controller または Cloud Connector から Controller または Cloud Connector に登録済みの VDA に最新のリストが送信され、キャッシュが更新されます。VDA は、最近キャッシュ化されたリストに含まれているすべての Controller または Cloud Connector からの接続を受け入れます。
- VDA が受信したリストに登録先の Controller または Cloud Connector が含まれていない場合（つまり、その Controller または Cloud Connector がサイトから削除された場合）、ListOfDDCs のいずれかの Controller または Cloud Connector に VDA が再登録されます。

例:

- 環境内に 3 つの Controller A、B、C があります。VDA は（VDA のインストール時に指定した）Controller B に登録されています。
- その後、サイトに 2 つの Controller（D および E）を追加します。90 分以内に、更新されたリストが VDA に送信されます。これにより、VDA は Controller A、B、C、D、E からの接続を受け入れるようになります（VDA を再起動するまでは、すべての Controller 間で負荷分散は行われません）。
- さらにそのあとで、Controller B を別のサイトに移動します。前回のチェック以降にサイトの Controller に変更があったため、元のサイトの VDA は 90 分以内に更新済みのリストを受信します。初めに Controller B（リストから削除されています）に登録されていた VDA は、現在のリストに含まれる Controller（A、C、D、E）のいずれかに再登録されます。

マルチゾーン展開のサテライトゾーンでは、まず自動更新によりすべてのローカル Controller がキャッシュ化されます。プライマリゾーンの Controller はすべて、バックアップグループにキャッシュ化されます。サテライトゾーンのローカル Controller を利用できない場合、プライマリゾーンの Controller への登録が試みられます。

以下の例に示すように、キャッシュファイルにはホスト名およびセキュリティ ID のリスト（ListOfSID）が含まれています。VDA は SID を照会しないため、Active Directory の負荷が抑えられます。

```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      - <d2p1:ArrayOfstring>
            <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
            <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
        </d2p1:ArrayOfstring>
    </_x003C_GroupsOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
    </_x003C_ListOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
        <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
        <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
    </_x003C_ListOfSids_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```

このキャッシュファイルは、WMI 呼び出しを使用することで取得できます。ただし、このファイルは SYSTEM アカウントのみが読み取り可能な場所に格納されています。この情報は説明のみを目的として紹介しています。このファイルは変更しないでください。このファイルまたはフォルダーを変更すると、構成はサポート対象外となります。


```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesk
" -Property "PersistentDataLocation"
```

セキュリティ上の理由で（Active Directory の負荷の抑制とは異なる理由で）ListOfSIDs を手動で構成する必要がある場合、自動更新は使用できません。詳しくは、「ListOfSIDs」を参照してください。

自動更新の優先度の例外

通常、自動更新はすべての VDA 登録方法の中で最も優先度が高くなっており、ほかの方法の設定を上書きしますが、例外も存在します。キャッシュの`NonAutoListOfDDCs`要素により、初回の VDA 構成方法が指定されます。自動更新ではこの情報を監視しています。初回登録の方法が変更されると、登録プロセスでは自動更新が省略され、優先度が次に高く構成されている方法が使用されます。これは、（障害復旧時など）VDA を別のサイトに移動する場合に役立ちます。

構成に関する考慮事項

Controller または **Cloud Connector** のアドレス

Controller または Cloud Connector の指定に使用する方法にかかわらず、Citrix では FQDN アドレスを使用することをお勧めします。IP アドレスは DNS レコードよりも侵害されやすいため、信頼性の高い構成とは言えません。ListOfSIDs を手動で入力する場合は、ListOfDDCs の IP を使用できます。ただし、この場合でも FQDN が推奨されています。

負荷分散

前述のとおり、VDA は ListOfDDCs に含まれるすべての Controller または Cloud Connector で接続を自動的に分散させます。フェールオーバーおよび負荷分散機能は、Citrix Brokering Protocol（CBP）に組み込まれています。構成内で複数の Controller または Cloud Connector を指定する場合、登録では必要に応じてこれらの Controller または Cloud Connector 間で自動的にフェールオーバーが行われます。自動更新を使用すると、すべての VDA で自動フェールオーバーが自動的に行われます。

セキュリティ上の理由から、Citrix ADC などのネットワークロードバランサーは使用できません。VDA 登録では Kerberos 相互認証を使用しており、クライアント（VDA）はその身元をサービス（Controller）に対して証明する必要があります。また、Controller または Cloud Connector はその身元を VDA に対して証明する必要があります。つまり、VDA と Controller または Cloud Connector は、サーバーであるのと同時にクライアントとしても動作するということです。本記事の初めに述べたように、通信チャネルには、VDA から Controller/Cloud Connector と Controller/Cloud Connector から VDA の 2 つが存在します。

このプロセスのコンポーネントはサービスプリンシパル名（SPN）と呼ばれ、Active Directory コンピューターオブジェクトにプロパティとして格納されます。VDA は、Controller または Cloud Connector に接続する場合、通信相手が「誰」かを指定する必要があります。このアドレスが SPN です。負荷分散 IP を使用する場合、Kerberos 相互認証では、この IP が目的の Controller または Cloud Connector に属していないことが適切に認識されます。

詳しくは、次のトピックを参照してください:

- Kerberos の概要: https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/
- Kerberos を使用した相互認証: https://docs.microsoft.com/en-us/windows/win32/ad/mutual-authentication-using-kerberos?redirectedfrom=MSDN

CNAME から自動更新への移行

自動更新機能は、バージョン 7.x 以前の XenApp および XenDesktop の CNAME（DNS エイリアス）機能に代わるものです。XenApp および XenDesktop 7 以降では、CNAME 機能は無効になっています。CNAME の代わりに自動更新を使用してください（CNAME を使用する必要がある場合は、CTX137960を参照してください。DNS エイリアスの動作の一貫性を保つため、自動更新と CNAME の両方を同時に使用しないでください）。

Controller/Cloud Connector グループ

Controller と Cloud Connector はグループで処理することをお勧めします。グループ化すると、一方のグループが優先され、すべての Controller または Cloud Connector で障害が発生した場合、もう一方のグループがフェールオーバーに使用されます。Controller または Cloud Connector はリストからランダムに選択されるものであるため、グループ化すると優先的な使用を指定しやすくなります。

Controller または Cloud Connector のグループを指定するにはかっこを使用します。たとえば Controller が 4 つ（主に使用するものが 2 つとバックアップ用が 2 つ）ある場合、次のようにグループ化します。

(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)。

この例では、最初のグループの Controller（001 と 002）が初めに処理されます。両方で障害が発生した場合、2 番目のグループの Controller（003 と 004）が処理されます。

ListOfSIDs

登録時に VDA が通信可能な Controller をまとめたものが ListOfDDCs です。VDA はどの Controller が信頼可能であるかも把握する必要があります。VDA は、ListOfDDCs に含まれている Controller を自動的に信頼するわけではありません。ListOfSIDs（セキュリティ ID）により、信頼可能な Controller が指定されます。VDA が登録を試みるのは、信頼されている Controller だけです。

ほとんどの環境では、ListOfSIDs は ListOfDDCs から自動で作成されます。CDF トレースを使用して ListOfSIDs を読み取ることができます。

一般には、ListOfSIDs を手動で変更する必要はありません。ただし、いくつかの例外があります。最初の 2 つの例外は、新しいテクノロジーが使用可能になったため有効ではなくなりました。

- **Controller** の役割の分離: XenApp および XenDesktop 7.7 でゾーンが導入される前は、登録に Controller のサブセットのみを使用する場合 ListOfSIDs を手動で構成していました。たとえば、XDC-001 と XDC-002

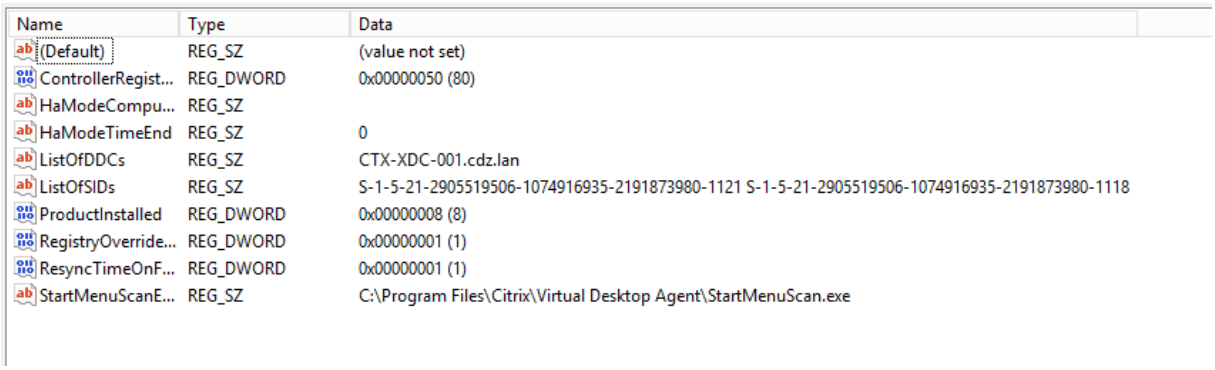
を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、ListOfSIDs にはすべての Controller を指定し、ListOfDDCs には XDC-003 と XDC-004 を指定していました。これは一般的に推奨される構成ではないため、新しい環境では使用されていません。代わりにゾーンが使用されています。

- **Active Directory** の負荷の削減： XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、ドメインコントローラーに対する負荷を抑えるために ListOfSIDs を使用していました。ListOfSIDs を事前に指定しておくことで、DNS 名から SID への解決を省略できることがあります。しかし、自動更新機能では永続キャッシュに SID が含まれるようになったため、この作業を行う必要はなくなりました。自動更新機能は有効にしておくことを Citrix ではお勧めします。
- セキュリティ： 高度なセキュリティで保護された環境では、侵害された DNS サーバーからのセキュリティ上の脅威を防ぐために、信頼されている Controller の SID を手動で構成していました。ただし、この構成を行うには、自動更新機能を無効にする必要があります。無効にしない場合、永続キャッシュの構成が使用されます。

このため、特別な理由がない限り ListOfSIDs は変更しないでください。

ListOfSIDs を変更する必要がある場合は、HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent の下に ListOfSIDs という名前のレジストリキー（REG_SZ）を作成します。値には、信頼できる SID の一覧を指定します。SID が複数ある場合はスペースで区切って指定します。

次の例では、1 つの Controller を VDA の登録に使用しますが（ListOfDDCs）、2 つの Controller は仲介に使用します（ListOfSIDs）。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

VDA 登録中の Controller の検索

VDA が登録しようとすると、Broker Agent は最初にローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できるようにします。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックトップダウンクエリを開始することがあります。このクエリは、すべてのドメインを検索し、頻繁に繰り返します。Controller のアドレスが無効である場合（たとえば、管理者が VDA のインストール時に誤った FQDN を入力した場合）、そのクエリのアクティビティにより、ドメインコントローラーで分散サービス拒否（DDoS）状態が発生する可能性があります。

次のレジストリキーは、Broker Agent が最初の検索時に Controller を検出できない場合に、フォールバックトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- 値の名前：`DisableDdcWildcardNameLookup`
- 種類：`DWORD`
- 値：`1`（デフォルト）または`0`

`1`に設定すると、フォールバック検索は無効になります。Controller の初回検索が失敗すると、Broker Agent は検索を停止します。これがデフォルトの設定です。
`0`に設定すると、フォールバック検索が有効になります。Controller の初回検索が失敗した場合、フォールバックトップダウン検索が開始されます。

VDA 登録の問題のトラブルシューティング

先に述べたように、仲介セッションを起動する場合、対象の Delivery Controller に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Studio では、カタログ作成ウィザード内で、およびカタログをデリバリーグループに登録した後に、トラブルシューティング情報が提供されます。

マシンカタログの作成時に問題を特定する：

カタログ作成ウィザードで、既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが示された場合は、該当のマシンを（[削除] ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（Delivery Controller で登録されたことがないなどの理由により）マシンに関する情報を取得されていないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しい VDA が必要な場合があります。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能がカタログで利用できるようになります。ただし、以前の VDA バージョンのカタログにあるマシンは登録できません。

デリバリーグループの作成後に問題を特定する：

デリバリーグループを作成すると、そのグループと関連付けられているマシンの詳細が Studio に表示されます。デリバリーグループの［詳細］ペインに、登録されている必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードでないはないのに、Controller に現在登録されていないマシンが 1 台または複数台存在することが考えられます。「未登録だが登録する必要がある」マシンが表示された場合は、［詳細］ペインの ［トラブルシューティング］タブで、考えられる原因と推奨される修正アクションを確認します。

機能レベルについて詳しくは、「マシンカタログの作成」の「*VDA* バージョンと機能レベル」を参照してください。

VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

Citrix Health Assistant を使用して、VDA 登録とセッションの開始に関するトラブルシューティングを行うことも可能です。詳しくは、CTX207624を参照してください。

セッション

August 24, 2021

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。

「ログオン間隔」セクションでは、デフォルト設定の変更方法について説明します。

また、ユーザーのセッションからのログオフ、セッションの切断、およびセッションの事前起動と残留の構成も実行できます。「デリバリーグループの管理」を参照してください。

セッション画面の保持

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に有用です。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、通常はセッションが切断され、セッションの画面が表示されなくなります。この場合、切断セッションに再接続されるまで、そのセッションでは何もできません。セッション画面の保持機能を有効にすると、データを損失することなくセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止し、カーソルの形が砂時計に変わるため、ユーザーにもネットワークが切断されていることがわかります。このとき、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

Citrix Receiver のユーザーには、Controller 側の設定が自動的に適用されます。

セッション画面の保持機能と共に、TLS（Transport Layer Security）を使用できます。TLS はユーザーデバイスと NetScaler Gateway 間で送信されるデータのみを暗号化します。

セッション画面の保持機能は、以下のポリシー設定で構成します。

- ［セッション画面の保持］ポリシー設定により、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］ポリシー設定には、デフォルトで 180 秒（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］ポリシー設定を構成して、中断されたセッションにユーザーが再接続する時に再認証を要求することができます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後でクライアントの自動再接続のポリシー設定が有効になり、切断セッションへの再接続が行われます。

クライアントの自動再接続

クライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションを Citrix Receiver が検出して、そのセッションに自動的に再接続します。この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。

アプリケーションセッションでは、Citrix Receiver は、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。

デスクトップセッションでは、Citrix Receiver は、指定された時間、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。デフォルトでは、この時間は 5 分です。この時間を変更するには、ユーザーデバイスで以下のレジストリを編集します。

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds、DWORD、<seconds>

<seconds> には、セッションの再接続の試行をやめるまでの時間を秒数で指定します。

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できます。セッションがリセットされた場合、再接続しようとすると、切断前の作業状態からセッションが復元されるのではなく、アプリケーションが再起動されて新しいセッションが開始されます。
- セッションがリセットされるようにサーバーが構成されている場合、クライアントの自動再接続により新しいセッションが開始されます。この場合、ユーザーが自分の資格情報を入力して、サーバーにログオンし直す必要があります。
- 外部からの侵入などによってクライアント側から正しくない認証情報が送信された場合、またはセッションの切断が検出されてから自動再接続までの時間が長すぎた場合は、自動再接続に失敗することがあります。

ICA Keep-Alive

ICA Keep-Alive 機能を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。この機能が有効な場合、セッションのアイドル状態（たとえばクロックデータの更新、マウス操作、画面更新などがない状態）が検出されたときに、リモートデスクトップサービスによりセッションが切断されることを防ぐことができます。サーバーは、定期的に Keep-Alive パケットを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、サーバーにより「切断」状態として認識されます。

> 注:
>
> ICA Keep-Alive は、セッション画面の保持機能を使用しない環境でのみ正しく動作します。セッション画面の保持機能では、ICA Keep-Alive とは異なるメカニズムで切断セッションが管理されます。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Alive を有効にしてください。

ここでの Keep-Alive 機能の設定は、Windows のグループポリシーによる同様の設定よりも優先されます。

ICA Keep-Alive 機能は、以下のポリシー設定で構成します。

- **ICA Keep-Alive** タイムアウト。ICA Keep-Alive メッセージの送信間隔を 1〜3600 秒の範囲で指定します。ただし、ネットワークの問題によるセッションの切断が少なく、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に閉じるように設定している環境では、このオプションを構成しないでください。

  デフォルト値は 60 秒で、サーバーからユーザーデバイスに ICA Keep-Alive パケットが 60 秒おきに送信されます。クライアントが 60 秒以内に応答しない場合、そのセッションは「切断」状態（タイムアウト）と認識されます。

- **ICA Keep-Alive**。ICA Keep-Alive メッセージを送信するかどうかを指定します。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス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か、StoreFront だけからログオフするのかを管理者が構成できます。
- 切断：ユーザーは、実行中のすべてのデスクトップやアプリケーションを一度に切断できます。個々に切断する必要はありません。

ワークスペースコントロールは、Citrix Receiver ユーザーが Citrix StoreFront 経由でデスクトップやアプリケーションにアクセスする場合にのみ使用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールが無効になり、ホストされたアプリケーションセッションでは有効になります。公開デスクトップ上で公開アプリケーションを実行する場合、デフォルトではこれらのセッションは共有されません。

ユーザーが別のクライアントデバイスに移動すると、ポリシー、クライアント側ドライブのマッピング、およびプリンターの設定が適切に変更されます。ポリシーとクライアント側ドライブのマッピングは、ユーザーがセッションにログオンするクライアントデバイスの条件に基づいて適用されます。たとえば、医療従事者が緊急治療室のクライアントデバイスからログオフして、レントゲン室のワークステーションにログオンして自分のワークスペースに再接続した場合は、レントゲン室でのセッションに適したポリシー、プリンターマッピング、およびクライアント側ドライブのマッピング設定がセッションの開始時に有効になります。

管理者は、ユーザーが場所を移動したときに使用可能になるプリンターをカスタマイズできます。また、ローカルプリンターでの印刷の可否やリモート接続時に使用される帯域幅などの印刷環境を制御することもできます。

ワークスペースコントロール機能を有効にして構成する方法については、StoreFront のドキュメントを参照してください。

セッションローミング

デフォルトでは、ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。多くの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。

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ほかのリソースが決定されます。その日のうちに、生産管理者は

隣の建物のオフィスに移動し、プリンターを使用する必要があるミーティングに出席します。

- セッションローミングが有効な場合、生産管理者は会議室の近くにあるプリンターを使用できない可能性があります。ミーティングより前に自分のオフィス内でアプリケーションを起動したため、オフィスの近くにあるプリンターやそのほかのリソースへの割り当てが行われているためです。
- セッションローミングが無効な場合、（同じ資格情報を使用して）別のマシンにログオンすると、新たなセッションが開始され、近くにあるプリンターやリソースを使用できるようになります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを含む以下の資格ポリシー規則コマンドレットを使用します。必要に応じて、「LeasingBehavior」プロパティも指定できます。後述の「接続リース機能およびセッションローミング」を参照してください。

デスクトップセッションの場合：

Set-BrokerEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed | Disallowed

アプリケーションセッションの場合：

Set-BrokerAppEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed | Disallowed

<*value*> には、次のいずれかの値を指定できます：

- **Always**。クライアントデバイスに関係なく、セッションが接続中でも、切断中でも、セッションローミングが常に実行されます。これがデフォルト値です。
- **DisconnectedOnly**。既に切断されているセッションのみに再接続します。それ以外のセッションについては、新規セッションを開始します（最初に切断するか、ワークスペースコントロールを使用して明示的にローミングすることによって、クライアントデバイス間のセッションローミングを実行することができます）。別のクライアントデバイスからのアクティブな接続済みセッションは、使用されません。代わりに、新規セッションが開始されます。
- **SameEndpointOnly**。ユーザーが使用する各クライアントデバイスに対し、一意のセッションが割り当てられます。ローミングは、完全に無効になります。ユーザーは、セッションで過去に使用されたものと同じデバイスのみに再接続できます。

「LeasingBehavior」プロパティについては、後述の説明を参照してください。

ほかの設定による影響

セッションローミングの無効化は、デリバリーグループにおけるアプリケーションのプロパティのアプリケーション制限「1 ユーザーあたり 1 インスタンスのみ許可する」の影響を受けます。

- セッションローミングを無効にする場合、このアプリケーション制限も無効にします。

- このアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する 2 つの値は、どちらも設定しないでください。

接続リース機能とセッションローミング

接続リース機能について詳しくは、「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。

理由は次のとおりです。このシナリオでは、1 つのセッションがすべてのデバイスで共有されます。たとえば、Controller がリース接続モードである間に、1 人のユーザーが、同じ資格情報で再接続するほかのユーザーに見られることを意図していない機密情報を表示している場合、この状況は好ましくありません。

資格ポリシーで接続リース機能を無効にすることにより、この可能性が排除されます。ユーザーは、Controller がリース接続モードであっても、同じログオン資格情報を使用する別のユーザーのセッションを表示することができなくなります。ほかの資格ポリシーは、影響を受けません。個別のユーザーアカウントで、個別の資格に基づいて接続リース機能を使用することができます。

資格ポリシーで接続リース機能を無効にするには、「LeasingBehavior Disallowed」プロパティを資格ポリシーコマンドレットに追加します。接続リース機能を無効にする場合、既に作成され、該当する資格ポリシーに対してキャッシュされている起動リースを手動で削除する必要があります。削除しない場合、ユーザーは引き続き、データベースのダウン中に再接続できます。

ログオン間隔

デスクトップ VDA がインストールされている仮想マシンが、ログオンプロセスが完了する前に終了する場合は、プロセスにより多くの時間を割り当てることができます。7.6 以降のバージョンのデフォルトは 180 秒です（7.0〜7.5 は 90 秒です）。

マシン上（またはマシンカタログで使用されるマスターイメージ上）で、以下のレジストリキーを設定します：

キー：HKLM\SOFTWARE\Citrix\PortICA

値：AutoLogonTimeout

種類：DWORD

十進法時間（秒）を 0〜3600 の範囲で指定します。

マスターイメージを変更する場合は、カタログを更新してください。

> 注:
>
> この設定は、デスクトップ（ワークステーション）のある仮想マシンにのみ適用されます。Microsoft の場合は、サーバー 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

August 24, 2021

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］タブや［デリバリーグループ］タブで［検索］ボックスを使用して検索できません。ナビゲーションペインの［検索］ノードを使用してください。

   追加の検索条件を表示するには、［検索］ボックスの横にあるプラス記号をクリックします。マイナス記号をクリックすると、その検索条件が削除されます。

2. 検索する項目の名前を入力するか、ドロップダウン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。保存した検索は、［保存済みの検索］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:

- いずれかの列を右クリックして［列の選択］を選択すると追加の特性を表示することができ、その特性を基準にして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］、［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、目的のグループを選択して、［操作］ペインで［マシンの表示］を選択します。

タグ

August 24, 2021

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどといった項目を識別する文字列です。タグを作成してアイテムに追加すると、以下のように、特定の操作を指定されたタグのあるアイテムのみに適用するように調整できます。

- Studio での検索結果の表示を調整する。

たとえば、テスターに最適化されているアプリケーションのみを表示するには、「テスト」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Studio の検索結果を「テスト」タグでフィルタリングできます。

- 選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループまたは特定のデスクトップからアプリケーションを公開する。この機能は、タグ制約と呼ばれます。

タグ制約で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制約は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。その機能は、7.x より前のリリースの XenApp ワーカーグループに類似していますが、同一ではありません。

タグ制約のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

タグ制約の使用の詳細と例については、下記を参照してください。

- デリバリーグループ内のマシンのサブセットの定期再起動をスケジューリングする。

マシンでタグ制約を使用すると、新しい PowerShell コマンドレットを使用して、デリバリーグループ内のマシンのサブセットに対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」セクションの「デリバリーグループのマシンに対する再起動スケジュールの作成」を参照してください。

- デリバリーグループのマシンのサブセット、デリバリーグループの種類、指定されたタグを持つ（または持たない）OU への Citrix ポリシーの適用（割り当て）を調整する。

たとえば、より強力なワークステーションにのみ Citrix ポリシーを適用するには、それらのマシンに「ハイパワー」という名前のタグを追加します。その後、［ポリシーの作成］ウィザードの ［ポリシーの割り当て］ページでこのタグを選択し、［有効化］チェックボックスをオンにします。デリバリーグループにタグを追加し、そのデリバリーグループに Citrix ポリシーを適用することもできます。詳しくは、「ポリシーの作成」を参照してください。（マシンにタグを追加する Studio インターフェイスがブログ記事の公開時から変更されていることに注意してください）。

次の項目にタグを適用できます：

- マシン
- アプリケーション
- デリバリーグループ
- アプリケーショングループ

タグ制約は、Studio で次のものを作成または編集するときに構成できます。

- 共有デリバリーグループのデスクトップ
- アプリケーショングループ

デスクトップまたはアプリケーショングループのタグ制約

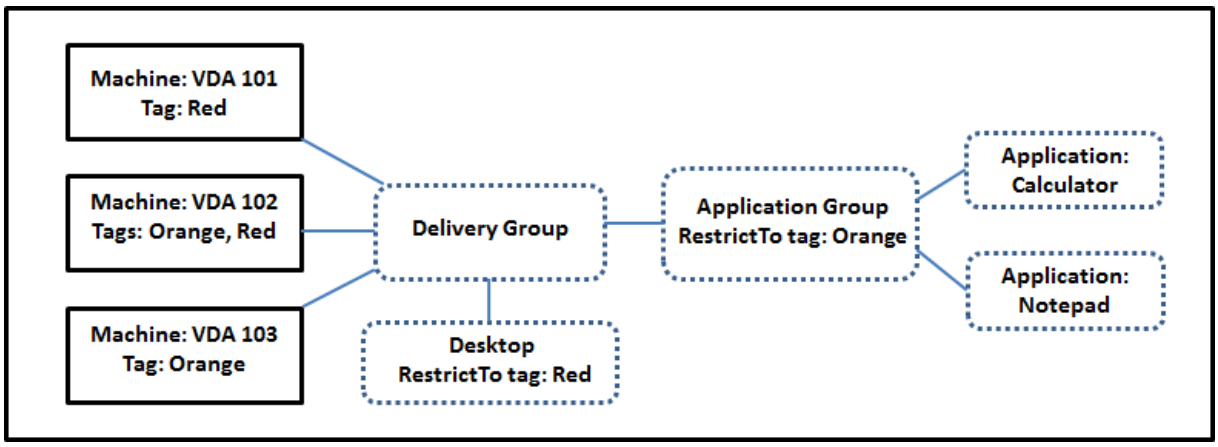
タグ制約には、いくつかの手順があります：

- タグを作成し、マシンに追加（適用）します。
- タグ制約を持つグループを作成または編集します（言い換えると、タグ x を持つマシンに起動を制約します）。

タグ制約は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、関連するデリバリーグループから、アクセスポリシー、構成されたユーザーの一覧、ゾーン優先度、起動対応度、およびタグ制約（存在する場合）に従うマシンを選択します。アプリケーションの場合、ブローカーは優先度順に他のデリバリーグループにフォールバックし、関係する各デリバリーグループに同じマシン選択規則を適用します。

例 **1**

この例では、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグ制約を使用して制限する単純なレイアウトを紹介します。サイトには、1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



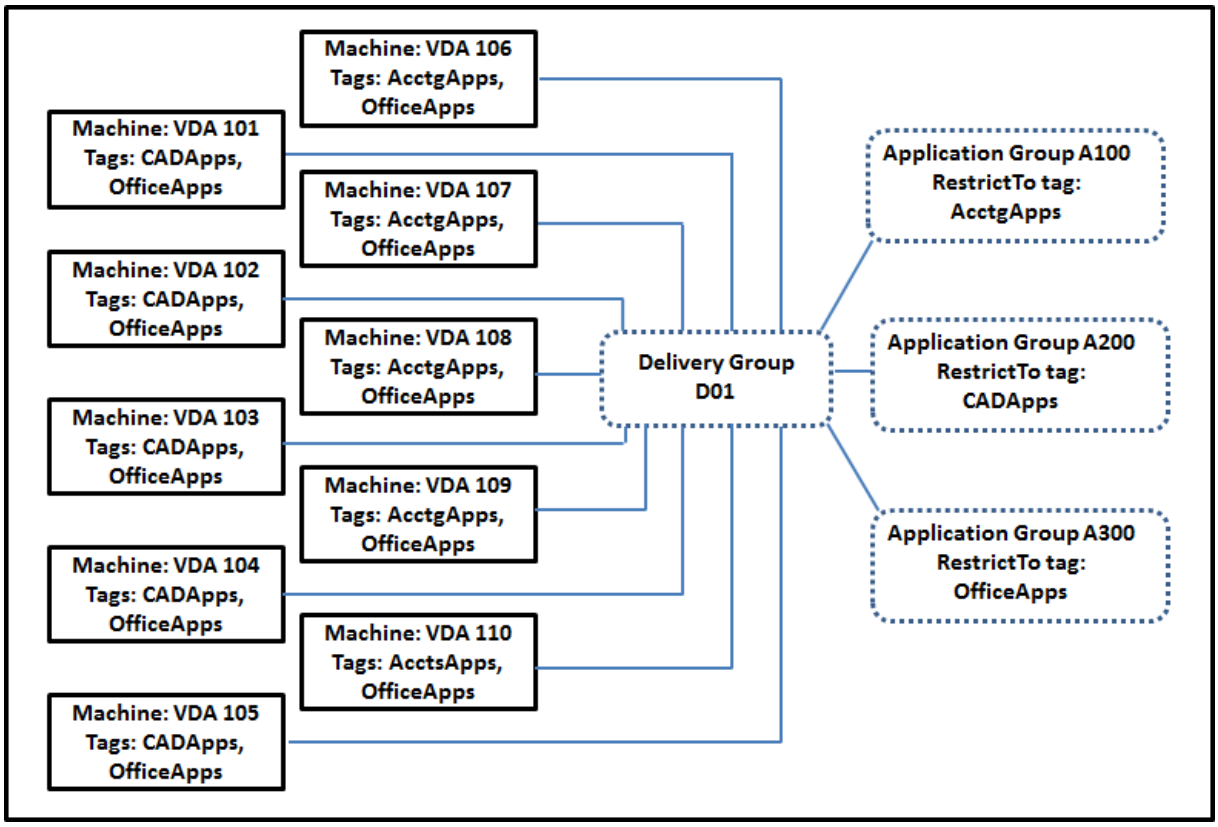
- 3 台のマシン（VDA 101～103）それぞれにタグが追加されています。
- 共有デリバリーグループのデスクトップは「Red」という名前のタグ制約を付けて作成されているため、デリバリーグループの、「Red」という名前のタグを持つマシン（VDA 101 および 102）上でのみ起動できます。
- アプリケーショングループは「Orange」のタグ制約で作成されているので、各アプリケーション（計算機とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン：VDA 102 および 103 上でのみ起動できます。

マシン VDA 102 が両方のタグ（Red および Orange）を持っており、したがってアプリケーションとデスクトップの起動に関与できる点に注意してください。

例 **2**

この例には、タグ制約付きで作成された複数のアプリケーショングループが含まれます。これにより、デリバリーグループのみを使用する場合に必要な数より少ないマシンでより多くのアプリケーションを提供できます

（「例 2 を構成する方法」のセクションでは、タグを作成、適用し、この例のタグ制限を構成するために使用される手順を示します）。



この例では、10 台のマシン（VDA 101～110）、1 つのデリバリーグループ（D01）、および 3 つのアプリケーショングループ（A100、A200、A300）を使用します。各アプリケーショングループの作成時に、各マシンにタグを適用し、タグ制約を指定することにより、以下のことが可能です：

- グループ内の会計ユーザーは、5 台のマシン（VDA 101～105）上で、必要なアプリにアクセスできます。
- グループ内の CAD デザイナーは、5 台のマシン（VDA 106～110）上で、必要なアプリにアクセスできます。
- Office アプリケーションを必要とするグループのユーザーは、10 台のマシン（VDA 101～110）上で、Office アプリにアクセスできます。

1 つのデリバリーグループで、10 台のマシンのみが使用されています。1 台のマシンは 1 つのデリバリーグループにのみ属することができるので、デリバリーグループのみを使用する場合は（アプリケーショングループ不使用時）、2 倍のマシンが必要になります。

タグとタグ制約の管理

タグの作成、追加（適用）、編集、適用済みのアイテムからの削除は、Studio の ［タグの管理］操作を使用して行います

例外：ポリシー割り当てのために使用されるタグは、Studio の［タグの管理］アクションを介して作成、編集、削除されます。ただし、タグが適用される（割り当てられる）のはポリシーの作成時です。詳しくは「ポリシーの作成」を

参照してください。

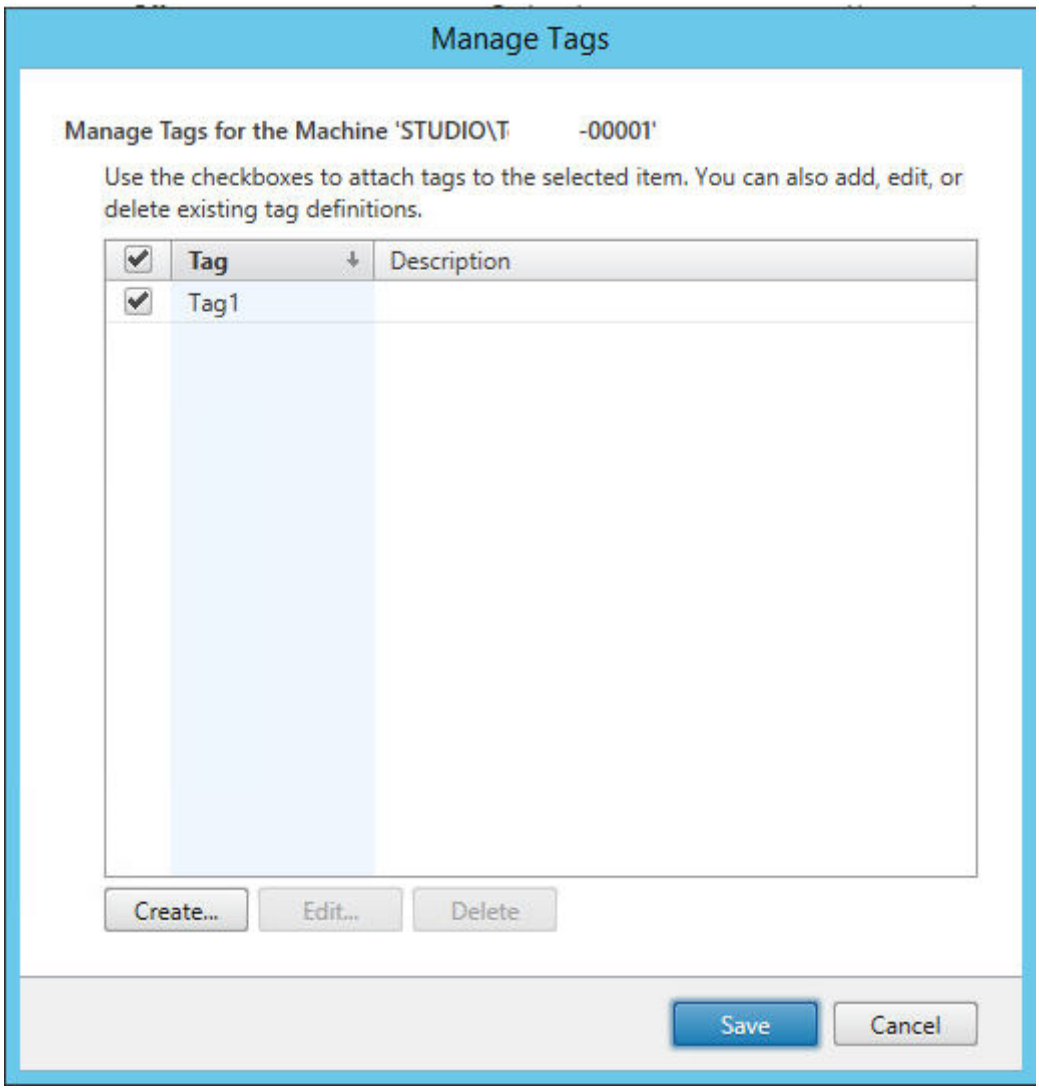
タグ制約は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。グループの作成と編集について詳しくは、次の記事を参照してください:

- デリバリーグループの作成
- デリバリーグループの管理
- アプリケーショングループの作成
- アプリケーショングループの管理

Studio での［タグの管理］ダイアログの使用

Studio で、タグの適用先となる項目（1 つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ）を選び、［操作］ペインで［タグの管理］を選択します。［タグの管理］ダイアログボックスに、選択した項目のタグだけでなく、サイトで作成されたすべてのタグが表示されます。

- チェックマークが付いているチェックボックスは、タグが選択した項目に既に追加されていることを表します（下の画面キャプチャで、選択されたマシンには「Tag1」という名前のタグが適用されています）。
- 複数の項目を選択した場合、ハイフンを含むチェックボックスは、一部の項目（すべての項目ではない）にそのタグが追加されていることを表します。



［タグの管理］ダイアログボックスでは、以下の操作を実行できます。注意のセクションを確認してください。

タグを作成するには：

［作成］をクリックします。名前と説明を入力します。タグの名前は一意でなければならず、大文字と小文字は区別されません。［**OK**］をクリックします。（タグを作成しても、選択しているアイテムに自動的に適用されることはありません。チェックボックスを使用してタグを適用します。）

1 つまたは複数のタグを追加（適用）するには：

タグ名の隣にあるチェックボックスをオンにします。注：複数の項目を選択し、タグの隣のチェックボックスにハイフンが付いている場合（選択された項目の一部（すべてではない）に、タグが既に適用されていることを示す）、それをチェックマークにすると、選択されているすべてのマシンに影響が及びます。

1 つまたは複数のマシンにタグを追加しようとしていて、そのタグが現在アプリケーショングループの制約として使用されている場合、その操作により、それらのマシンが起動対象になることがあるという警告が表示されます。それが意図どおりであれば続行します。

1 つまたは複数のタグを削除するには:

タグ名の隣にあるチェックボックスをオフにします。注:複数の項目を選択し、タグの隣のチェックボックスにハイフンが付いている場合(選択された項目の一部(すべてではない)に、タグが既に適用されていることを示す)、チェックボックスをオフにすると、選択されているすべてのマシンからタグが削除されます。

タグを制約として使用しているマシンからそのタグを削除しようとすると、起動対象となるマシンに影響を与える場合があるという警告メッセージが表示されます。それが意図どおりであれば続行します。

タグを編集するには:

タグを選択し、[編集]をクリックします。新しい名前や説明を入力します。同時に編集できるタグは 1 つのみです。

1 つまたは複数のタグを削除するには:

タグを選択し、[削除]をクリックします。[タグの削除]ダイアログボックスに、選択したタグを現在使用しているアイテムの数が表示されます(「2 台のマシン」など)。アイテムをクリックすると、詳細が表示されます。たとえば、[2 台のマシン]というアイテムをクリックすると、そのタグを適用されている 2 台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

Studio を使用して、制約として使用されているタグを削除することはできません。先にアプリケーショングループを編集してから、タグ制約を削除するか、異なるタグを選択する必要があります。

[タグの管理]ダイアログボックスでの操作が完了したら、[保存]をクリックします。

ヒント:マシンにタグが適用されているかどうかを確認するには:

ナビゲーションペインで [デリバリーグループ]を選択します。中央ペインでデリバリーグループを選択して、[操作]ペインで [マシンの表示]を選択します。中央のペインでマシンを選択し、下の[詳細]ペインで[タグ]タブを選択します。

タグ制約の管理

タグ制約の構成は複数の手順があるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制約を追加します。

タグの作成と適用:

上記の [タグの管理]操作を使用して、タグを作成してマシンに追加(適用)します。タグを追加したマシンには、タグ制約の影響が生じます。

アプリケーショングループにタグ制約を追加するには:

アプリケーショングループを作成または編集します。[デリバリーグループ]ページで、[タグでマシンの起動を制限します:]を選択し、ドロップダウンからタグを選択します。

アプリケーショングループのタグ制約を変更または削除するには:

グループを編集します。[デリバリーグループ]ページで、異なるタグをドロップダウンから選択するか、[タグでマシンの起動を制限します:]をオフにしてタグ制約を完全に削除します。

デスクトップにタグ制約を追加するには:

デリバリーグループを作成または編集します。[デスクトップ] ページで [追加] または [編集] をクリックします。[デスクトップの追加] ダイアログボックスで、[次のタグを持つマシンに起動を制約する:] を選択し、ドロップダウンからタグを選択します。

デリバリーグループのタグ制約を変更または削除するには:

グループを編集します。[デスクトップ] ページで [編集] をクリックします。ダイアログボックスで、異なるタグをドロップダウンから選択するか、[タグでマシンの起動を制限します:] をオフにしてタグ制約を完全に削除します。

タグを項目に追加または削除する場合の注意事項

項目に適用されるタグはさまざまな目的に使用できるため、タグの追加や削除が意図しない結果になる可能性があることに注意してください。タグを使用して Studio 検索フィールドのマシン表示を並べ替えることができます。アプリケーショングループまたはデスクトップの構成時に同じタグを制約として使用すると、そのタグが付いている指定されたデリバリーグループのマシンだけに起動対象を制限できます。

タグがデスクトップまたはアプリケーショングループのタグ制約として構成されている場合に 1 つまたは複数のマシンにタグを追加しようとすると、それらのマシンでその他のアプリケーションやデスクトップの起動が可能になることがあるという警告が表示されます。それが意図どおりであれば続行します。そうでない場合は、操作を取り消すこともできます。

たとえば、「Red」というタグ制約を持つアプリケーショングループを作成するとします。後から、そのアプリケーショングループによって使用される同じデリバリーグループに、他のマシンをいくつか追加します。それらのマシンに「Red」というタグを追加すると、おおむね次のようなメッセージが表示されます:「タグ「Red」は、次のアプリケーショングループ上の制約として使用されています。このタグを追加すると、選択されたマシンからこのアプリケーショングループのアプリケーションが起動可能になる可能性があります」。次に、それらの追加マシンへのそのタグの追加を確認またはキャンセルできます。

同様に、アプリケーショングループで起動を制限するためにタグが使用されている場合、グループを編集してタグ制約を削除するまで、そのタグを削除できないという警告が表示されます（アプリケーショングループの制約として使用されているタグの削除を許可されている場合、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動を許可することになる可能性があります)。デスクトップ起動の制約として現在タグが使用されている場合も、タグの削除は同様に不可能です。アプリケーショングループまたはデリバリーグループ内のデスクトップを編集してタグ制約を削除すれば、タグを削除できます。

すべてのマシンが同一セットのアプリケーションを持つとは限りません。1 人のユーザーが、それぞれ異なるタグ制約を持ち、デリバリーグループのマシン構成が異なるか重なり合っている複数のアプリケーショングループに属する場合があります。次の表に、対象マシンがどのように決まるかを示します。

アプリケーションの追加先	選択したデリバリーグループ内で起動対象となるマシン
タグ制約を持たない 1 つのアプリケーショングループ	すべてのマシン
タグ制約 A を持つ 1 つのアプリケーショングループ	タグ A が適用されているマシン
2 つのアプリケーショングループ。タグ制約 A を持つグループとタグ制約 B を持つグループ	タグ A とタグ B を持っているマシン。存在しない場合、タグ A またはタグ B を持っているマシン
2 つのアプリケーショングループ。タグ制約 A を持つグループとタグ制約を持たないグループ	タグ A を持つマシン。存在しない場合、すべてのマシン

マシン再起動スケジュールでタグ制限を使用している場合、タグ適用またはタグ制限に影響する変更はすべて、次のマシン再起動サイクルに影響を与えます。変更の実行中に進行している再起動サイクルには影響しません（「デリバリーグループの管理」を参照してください）。

例 **2** を構成する方法

次の手順は、タグを作成、適用し、上の 2 番目の例で示したアプリケーショングループのためにタグ制約を構成する方法を示しています。

VDA とアプリケーションはマシンに既にインストール済み、デリバリーグループは作成済みです。

マシンにタグを作成し、適用します:

1. Studio でデリバリーグループ D01 を選択して、［操作］ペインで ［マシンの表示］を選択します。
2. マシン VDA 101～105 を選択して、［操作］ペインで ［タグの管理］を選択します。
3. ［タグの管理］ダイアログボックスで ［作成］をクリックし、CADApps という名前のタグを作成します。［**OK**］をクリックします。
4. ［作成］を再度クリックして、OfficeApps という名前のタグを作成します。［**OK**］をクリックします。
5. ［タグの管理］ダイアログボックスで、各タグ名（CADApps および OfficeApps）の隣にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）し、ダイアログボックスを閉じます。
6. デリバリーグループ D01 を選択して、［操作］ペインで ［マシンの表示］を選択します。
7. マシン VDA 106～110 を選択して、［操作］ペインで ［タグの管理］を選択します。
8. ［タグの管理］ダイアログボックスで［作成］をクリックし、AcctgApps という名前のタグを作成します。［**OK**］をクリックします。
9. 各タグ名の隣にあるチェックボックスをオンにして、新しく作成した AcctgApps タグと OfficeApps タグを選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制約を持つアプリケーショングループを作成します。

1. Studio のナビゲーションペインで ［アプリケーション］を選択し、次に［操作］ペインで ［アプリケーショングループの作成］を選択します。アプリケーショングループの作成ウィザードが起動します。

2. ウィザードの ［デリバリーグループ］ページで、デリバリーグループ D01 を選択します。［タグでマシンの起動を制限します:］を選択し、ドロップダウンから AcctgApps タグを選択します。
3. 会計ユーザーと会計アプリケーションを指定して、ウィザードを完了します（アプリケーションを追加するときに［[スタート］メニューから］を選択すると、AcctgApps タグが適用されているマシン上にあるアプリケーションが検索されます）。［概要］ページで、グループに A100 という名前を付けます。
4. 前の手順を繰り返してアプリケーショングループ A200 を作成して、CADApps タグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。
5. 手順を繰り返してアプリケーショングループ A300 を作成して、OfficeApps タグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。

詳細情報

ブログ記事：How to Assign Desktops to Specific Servers。この記事には次のビデオも含まれています。

IPv4/IPv6 サポート

February 3, 2020

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。

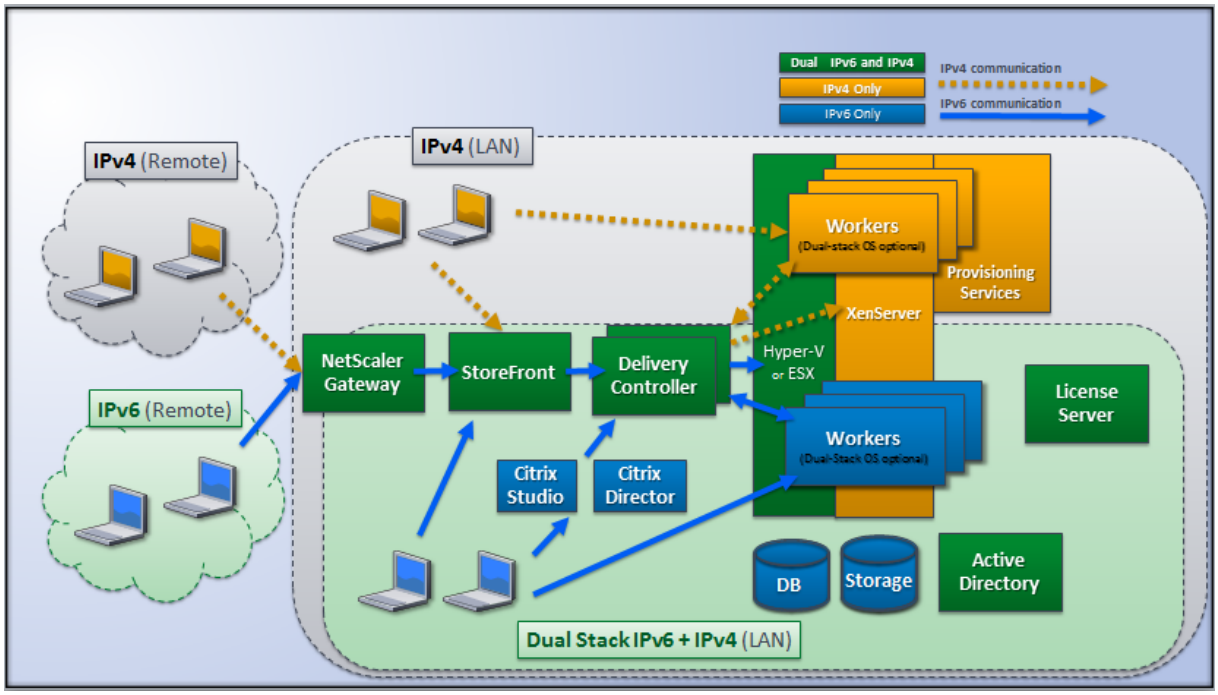
IPv6 通信は、Virtual Delivery Agent（VDA）接続関連の 2 つの Citrix ポリシー設定で制御されます。

- 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。

デュアルスタック IPv4/IPv6 展開

次の図は、デュアルスタック IPv4/IPv6 展開を示しています。このシナリオで、「ワーカー」とはハイパーバイザーまたは物理システム上にインストールされた VDA を指し、主にアプリケーションやデスクトップへの接続を可能にするために使用されます。デュアル IPv6 および IPv4 をサポートするコンポーネントは、トンネリングまたはデュアルプロトコルソフトウェアを使用するオペレーティングシステム上で実行されます。



次の Citrix 製品、コンポーネント、および機能では IPv4 のみがサポートされます。

- Provisioning Services
- XenServer 6.x
- [**IPv6 Controller** 登録のみを使用する] ポリシー設定が設定されていない 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

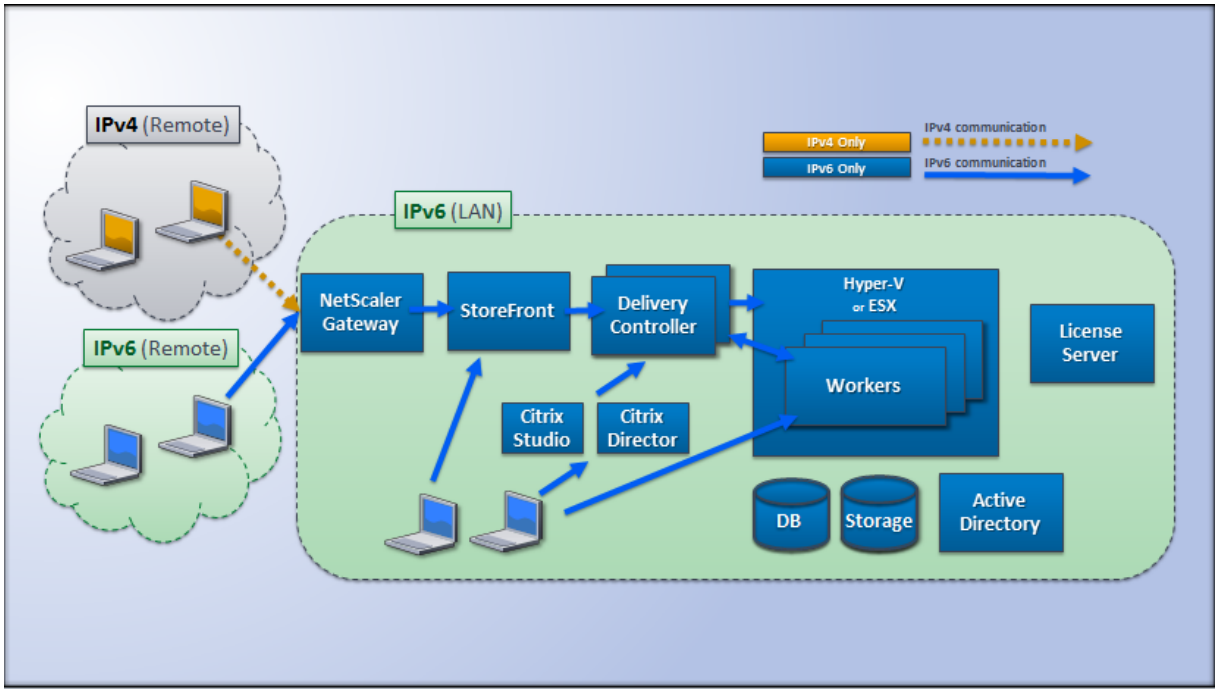
この展開は、以下のように管理されます。

- 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、管理者はプライマリの IPv6 ポリシー設定（つまり［IPv6 Controller 登録のみを使用する］）が有効な組織単位（OU）またはワーカーイメージを使用して IPv6 デスクトップとアプリケーションを公開します。
- ユーザーによる IPv4 ネットワークの使用頻度が高い場合、管理者はプライマリの IPv6 ポリシー設定（つまり［IPv6 Controller 登録のみを使用する］）が無効（デフォルト）な OU またはワーカーイメージを使用して IPv4 デスクトップとアプリケーションを公開します。

ピュア **IPv6** 展開

次の図は、ピュア IPv6 展開を示しています。このシナリオの内容は以下のとおりです。

- 各コンポーネントは、IPv6 ネットワークのサポートが構成されたオペレーティングシステム上で実行されている。
- すべての VDA に対してプライマリの IPv6 ポリシー設定（[IPv6 Controller 登録のみを使用する]）が有効になっている。つまり、VDA を IPv6 アドレスを使って Controller に登録する必要がある。



IPv6 用のポリシー設定

Citrix ポリシーには、ピュア IPv6 環境や IPv4/IPv6 デュアルスタック環境をサポートするための 2 つのポリシー設定があります。次の接続関連ポリシーを構成します。

- **IPv6 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：これらのポリシー設定によってのみ、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 Controller** 登録のみを使用する] 設定を有効にしたポリシーを適用する必要があります。

展開に関する考慮事項

環境内に IPv4 と IPv6 の両方のネットワークがある場合、IPv4 のみのクライアントと IPv6 ネットワークにアクセスできるクライアントに対して、別個のデリバリーグループ構成が必要です。ユーザーを区別するために、名前付け、手動 Active Directory グループ割り当て、または SmartAccess フィルターの使用を検討してください。

IPv6 ネットワークで接続されたセッションに IPv4 アクセスのみの内部クライアントから再接続する場合、再接続に失敗することがあります。

ユーザープロファイル

August 24, 2021

デフォルトでは、マスターイメージ上に Virtual Delivery Agent をインストールするときに Citrix Profile Management が自動的にインストールされます。ただし、プロファイル管理ツールとしてこのコンポーネントを常に使用しなければならないということではありません。

ユーザーのニーズに応じて XenApp/XenDesktop ポリシーを構成して、各デリバリーグループ内のマシンに異なるプロファイル処理を適用できます。たとえば、あるデリバリーグループではネットワーク上の特定の場所にテンプレートが格納される Citrix 固定プロファイルを使用して、別のデリバリーグループではいくつかのリダイレクトフォルダーと共に別の場所に格納される Citrix 移動プロファイルを使用するポリシーを構成できます。

- 組織内のほかの管理者が XenApp/XenDesktop ポリシーを管理する場合は、すべてのデリバリーグループにプロファイル関連のポリシーが正しく適用されるように共同で作業する必要があります。
- Profile Management ポリシーは、グループポリシーや Profile Management の INI ファイルで設定したり、各仮想マシン上でローカルに設定したりできます。これらの設定は、以下の順に読み取られます。

  1. グループポリシー（ADM または ADMX ファイル）
  2. ［ポリシー］ノードの XenApp/XenDesktop ポリシー
  3. ユーザーが接続する仮想マシン上のローカルポリシー
  4. Profile Management の INI ファイル

  たとえば、グループポリシーと［ポリシー］ノードの両方で同じポリシーを構成する場合、グループポリシーのポリシー設定が適用され、XenApp/XenDesktop ポリシー設定は無視されます。

いずれのプロフィル処理でも、Director 管理者はユーザープロファイルの診断情報にアクセスしたりトラブルシューティングを行ったりできます。詳しくは、Director のドキュメントを参照してください。

Personal vDisk 機能を使用する場合、Citrix ユーザープロファイルはデフォルトで仮想デスクトップの Personal vDisk に格納されます。Personal vDisk にプロファイルのコピーが残っている間は、ユーザーストア内のコピーを削除しないでください。これを削除すると Profile Management でエラーが発生し、仮想デスクトップへのログオンに一時プロファイルが使用されることになります。

自動構成

デスクトップの種類は、インストールされている Virtual Delivery Agent に基づいて自動的に検出され、それに応じて Studio での構成オプションや Profile Management のデフォルトの動作が設定されます。

Profile Management で設定されるポリシーは、以下の表のとおりです。ポリシーの非デフォルトの設定は保持され、この機能で上書きされることはありません。各ポリシーについて詳しくは、Profile Management のドキュメントを参照してください。プロファイルを作成するマシンの種類により、調整されるポリシーが異なります。最初の要因は、マシンの種類が固定なのかプロビジョニングなのかという点です。次の要因は、それが複数のユーザーによって共有されるのか特定のユーザーに専用のものなのかという点です。

固定システムにはある種のローカルストレージが備わっていて、システムの電源がオフになってもシステムの内容を維持することができます。固定システムでは、ローカルディスクとして記憶域ネットワーク（SAN）のような記憶域テクノロジを使用できます。これと対照的に、プロビジョニングシステムは基本ディスクとある種の ID ディスクから「オンザフライ」で作成されます。通常、RAM ディスクまたはネットワークディスクがローカルストレージとして使用され、ネットワークディスクはしばしば高速リンクの SAN によって提供されます。プロビジョニングテクノロジとは、一般的に Provisioning Services または Machine Creation Services（またはサードパーティの同等物）を指します。場合により、プロビジョニングされたシステムが Personal vDisk によって提供される固定ローカルストレージを伴うことがあります。この場合は固定システムとして分類されます。

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や、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。

固定マシン

ポリシー	固定かつ専用	固定かつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	有効
プロファイルストリーミング	無効	有効
常時キャッシュ	有効（注 1）	無効（注 2）
アクティブライトバック	無効	無効（注 3）
ローカル管理者のログオン処理	有効	無効（注 4）

プロビジョニングされたマシン

ポリシー	プロビジョニングかつ専用	プロビジョニングかつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効（注 5）	有効
プロファイルストリーミング	有効	有効
常時キャッシュ	無効（注 6）	無効
アクティブライトバック	有効	有効
ローカル管理者のログオン処理	有効	有効（注 7）

1. このマシンの種類では［プロファイルストリーミング］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。

フォルダーのリダイレクト

フォルダーリダイレクトを有効にすると、ユーザーデータをユーザープロファイルとは異なるネットワーク共有上に格納できます。これにより、プロファイルのサイズが小さくなるため短時間でロードされるようになりますが、ネットワーク帯域幅が消費されます。フォルダーリダイレクト機能では、Citrix ユーザープロファイルを使用する必要はありません。管理者は独自にユーザーのプロファイルを管理して、フォルダーをリダイレクトできます。

フォルダーリダイレクトを構成するには、Studio で Citrix ポリシーを使用します。

- フォルダーのリダイレクト先のネットワーク共有が使用可能であり、適切なアクセス権が設定されていることを確認します。リダイレクト先のプロパティは自動的に検証されます。
- リダイレクト先のネットワーク共有をセットアップすると、ユーザーの次回ログオン時にプロファイルがリダイレクトされます。

注：フォルダーリダイレクト機能は、Citrix ポリシーまたは Active Directory グループポリシーオブジェクトのいずれか一方を使用して構成してください。両方のポリシーエンジンを使用すると、予期しない問題が発生することがあります。

詳細なフォルダーリダイレクト

複数のオペレーティングシステムが混在する展開環境では、ユーザープロファイルの一部がすべてのオペレーティングシステムで共有されるように構成できます。プロファイルの残りの部分は共有されず、単一のオペレーティングシステムでのみ使用されます。異なるオペレーティングシステム上で一貫したユーザーエクスペリエンスを提供するには、オペレーティングシステムごとに異なる構成が必要です。これを詳細なフォルダーリダイレクトと呼びます。たとえば、2 つのオペレーティングシステム上で使用される異なるバージョンのアプリケーションで共通のファイルがロードされるようにするには、そのファイルをネットワーク上の単一の場所にリダイレクトします。また、［スタートメニュー］フォルダーの構造が 2 つのオペレーティングシステムで異なる場合は、どちらか一方のオペレーティングシステムのフォルダーのみがリダイレクトされるように設定できます。これにより、各オペレーティングシステムでこのフォルダーおよびその内容が分離され、ユーザーに一貫したエクスペリエンスを提供できます。

詳細なフォルダーリダイレクトを使用する場合は、ユーザープロファイル内のデータ構造を理解して、どの部分をオペレーティングシステム間で共有できるかを確認する必要があります。これは、フォルダーリダイレクトによる予期せぬ問題の発生を避けるために重要です。

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
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存したゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- オペレーティングシステム間で共有されるフォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「アドレス帳」フォルダーと「お気に入り」フォルダーのリダイレクトを設定する前に、異なるバージョンの Outlook と Internet Explorer でユーザーデータのフォルダー構造を確認してください。
  - 「マイドキュメント」、「マイミュージック」、「マイピクチャ」、および「マイビデオ」の各フォルダーの構造はこれらのオペレーティングシステムで共通なので、両方のデリバリーグループで同じネットワーク

共有にリダイレクトできます。

- オペレーティングシステム間で共有できないフォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「デスクトップ」、「リンク」、「検索」、および「スタートメニュー」の各フォルダーの構造はこれらのオペレーティングシステムで異なるため、Windows Server 2008 用のデリバリーグループではリダイレクトされないように設定します。これにより、これらのデータは共有されなくなります。
  - 予期せぬ問題の発生を避けるため、これらのフォルダーは Windows 8 用のデリバリーグループでのみリダイレクトします。これは、通常の業務ではユーザーが Windows 8 を使用することが多く、Windows Server 2008 で提供されるアプリケーションには頻繁にアクセスしないためです。また、これらのデータは、アプリケーション環境よりもデスクトップ環境のものの方が実用的です。たとえば、デスクトップ上のショートカットは「デスクトップ」フォルダーに格納されるため、Windows Server 2008 マシンよりも Windows 8 マシンのデスクトップショートカットをリダイレクトした方が便利です。
- 以下のフォルダーは、オペレーティングシステム間での共有に向いていません。
  - ユーザーがダウンロードしたファイルがサーバー上にコピーされるのを防ぐため、「ダウンロード」フォルダーはリダイレクトしません。
  - 個々のアプリケーションのデータにより互換性やパフォーマンス上の問題が生じることがあるので、「アプリケーションデータ」フォルダーはリダイレクトしません。

詳しくは、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766489(v=ws.10)?redirectedfrom=MSDNを参照してください。

フォルダーリダイレクトと除外設定

Studio 外で 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

August 24, 2021

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrix が提供するプラットフォームです。この計測機能と利用統計情報機能を使用することで、技術ユーザー（顧客、パートナー、エンジニア）は自己診断を行い、問題を解決し、環境を最適化することができます。CIS の詳細、最新情報、および機能について詳しくは、https://cis.citrix.comを参照してください（Citrix アカウントの資格情報が必要です）。

Citrix Insight Services で提供される機能は拡大と進化を続けており、今や Citrix Smart Tools に不可欠な要素となっています。Citrix Smart Tools では展開タスク、ヘルスチェック、電源管理を自動化できます。これらのテクノロジについては、Citrix Smart Tools のドキュメントを参照してください。

Citrix にアップロードされた情報はすべて、トラブルシューティングや診断、および以下の対象となる製品の品質、信頼性、パフォーマンス向上を目的として使用されます。

- Citrix Insight Services ポリシー：https://cis.citrix.com/legal
- Citrix のプライバシーポリシー：https://www.citrix.com/about/legal/privacy.html

この XenApp および XenDesktop のリリースでは、以下のツールと技術がサポートされます。

- XenApp および XenDesktop のインストールとアップグレードの分析
- Citrix カスタマーエクスペリエンス向上プログラム
- Citrix Smart Tools
- Citrix Call Home（Citrix Smart Tools の一部）
- Citrix Scout

インストールとアップグレード分析

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

この情報は、ローカルの%ProgramData%\Citrix\CTQs に保存されます。

このデータの自動アップロードは、全製品インストーラーのグラフィックおよびコマンドラインインターフェイスの両方で、デフォルトで有効です。

- デフォルト値はレジストリ設定で変更できます。インストール/アップグレードの前にレジストリ設定を変更すると、全製品インストーラーの使用時にその値が使用されます。
- コマンドラインインターフェイスを使用して、コマンドにオプションを指定してインストール/アップグレードする場合、デフォルト設定をオーバーライドできます。

インストール/アップグレード分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）：

場所：HKLM:\Software\Citrix\MetaInstall
Name：SendExperienceMetrics
Value：0 = 無効、1 = 有効

PowerShell を使用する場合、次のコマンドレットはインストール/アップグレード分析機能の自動アップロードを無効にします。

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0

XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、/disableexperiencemetrics オプションを含めます。

XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、/sendexperiencemetrics オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム（**CEIP**）

Citrix 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、シトリックス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、https://more.citrix.com/XD-CEIPを参照してください。

サイトの作成中またはアップグレード中の登録

XenApp または XenDesktop サイトを作成するときに、自動的に CEIP に登録されます（最初の Delivery Controller のインストール後）。サイトの作成からおよそ 7 日後に、初回データアップロードが行われます。このプログラムへの参加の停止はサイト作成後いつでも自由に行えます。［製品サポート］タブの Studio のナビゲーションペインで ［構成］ノードを選択して、表示される手順に従ってください。

XenApp または XenDesktop 展開をアップグレードする場合は次のようになります:

- CEIP をサポートしないバージョンからアップグレードする場合、参加するかどうかを確認するメッセージが表示されます。
- CEIP をサポートするバージョンからアップグレードし、参加が有効になっていた場合、CEIP はアップグレードしたサイトで有効になります。
- CEIP をサポートするバージョンからアップグレードし、参加が無効になっていた場合、CEIP はアップグレードしたサイトでは無効になります。
- CEIP をサポートするバージョンからアップグレードし、参加が不明な場合、参加するかどうかを確認するメッセージが表示されます。

収集された情報は匿名になるため、Citrix Insight Services へのアップグレード後は表示されません。

VDA のインストール時の登録

デフォルトでは、ユーザーは Windows VDA のインストール時に CEIP に自動登録されます。このデフォルトはレジストリ設定で変更できます。VDA インストールの前にレジストリ設定を変更すると、その値が使用されます。

CEIP への自動登録を制御するレジストリ設定（デフォルト = 1）:

場所：HKLM:\Software\Citrix\Telemetry\CEIP
Name：Enabled
Value：0 = 無効、1 = 有効

デフォルトで、「Enabled」プロパティはレジストリに表示されません。未指定のままの場合、自動アップロード機能は有効です。

PowerShell を使用する場合、次のコマンドレットは CEIP への登録を無効にします。

New-ItemProperty -Path HKEY_LOCAL_MACHINE:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0

収集されたランタイムデータポイントは、定期的に出力フォルダ（デフォルトは%programdata%/Citrix/VdaCeip）にファイルとして書き込まれます。

VDA のインストールからおよそ 7 日後に、初回データアップロードが行われます。

他の製品およびコンポーネントのインストール時の登録

CEIP へは、関連する Citrix 製品、コンポーネント、テクノロジ（Provisioning Services、AppDNA、Citrix License Server、Citrix Receiver for Windows、ユニバーサルプリントサーバー、Session Recording）のインストール時にも参加できます。インストールと参加のデフォルト値について詳しくは、該当のドキュメントを参照してください。

Citrix Smart Tools

Delivery Controller のインストール時に、Smart Tools のアクセスを有効にできます。

Smart Tools のアクセス（およびまだ有効でない場合には Call Home への参加）を有効にするオプションは、デフォルトで選択されています。［接続］をクリックします。ブラウザーウィンドウが開いて、［Smart Services］Web ページに自動的に移動します。ここで、Citrix Cloud アカウントの資格情報を入力します。（Citrix Cloud アカウントをお持ちでない場合、Citrix アカウントの資格情報を入力すると、新しい Citrix Cloud アカウントが自動的に作成されます）。認証後、Smart Tools Agent ディレクトリに証明書がサイレントインストールされます。

Smart Tools テクノロジの使用方法については、Smart Tools のドキュメントを参照してください。

Citrix Call Home

XenApp または XenDesktop で特定のコンポーネントおよび機能をインストールする場合、Citrix Call Home に参加するかどうかを選択できるページが表示されます。Call Home は診断データを収集し、その後そのデータを含む利用統計情報パッケージを、分析およびトラブルシューティングの目的で定期的に Citrix Insight Services に直接アップロードします（デフォルトポート 443 上の HTTPS 経由）。

XenApp および XenDesktop では、Call Home は Citrix Telemetry Service という名前のバックグラウンドサービスとして実行されます。詳しくは、https://more.citrix.com/XD-CALLHOMEを参照してください。

Citrix Scout では、Call Home のスケジュール機能も使用できます。詳しくは、「Citrix Scout」を参照してください。

収集される項目

Citrix Diagnostic Facility（CDF）トレースは、トラブルシューティングに役立つ情報を記録します。Call Home は、一般的な障害（VDA の登録やアプリケーション/デスクトップの起動など）のトラブルシューティングに役立つ CDF トレースのサブセットを収集します。このテクノロジは、常時トレース（AOT）と呼ばれます。Call Home で

はその他の Event Tracing for Windows（ETW）情報が収集されることはなく、収集されるように設定することもできません。

また、Call Home では以下の情報も収集されます:

- XenApp および XenDesktop によって HKEY_LOCAL_MACHINE\SOFTWARE\Citrix で作成されたレジストリ
- Citrix 名前空間の Windows Management Instrumentation（WMI）情報
- 実行中のプロセス一覧
- %PROGRAM DATA%\Citrix\CDF に保存されている Citrix プロセスのクラッシュダンプ

トレース情報は収集時に圧縮されます。Citrix Telemetry Service は、最長 8 日間、圧縮されたトレース情報を最大 10MB 保持します。

- データを圧縮することで、Call Home の VDA 上の占有領域を小さくできます。
- プロビジョニングされたマシンでの IOP を避けるため、トレースはメモリで保持されます。
- トレースバッファでは、循環メカニズムを使用してトレースがメモリで保持されます。

Call Home は、「Call Home のキーデータポイント」に記載のキーデータポイントを収集します。

サマリーの構成と管理

全製品インストールウィザードの使用時、またはそれ以降に、PowerShell コマンドレットを使用して、Call Home に登録することができます。登録すると、デフォルトで、ローカルタイムの毎日曜日午前 3 時頃に診断情報が収集され、Citrix にアップロードされます。アップロードは、指定された時間の前後 2 時間以内に行われます。つまり、デフォルトのスケジュールの場合、アップロードは午前 3 時から午前 5 時の間に行われます。

診断情報をスケジュールベースでアップロードしない場合（またはスケジュールを変更する場合）は、PowerShell コマンドレットを使用して診断情報を手動で収集し、アップロードするかローカルに保存してください。

Call Home のスケジュールによるアップロード登録する場合、および診断情報を手動で Citrix にアップロードする場合は、Citrix のアカウントまたは Citrix Cloud の資格情報を入力します。Citrix は、アカウント資格情報を、顧客の識別とデータのアップロードに使用されるアップロードトークンに交換します。アカウント資格情報は保存されません。

アップロードが実行されると、Citrix アカウントに関連付けられたアドレスに通知メールが送信されます。

前提条件

- PowerShell 3.0 またはそれ以降が実行されている必要があります。
- Citrix Telemetry Service が実行されている必要があります。
- システム変数 PSModulePath は、C:\Program Files\Citrix\Telemetry Service\などの、Telemetry のインストールパスに設定する必要があります。

コンポーネントインストール時の **Call Home** の有効化

VDA のインストールまたはアップグレード時：全製品インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする場合には、Call Home に参加するかどうかを確認するメッセージが表示されます。2 つのオプションがあります。

- Call Home に参加します。
- Call Home に参加しません。

VDA をアップグレードしていて、Call Home に以前参加していた場合には、そのウィザードページは表示されません。

Controller のインストールまたはアップグレード時：グラフィカルインターフェイスを使用して Delivery Controller をインストールまたはアップグレードする場合には、Call Home に参加するかどうか、および Citrix Smart Tools に接続するかどうかを確認するメッセージが表示されます。3 つのオプションがあります。

- Citrix Smart Tools に接続する。これには、Smart Tools エージェントを介した Call Home 機能が含まれます。これがデフォルトで、推奨されるオプションです。このオプションを選択すると、Smart Tools エージェントが構成されます。（このオプションが選択されているかどうかに関わらず、Smart Tools エージェントはインストールされます）。
- Call Home に参加するのみで、Smart Tools には接続しない。このオプションを選択すると、Smart Tools エージェントはインストールされますが、構成されません。Call Home 機能は Citrix Telemetry Service および Citrix Insight Services を介して提供されます。
- Smart Tools に接続しない、または Call Home に参加しない。

Controller をインストールする場合、そのサーバーがポリシー設定「サービスとしてログオン」が適用される Active Directory GPO を持っていると、インストールウィザードで Call Home ページ上の情報を構成できません。詳しくは、CTX218094を参照してください。

Controller をアップグレードしていて、Call Home に以前登録していた場合、Smart Tools に関することのみを確認するメッセージが表示されます。Call Home に登録済みで、Smart Agent が既にインストールされている場合、ウィザードページは表示されません。

Smart Tools については、Smart Tools のドキュメントを参照してください。

PowerShell コマンドレット

各コマンドレットの説明や、上記の一般的なユースケースでは使用されないパラメーターを含む包括的な構文は、PowerShell ヘルプに記載されています。

プロキシサーバーを使用してアップグレードする方法については、「プロキシサーバーの構成」を参照してください。

スケジュールによるアップロードの有効化

収集された診断情報は、シトリックスに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。


```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
```

スケジュールによるアップロードが有効になっていることを確認するには「Get-CitrixCallHome」と入力します。有効な場合は、「IsEnabled=True」および「IsMasterImage=False」が返されます。

マスターイメージから作成されたマシンに対するスケジュールによるアップロードの有効化

マスターイメージでのスケジュールによるアップロードを有効にすると、マシンカタログで作成された各マシンを構成する必要がなくなります。

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

スケジュールによるアップロードが有効になっていることを確認するには「Get-CitrixCallHome」と入力します。有効な場合は、「IsEnabled=True」および「IsMasterImage=True」が返されます。

カスタムスケジュールの作成

診断情報の収集およびアップロードのスケジュールを、日次または週次で作成できます。

```
$timespan = New-TimeSpan –Hours <hours> -Minutes <minutes>
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek <day> -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しても、PowerShell コマンドレットを使用して診断データをアップロードできます。

```
Disable-CitrixCallHome
```

スケジュールによるアップロードが無効になっていることを確認するには、「Get-CitrixCallHome」と入力します。無効な場合は、「IsEnabled=False」および「IsMasterImage=False」が返されます。

例

次のコマンドレットでは、毎日午後 11 時 20 分にデータを収集してアップロードするスケジュールが作成されます。Hours パラメーターには、24 時間形式を使用します。UploadFrequency パラメーターの値が Daily の場合、DayOfWeek パラメーターは無視されます（指定されている場合）。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上述の例の場合、「Start-Time=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
```

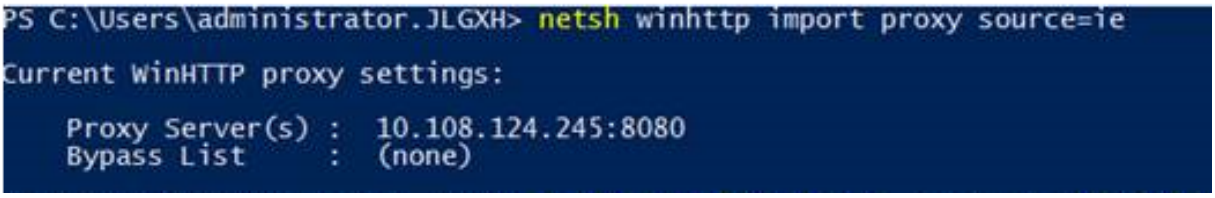
スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上述の例の場合、「Start-Time=22:20:00」、「DayOfWeek=Wednesday」、「Upload Frequency=Weekly」が返されます。

Call Home のアップロードのためにプロキシサーバーを構成

Call Home が有効に設定されたマシンで、以下のタスクを実行します。以下の手順のサンプル図では、サーバーアドレスおよびポートは 10.158.139.37:3128 となっています。お客様の情報はこれとは異なります。

手順 **1**: Web ブラウザーにプロキシサーバー情報を追加します。Internet Explorer で、［インターネットオプション］**>**［接続］**>**［**LAN** の設定］の順に選択します。［**LAN** にプロキシサーバーを使用する］をオンにして、プロキシサーバーのアドレスとポート番号を入力します。

手順 **2**: PowerShell で、**netsh winhttp import proxy source=ie** を実行します。



手順 **3**: テキストエディターを使用して、TelemetryService.exe 構成ファイルを編集します。このファイルは、C:\Program Files\Citrix\Telemetry Service にあります。以下の赤いボックス内に示す情報を追加します。

手順 **4**: Telemetry Service を再起動します。

PowerShell で Call Home コマンドレットを実行します。

手動による診断情報の収集およびアップロード

CIS Web サイトを使用して、診断情報のバンドルを CIS にアップロードすることができます。PowerShell コマンドレットを使って、診断情報を収集して CIS にアップロードすることもできます。

CIS Web サイトを使用してバンドルをアップロードするには、以下の手順に従います。

1. Citrix のアカウント資格情報を使用して Citrix Insight Services にログオンします。
2. [**My Workspace**] を選択します。
3. [**Healthcheck**] 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（パッケージ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] <PSCredential> [-InputPath <String>] [-Description <String>] [-IncidentTime <String>] [-SRNumber <String>] [-Name <String>] [-UploadHeader <String>] [-AppendHeaders <String>] [-Collect <String>] [<CommonParameters>]

データの収集およびローカルへの保存

Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath <String>] [-Description <String>] [-IncidentTime <String>] [-SRNumber <String>] [-Name <String>] [-UploaderHeader <String>] [-AppendHeaders <String>] [-Collect <String>] [<CommonParameters>]

パラメーター	説明
資格情報	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	シトリックス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。ここで、Boolean は true または false です。有効な collector 値は、’wmi’、’process’、’registry’、’crashreport’、’trace’、’localdata’、’sitedata’、’sfb’ です。デフォルトでは、’sfb’ 以外のすべての collector が有効です。’sfb’ collector は、Skype for Business の問題を診断するためにオンデマンドで使用するよう設計されています。’sfb’ collector は、’enabled’ パラメーターに加えて、ターゲットユーザーを指定する’account’ パラメーターと’accounts’ パラメーターをサポートします。次のいずれかのフォームを使用してください：”-Collect “{‘sfb’:{‘account’:’domain\user1’}}”、-Collect “{‘sfb’:{‘accounts’:[‘domain\user1’, ‘domain\user2’]}}”
一般的なパラメーター	PowerShell のヘルプを参照してください。

以前ローカルに保存されたデータのアップロード

Send-CitrixCallHomeBundle -Credential <PSCredential> -Path <String> [<CommonParameters>]

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。保存されるパッケージには、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パッケージがアップロードされます。

$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip

Citrix Scout

詳しくは、「Citrix Scout」を参照してください。

Citrix Scout

October 22, 2021

はじめに

Citrix Scout では、XenApp および XenDesktop 展開環境での予防的な保守に使用できる診断データを収集します。シトリックスでは、Citrix Insight Services を通じて包括的な自動分析機能を提供しています。Scout を使用して、お客様単独で、または Citrix Support の支援を受けながら問題のトラブルシューティングを行うこともできます。収集ファイルを Citrix にアップロードすると、Citrix Support による分析と支援を受けることができます。ま

たは、収集ファイルをローカルに保存してお客様自身でレビューを行い、その後 Citrix にアップロードして分析を受けることもできます。

Scout には 3 つの主要手順があります。

- 収集：サイト内の選択したマシン上で 1 度だけ診断情報収集を実行します。次に、収集した情報が含まれるファイルを Citrix にアップロードするか、ローカルに保存します。
- トレースおよび再現：選択したマシン上で手動でトレースを開始します。次に、そのマシン上で問題を再現します。問題を再現すると、トレースは停止します。次に、Scout はその他の診断情報を収集し、トレース情報と収集情報を含むファイルを Citrix にアップロードするか、ローカルに保存します。
- スケジュール：選択したマシン上で、日次または週次の指定時刻に診断情報を収集するようスケジュールを設定します。それぞれの収集情報を含むファイルは自動で Citrix にアップロードされます。

この記事で説明するグラフィカルインターフェイスは、Scout を使用する初歩的な手段です。代わりに PowerShell インターフェイスを使用して、診断情報の収集とアップロードを一度だけまたは定期的に実行するように構成することもできます。「Call Home」を参照してください。

Scout は次の場所で実行します：

- オンプレミスの XenApp および XenDesktop 展開環境では、1 つまたは複数の Virtual Delivery Agent（VDA）および Delivery Controller から診断情報を収集する場合は、Delivery Controller から Scout を実行します。VDA から Scout を実行してローカルの診断情報を収集することもできます。
- XenApp および XenDesktop サービスを使用する Citrix Cloud 環境では、Scout を VDA から実行してローカルの診断情報を収集します。

収集される項目

Scout により収集される診断情報には、Citrix Diagnostic Facility（CDF）のトレースログファイルが含まれます。常時トレース（AOT）と呼ばれる CDF トレースファイルのサブセットも対象となります。AOT の情報は、VDA の登録やアプリケーションまたはデスクトップの起動など、よくある問題の解決に役立ちます。その他の Event Tracing for Windows（ETW）情報が収集されることはありません。

収集される情報は次のとおりです：

- XenApp および XenDesktop によって HKEY_LOCAL_MACHINE\SOFTWARE\Citrix 以下に作成されたレジストリ
- Citrix 名前空間の Windows Management Instrumentation（WMI）情報
- 実行中のプロセス
- %PROGRAM DATA%\Citrix\CDF に保存されている Citrix プロセスのクラッシュダンプ

トレース情報の概要を以下に示します。

- マシン上の占有領域を抑えるため、トレース情報は収集時に圧縮されます。
- Citrix Telemetry Service は、最長 8 日間、圧縮されたトレース情報を各マシン上に最大 10MB 保持します。
- プロビジョニングされたマシンでの IOP を避けるため、トレースはメモリで保持されます。

- トレースバッファーでは、循環メカニズムを使用してトレースがメモリで保持されます。

Scout で収集されるデータポイントの一覧については、「Scout のキーデータポイント」を参照してください。

要件と考慮事項

権限

- 診断情報の収集元になる各マシンのローカル管理者およびドメインユーザーである必要があります。
- 各マシン上の LocalAppData ディレクトリに書き込む権限がある必要があります。
- Scout の起動時には ［管理者として実行］ を使用してください。

診断情報の収集元になる各マシンには、次が必要です。

- Scout は当該マシンと通信できる必要があります。
- ファイルとプリンターの共有は設定されている必要があります。
- PSRemoting と WinRM は有効になっている必要があります。PowerShell 3.0 以降が実行されている必要もあります。
- Citrix Telemetry Service が実行されている必要があります。
- 診断情報の収集のスケジュールを設定するには、XenApp および XenDesktop 7.14 以降でサポートされるバージョンで提供される Scout のバージョンが実行されている必要があります。

Scout では指定したマシン上で確認テストが実行され、これらの要件が満たされているか確認されます。

確認テスト

診断情報の収集の開始前に、指定した各マシンについて自動で確認テストが実行されます。これらのテストで、上記の要件が満たされているか確認されます。あるマシンでテストが失敗した場合、Scout には修正アクション案を含むメッセージが表示されます。

エラーメッセージ	修正アクション
Scout はこのマシンに接続できません	マシンの電源が入っていることを確認します。ネットワーク接続が正しく動作していることを確認します。（これにはファイアウォールが正しく構成されていることを含みます。）ファイルおよびプリンターの共有が設定されていることを確認します。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。
PSRemoting および WinRM を有効にする	PowerShell リモート処理と WinRM を同時に有効にすることができます。**Enable-PSRemoting** コマンドレットを、［管理者として実行］ で実行します。詳しくは、Microsoft のコマンドレットのヘルプを参照してください。

エラーメッセージ	修正アクション
Scout には PowerShell 3.0 以降が必要です	マシンに PowerShell 3.0（以降）をインストールして、PowerShell リモート処理を有効にします。
このマシンの LocalAppData ディレクトリにアクセスできません	マシン上の LocalAppData ディレクトリに書き込む権限がアカウントにあることを確認してください。
Citrix Telemetry Service が見つかりません	Citrix Telemetry Service がマシンにインストールされ、開始されたことを確認してください。
スケジュールを取得できません	マシンを XenApp および XenDesktop 7.14 以降にアップグレードしてください。

バージョンの互換性

本バージョンの Scout（3.x）は、XenApp および XenDesktop 7.14 以降の Controller と VDA 上での実行を想定しています。

旧バージョンの Scout は、過去の XenApp および XenDesktop 展開で提供されています。旧バージョンについて詳しくは、CTX130147を参照してください。

バージョン 7.14 より前の Controller または VDA をバージョン 7.14（以降のサポートするバージョン）にアップグレードすると、旧バージョンの Scout が最新バージョンに置き換えられます。

機能	Scout 2.23	Scout 3.0
XenApp および XenDesktop 7.14 以降のサポート	はい	はい
XenDesktop 5.x、7.1～7.13 のサポート	はい	いいえ
XenApp 6.x、7.5～7.13 のサポート	はい	いいえ
製品への同梱	7.1～7.13	7.14 以降
CTX 記事からのダウンロード	はい	いいえ
CDF トレースのキャプチャ	はい	はい
常時トレース（AOT）のキャプチャ	いいえ	はい
診断データの収集対象	一度に 10 台のマシンまで（デフォルト）	無制限（リソースの可用性に依存）
Citrix への診断データの送信	はい	はい
診断データのローカルへの保存	はい	はい

機能	Scout 2.23	Scout 3.0
Citrix Cloud 資格情報のサポート	いいえ	はい
Citrix の資格情報のサポート	はい	はい
アップロード用プロキシサーバーのサポート	はい	はい
スケジュールの調整	-	はい
スクリプトのサポート	コマンドライン（ローカルの Controller のみ）	Call Home コマンドレットを使用した PowerShell（テレメトリをインストール済みのすべてのマシン）

インストール

デフォルトでは、Scout は VDA または Controller のインストール時に Citrix Telemetry Service の一部として自動でインストールされます。

VDA のインストール時に Citrix Telemetry Service を除外した場合、またはこのサービスを後で削除した場合には、XenApp または XenDesktop ISO の x64\Virtual Desktop Components フォルダーまたは x86\Virtual Desktop Components フォルダーにある TelemetryServiceInstaller_xx.msi を実行します。

アップロードの認証

収集した診断情報を Citrix にアップロードする場合、Citrix または Citrix Cloud のアカウントが必要になります（これらのアカウントは、Citrix ダウンロードまたは Citrix Cloud Control Center へのアクセス時に使用する資格情報です）。アカウントの資格情報の検証後、トークンが発行されます。

- Citrix アカウントを使用して認証を行う場合、トークンの発行プロセスは表示されません。アカウント資格情報を入力するだけで済みます。Citrix で資格情報が検証されると、Scout ウィザードの手順を進めることができるようになります。
- Citrix Cloud アカウントを使用して認証を行う場合はリンクをクリックし、HTTPS を使用してデフォルトのブラウザーで Citrix Cloud にアクセスします。Citrix Cloud 資格情報を入力すると、トークンが表示されます。このトークンをコピーして Scout に貼り付けます。Scout ウィザードの手順を進めることができるようになります。

トークンは、Scout が実行されているマシンにローカルに保存されます。このトークンを次回も使用するには、［収集］または ［トレースおよび再現］を選択してから、［トークンを保存して次回以降この手順を省略する］チェックボックスをオンにします。

Scout の開始ページで ［スケジュール］を選択するたびに再度認証を行う必要があります。スケジュールの作成時または変更時には、保存したトークンは使用できません。

アップロードでのプロキシの使用

プロキシサーバーを使用して Citrix へ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。

診断の収集

収集の手順では、マシンを選択し、診断情報の収集を開始してから、収集結果のファイルをシトリックスにアップロードするかローカルに保存します。

手順 **1**：**Scout** の起動。

マシンの［スタート］メニューで ［**Citrix**］**>** ［**Citrix Scout**］の順に選択します。開始ページで ［収集］をクリックします。

手順 **2**：マシンの選択。

［マシンの選択］ページには、サイト内にあるすべての VDA と Controller が一覧表示されます。表示される項目をマシン名で絞り込むことができます。診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。確認テストで不合格になると、［状態］列にメッセージが表示され該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報は収集されません。

確認テストが完了したら、［続行］をクリックします。

手順 **3**：マシンの診断データの収集。

概要に、診断情報の収集元になるマシン（選択し、確認テストに合格したマシン）がすべて一覧表示されます。［収集の開始］をクリックします。

収集は以下のように進行します。

- ［状態］列には、マシンの現在の収集状態が表示されます。
- 1 台のマシンで進行中の収集を停止するには、そのマシンの［操作］列の ［キャンセル］をクリックします。
- 進行中の収集をすべて停止するには、ページの右下隅にある ［収集の停止］をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの［操作］列で ［再試行］をクリックします。
- すべての選択したマシンで収集が完了すると、右下隅にある ［収集の停止］が ［続行］に変わります。
- あるマシンの収集が正常に完了した場合にそのマシンの診断情報を再び収集するには、該当するマシンの［操作］列で ［再収集］をクリックします。新しい収集情報によって過去の収集情報が上書きされます。

- 収集が失敗した場合は、［操作］列の ［再試行］をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。
- すべてのマシンで収集が完了した後に、［戻る］をクリックしないでください。このボタンをクリックしてプロンプトで確定すると、収集した情報が失われます。

収集が完了したら、［続行］をクリックします。

手順 **4**：収集情報の保存またはアップロード。

収集した診断情報が含まれるファイルを Citrix にアップロードするか、ローカルのマシンに保存するかを選択します。

このファイルをすぐにアップロードすることを選択した場合は、手順 5 に進んでください。

このファイルをローカルに保存することを選択した場合は、次の操作を行います。

- Windows の［保存］ダイアログボックスが開きます。保存場所を指定します。
- ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。ファイルは後で Citrix からアップロードできます。Citrix Insight Services の場合はCTX136396を、それ以外の場合は「Smart Tools サポート」を参照してください。

［完了］をクリックして Scout の開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

手順 **5**：アップロードの認証とプロキシの指定（オプション）。

このプロセスについて詳しくは、「アップロードの認証」を参照してください。

- 以前に Scout で認証を行ったことがない場合は、以下の手順を実行します。
- 以前に Scout で認証を行っている場合、デフォルトでは保存済みの認証トークンが使用されます。これで問題がない場合はこのオプションを選択し、［続行］をクリックします。今回の収集では資格情報は求められません。手順 6 に進んでください。
- 以前に認証を行っているものの、再度認証を行って新しいトークンを発行する場合は、［変更/再認証］をクリックして以下の手順を実行します。

アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。プロキシサーバーを使用して Citrix へ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトのブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
- Citrix アカウントの場合はお使いの資格情報を入力します。

入力が完了したら、［続行］をクリックします。

手順 **6**：アップロードに関する情報の指定。

アップロードの詳細を入力します。

- ［名前］フィールドには、収集した情報が含まれるファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
- オプションとして、8 桁の Citrix Support ケース番号を指定します。
- 該当する場合、オプションの［説明］フィールドに問題の詳細と発生時期を入力します。

完了したら、［アップロードの開始］をクリックします。

アップロード中、ページの左下にアップロードのおおよそ何% が完了したかが表示されます。進行中のアップロードをキャンセルするには、［アップロードの停止］をクリックします。

アップロードが完了すると、アップロード先の URL リンクが表示されます。この Citrix のアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

［完了］をクリックして Scout の開始ページに戻ります。

トレースと再現

トレースと再現の手順では、マシンを選択し、選択したマシンでトレースを開始して問題を再現し、診断情報の収集を開始してから、トレースと収集情報が含まれるファイルを Citrix にアップロードするかローカルに保存します。

この手順は、標準の収集手順と同様です。ただし、マシン上でトレースを開始し、問題を再現することができます。すべての収集される診断情報には AOT トレース情報が含まれますが、この手順ではトラブルシューティングに役立つ CDF トレースも追加されます。

手順 **1**：**Scout** の起動。

マシンの［スタート］メニューで［**Citrix**］**>**［**Citrix Scout**］の順に選択します。開始ページで、［トレースと再現］をクリックします。

手順 **2**：マシンの選択。

［マシンの選択］ページには、サイト内にあるすべての VDA と Controller が一覧表示されます。表示される項目をマシン名で絞り込むことができます。トレースと診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

選択した各マシン上で確認テストが開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報とトレースは収集されません。

確認テストが完了したら、［続行］をクリックします。

手順 **3**：トレース。

概要に、トレースの収集対象になるすべてのマシンが一覧表示されます。［トレースの開始］をクリックします。

選択した 1 台または複数台のマシンで、経験した問題を再現します。この間もトレースの収集は継続されています。問題の再現が完了したら、Scout で ［続行］をクリックします。これによりトレースが停止されます。

トレースの停止後、このトレース中に問題を再現したかどうかを指定します。

手順 **4**：マシンの診断データの収集。

［収集の開始］をクリックします。

収集は以下のように進行します。

- ［状態］列には、マシンの現在の収集状態が表示されます。
- 1 台のマシンで進行中の収集を停止するには、そのマシンの［操作］列の ［キャンセル］をクリックします。
- 進行中の収集をすべて停止するには、ページの右下隅にある ［収集の停止］をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの［操作］列で ［再試行］をクリックします。
- すべての選択したマシンで収集が完了すると、右下隅にある ［収集の停止］が ［続行］に変わります。
- あるマシンの収集が正常に完了した場合にそのマシンの診断情報を再び収集するには、該当するマシンの［操作］列で ［再収集］をクリックします。新しい収集情報によって過去の収集情報が上書きされます。
- 収集が失敗した場合は、［操作］列の ［再試行］をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。
- すべてのマシンで収集が完了した後に、［戻る］ボタンをクリックしないでください。このボタンをクリックしてプロンプトで確定すると、収集した情報が失われます。

収集が完了したら、［続行］をクリックします。

手順 **5**：収集情報の保存またはアップロード。

収集した診断情報が含まれるファイルを Citrix にアップロードするか、ローカルのマシンに保存するかを選択します。

このファイルをすぐにアップロードすることを選択した場合は、手順 6 に進んでください。

このファイルをローカルに保存することを選択した場合は、次の操作を行います。

- Windows の［保存］ダイアログボックスが開きます。保存先を選択します。
- ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。注：ファイルは後で Citrix からアップロードできます。Citrix Insight Services の場合はCTX136396を、それ以外の場合は「Citrix Smart Tools」を参照してください。

［完了］をクリックして Scout の開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

手順 **6**：アップロードの認証とプロキシの指定（オプション）。

このプロセスについて詳しくは、「アップロードの認証」を参照してください。

- 以前に Scout で認証を行ったことがない場合は、以下の手順を実行します。
- 以前に Scout で認証を行っている場合、デフォルトでは保存済みの認証トークンが使用されます。これで問題がない場合はこのオプションを選択し、［続行］をクリックします。今回の収集では資格情報は求められません。手順 7 に進んでください。
- 以前に認証を行っているものの、再度認証を行って新しいトークンを発行する場合は、［変更/再認証］をクリックして以下の手順を実行します。

アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。プロキシサーバーを使用して Citrix へ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトのブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
- Citrix アカウントの場合はお使いの資格情報を入力します。

入力が完了したら、［続行］をクリックします。

手順 **7**：アップロードに関する情報の指定。

アップロードの詳細を入力します。

- ［名前］フィールドには、収集した情報が含まれるファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
- オプションとして、8 桁の Citrix Support ケース番号を指定します。
- 該当する場合、オプションの［説明］フィールドに問題の詳細と発生時期を入力します。

完了したら、［アップロードの開始］をクリックします。

アップロード中、ページの左下にアップロードのおおよそ何% が完了したかが表示されます。進行中のアップロードをキャンセルするには、［アップロードの停止］をクリックします。

アップロードが完了すると、アップロード先の URL リンクが表示されます。この Citrix のアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

［完了］をクリックして Scout の開始ページに戻ります。

収集スケジュールの設定

スケジュール設定手順では、マシンを選択し、スケジュールを設定またはキャンセルします。スケジュールで収集された診断情報は、Citrix に自動的にアップロードされます（PowerShell インターフェイスを使用すると、スケジュ

ールにより収集されたデータをローカルに保存できます。「Citrix Call Home」を参照してください。）

手順 **1**：**Scout** の起動。

マシンの［スタート］メニューで ［**Citrix**］**>**［**Citrix Scout**］の順に選択します。開始ページで ［スケジュール］をクリックします。

手順 **2**：マシンの選択。

［マシンの選択］ページには、サイト内にあるすべての VDA と Controller が一覧表示されます。表示される項目をマシン名で絞り込むことができます。

グラフィカルインターフェイスを使用して VDA および Controller をインストールした場合、Call Home への参加に関する情報が表示されます。詳しくは、「Citrix Call Home」を参照してください（Call Home には Scout と同等のスケジュール設定機能が含まれています）。デフォルトでは、Scout にはこれらの設定が表示されます。このバージョンの Scout では、スケジュール済みの収集を初めて開始するか、構成済みのスケジュールを変更できます。

Call Home はマシンごとに有効化または無効化しますが、Scout のスケジュール設定でも同じコマンドを使用します。ただし、選択したマシンすべてがコマンドの影響を受けます。

診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

選択した各マシン上で確認テストが開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います。

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報（またはトレース）は収集されません。

確認テストが完了したら、［続行］をクリックします。

［概要］ページに、スケジュールが適用されるマシンが一覧表示されます。［続行］をクリックします。

手順 **3**：スケジュールの設定。

診断情報を収集するタイミングを指定します。注：スケジュールは選択したマシンすべてに影響します。

- 選択したマシンについて週次のスケジュールを構成するには、［毎週］をクリックします。曜日を選択し、診断情報の収集を開始する時刻（24 時間形式）を入力します。
- 選択したマシンについて日次のスケジュールを構成するには、［毎日］をクリックします。診断情報の収集を開始する時刻（24 時間形式）を入力します。
- （別のスケジュールに置き換えずに）選択したマシンの既存のスケジュールをキャンセルするには、［オフ］をクリックします。選択したマシンで構成済みのスケジュールがすべてキャンセルされます。

［続行］をクリックします。

手順 **4**：アップロードの認証とプロキシの指定（オプション）。

このプロセスについて詳しくは、「アップロードの認証」を参照してください。注：Scout のスケジュールを使用する場合、保存済みのトークンを使用して認証を行うことはできません。

アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。プロキシサーバーを使用して Citrix へ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトのブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
- Citrix アカウントの場合はお使いの資格情報を入力します。

入力が完了したら、［続行］をクリックします。

構成済みのスケジュールを確認します。［完了］をクリックして Scout の開始ページに戻ります。

スケジュールした収集が行われるたびに、選択した各マシンの Windows アプリケーションログに収集とアップロードの情報が書き込まれます。

モニター

August 24, 2021

管理者およびヘルプデスク担当者は、さまざまな機能やツールを使用して、XenApp や XenDesktop のサイトをモニターできます。これらのツールを使って、モニターできるものは以下のとおりです。

- ユーザーセッションおよびセッションの利用状況
- ログオン処理のパフォーマンス
- 接続とマシン（エラーを含む）
- 負荷評価
- 履歴傾向
- インフラストラクチャ

Citrix Director

リアルタイム Web ツールである Director を使用して、セッションの監視、トラブルシューティングなど、エンドユーザーに対するサポートタスクを実行できます。

詳しくは、「Director」の記事を参照してください。

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、だれによって行われたかを確認して、問題の原因究明に役立てることができます。このビューには、構成情報が以下の 3 つのカテゴリに分けて表示されます。

- 接続エラー
- 障害が発生したデスクトップマシン
- 障害が発生したサーバーマシン

構成ログ機能の有効化と構成方法について詳細は、「構成ログ機能」の記事を参照してください。「Director」には、このツールを使って、ログ情報を表示する方法を記載した記事があります。

イベントログ

XenApp および XenDesktop サービスは、発生するイベントを記録します。イベントログは、操作を監視およびトラブルシューティングするために使用できます。

詳しくは、「イベントログ」を参照してください。個別の機能に関する記事には、イベント情報も含まれることがあります。

Session Recording 7.15

August 24, 2021

Session Recording を使用すると、企業ポリシーおよび法規制の順守の要件に準拠して、接続の種類を問わず、VDA for Server OS または VDA for Desktop OS でホストされる任意のユーザーセッションで行われる、画面上のアクティビティを録画することができます。Session Recording により録画、カタログ化、およびアーカイブされるセッションを、後で取得して再生することができます。

アプリケーションおよびデスクトップセッションの録画を自動的に起動する、柔軟性の高いポリシーが提供されます。この機能により、IT 担当者はアプリケーションセッションおよびデスクトップセッションのユーザーアクティビティを監視および確認できます。このように、Session Recording は、企業が法規制順守やセキュリティ監視に関する内部統制を行ううえで役に立ちます。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

ログと監視によるセキュリティの強化。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。

高機能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、Citrix で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

April 17, 2020

次の手順を実行すると、XenApp および XenDesktop セッションを録画し、検証できるようになります。

1. Session Recording コンポーネントを理解する。
2. 環境に合う展開シナリオを選択する。
3. インストール要件を確認する。

4. Windows の役割と機能の前提条件をインストールする。
5. Session Recording をインストールする。
6. Session Recording コンポーネントを構成して、録画およびセッションの表示を許可する。

Session Recording は 5 つのコンポーネントから構成されます:

- **Session Recording Agent**。各 VDA for Server OS または VDA for Desktop OS にインストールする、録画処理を有効にするコンポーネントです。これによりセッションデータが録画されます。
- **Session Recording** サーバー。次のサービスをホストするサーバーです。
  - ブローカー: IIS 6.0 以降によりホストされる Web アプリケーションです。これにより、Session Recording Player からの検索クエリおよびファイルダウンロード要求と、Session Recording ポリシーコンソールからのポリシー管理要求が制御されます。また、XenApp および XenDesktop の各セッションの録画ポリシーが評価されます。
  - ストレージマネージャー: Windows サービスです。これにより、XenApp と XenDesktop を実行中の Session Recording が有効な各コンピューターから受信する、セッションの録画ファイルが管理されます。
  - 管理者ログ: Session Recording サーバーでインストールされる、管理アクティビティを記録するためのオプションのサブコンポーネントです。ログデータはすべて、デフォルトで **CitrixSessionRecordingLogging** という名前の個別の SQL Server データベースに格納されます。データベース名はカスタマイズすることができます。
- **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、デフォルトで **CitrixSessionRecording** という名前のデータベースが作成されます。データベース名はカスタマイズすることができます。
- **Session Recording** ポリシーコンソール。録画するセッションを指定するポリシーを作成するコンソールです。

この図は Session Recording コンポーネントおよび各コンポーネントの関係を示しています:

この展開例では、Session Recording Agent、Session Recording サーバー、Session Recording データベース、Session Recording ポリシーコンソール、および Session Recording Player のすべてが、セキュリティファイアウォールの内部に設置されています。Session Recording Agent は、VDA for Server OS または VDA for Desktop OS にインストールされます。第 2 のサーバーは Session Recording ポリシーコンソールをホストし、第 3 のサーバーは Session Recording サーバーとして機能します。そして、第 4 のサーバーは Session Recording データベースをホストします。Session Recording Player はワークステーションにインストールされます。ファイアウォール外部のクライアントデバイスは、Session Recording Agent がインストールされている VDA for Server OS に接続します。ファイアウォール内では、Session Recording Agent、Session Recording ポリシーコンソール、Session Recording Player、および Session Recording データベースはすべて Session Recording サーバーに接続します。

導入計画

August 24, 2021

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。

Session Recording では、Framehawk の表示モードはサポートされません。このため、Framehawk の表示モードのセッションを正しく録画および再生することはできません。Framehawk の表示モードで録画されたセッションには、セッションアクティビティが含まれない可能性があります。

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。

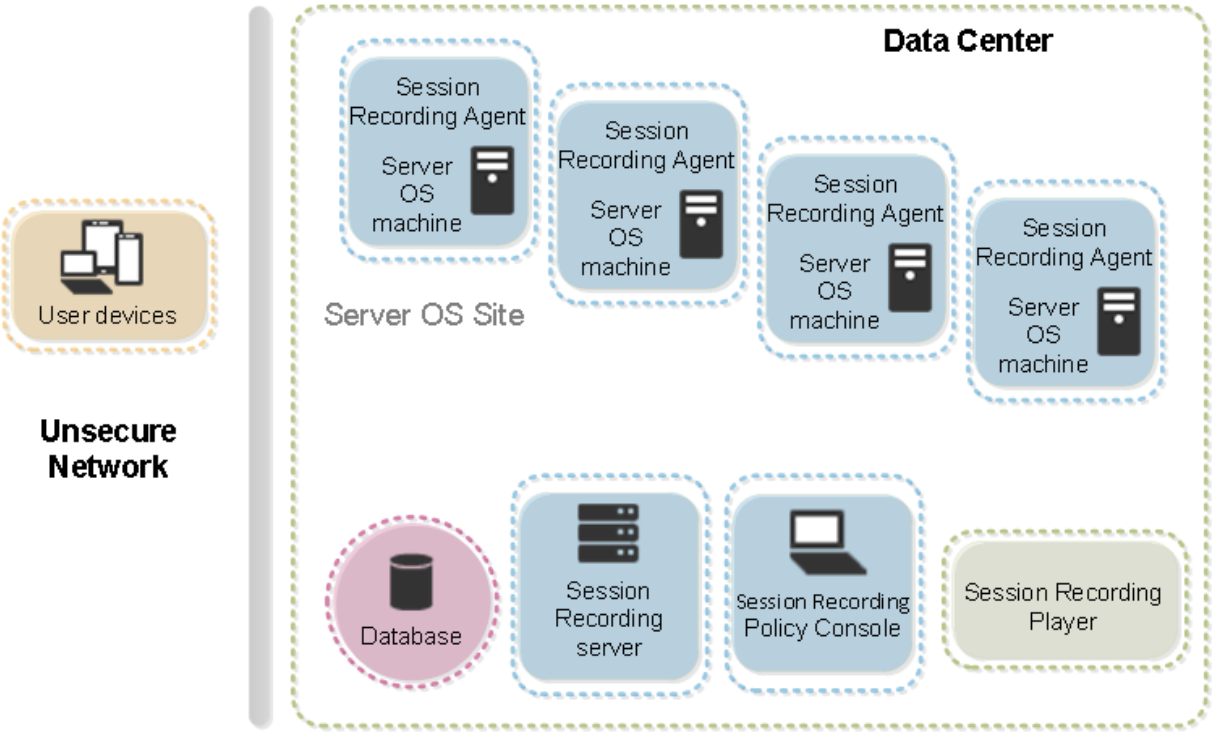
環境に応じ、異なるシナリオに基づいて Session Recording コンポーネントを展開できます。

Session Recording を単一のサイトのみに限って展開するという制限はありません。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 サーバーを使用するように設定できます。

複数のエージェントを展開した大規模なサイトがあり、画像処理にかなりリソースを消費するアプリケーション（AutoCAD など）を数多く録画したり、多数のセッションを録画したりすることが予測される場合、Session Recording サーバー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 サーバーを異なるマシンにインストールし、Session Recording Agent がそれらのマシンと連携するように設定できます。エージェントで一度に参照できるのは 1 つのサーバーのみであることに留意してください。

提案されたサーバーサイトの構成

1 つまたは複数のサイトのセッションを録画する場合は、この構成を使用します。Session Recording Agent はサイト内の各 VDA for Server OS にインストールされます。サイトはセキュリティファイアウォール内のデータセンターにあります。Session Recording Administration コンポーネント（Session Recording データベース、Session Recording サーバー、Session Recording ポリシーコンソール）を別の複数のサーバーにインストールし、Session Recording Player はワークステーションにインストールします。これらのコンピューターはファイアウォール内ですがデータセンターの外部にあります。



展開に関する重要な注意事項

- Session Recording コンポーネントを有効にして各コンポーネント間で通信できるようにするには、同じドメイン内か、推移的な信頼関係を持つ信頼されているドメイン間にインストールします。ワークグループまたは外部の信頼関係を持つドメイン間にはインストールできません。
- 映像を処理するアプリケーションであり、サイズの大きな録画を再生するときは多くのメモリが使用されるため、Session Recording Player を公開アプリケーションとしてインストールすることはお勧めしません。
- デフォルトでは、Session Recording は TLS/HTTPS を使用して通信するように設定されます。Session Recording サーバーに証明書をインストールし、ルート証明機関（CA）が Session Recording コンポーネントで信頼されていることを確認します。
- Session Recording データベースを SQL Server 2016 Express Edition、SQL Server 2014 Express Edition、SQL Server 2012 Express Edition、または SQL Server 2008 R2 Express Edition が動作するスタンドアロンサーバーにインストールする場合は、そのサーバーで TCP/IP プロトコルを有効にして SQL Server Browser サービスを実行する必要があります。これらの設定はデフォルトでは無効になっていますが、Session Recording サーバーとデータベースの間で通信を行うために有効にする必要があります。これらの設定の有効化について詳しくは、Microsoft 社の「SQL Server の TCP/IP ネットワークプロトコルの有効化」および「SQL Server Browser サービス」を参照してください。
- Session Recording の展開を計画するときは、セッション共有の影響を考慮します。公開アプリケーションのセッションを共有すると、Session Recording の公開アプリケーションの録画ポリシー規則と競合する可能性があります。Session Recording では、アクティブなポリシーと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。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、パフォーマンスの問題があるため、この操作をお勧めしません。
- Session Recording ポリシーコンソールを Delivery Controller にインストールできます。
- Session Recording サーバーと Session Recording ポリシーコンソールは同じシステムにインストールできます。
- Session Recording サーバーの NetBIOS 名が 15 文字を超えないようにしてください（Microsoft にはホスト名長に 15 文字の制限があります）。
- カスタムイベントログを記録するには、PowerShell 5.1 以降が必要です。PowerShell 4.0 がインストールされている Windows Server 2012 R2 に Session Recording Agent をインストールする場合は、PowerShell をアップグレードします。アップグレードしなかった場合、API 呼び出しが失敗する可能性があります。

セキュリティの推奨事項

August 24, 2021

Session Recording は、セキュア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。デフォルトの構成はシンプルなシステムです。デジタル署名や暗号化などのセキュリティ機能はオプションで設定できます。

Session Recording コンポーネント間の通信は、インターネットインフォメーションサービス（IIS）と Microsoft メッセージキュー（MSMQ）を通じて実現されます。IIS により、各 Session Recording コンポーネント間の Web サービスの通信リンクが提供されます。MSMQ により、Session Recording Agent から Session Recording サーバーへセッションの録画データを送信するための、信頼できるデータ伝送メカニズムが提供されます。

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

展開計画を立てるときに、セキュリティに関する次の推奨事項について検討します：

- 社内ネットワーク、Session Recording、または個々のマシンで各種管理者の役割を適切に分離する。このようにしないと、セキュリティ上の脅威にさらされ、システム機能が影響を受けたり、システムが不正利用さ

れたりする可能性があります。ユーザーやアカウントごとに異なる管理者の役割（ロール）を割り当てることをお勧めします。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してください。

- 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ます。
- VDA 管理者権限を一般的なセッションユーザーに、特にリモート PC アクセスを使用している場合には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をお勧めします。

- Session Recording では、データの機密性にかかわらず、セッショングラフィックスアクティビティが録画されます。特定の状況においては、機密データ（ユーザーの資格情報、プライバシー情報、サードパーティの画面など。ただしこれらに限定されるものではありません）が誤って録画される場合があります。このリスクを回避するには、以下の措置を講じます：

  - 特定のトラブルシューティングの場合を除き、VDA のコアメモリダンプを無効にします。

    コアメモリダンプを無効にするには、以下の手順に従います。

    1. ［マイコンピューター］を右クリックし、［プロパティ］を選択します。
    2. ［詳細設定］タブをクリックし、［起動と回復］の ［設定］をクリックします。
    3. ［デバッグ情報の書き込み］で ［(なし)］を選択します。

    Microsoft の記事（https://support.microsoft.com/en-us/kb/307973）を参照してください。

  - セッションの所有者は、デスクトップセッションが録画されている場合は、オンライン会議と Microsoft Remote Assistance ソフトウェアが録画される可能性があることを出席者に知らせます。

  - ログオン資格情報またはセキュリティ情報が、社内で公開または使用されるすべてのローカルアプリケーションと Web アプリケーションに表示されないようにします。そうしない場合、そのような情報が Session Recording で録画されます。

  - 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ます。

  - 公開デスクトップまたは Software as a Service（SaaS）アプリケーションへのアクセスには、自動認証方法（シングルサインオン、スマートカードなど）のみをお勧めします。

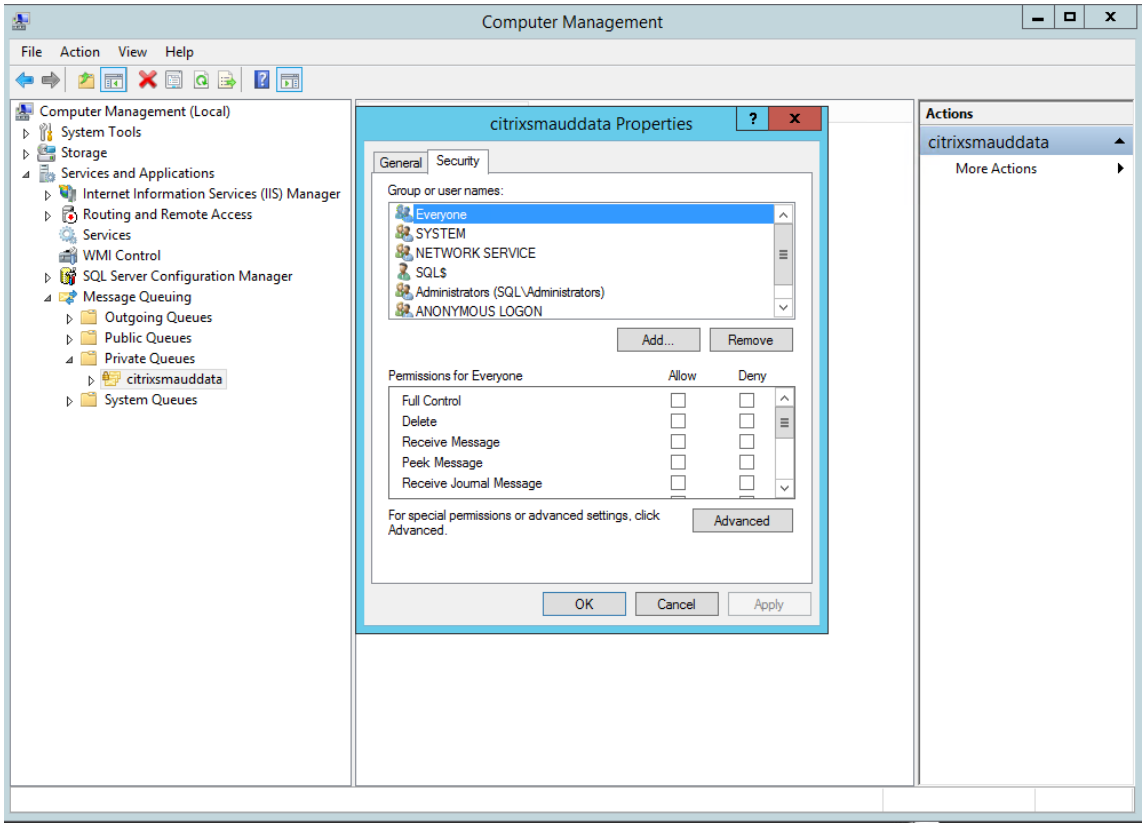
- Session Recording は、正常に機能し、セキュリティニーズを満たす上で、特定のハードウェアとハードウ

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。

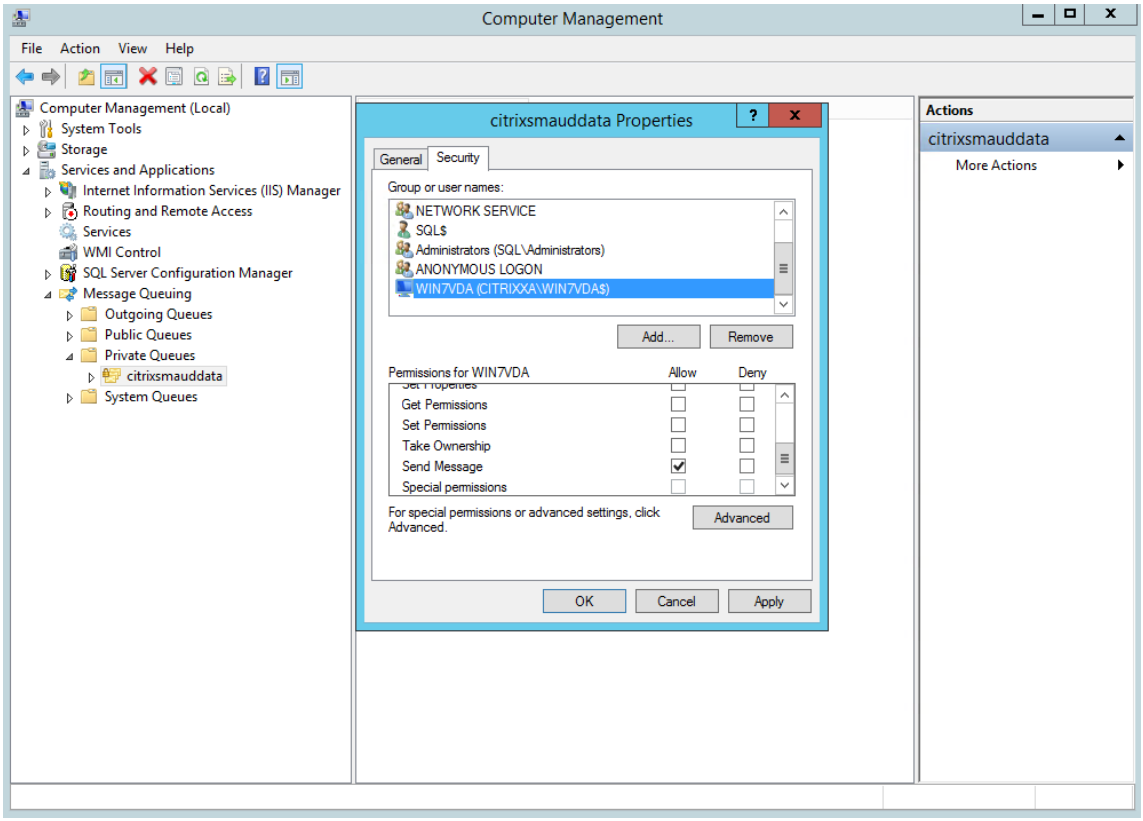
  - Session Recording をサポートするネットワークインフラストラクチャを適切に保護し、利用可能な状態を維持します。
  - サードパーティ製のセキュリティソリューションまたは Windows のメカニズムを使用して、Session Recording コンポーネントを保護することをお勧めします。Session Recording コンポーネントには以下が含まれます：
    * Session Recording サーバー上
      - プロセス：SsRecStoragemanager.exe および SsRecAnalyticsService.exe
      - サービス：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
      - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server にあるレジストリキー値
    * 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
      - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent にあるレジストリキー値

- 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します。

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 をインストールします。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 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使用してイベントログを保護するか、イベントログをリモートサーバーにリダイレクトすることが推奨されます。
- Session Recording コンポーネントが動作するサーバーを物理的に保護する。可能であれば、権限を持つ人のみが入室できる安全なサーバー室にコンピューターを設置します。
- Session Recording コンポーネントが動作するサーバーを別のサブネットまたはドメインに分離する。
- Session Recording サーバーとほかのサーバーの間にファイアウォールを設置し、ほかのサーバーにアクセスするユーザーからセッションの録画データを保護する。
- Microsoft からの最新のセキュリティアップデートにより、Session Recording Administration サーバーおよび SQL データベースを最新に保ちます。
- 管理者以外の人が管理マシンにログオンできないように制限する。
- 録画ポリシーの変更およびセッションの録画ファイルの表示を行う権限を持つユーザーを厳しく制限する。
- デジタル証明書をインストールし、Session Recording のファイル署名機能を使用し、IIS で TLS 通信をセットアップする。
- MSMQ の通信で HTTPS が使用されるように設定する。そのためには、[**Session Recording Agent** のプロパティ] に表示される MSMQ プロトコルを HTTPS に設定します。詳しくは、「MSMQ のトラブルシューティング」を参照してください。

- TLS 1.1 または TLS 1.2（推奨）を使い SSLv2、SSLv3、および TLS 1.0 を Session Recording サーバーと Session Recording データベースで無効にします。詳しくは、Microsoft 社のhttps://support.microsoft.com/default.aspx?scid=kb;en-us;187498を参照してください。

  Session Recording サーバーと Session Recording データベースで、TLS 用の RC4 暗号スイートを無効にする。

1. Microsoft のグループポリシーエディターを使用して、［コンピューターの構成］>［管理用テンプレート］>［ネットワーク］>［**SSL** 構成設定］に移動します。
2. ［**SSL** 暗号の順位］ポリシーを ［有効］に設定します。デフォルトでは、このポリシーは ［未構成］に設定されています。
3. RC4 暗号スイートをすべて削除します。

- 再生データの保護機能を使用する。再生データの保護は Session Recording の機能の 1 つで、これにより、Session Recording Player にダウンロードされる前に、セッションの録画ファイルが暗号化されます。このオプションは ［**Session Recording** サーバーのプロパティ］にあり、デフォルトで有効に設定されます。
- 暗号化キー長および暗号化アルゴリズムの NSIT ガイダンスに従います。
- TLS 1.2 の Session Recording サポートを構成します。
  - Session Recording コンポーネントのエンドツーエンドセキュリティを確実にするためには、通信プロトコルとして TLS 1.2 を使用されることをお勧めします。

    TLS 1.2 の **Session Recording** サポートを構成するには：

    1. Session Recording サーバーをホストするマシンにログオンします。適切な SQL Server クライアントコンポーネントとドライバーをインストールし、.NET Framework（バージョン 4 以降）に対して強固な暗号を設定します。
       1. Microsoft ODBC Driver for SQL Server バージョン 11 以降をインストールします。
       2. .NET フレームワークの最新のホットフィックスロールアップを適用します。
       3. 使用している.NET フレームワークのバージョンに基づいて`ADO.NET - SqlClient`をインストールします。詳しくは、「https://support.microsoft.com/en-us/kb/3135244」を参照してください。
       4. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 および HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319 の下に、DWORD 値 SchUseStrongCrypto=1 を追加します。
       5. マシンを再起動してください。

       2. Session Recording ポリシーコンソールをホストするマシンにログオンします。.NET Framework の最新の Hotfix ロールアップを適用し、.NET Framework（バージョン 4 以降）に対して強固な暗号を設定します。強固な暗号を設定する方法は、下位手順 1-d および 1-e と同じです。Session Recording サーバーと同じコンピューターで Session Recording ポリシーコンソールをインストールするように選択している場合は、これらの手順を実行する必要はありません。

2016 より前のバージョンの SQL Server に対する TLS 1.2 サポートを構成するには、https://support.microsoft.com/en-us/kb/3135244を参照してください。TLS 1.2 を使用するには、HTTPS を、Session Recording コンポーネントのための通信プロトコルとして構成します。

Session Recording セキュリティ機能の構成について詳しくは、Knowledge Center の「Session Recording のセキュリティ機能の構成」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

August 24, 2021

Session Recording は、数千の、または数万のセッションを処理する高スケーラブルなシステムです。Session Recording のインストールと実行のために、XenApp および XenDesktop 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可能性がある場合、または画像処理に多くのリソースを消費するアプリケーションを録画するなど、セッションの録画ファイルのサイズが大きくなることが予測される場合は、Session Recording の展開計画を立てるときに、使用するシステムのパフォーマンスについて検討します。

ここでは、Session Recording によって高いスケーラビリティを実現し、最低限のコストで録画システムを最大限に活用できる方法について説明します。

Session Recording のスケーラビリティが高い理由

Session Recording が同様の他社製品と比べて高いスケーラビリティを提供できるのには、主に 2 つの理由があります:

- 小さなファイルサイズ

  Session Recording で作成されたセッションの録画ファイルは比較的小さなサイズです。スクリーンスクレイピングによるソリューションで作成された同様のビデオ録画に比べると、けた外れに小さなサイズです。各 Session Recording ファイルの転送および格納に必要なネットワーク帯域幅、ディスクスペース、ディスク IOPS は通常、同様のビデオファイルの 10 分の 1 以下です。

  セッションの録画ファイルのサイズが小さいと、ビデオフレームのレンダリングもより高速かつスムースになります。また、録画は完全に無損失で、大半の小さなサイズのビデオ形式で発生しがちな表示の滑らかさの問題もありません。録画の中のテキストは、再生中でも元のセッションと同じくらい読み取りやすい状態です。ファイルサイズの小ささを維持するために、Session Recording はファイル内でキーフレームを記録しません。

- ファイルの生成に必要な処理が少ない

  セッションの録画ファイルには、実質的には本来の形式で抽出されたセッションの ICA プロトコルデータが含まれます。つまり、ファイルは Citrix Workspace アプリと通信していた ICA プロトコルデータストリームをキャプチャします。リアルタイムでデータを変換するために高価なトランスコードやエンコード用のソフトウェアコンポーネントを実行する必要はありません。VDA のスケーラビリティでは、処理の量を抑えることも重要です。これによって、同じ VDA から多くのセッションが録画された場合でも、エンドユーザーエクスペリエンスが維持されます。

また、再生が可能な ICA 仮想チャネルのみが録画されるため、さらに最適化が促進されます。たとえば、プリンターやクライアントドライブマッピングチャネルはビデオの再生時に必要がなく生成するデータ量も多いため、録画の対象外です。

データの入力速度および処理速度の推定

Session Recording サーバーは、セッションの録画ファイルを一元的に収集する場所です。マルチセッション OS VDA を実行している各マシンで Session Recording を有効にすると、セッションの録画データを Session Recording サーバーに送信します。Session Recording は大量のデータを処理することができ、バーストや障害にも耐性がありますが、どのようなサーバーでも物理的なデータ量の限界はあります。

各 Session Recording サーバーに送信するデータの量と、サーバーでこのデータを処理し格納するのにかかる時間について考慮します。受信データを格納する速度がデータ入力速度より高速である必要があります。

データ入力速度を推定するには、録画対象のセッションの数をその平均サイズで乗算してから、セッションの録画時間で除算します。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、データの入力速度は約 3.5Mbps です（5,000 セッション ×20MB÷8 時間 ÷3,600 秒）。通常、100Mbps LAN に接続され、記録されたデータを格納する十分なディスクスペースがある Session Recording サーバーは、ディスクおよびネットワーク IOPS による物理的な制限を考慮すると、データを約 5.0Mbps で処理できます。これが、処理速度です。この例では、処理速度（5.0Mbps）は入力速度（3.5Mbps）より高い値であるため、5,000 件の Outlook セッションを録画することが可能です。

セッションごとのデータ量は録画される内容によって大きく異なり、画面の解像度、色数、グラフィックモードなどのその他の要素も影響します。グラフィック操作が一定して多い CAD パッケージを実行しているセッションでは、エンドユーザーが Microsoft Outlook でメールを送受信するセッションよりも、大幅に大きなサイズの録画データが生成されることが予想できます。したがって、同じ数でも CAD セッションはきわめて高い入力速度を必要とし、Session Recording サーバーの使用率も高くなります。

バーストや障害

前述の例では、非常にシンプルで均一なデータのスループットを想定しましたが、短い時間に高いアクティビティが発生するバーストといわれる状態をシステムが処理する方法については、また異なります。バーストは、すべてのユーザーが朝の同じ時間に一斉にログオンするとき（9 時台のラッシュ）や、全員が一斉に Outlook の受信ボックスで同じメールを受信した場合などに発生することがあります。このような急激な需要には、Session Recording サーバーの 5.0Mbps という処理速度では対応が不十分になります。

各 VDA で実行されている Session Recording Agent は、Microsoft メッセージキュー（MSMQ）を使用して記録されたデータを Session Recording サーバーに送信します。データは、ストアアンドフォワード方式で送信されます。これは、メールが送信者、メールサーバー、受信者との間で送受信される方法と似たような方式です。Session Recording サーバーやネットワークがバースト時の大量のデータを処理できない場合、セッションの録画データはデータメッセージのバックログが消去されるまで一時的に格納されます。ネットワークが混雑した場合、データメッセージは一時的に発信キューに格納されることがあります。または、データがネットワークを経由してもストレージ

マネージャーが他のメッセージの処理でビジー状態の場合、Session Recording サーバーの受信キューに格納されることがあります。

MSMQ はフォールトトレランスメカニズムとしても機能します。Session Recording サーバーがダウンするかリンクが破損している場合、記録されたデータは各 VDA の発信キューにとどまります。障害が解消されると、キューのすべてのデータが一度に送信されます。MSMQ を使用することで、現在のセッションの録画を中断したりデータを失ったりすることなく Session Recording サーバーをオフラインでアップグレードやメンテナンスすることもできます。

MSMQ の主な制限は、データメッセージの一時ストレージとしてのディスクスペースが限られていることです。このため、バースト、障害、またはメンテナンスイベントが長引く場合、最終的にデータが失われることがあります。データ損失後も総合的なシステムは機能し続けますが、この状況では個別の記録内でデータの一部が失われます。データが失われたファイルは再生可能ですが、最初に失われたデータの箇所まで進むと再生が停止します。以下の点に注意してください:

- 各サーバー、特に Session Recording サーバーにディスクスペースを追加して MSMQ で使用できるようにすると、バーストや障害時の許容値が上昇します。
- 各 Session Recording Agent でメッセージの有効期間を適切なレベルに設定することが重要です（Session Recording Agent プロパティの ［接続］タブ）。デフォルト値の 7,200 秒（2 時間）は、記録された各データメッセージが破棄され、録画ファイルが破損する前にストレージマネージャーに到達するのに 2 時間の猶予があることを意味します。利用可能なディスクスペースが増えると（または録画するセッションを削減すると）、この値を増やすことを選択できます。最大値は 365 日です。

MSMQ のその他の制限は、データのバックログが作成されると、データメッセージの読み取りと書き込みのために追加のディスク IOPS が発生するということです。通常の状態であれば、ストレージマネージャーはネットワークから直接データを受信して処理し、データメッセージがディスクに書き込まれることはありません。データを格納するためには、セッションの録画ファイルを追加するためにディスクへの一度の書き込み操作が必要になります。データのバックログが作成された場合、ディスク IOPS が 3 倍になります。これは、各メッセージがディスクに書き込まれ、ディスクから読み取られ、ファイルに書き込まれる必要があるためです。ストレージマネージャーは IOPS に大幅に影響を受けるため、Session Recording サーバーの処理率はメッセージのバックログが消去されるまで低下します。この追加の IOPS の影響を緩和するため、以下の推奨事項を採用します:

- MSMQ がメッセージを格納するディスクは、録画ファイルのストレージフォルダーとは異なるディスクを使用してください。IOPS バストラフィックが 3 倍になっても、実際の処理率の低下は深刻なものにはなりません。
- 計画的な停止をピーク時以外のみにとどめます。予算の制限によっては、高可用性サーバーの構築で実証済みのアプローチを使用します。このアプローチには、UPS、デュアル NIC、スイッチの冗長化、ホットスワップ対応メモリとディスクの使用が含まれます。

処理能力を重視した設計

セッションの録画データが均一であることは少なく、バーストや障害が発生する可能性があり、メッセージのバックログの消去は IOPS を増加させます。このため、各 Session Recording サーバーは処理能力に余裕をもって設計し

ます。後のセクションで説明するように、サーバーを追加するか既存のサーバーの仕様を改善することで、より多くの処理能力を獲得できます。一般的な目安は、各 Session Recording サーバーを合計処理能力の最大 50% で実行することです。前述の例のように、サーバーが 5.0Mbps で処理することができる場合、システムは 2.5 Mbps で実行することを目標にします。1 つの Session Recording サーバーで 5,000 件の Outlook セッションの録画では 3.5Mbps ですが、これを 3,500 件のセッションに抑えると約 2.5Mbps になります。

バックログとライブ再生

ライブ再生とは、セッションがアクティブなときに閲覧者がセッションの録画を開いて再生することです。ライブ再生中に、そのセッションを担当する Session Recording Agent がストリーミングモードに切り替え、録画データを内部バッファリングなしにストレージマネージャーに即座に送信します。録画ファイルは常に更新され、Player は引き続きライブセッションからの最新データを取得します。Agent からストレージマネージャーに送信されたデータは MSMQ を経由し、前述のキューの規則が適用されます。このシナリオでは、問題が発生する可能性があります。MSMQ のバックログが作成されると、ライブ再生で利用可能な新しい録画データは、他のすべてのデータメッセージのようにキューに登録されます。閲覧者がファイルを再生することはできますが、ライブで記録された最新のデータの閲覧には遅延が発生します。ライブ再生が閲覧者にとって重要である場合は、展開でバックログの必要性が低くなるように処理能力やフォールトトレランスを設計してください。

XenApp および **XenDesktop** のスケーラビリティ

Session Recording がセッションのパフォーマンスを低下させたり、記録されたデータバックログへの応答でセッションを停止させたりすることは決してありません。エンドユーザーエクスペリエンスや単一サーバーのスケーラビリティを維持することが、Session Recording システムの設計において何よりも優先されます。記録システムが不可逆的に過負荷になった場合、記録されたセッションのデータは破棄されます。シトリックスが実施した広範囲にわたるスケーラビリティテストによると、ICA セッションの録画が XenApp および XenDesktop サーバーのパフォーマンスとスケーラビリティに与える影響は大きくありません。影響の大きさは、プラットフォーム、利用可能なメモリ、録画されたセッションの画像の性質によって異なります。以下の構成では、単一サーバーのスケーラビリティへの影響は 1 ～ 5% 程度と予想されます。つまり、Session Recording をインストールしない場合に 100 ユーザーをホストできるサーバーの場合、インストール後は 95～99 人のユーザーをホストすることができます:

- マルチセッション OS VDA を実行している 8GB RAM の 64 ビットサーバー
- Office 業務アプリケーション（Outlook や Excel）を実行しているすべてのセッション
- アプリケーションの使用が可能で維持される
- すべてのセッションが Session Recording ポリシーの構成に従って録画される

録画されているセッションが少数か、維持されるセッションアクティビティが少なく散発的であれば、影響は大きくありません。多くの場合、スケーラビリティへの影響は無視できる範囲で、サーバーあたりのユーザー密度に変化はありません。前述したように、影響が少ないのは各 VDA にインストールされた Session Recording コンポーネントの処理要件がシンプルであるためです。記録済みのデータは、ICA セッションスタックから抽出され、そのまま MSMQ 経由で Session Recording サーバーに送信されるだけです。コストがかかるデータのエンコードは発生しません。

セッションが録画されていない場合でも、Session Recording の使用には多少のオーバーヘッドが発生します。この影響は大きくありませんが、特定のサーバーから録画されるセッションがないことが分かっている場合は、そのサーバーの録画を無効にできます。Session Recording を削除する方法もあります。より影響の少ないアプローチは、Session Recording Agent の［**Session Recording**］タブで［この **VDA** マシンでセッションを録画する］チェックボックスをオフにすることです。あとからセッションの録画が必要になった場合、このチェックボックスを再度オンにします。

スループットの測定

セッションの録画データを VDA から送信して Session Recording サーバーで受信する場合のスループットを測定するには、さまざまな方法があります。最も簡単かつ効果的なアプローチの 1 つは、録画されたファイルのサイズ、および Session Recording サーバーでディスクスペースが消費される速度を測定することです。ディスクに書き込まれるデータの量は、生成されるネットワークトラフィックの量をほぼ反映しています。Session Recording で提供されるカウンターに加えて、Windows パフォーマンスモニターツール（perfmon.exe）には、監視可能なさまざまな標準のシステムカウンターがあります。カウンターは、スループットの測定だけでなく、ボトルネックやシステムの問題を特定するために使用できます。次の表では、最も有用なパフォーマンスカウンターの一部をまとめました。

パフォーマンスオブジェクト	カウンター名	説明
Citrix Session Recording Agent	アクティブな録画数	現在、特定の VDA に録画されているセッションの数を示します。
Citrix Session Recording Agent	Session Recording Driver からの読み取りバイト数	セッションデータ取得に必要なカーネルコンポーネントからの読み取りバイト数です。そのサーバーで録画されているすべてのセッションで単一 VDA が生成するデータ量を決定するために役立ちます。
Citrix Session Recording ストレージマネージャー	アクティブな録画数	Session Recording サーバーを除いては Citrix Session Recording Agent のカウンターと同様です。現在、すべてのサーバーで録画されているセッションの合計数を示します。

パフォーマンスオブジェクト	カウンター名	説明
Citrix Session Recording ストレージマネージャー	メッセージバイト/秒	すべての録画されたセッションのスループット。ストレージマネージャーがデータを処理する速度を決定するために使用できます。MSMQ でメッセージのバックログが作成されている場合は、ストレージマネージャーはフルスピードで動作します。この値は、ストレージマネージャーの最大処理速度を示すために使用することができます。
LogicalDisk	ディスク書き込みバイト/秒	ディスクのライトスループットを測定するために使用することができます。これは、Session Recording サーバーで高いスケーラビリティを達成する上で重要です。個々のドライブのパフォーマンスも測定することができます。
MSMQ キュー	キュー内のバイト数	このカウンターは CitrixSmAudData メッセージキュー内でバックログが作成されたデータの量を決定するために使用できます。時間の経過とともにこの値が増加した場合、ネットワークから録画データを受信する速度は、ストレージマネージャーがデータを処理できる速度よりも大きくなります。このカウンターは、データバーストや障害の影響を測定するために有用です。
MSMQ キュー	キュー内のメッセージ	キュー内のバイト数カウンターとほぼ同じですが、メッセージの数を測定します。

パフォーマンスオブジェクト	カウンター名	説明
ネットワークインターフェイス	合計バイト/秒	リンクの両側で、セッションの録画時に生成されるデータの量を測定するために使用できます。Session Recording サーバーで測定すると、このカウンターは受信データを受け取る速度を示します。データの処理速度を測定する Citrix Session Recording ストレージマネージャーのメッセージバイト/秒カウンターとは、対照的なカウンターです。ネットワークの速度がこの値よりも大きい場合は、メッセージがメッセージキューに構築されます。
プロセッサ	% プロセッサ時間	CPU がボトルネックになる可能性が低い場合でも、この値を監視することは役に立ちます。

Session Recording サーバーのハードウェア

Session Recording サーバーで使用されるハードウェアを慎重に選択することで、展開の処理能力を拡大できます。選択肢は、スケールアップ（各サーバーの処理能力を増やす）かスケールアウト（さらにサーバーを追加する）の 2 つです。最低限のコストでスケーラビリティを増やすことを念頭に、どちらかを選択します。

スケールアップ

単一の Session Recording サーバーの場合、予算内で最適なパフォーマンスを確保する次のベストプラクティスを検討してください。システムは、IOPS に依存しています。これによって、ネットワークからディスク間で録画されたデータの高いスループットを確保できます。そのため、適切なネットワークやディスクのハードウェアに投資することが重要です。高いパフォーマンスの Session Recording サーバーの場合、デュアル CPU またはデュアルコア CPU をお勧めしますが、これを超える仕様にしてもさほどパフォーマンスは上昇しません。64 ビットプロセッサをお勧めしますが、x86 プロセッサでも問題ありません。4GB の RAM をお勧めしますが、これを超える仕様にしてもパフォーマンスに大幅な変化はありません。

スケールアウト

スケールアップのベストプラクティスを使用しても、大量のセッションを録画する場合、1 つの Session Recording サーバーではパフォーマンスとスケーラビリティに限度があります。負荷に対応するために、追加のサーバーが必要な場合があります。複数の Session Recording サーバーを異なるマシンにインストールすることで、負荷分散プールとして機能させることができます。このタイプの展開では、Session Recording サーバーはストレージとデータベースを共有します。負荷を分散するには、Session Recording Agent を負荷分散を担当するロードバランサーに割り当てます。

ネットワークの性能

Session Recording サーバーに接続するには 100Mbps のネットワークリンクが適しています。ギガビットイーサネット接続ではパフォーマンスが向上するかもしれませんが、100Mbps のリンクの 10 倍のパフォーマンスが得られるわけではありません。実際には、スループットの増加量は大幅にダウンします。

Session Recording で使用するネットワークスイッチを、使用できるネットワーク帯域幅を求めて競合する可能性のあるサードパーティ製のアプリケーションと共有しないようにします。Session Recording サーバー専用のネットワークスイッチを用意することが理想的です。ネットワークの混雑がボトルネックであると判明した場合、ネットワークのアップグレードはシステムのスケーラビリティを向上させるうえで比較的安価な方法です。

ストレージ

ディスクとストレージハードウェアへの投資は、サーバーのスケーラビリティにおいて単独で最も重要な要因です。ディスクへの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。ストレージソリューションを選択する場合、読み取りパフォーマンスよりも書き込みパフォーマンスに重点を置いてください。

ローカルディスクコントローラーを使用した RAID、または SAN のいずれかとして制御されるローカルディスクのセットにデータを格納します。

> 注:
>
> SMB、CIFS、または NFS のようなファイルベースのプロトコルで NAS にデータを格納すると、深刻なパフォーマンスおよびセキュリティ上の問題が発生する可能性があります。この構成は、Session Recording の実稼働環境では決して使用しないでください。

ローカルドライブを使用する場合、キャッシュメモリが組み込まれたディスクコントローラーを検討してください。キャッシュによって、コントローラーはライトバック中に昇順に並べ替えることができるため、ディスクヘッドの動きを最小限にとどめ、物理ディスクの操作が完了するのを待機せずに書き込み操作を完了できます。このため、最小限の追加コストで大幅に書き込みパフォーマンスを向上させることができます。ただしキャッシュを使用する場合、停電時にデータ損失が発生する問題を検討する必要もあります。データとファイルシステムの整合性を確保するには、キャッシュ機能付きディスクコントローラーに予備電源装置を付け、停電時にもデータキャッシュが保持され、復旧したときにデータがディスクにライトバックされるようにします。

適切な RAID ストレージソリューションを使用するようにしてください。パフォーマンスと冗長性の要件に対応した、多くの RAID レベルがあります。次の表は、各 RAID レベルと各標準が Session Recording にどのように適用されるかを示します。

RAID レベル	種類	最小ディスク数	説明
RAID 0	パリティなしのストライピング設定	2	冗長性なしの高いパフォーマンスを提供します。いずれかのディスクが失われるとアレイが破損します。セッションの録画ファイルを格納する低コストソリューションで、データ損失の影響も抑えられます。さらにディスクを追加することで、簡単にパフォーマンスをスケールアップできます。
RAID 1	パリティなしのミラーリング設定	2	1 つのディスクではパフォーマンスの向上が見られず、比較的コストの高いソリューションです。高いレベルの冗長性が必要な場合にのみ、このソリューションを使用します。
RAID 3	専用パリティありのストライピング設定	3	RAID 5 に類似した冗長性傾向で、高い書き込みパフォーマンスを提供します。RAID 3 は、ビデオ制作やライブストリーミングアプリケーションで推奨されます。Session Recording は、この種類のアプリケーションであるため、RAID 3 が最も推奨されますが、一般的な選択肢ではありません。

RAID レベル	種類	最小ディスク数	説明
RAID 5	分散パリティありのストライピング設定	3	冗長性のある高い読み取りパフォーマンスを提供しますが、書き込み速度が遅くなります。RAID 5 は、汎用用途で最も一般的です。ただし書き込みパフォーマンスが遅いため、Session Recording には推奨されません。RAID 3 は、同程度のコストかつ大幅に良好なパフォーマンスで展開できます。
RAID 10	ミラーリング設定とストライピング設定	4	RAID 0 のパフォーマンス特性と RAID 1 の冗長性のメリットを提供します。コストの高いソリューションで、Session Recording には推奨されません。

RAID 0 と RAID 3 が、最も推奨される RAID レベルです。RAID 1 と RAID 5 は一般的な標準ですが、Session Recording には推奨されません。RAID 10 は、パフォーマンス上のいくつかのメリットを提供していますが、コストパフォーマンスは低くなります。

ディスクドライブの種類や仕様を決定します。IDE/ATA ドライブや外付け USB または FireWire ドライブは、Session Recording での使用に適していません。主な選択肢は、SATA か SCSI です。SATA ドライブは SCSI ドライブと比較して、MB 単位のコストが抑えられた十分高い転送速度を提供します。ただし、SCSI ドライブはより優れたパフォーマンスを提供し、サーバー展開でより一般的です。サーバー RAID ソリューションは、主に SCSI ドライブをサポートしますが、一部の SATA RAID 製品も利用可能になりました。ディスクドライブ製品の仕様を評価する場合、ディスクの回転速度および他のパフォーマンス特性を考慮してください。

一日あたり数千のセッションの録画は、相当量のディスクスペースを消費する可能性があるため、総合的な処理能力とパフォーマンスのどちらかを選択する必要があります。前述の例では、毎営業日に 8 時間、5,000 件の Outlook セッションを録画すると、約 100GB の記憶域を消費します。10 日間の録画（50,000 件のセッションの録画ファイル）を格納するには、1,000GB（1TB）が必要です。ディスクスペースに対するこうしたプレッシャーは、古い録画をアーカイブまたは削除する前の保有期間を短縮することで緩和できます。1TB のディスクスペースが利用でき、7 日間の保有期間が適切な場合、ディスクスペースの使用は約 700GB 程度にして、300GB は多忙な日のバッファとし

て確保します。Session Recording では、ファイルのアーカイブや削除が ICLDB ユーティリティでサポートされ、最短保有期間は 2 日間です。バックグラウンドタスクをスケジュール設定して、ピーク時以外に 1 日に 1 回実行できます。ICLDB コマンドおよびアーカイブについて詳しくは、「データベースレコードの管理」を参照してください。

ローカルドライブやコントローラーを使用する代わりに、ブロックレベルのディスクアクセスベースの SAN ストレージソリューションを使用できます。Session Recording サーバーには、ディスクアレイはローカルドライブとして表示されます。SAN はセットアップにコストがかかりますが、ディスクアレイが共有されると、管理が簡易化され一元化されというメリットがあります。SAN には、ファイバチャネルと iSCSI という 2 つの主な種類があります。iSCSI は基本的に TCP/IP を介した SCSI で、ギガビットイーサネットの導入以来ファイバチャネルよりも一般的になっています。

データベースのスケーラビリティ

Session Recording データベースでは、Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012、または Microsoft SQL Server 2008 R2 が必要です。データベースにはセッション録画のメタデータのみが格納されるため、データベースに送信されるデータ量は少なくなります。セッションの録画ファイル自体は別のディスクに書き込まれます。Session Recording イベント API を使用してセッションに検索可能なイベントを挿入するのでなければ、セッション録画 1 件につきデータベースに必要な容量は通常 1KB のみです。

Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012、および Microsoft SQL Server 2008 R2 の Express Edition では、データベースサイズの上限は 10GB です。1 件のセッション録画あたり 1KB のデータが書き込まれるとすれば、この制限があっても、4 百万件のセッションをデータベースでカタログ化できます。Microsoft SQL Server のほかのエディションではデータベースサイズの制限はなく、使用できるディスク容量によってのみ上限が決定されます。データベース内のセッション数が増加するにつれて、データベースのパフォーマンスと検索速度はごくわずかに低下します。

Session Recording イベント API によるカスタマイズを行わない場合は、録画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、検索可能な録画イベントそれぞれについて 1 件のトランザクションが生成されます。最も基本的な方式で展開したデータベースで、1 秒あたり何百件というトランザクションを制御できるため、データベースの処理負荷が高くなる可能性はほとんどありません。影響が十分に小さいため、XenApp または XenDesktop のデータストアデータベースを含めたほかのデータベースと同じ SQL Server で、Session Recording データベースを実行できます。

Session Recording のデータベースで何百万というセッション録画をカタログ化する必要がある場合は、SQL Server のスケーラビリティに関する Microsoft 社のガイドラインに従います。

Session Recording のインストール、アップグレード、およびアンインストール

August 24, 2021

この章では、XenApp および XenDesktop インストーラーを使用して Session Recording をインストールする方法について説明します。以下のセクションがあります:

インストールチェックリスト

バージョン 7.14 以降は、XenApp および XenDesktop インストーラーを使用して Session Recording のコンポーネントをインストールできます。

インストールを始める前に、以下のリストに記載されている作業を行います:

☒	手順
	Session Recording の各コンポーネントをインストールするマシンを選択し、各コンピューターがインストールするコンポーネントのハードウェアおよびソフトウェアの要件を満たしていることを確認します。
	Citrix アカウント資格情報を使用して、XenApp および XenDesktop のダウンロードページにアクセスし、製品の ISO ファイルをダウンロードします。ISO ファイルを解凍するか、ファイルの DVD を作成します。
	Session Recording コンポーネント間の通信に TLS プロトコルを使用するには、正しい証明書を環境にインストールします。
	Session Recording コンポーネントに必要な Hotfix をインストールします。Hotfix はCitrix サポートから入手できます。

	手順
	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 サーバーを使用する」を参照してください。

注:

- 公開アプリケーションのセッション共有は、同じデリバリーグループにあるとアクティブなポリシーと競合することがあるため、公開アプリケーションを Session Recording ポリシーをベースとした個別のデリバリーグループに分割することをお勧めします。Session Recording では、アクティブなポリシーとユーザーが最初に開いた公開アプリケーションを照合します。
- Machine Creation Services（MCS）または Provisioning Services を使用する計画がある場合は、一意な QMId を準備します。この手順の実行に失敗すると、録画データが損失する可能性があります。
- SQL Server では TCP/IP を有効にする必要があり、SQL Server Browser サービスが実行中で、また Windows 認証の使用が必要です。
- HTTPS を使用するには、TLS/HTTPS のサーバー証明書を構成します。
- [ローカルユーザーとグループ] > [グループ] > [ユーザー] のユーザーに C:\windows\Temp フォルダーに対する書き込み権限が付与されていることを確認します。

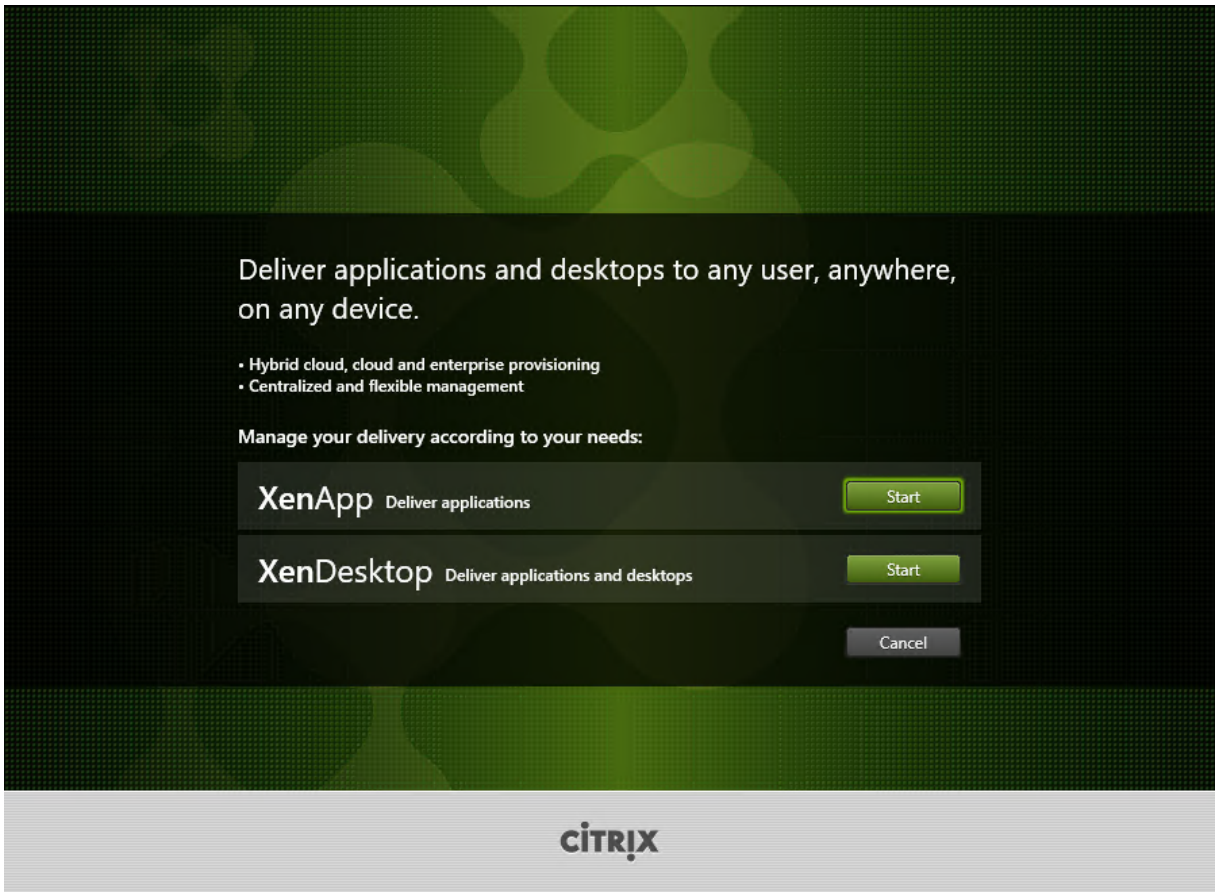
Session Recording Administration コンポーネントのインストール

シトリックスでは、Session Recording Administration、Session Recording Agent、および Session Recording Player の各コンポーネントを別々のサーバーにインストールすることをお勧めします。Session Recording Administration コンポーネントは、Session Recording データベース、Session Recording サーバー、および Session Recording ポリシーコンソールから構成されています。これらのコンポーネントのうち、サーバーにインストールするコンポーネントを選択できます。

手順 **1**: 製品ソフトウェアをダウンロードしてウィザードを起動する

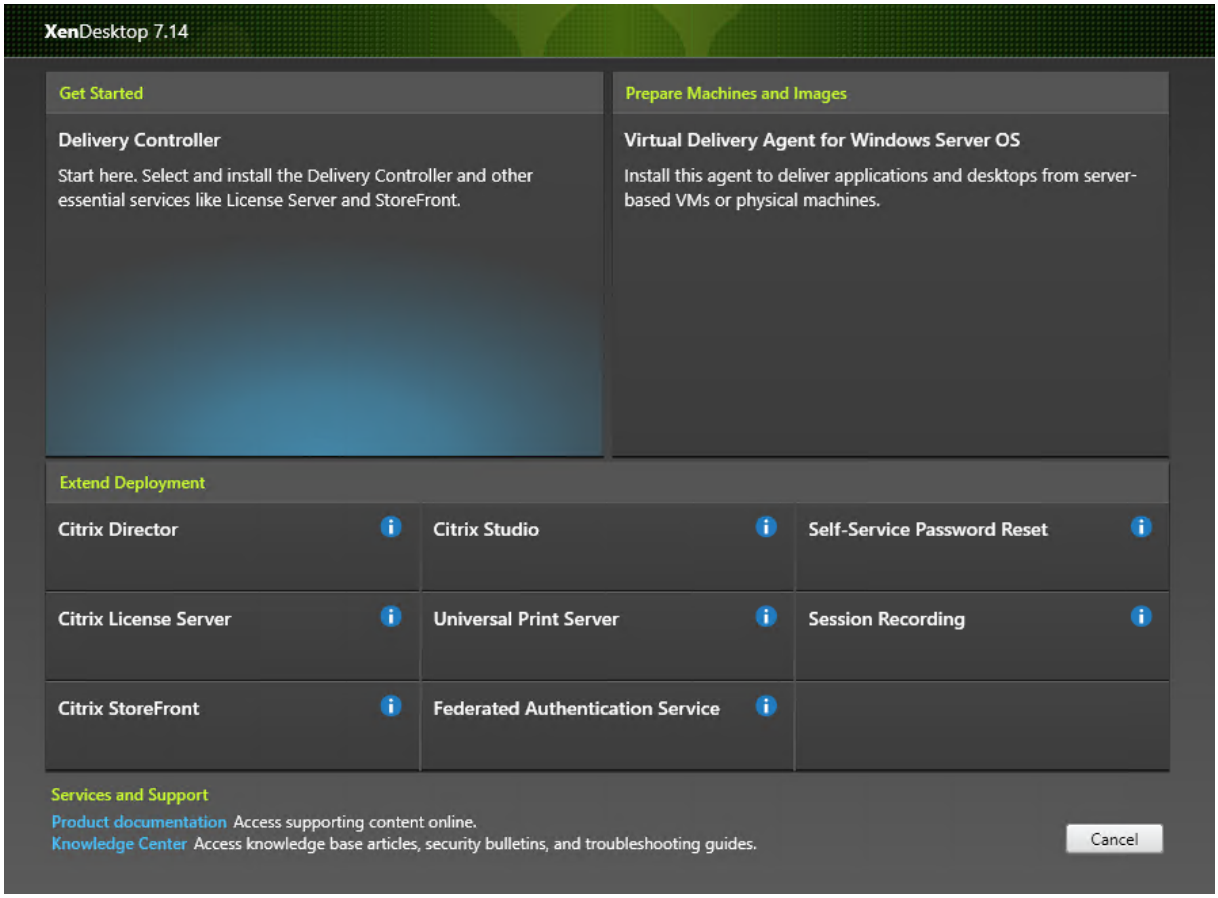
1. XenApp および XenDesktop の ISO のダウンロードが済んでいない場合は、Citrix アカウント資格情報を使用して XenApp および XenDesktop のダウンロードページにアクセスし、製品の ISO ファイルをダウンロードします。ISO ファイルを解凍するか、ファイルの DVD を作成します。
2. ローカルの管理者アカウントを使って、Session Recording Administration コンポーネントのインストール先マシンにログオンします。DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。
   インストールウィザードが起動します。

手順 **2**：インストールする製品を選択する



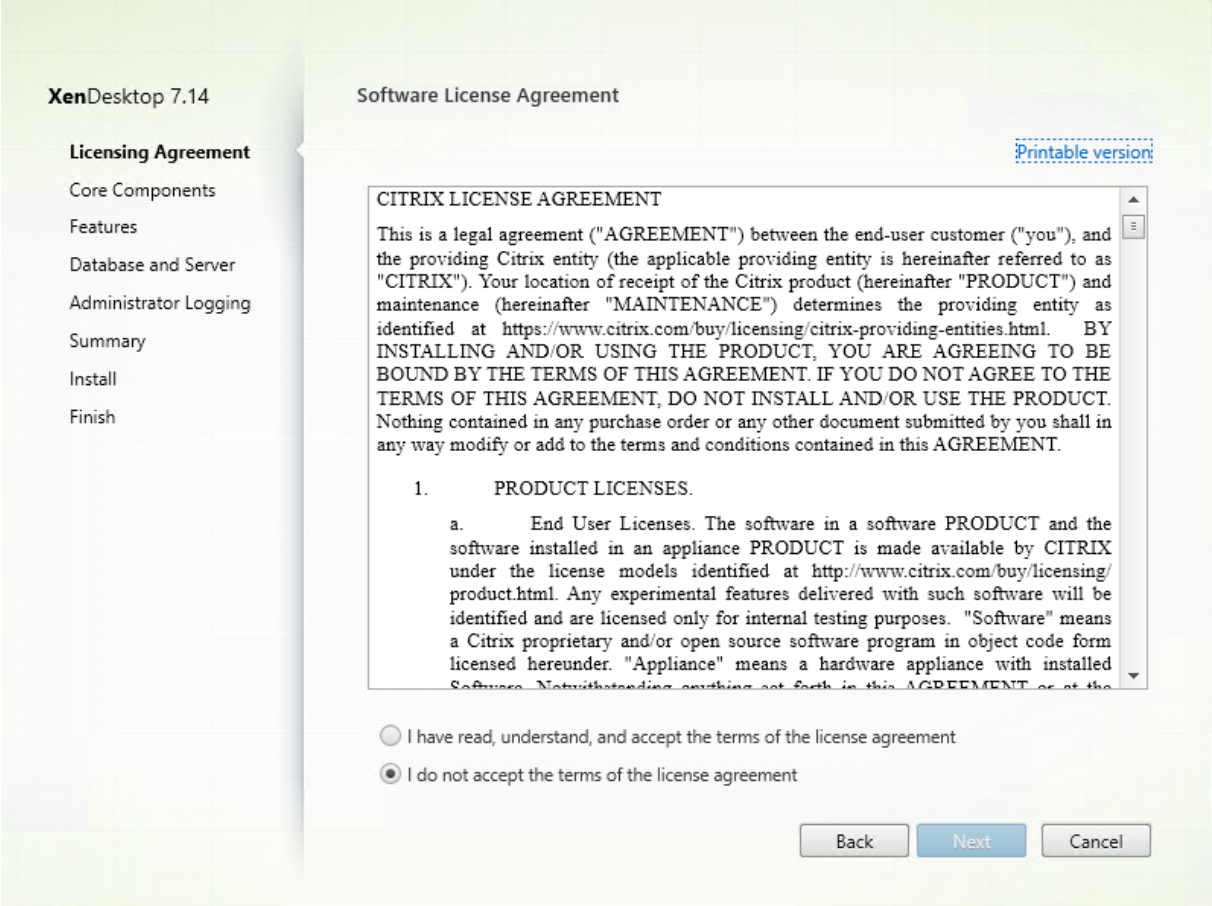
XenApp または **XenDesktop** の横にある ［開始］をクリックして、必要な製品をインストールします。

手順 **3**：**Session Recording** を選択する



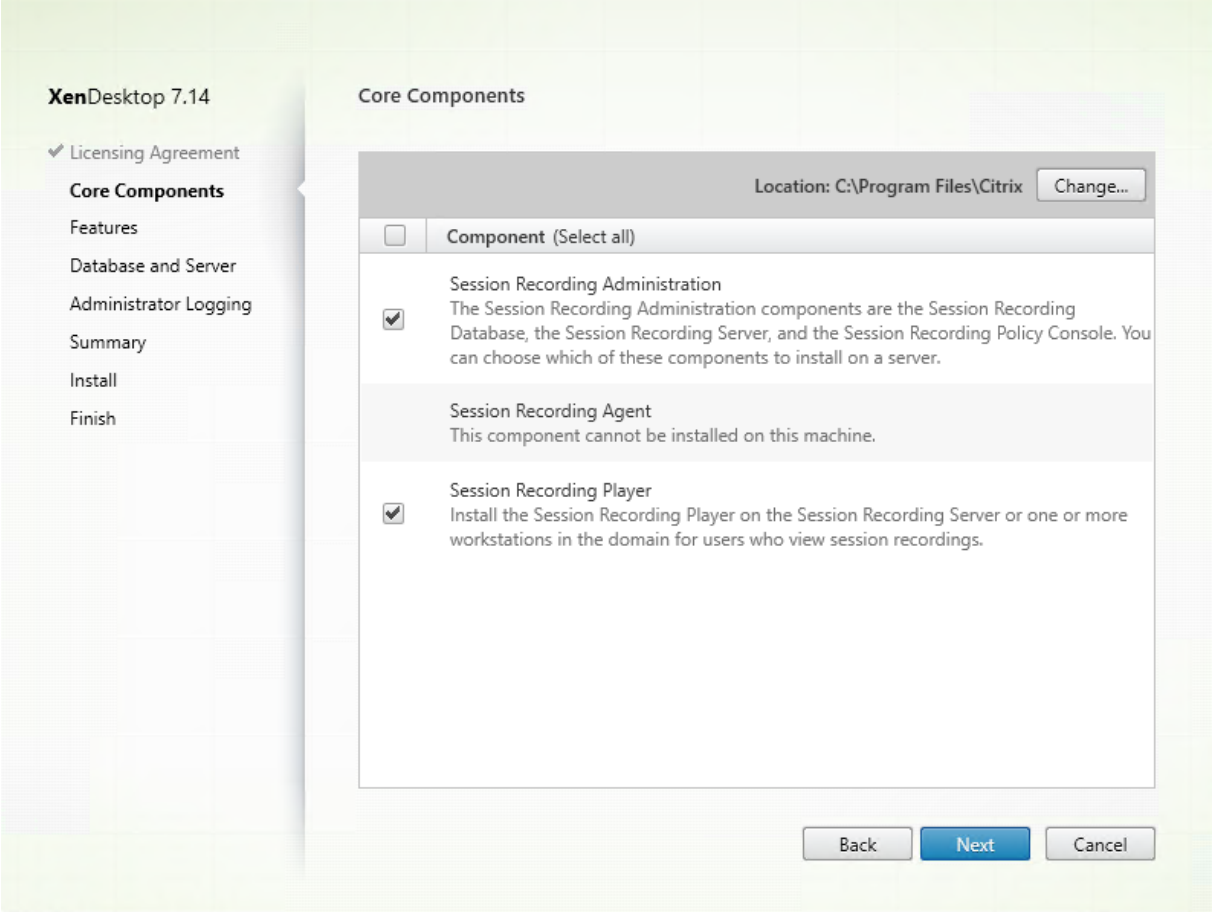
Session Recording エントリを選択します。

手順 **4**：ライセンス契約書を読み、同意する



［ソフトウェアライセンス契約］ページでライセンス契約を読み、同意して ［次へ］をクリックします。

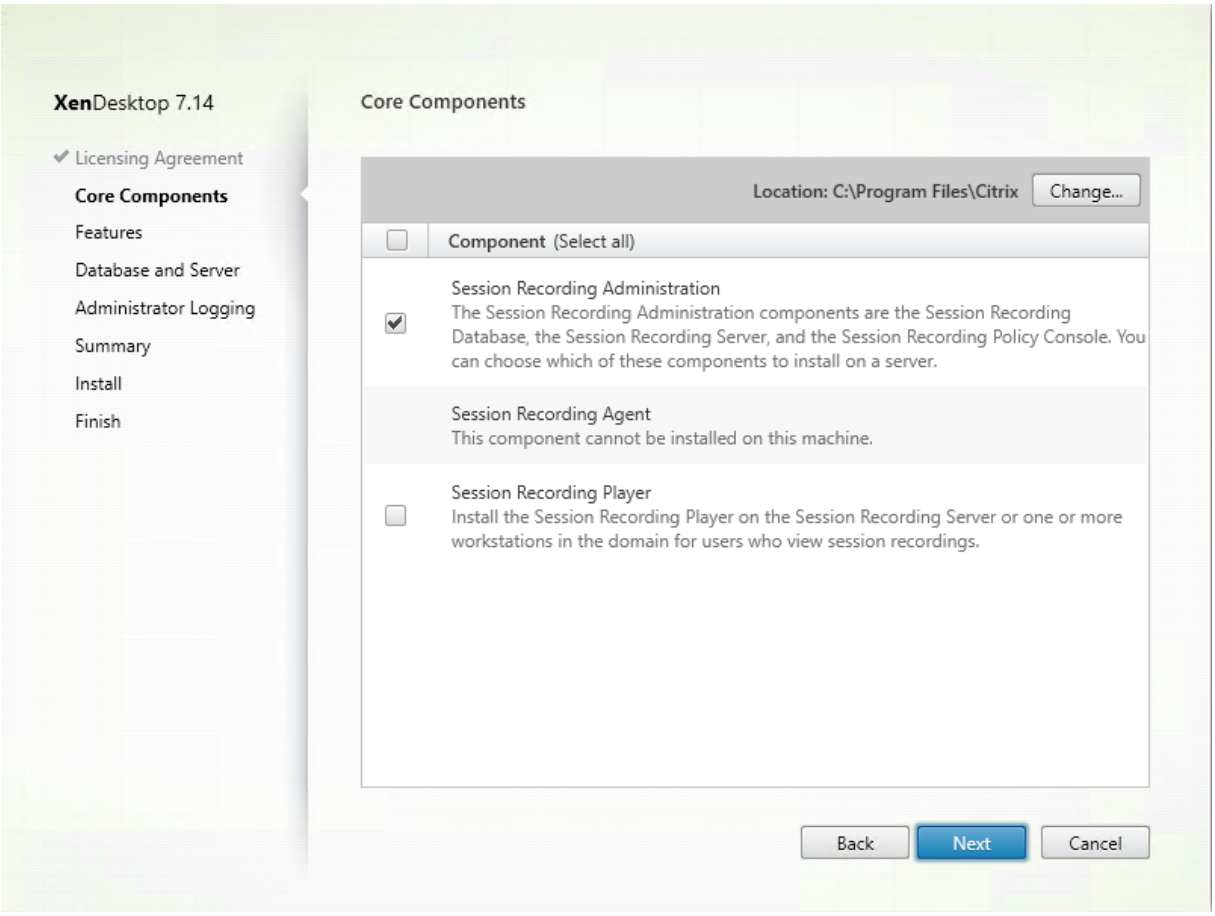
手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



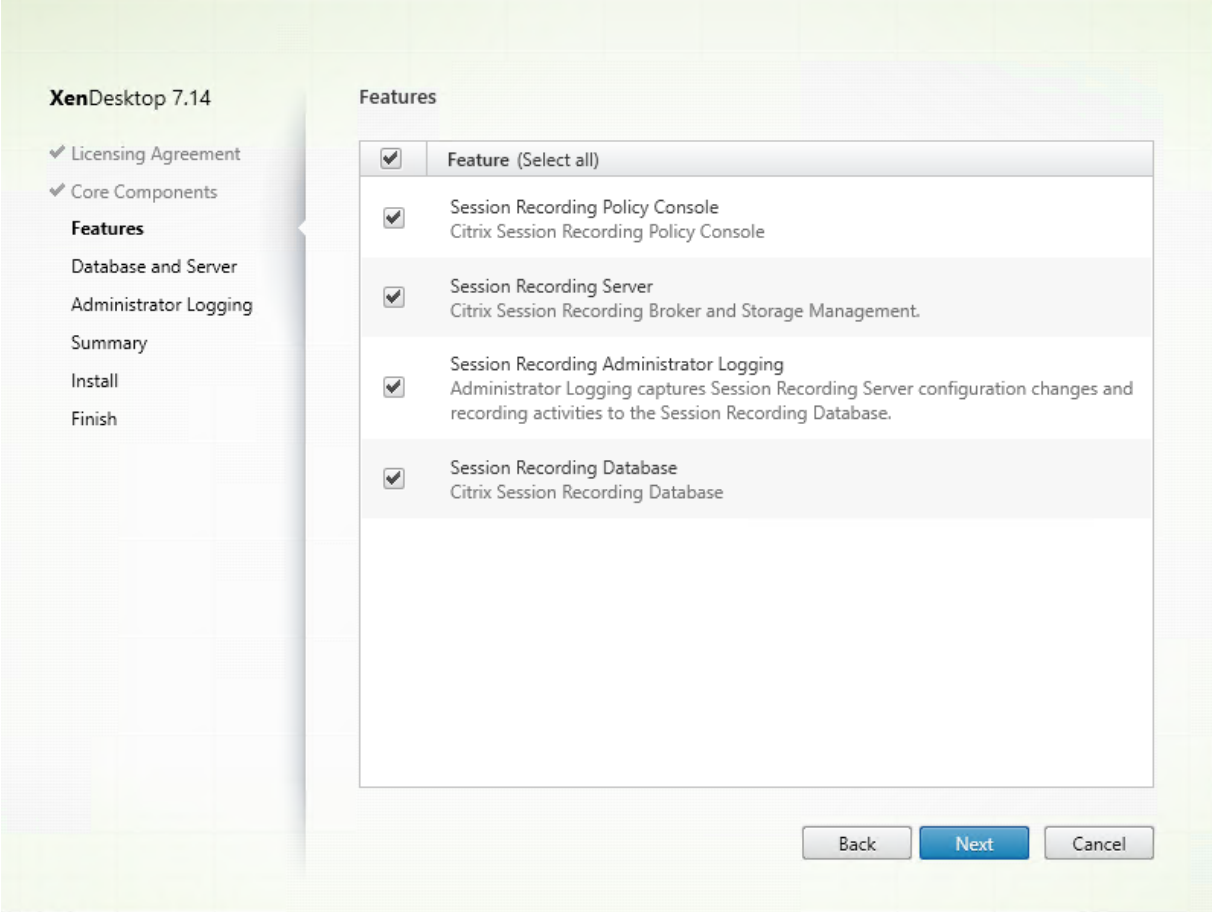
［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、C:\Program Files\Citrix に各コンポーネントがインストールされます。ほとんどの展開ではこれで十分です。任意のインストール場所を指定することもできます。
- コンポーネント：デフォルトでは、インストールするコンポーネントの隣のすべてのチェックボックスがオンになっています。インストーラーは、デスクトップ OS とサーバー OS のいずれの上で実行されているかを認識しています。Session Recording Administration コンポーネントのインストールはサーバー OS のみに許可されます。また、事前に VDA がインストールされていないマシンには、Session Recording Agent のインストールは許可されません。事前に VDA がインストールされていないマシンに Session Recording Agent をインストールする場合、**Session Recording Agent** のオプションは利用できません。

［**Session Recording Administration**］を選択して ［次へ］をクリックします。



手順 **6**：インストールする機能を選択する



［機能］ページで次の作業を行います：

- デフォルトでは、インストールする機能の隣のすべてのチェックボックスがオンになっています。概念実証では、これらすべての機能を 1 つのサーバーにインストールしても構いません。ただし、大規模な実稼働環境の場合は、シトリックスでは Session Recording ポリシーコンソールをインストールしたサーバーとは別のサーバーに、Session Recording サーバー、Session Recording 管理者ログ、および Session Recording データベースをインストールすることをお勧めします。Session Recording 管理者ログは、Session Recording サーバーのオプションのサブ機能であることに注意します。Session Recording 管理者ログを選択する前に、Session Recording サーバーを選択する必要があります。
- 選択した機能をインストールしたサーバーに別の機能を追加するには、MSI パッケージを使う方法に限られます。インストーラーを再実行することはできません。

インストールする機能を選択して ［次へ］をクリックします。

手順 **6.1**：**Session Recording** データベースのインストール

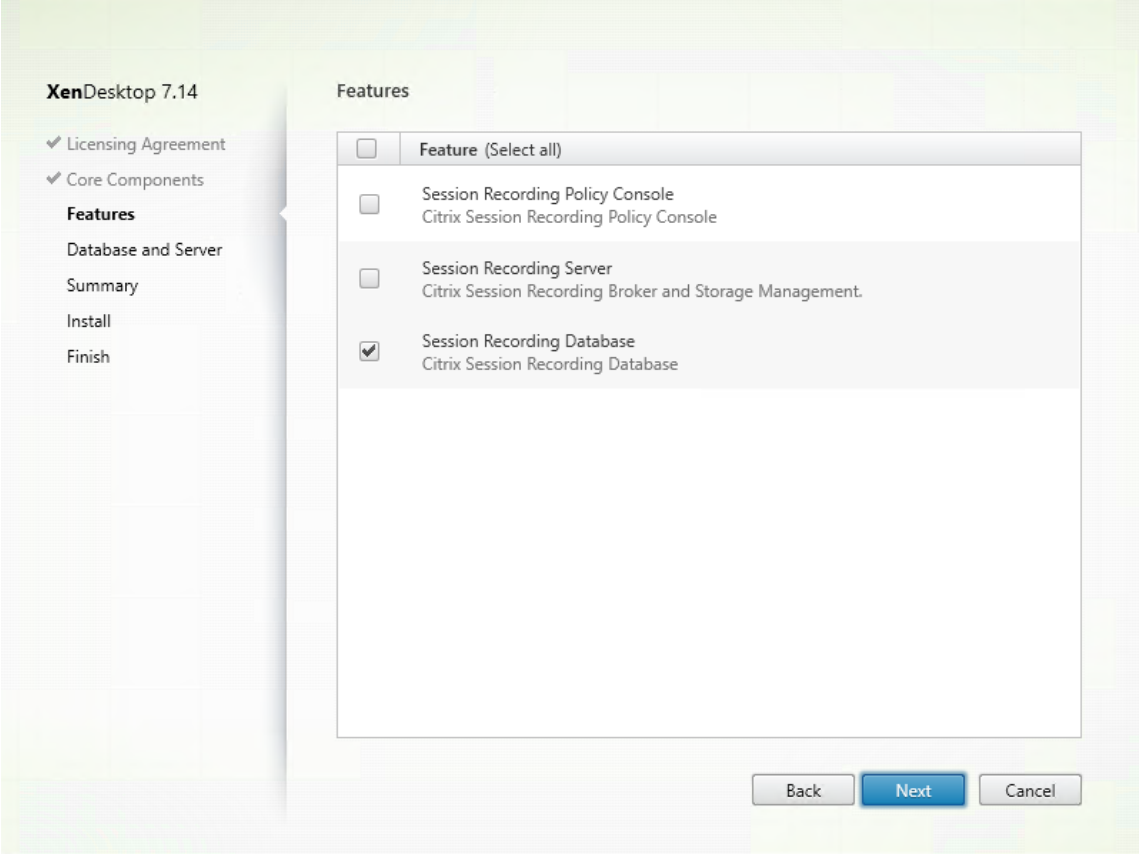
注： Session Recording データベースは実際のデータベースではありません。インストール中に Microsoft SQL Server インスタンスに必要なデータベースを作成して構成する役割のコンポーネントです。Session Recording

では、Microsoft SQL Server に基づくデータベースの高可用性のための 3 つのソリューションをサポートしています。詳しくは、「データベース高可用性をサポートする Session Recording のインストール」を参照してください。

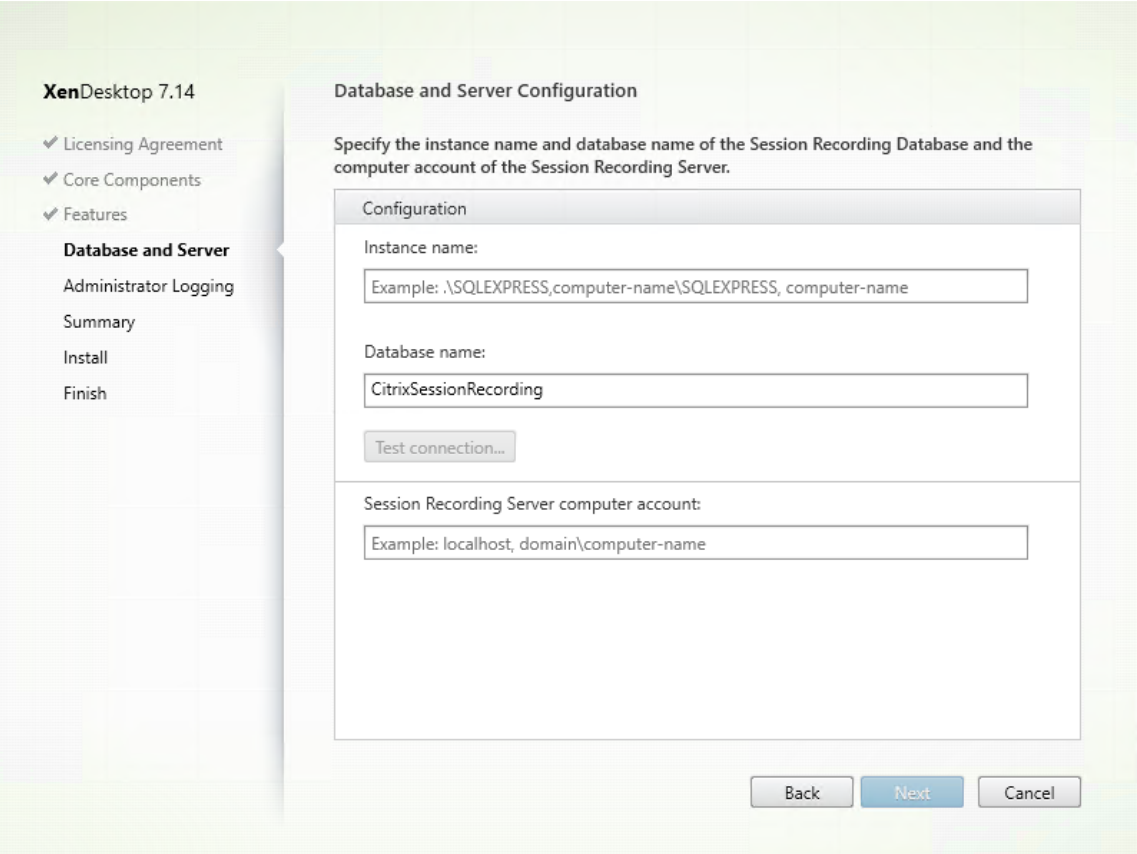
Session Recording データベースと Microsoft SQL Server の展開には、通常以下の 3 種類があります:

- 展開 1: Session Recording サーバーと Session Recording データベースを同じマシンにインストールし、Microsoft SQL Server をリモートマシンにインストールする（推奨）。
- 展開 2: Session Recording サーバー、Session Recording データベース、および Microsoft SQL Server を同じマシンにインストールする。
- 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. ［機能］ページで ［**Session Recording** データベース］を選択して ［次へ］をクリックします。



2. ［データベースおよびサーバーの構成］ページで、Session Recording データベースのインスタンス名とデータベース名、および Session Recording サーバーのコンピューターアカウントを指定します。［次へ］をクリックします。



［データベースおよびサーバーの構成］ページで、次の作業を行います：

- インスタンス名：データベースインスタンスが、インスタンスのセットアップ時に構成した名前付きインスタンスでない場合、SQL Server のコンピューター名のみを使用できます。名前付きインスタンスがある場合は、データベースインスタンス名として computer-name\instance-name を使用します。使用中のサーバーインスタンス名を確認するには、SQL Server で **select @@servername** を実行します。戻り値は、正確なデータベースインスタンス名です。SQL Server がカスタムポート（デフォルトポート 1433 以外）でリスンするように構成されている場合は、インスタンス名にコンマを追加してカスタムリスナーポートを設定します。たとえば、［インスタンス名］テキストボックスで「**DXSBC-SRD-1,2433**」と入力します。コンマの後の「2433」は、カスタムリスナーポートを示します。
- データベース名：［データベース名］テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名を使用します。［接続のテスト］をクリックして、SQL Server インスタンスへの接続とデータベース名の有効性をテストします。

> 重要：
>
> 自由なデータベース名に使用できる文字は、A～Z、a～z、0～9 のみで、123 文字を超えてはなりません。

- データベースの **securityadmin** および **dbcreator** サーバー役割権限が必要です。権限がない場合は、次を行います：
  - データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、

securityadmin および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。

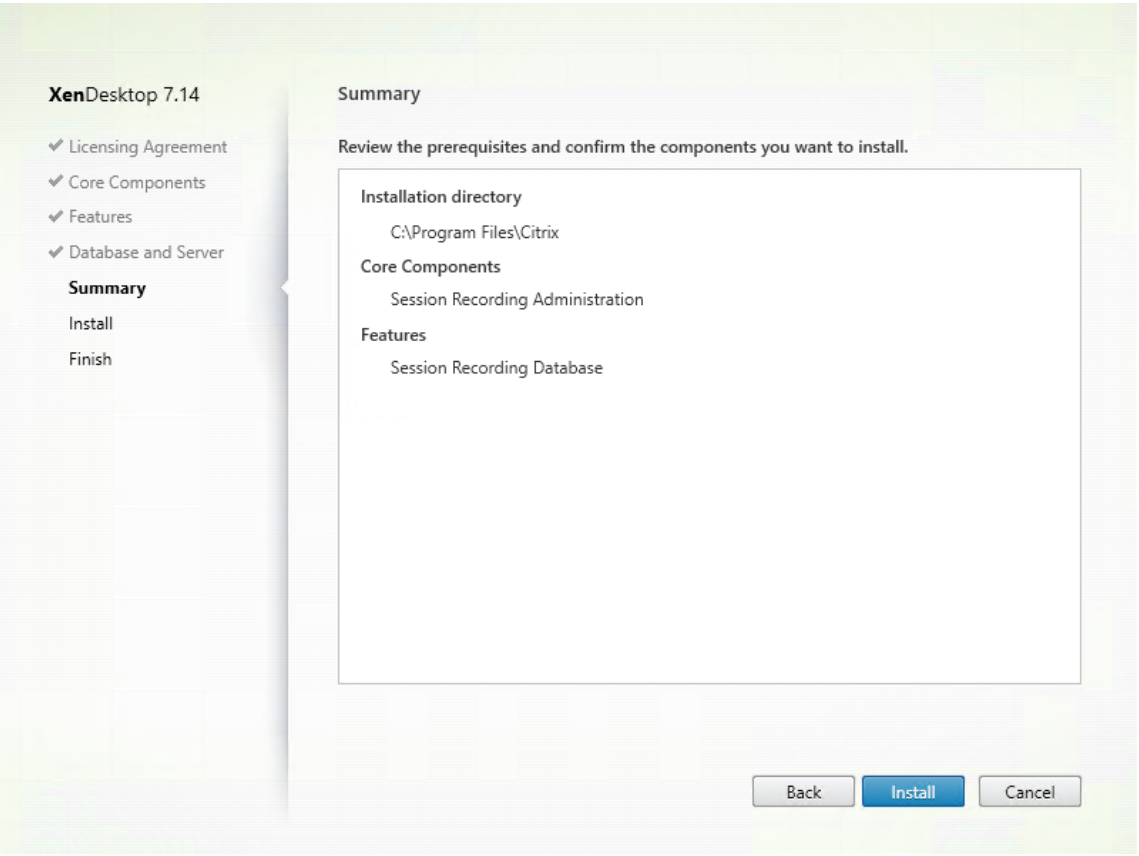
- または、SessionRecordingAdministrationx64.msi パッケージを使用します（ISO ファイルを解凍すると、この msi パッケージが...\x64\Session Recording の下にあります）。msi のインストール中、**securityadmin** および **dbcreator** サーバー役割権限と共に、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、[**OK**] をクリックし、インストールを続行します。

  インストールにより新しい Session Recording データベースが作成され、Session Recording サーバーのマシンアカウントが **db_owner** として追加されます。

- **Session Recording** サーバーのコンピューターアカウント:
  - 展開 **1** と展開 **2**: **Session Recording** サーバーの［コンピューターアカウント］フィールドで、「**localhost**」と入力します。
  - 展開 **3**: Session Recording サーバーをホストするコンピューターの名前を、「ドメイン\コンピューター名」の形式で入力します。Session Recording サーバーのコンピューターアカウントは、Session Recording データベースにアクセスするためのユーザーアカウントです。

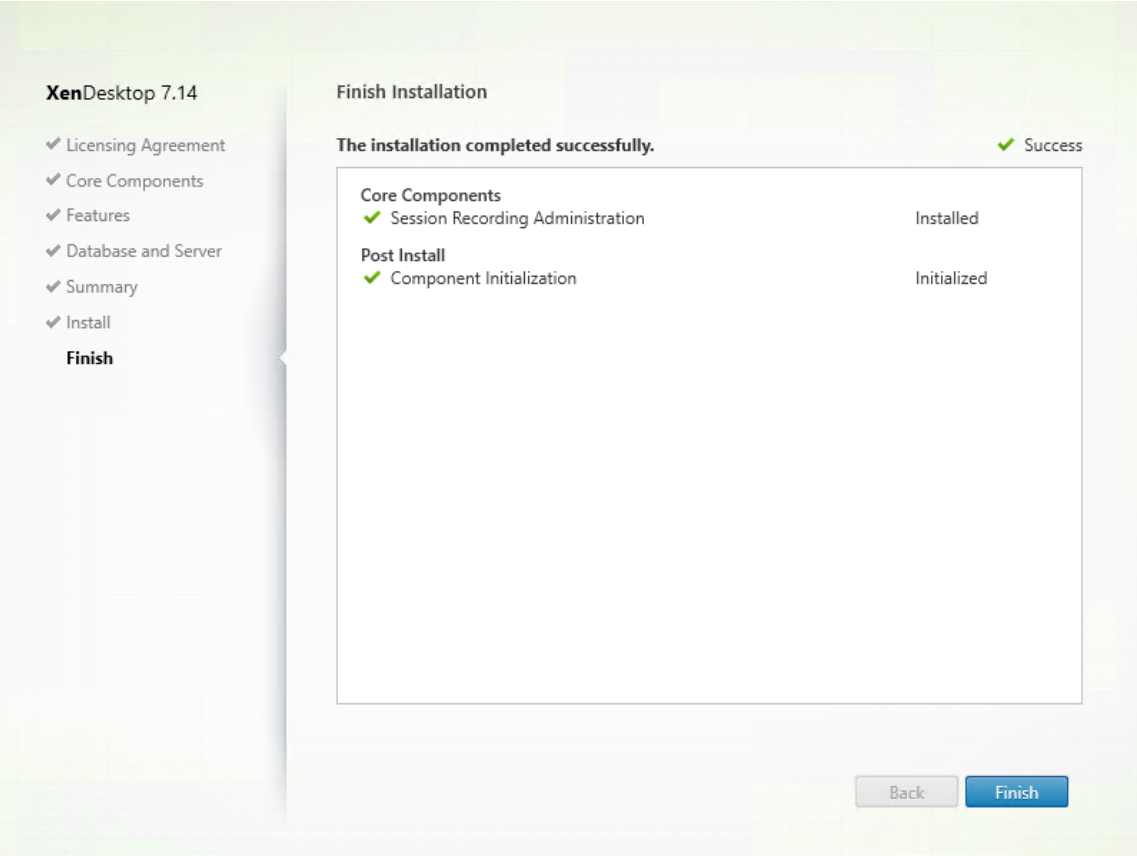
  注:［**Session Recording** サーバーコンピューターアカウント］フィールドにドメイン名が設定されているときに、Session Recording Administration コンポーネントをインストールしようとすると、エラーコード 1603 で失敗することがあります。回避策として、**localhost** または NetBIOS ドメイン名\マシン名を ［**Session Recording** サーバーコンピューターアカウント］フィールドに入力してください。

3. インストール前に前提条件を確認します。



［概要］ページにインストールの選択が表示されます。［戻る］をクリックして前のウィザードページに戻り、選択を変更できます。または、［インストール］をクリックしてインストールを開始します。

4. インストールを完了します。

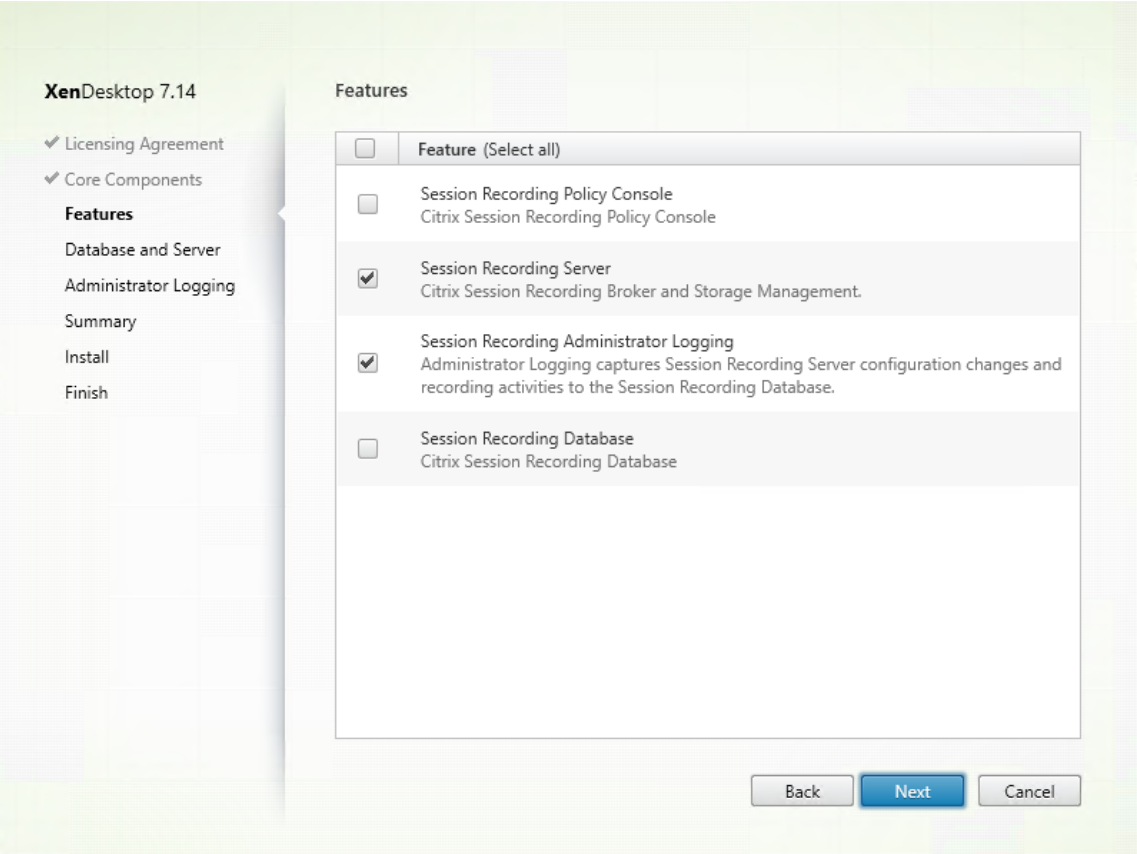


［インストールの完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックして Session Recording データベースのインストールを完了します。

手順 **6.2**：**Session Recording** サーバーのインストール

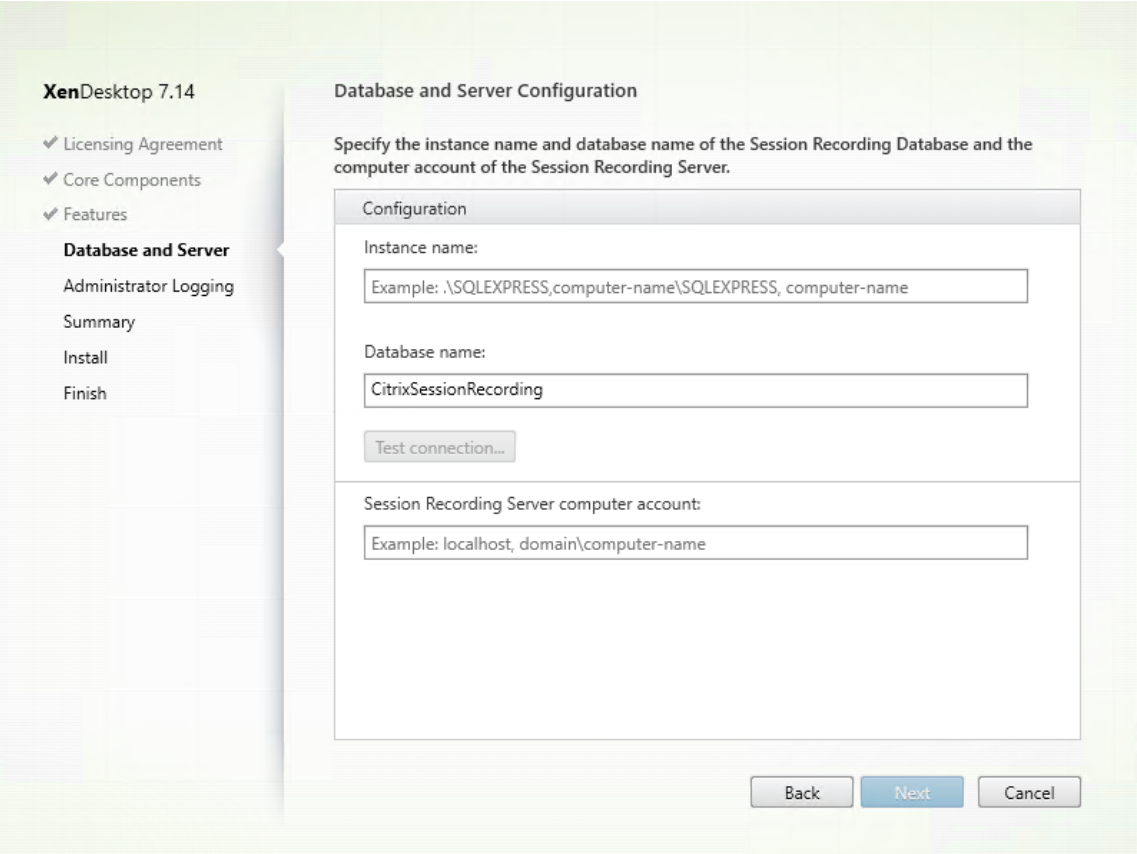
1. ［機能］ページで、［**Session Recording** サーバー］と ［**Session Recording** 管理者ログ］を選択します。［次へ］をクリックします。



注:

- Session Recording 管理者ログは、Session Recording サーバーのオプションのサブ機能です。Session Recording 管理者ログを選択する前に、Session Recording サーバーを選択する必要があります。
- シトリックスでは、Session Recording 管理者ログと Session Recording サーバーを同時にインストールすることをお勧めします。管理者ログ機能を有効にしない場合は、後のページで無効にできます。ただし、最初にこの機能をインストールしない選択をし、後で追加する場合は、SessionRecordingAdministrationx64.msi パッケージを使用して手動で追加するしかありません。

2. [データベースおよびサーバーの構成] ページで、構成を指定します。



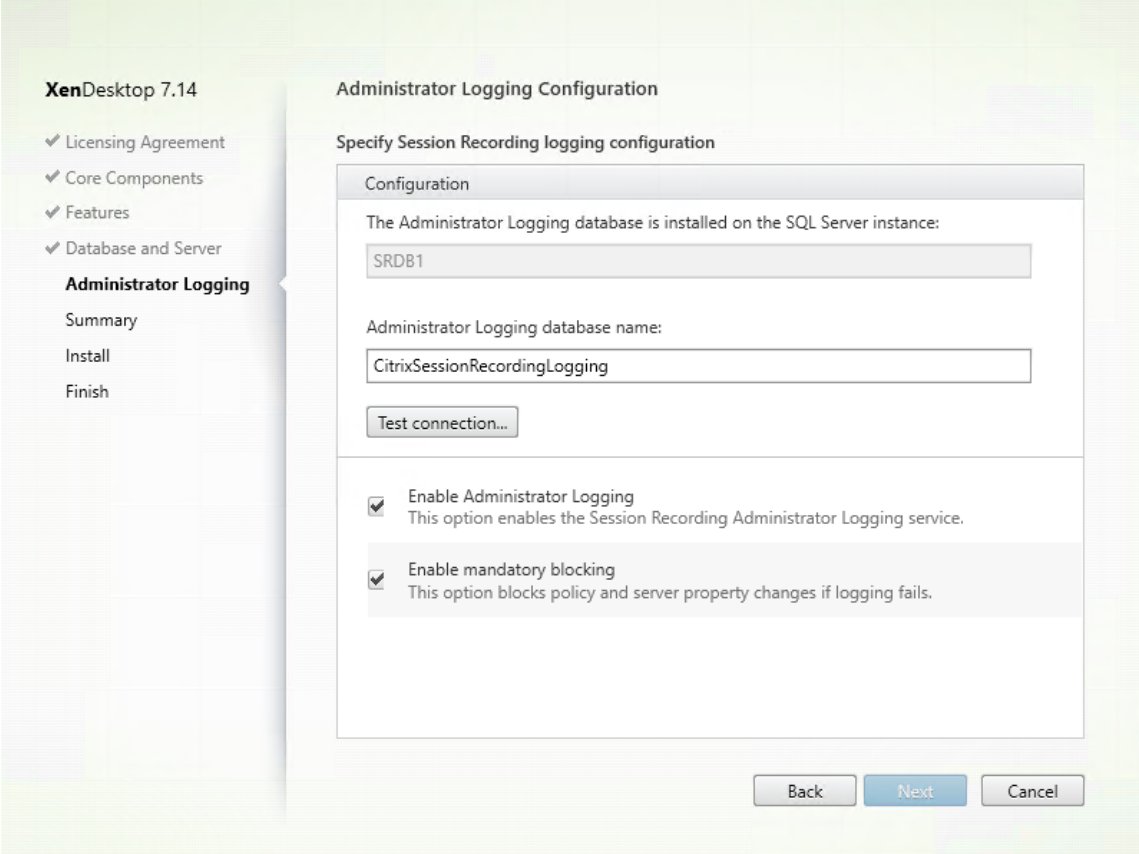
［データベースおよびサーバーの構成］ページで、次の作業を行います：

- インスタンス名：［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。SQL Server がカスタムポート（デフォルトポート 1433 以外）でリスンするように構成されている場合は、インスタンス名にコンマを追加してカスタムリスナーポートを設定します。たとえば、［インスタンス名］テキストボックスで「**DXSBC-SRD-1,2433**」と入力します。コンマの後の「2433」は、カスタムリスナーポートを示します。
- データベース名：［データベース名］テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名 **CitrixSessionRecording** を使用します。
- データベースの **securityadmin** および **dbcreator** サーバー役割権限が必要です。権限がない場合は、次を行います：
  - データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、**securityadmin** および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、SessionRecordingAdministrationx64.msi パッケージを使用して Session Recording サーバーをインストールします。msi のインストール中、**securityadmin** および **dbcreator** サーバー役割権限と共に、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、［**OK**］をクリックし、インストールを続行します。
- 正しいインスタンス名とデータベース名を入力したら、［接続のテスト］をクリックして Session

Recording データベースへの接続をテストします。

- Session Recording サーバーのコンピューターアカウントを入力して、［次へ］をクリックします。

3. ［管理者ログの構成］ページで、管理者ログ機能の構成を指定します。



［管理者ログの構成］ページで、次の作業を行います：

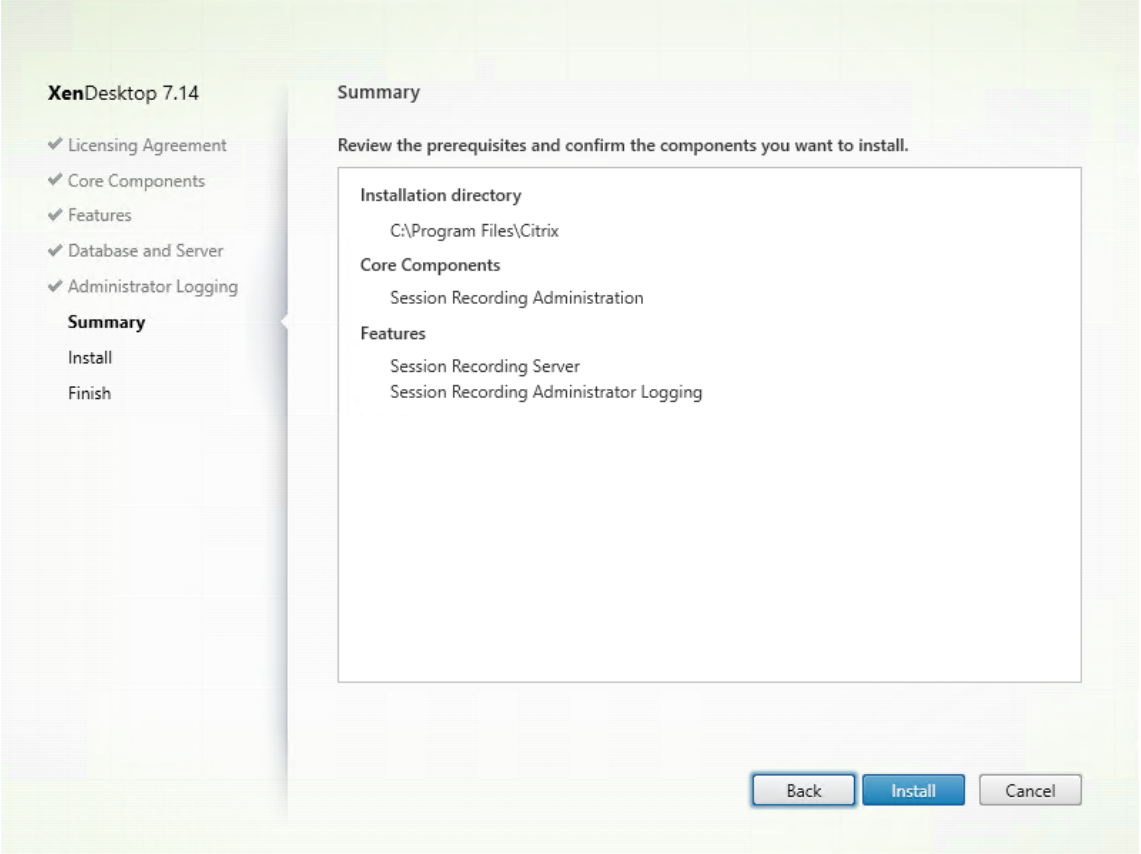
- 管理者ログデータベースは **SQL Server** インスタンスにインストールされます：このテキストボックスは編集できません。管理者ログデータベースの SQL Server インスタンス名は、［データベースおよびサーバーの構成］ページで入力したインスタンス名が自動的に適用されます。
- 管理者ログデータベース名：Session Recording 管理者ログ機能のインストールを選択した場合、このテキストボックスで管理者ログデータベースの任意のデータベース名を入力するか、またはテキストボックスに事前設定されたデフォルトのデータベース名 **CitrixSessionRecordingLogging** を使用します。

  注：管理者ログデータベース名は ［データベースとサーバーの構成］ページの ［データベース名］テキストボックスで設定した Session Recording データベース名と異なるものにする必要があります。
- 管理者ログデータベース名を入力したら、［接続のテスト］をクリックして管理者ログデータベースへの接続をテストします。
- 管理者ログを有効にする：デフォルトでは、管理者ログ機能は有効になっています。チェックボックスをオフにしてこの機能を無効にできます。
- 強制ブロッキングを有効にする：デフォルトでは強制ブロッキングが有効になっているため、ログが失

敗すると通常の機能がブロックされることがあります。チェックボックスをオフにして強制ブロッキングを無効にできます。

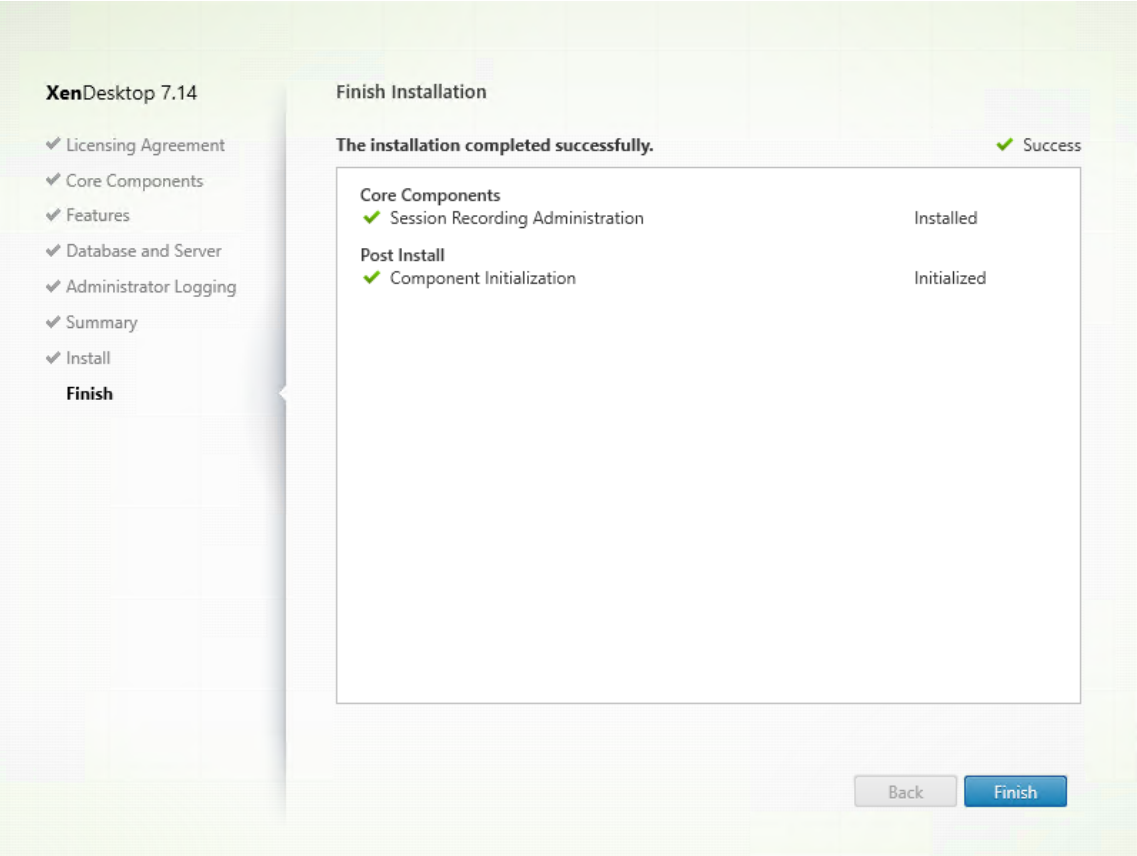
［次へ］をクリックしてインストールを続行します。

4. インストール前に前提条件を確認します。



［概要］ページにインストールの選択が表示されます。［戻る］をクリックして前のウィザードページに戻り、選択を変更できます。または、［インストール］をクリックしてインストールを開始します。

5. インストールを完了します。



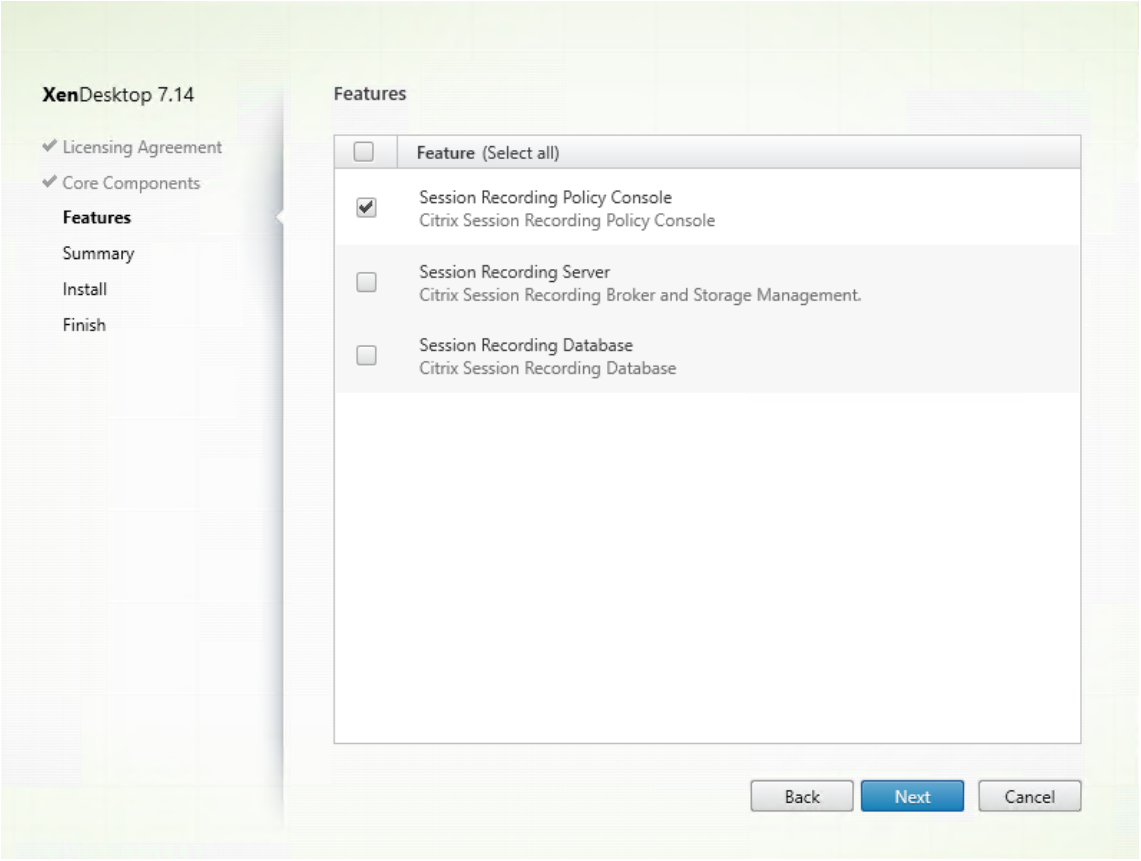
［インストールの完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックして Session Recording サーバーのインストールを完了します。

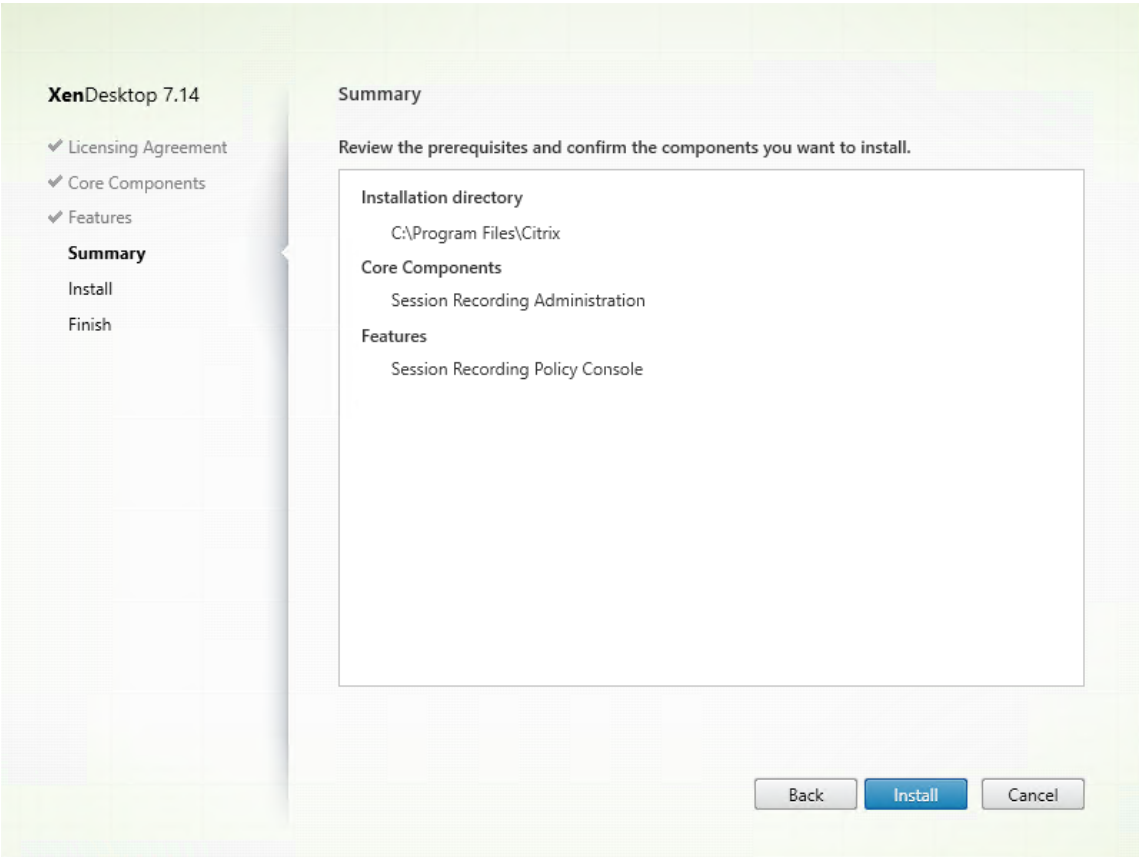
注： Session Recording サーバーのデフォルトのインストールでは、通信をセキュリティで保護するため HTTPS/TLS を使用します。Session Recording サーバーのデフォルト IIS サイトで TLS が構成されていない場合は、HTTP を使用します。これを実行するには、Session Recording Broker サイトに移動して IIS 管理コンソールで SSL を選択解除し、SSL 設定を開き、［**SSL** を必要とする］ボックスをオフにします。

手順 **6.3**：**Session Recording** ポリシーコンソールのインストール

1. ［機能］ページで ［**Session Recording** データベース］を選択して ［次へ］をクリックします。

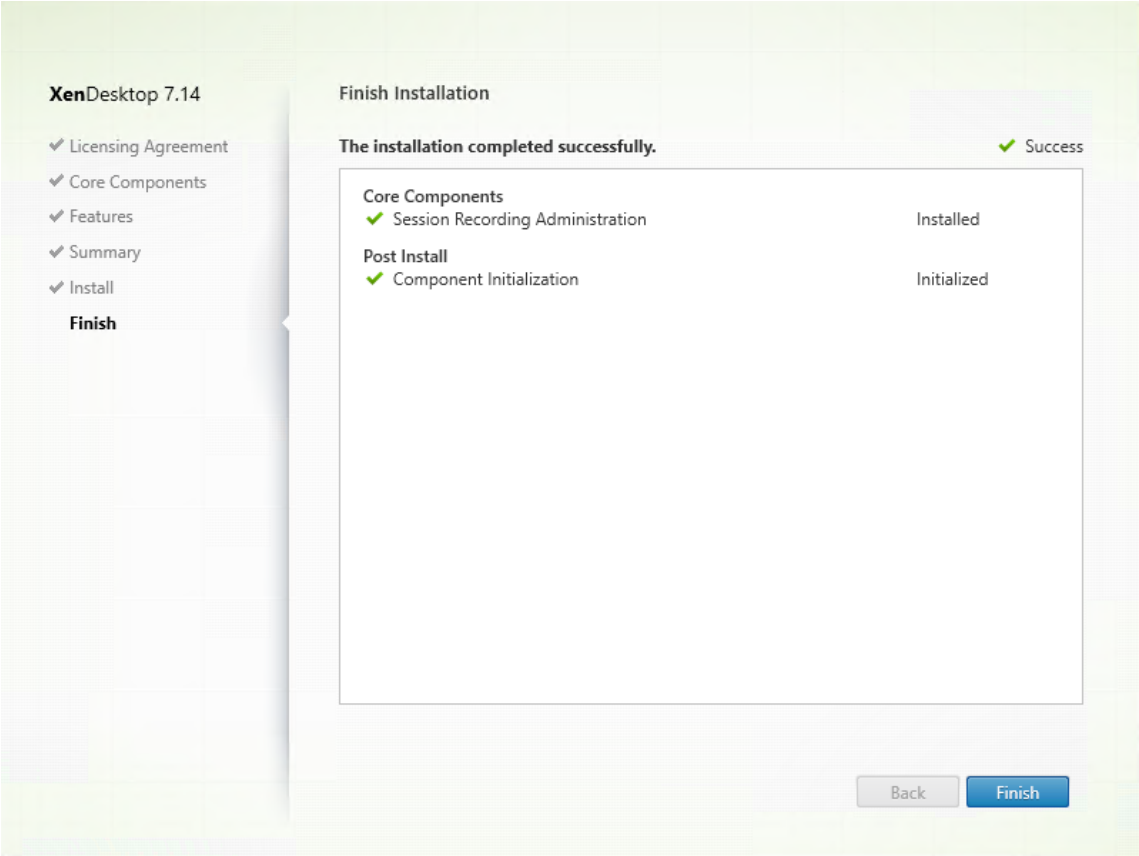


2. インストール前に前提条件を確認します。



［概要］ページにインストールの選択が表示されます。［戻る］をクリックして前のウィザードページに戻り、選択を変更できます。または、［インストール］をクリックしてインストールを開始します。

3. インストールを完了します。



［インストールの完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックして Session Recording ポリシーコンソールのインストールを完了します。

手順 **7**：**Broker_PowerShellSnapIn_x64.msi** をインストールする

重要： Session Recording ポリシーコンソールを使用するには、Broker PowerShell スナップイン（Broker_PowerShellSnapIn_x64.msi）をインストールする必要があります。スナップインは、インストーラーによって自動的にインストールされません。XenApp および XenDesktop の ISO（\layout\image-full\x64\Citrix Desktop Delivery Controller の下にあります）でスナップインを検索し、指示に従って手動でインストールする必要があります。従わない場合、エラーが発生する可能性があります。

Director を構成して **Session Recording** サーバーを使用する

Director コンソールを使用して、Session Recording ポリシーを作成およびアクティブ化できます。

1. HTTPS 接続の場合は、Director サーバーの［信頼されたルート証明書］に Session Recording サーバーを信頼する証明書をインストールします。
2. Session Recording サーバーを使用するように Director サーバーを構成するには、**C:\inetpub\wwwroot\Director\to /configsessionrecording** コマンドを実行します。

3. Director サーバーで、Session Recording サーバーの IP アドレスまたは FQDN、ポート番号、および Session Recording Agent が Session Recording Broker との接続に使用する接続の種類（HTTP または HTTPS）を入力します。

Session Recording Agent のインストール

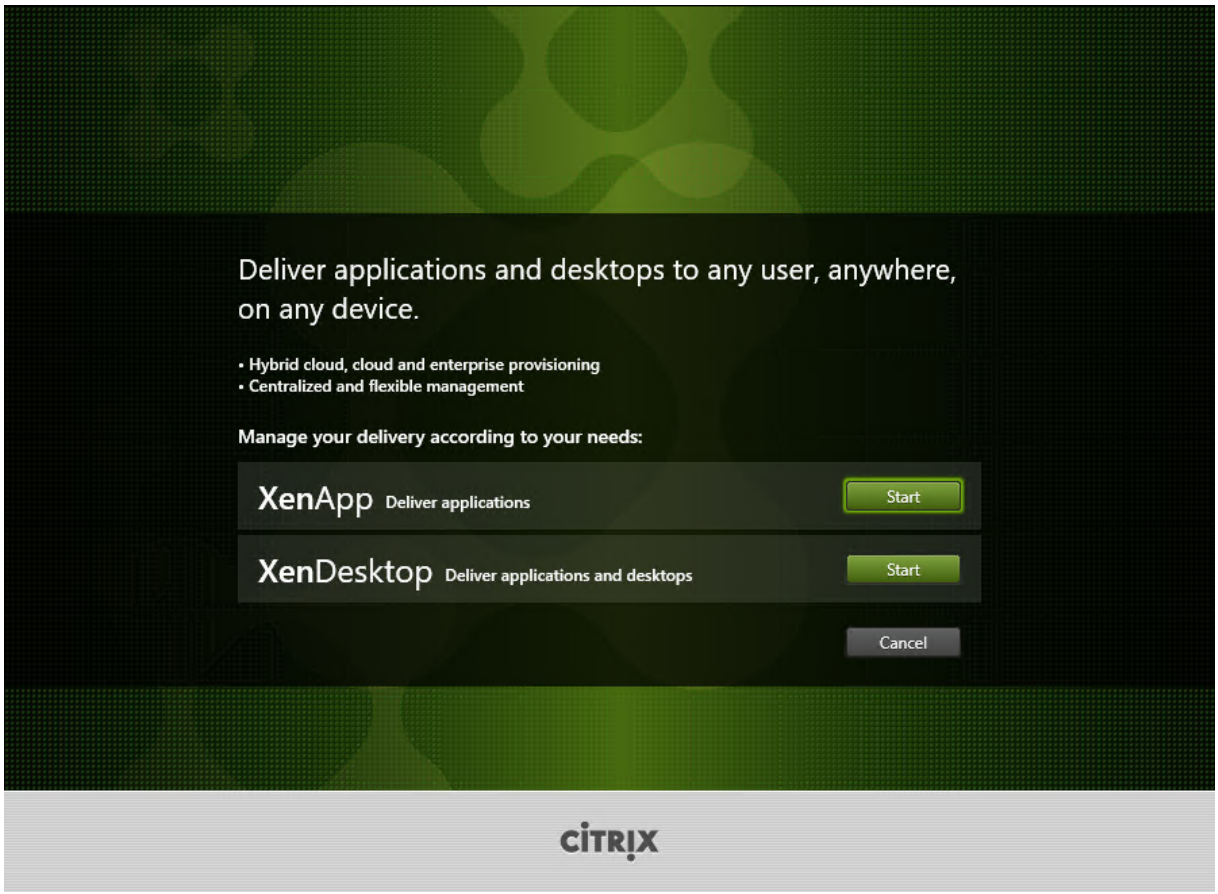
Session Recording Agent は、セッションを録画する VDA または VDI マシンにインストールする必要があります。

手順 **1**：製品ソフトウェアをダウンロードしてウィザードを起動する

ローカルの管理者アカウントを使って、Session Recording Agent コンポーネントのインストール先マシンにログオンします。DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

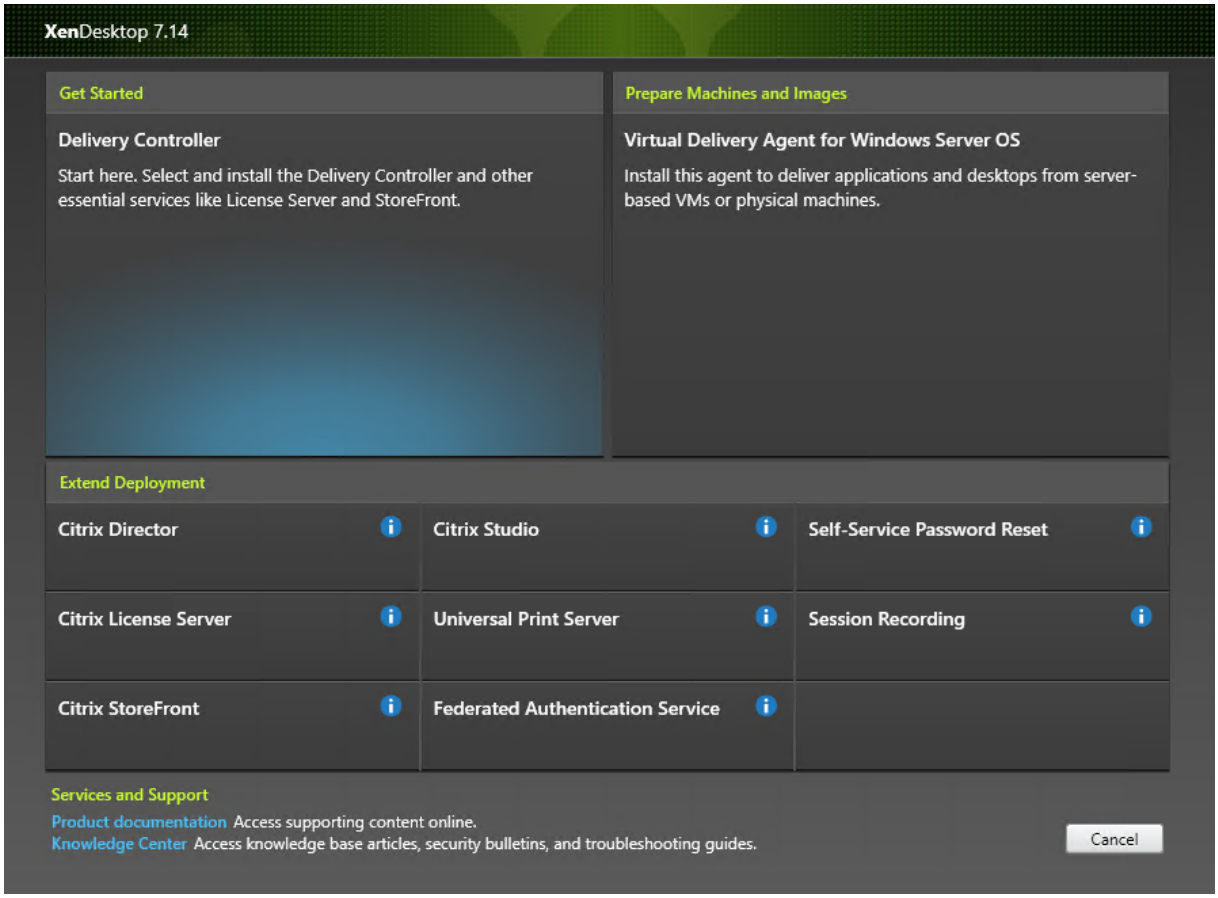
インストールウィザードが起動します。

手順 **2**：インストールする製品を選択する



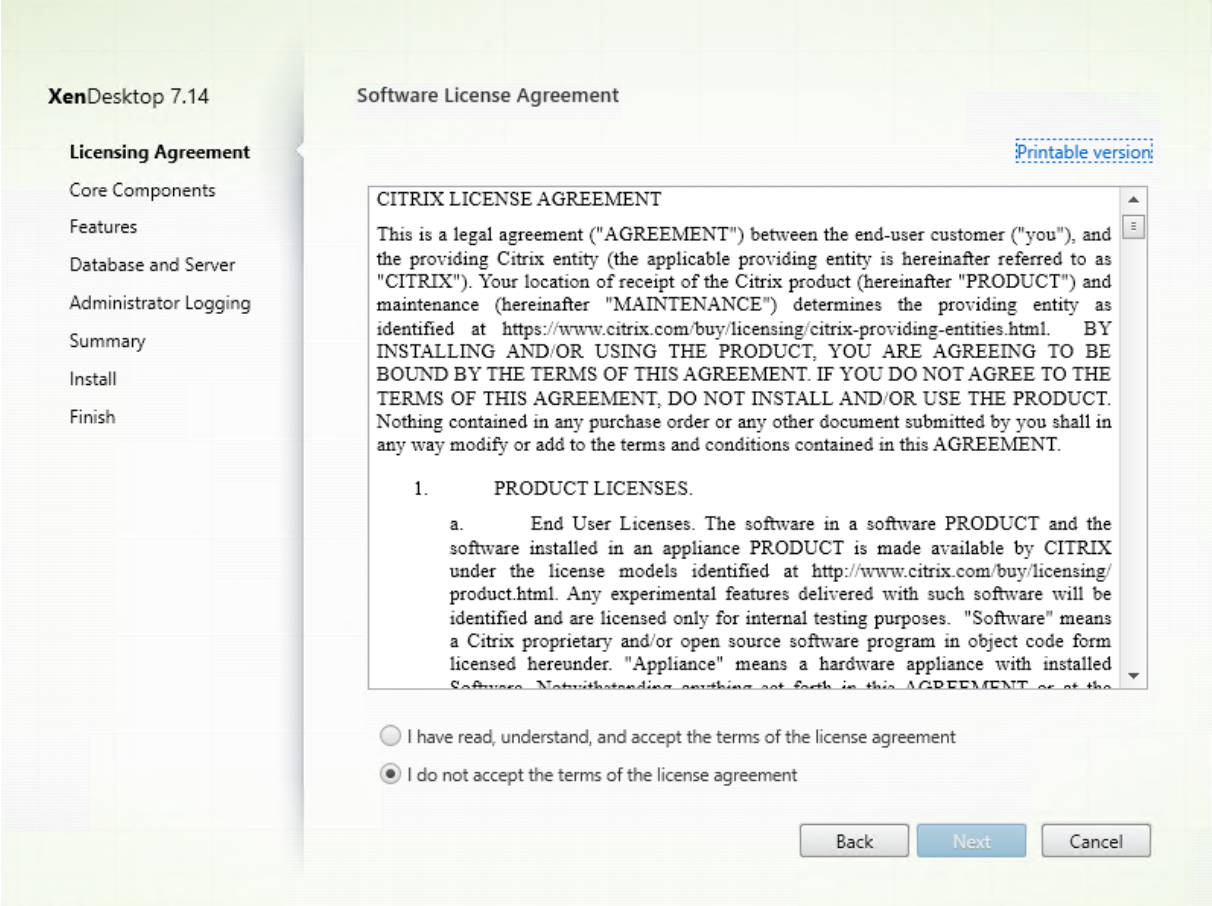
XenApp または **XenDesktop** の横にある ［開始］をクリックして、必要な製品をインストールします。

手順 **3**：**Session Recording** を選択する



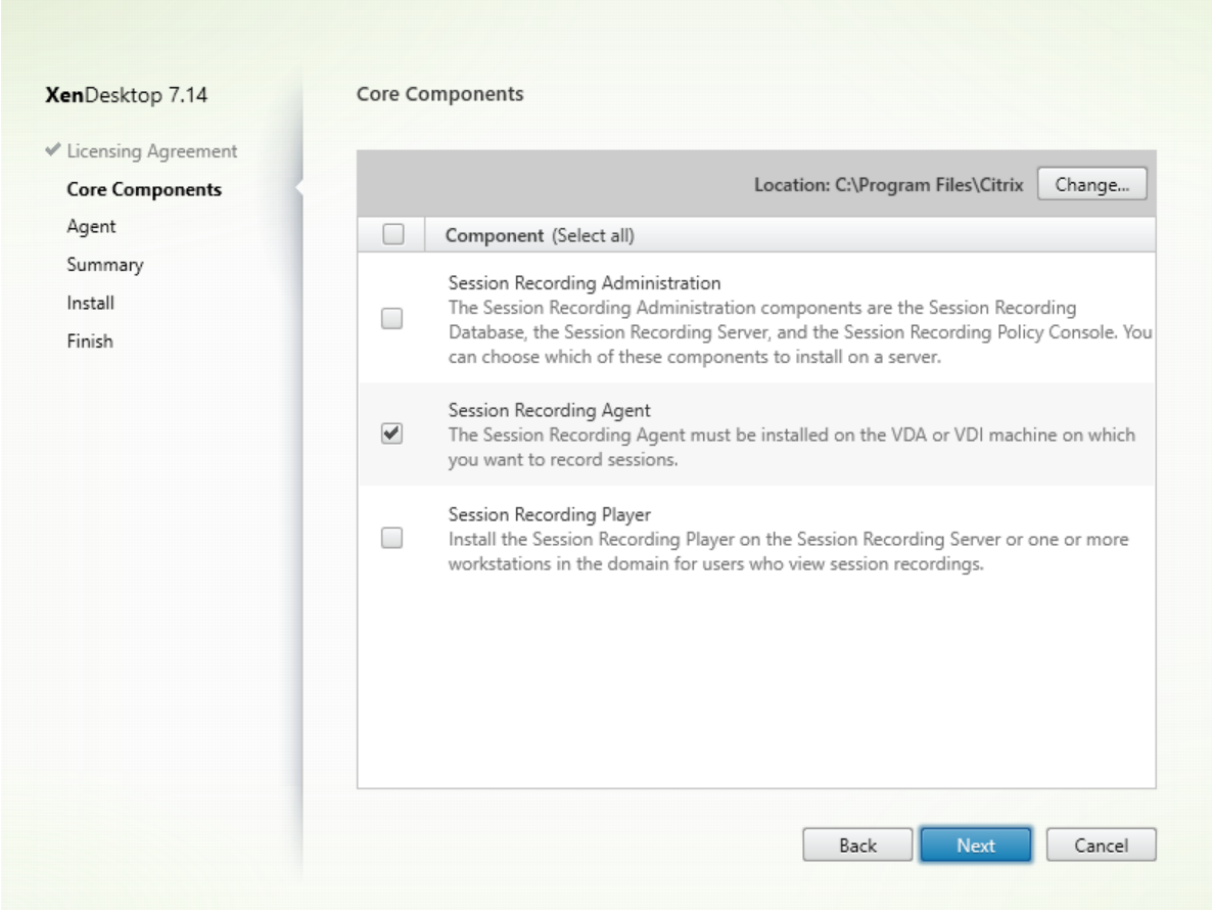
Session Recording エントリを選択します。

手順 **4**：ライセンス契約書を読み、同意する



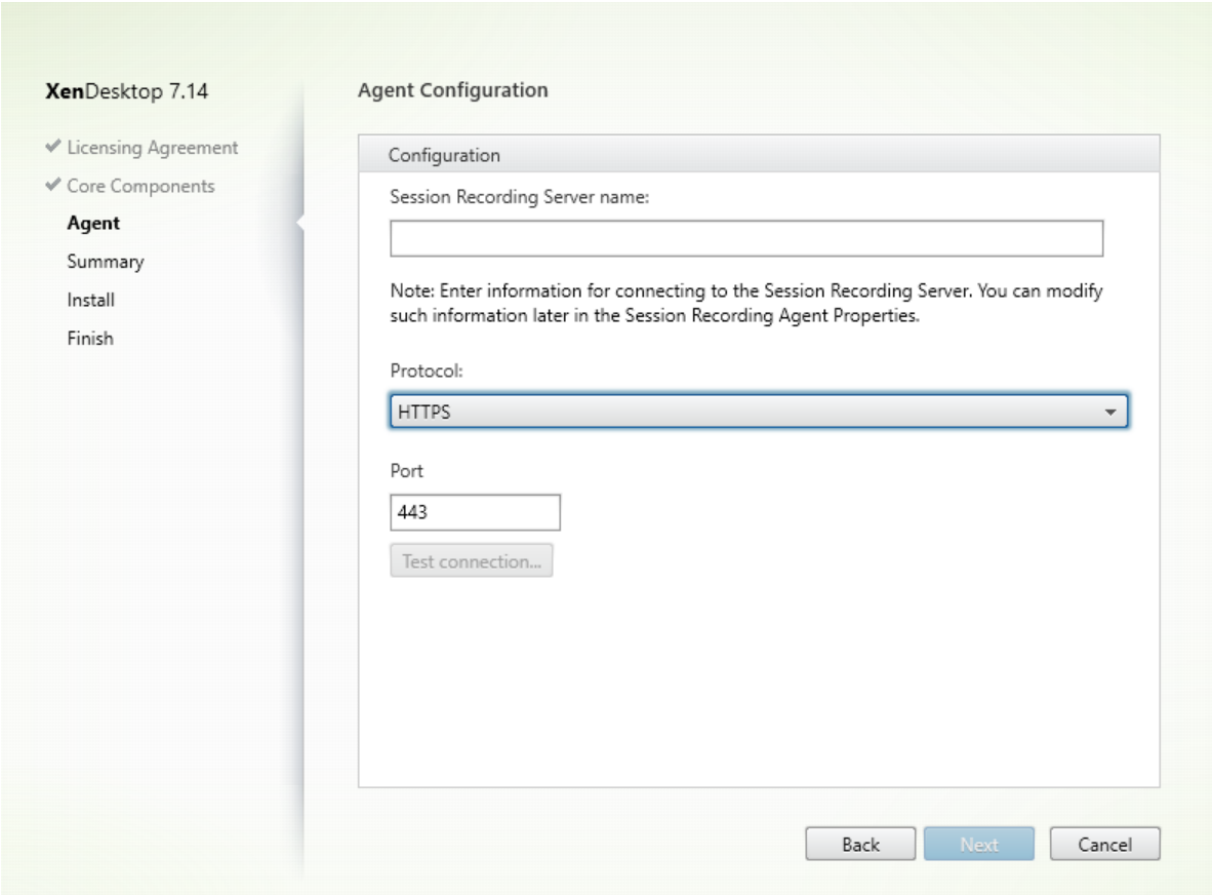
［ソフトウェアライセンス契約］ページでライセンス契約を読み、同意して ［次へ］をクリックします。

手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



［**Session Recording Agent**］を選択して ［次へ］をクリックします。

手順 **6**：**Agent** の構成を指定する

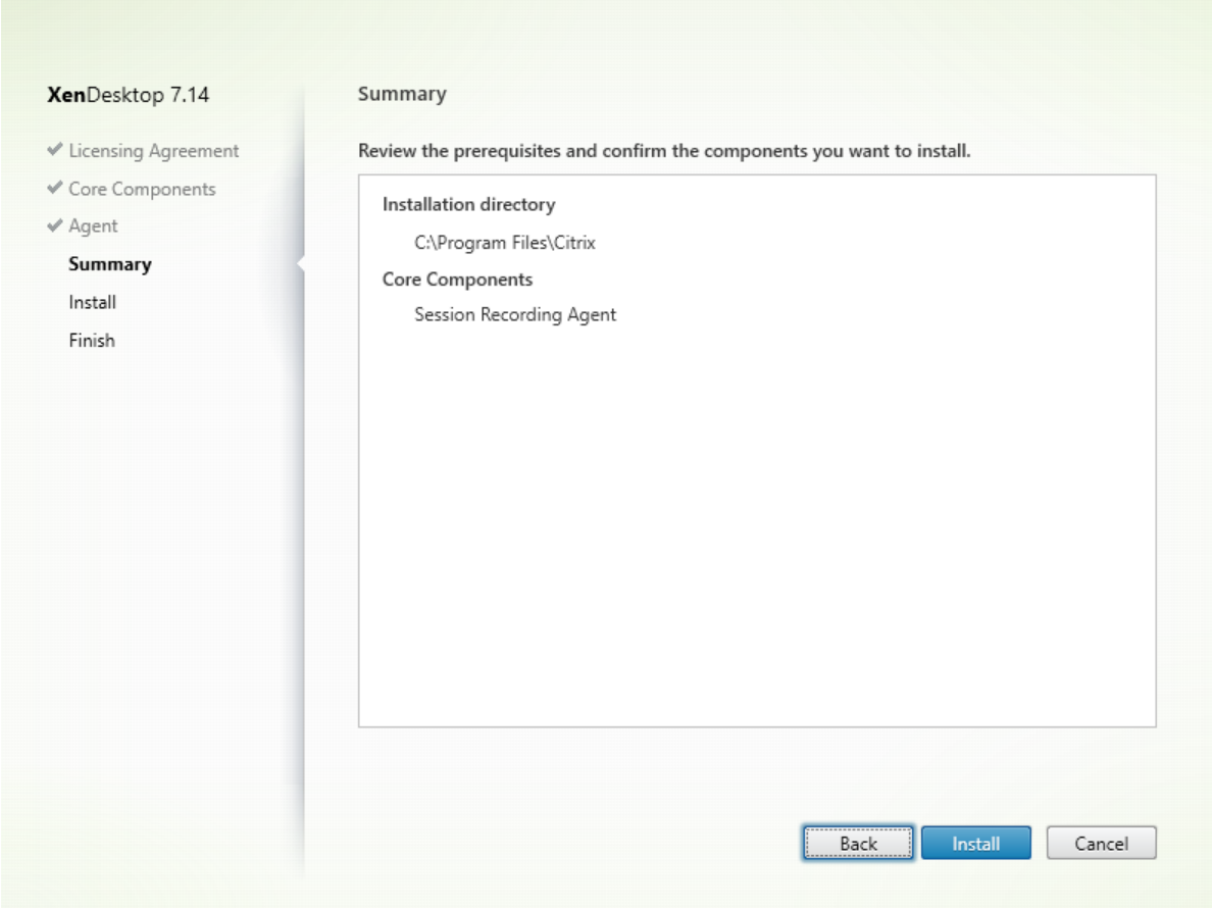


［エージェント構成］ページで、次の作業を行います：

- Session Recording サーバーを事前にインストールしている場合は、Session Recording サーバーをインストールしたコンピューターの名前と、Session Recording サーバーとの接続のプロトコルとポート情報を入力します。Session Recording のインストールが済んでいない場合は、後で ［**Session Recording Agent** のプロパティ］でこれらの情報を変更できます。

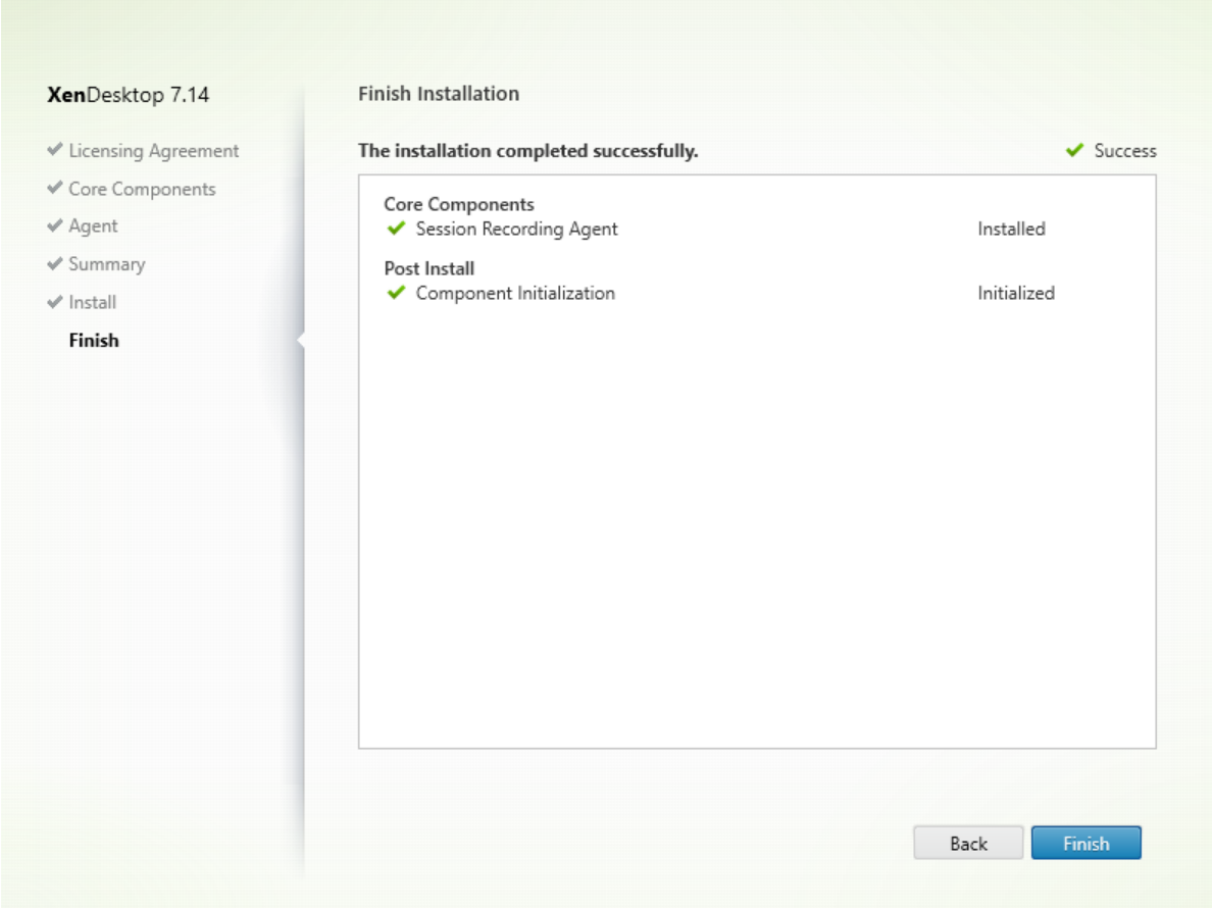
注：インストーラーのテスト接続機能には制限があります。「HTTPS が TLS 1.2 を必要とする」シナリオはサポートしていません。このシナリオでインストーラーを使用する場合はテスト接続に失敗しますが、失敗を無視して ［次へ］をクリックし、インストールを続行できます。これによって通常の機能が影響を受けることはありません。

手順 **7**：インストール前に前提条件を確認する



［概要］ページにインストールの選択が表示されます。［戻る］をクリックして前のウィザードページに戻り、選択を変更できます。または、［インストール］をクリックしてインストールを開始します。

手順 **8**：インストールを完了する



［インストールの完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックして Session Recording Agent のインストールを完了します。

注： Machine Creation Services（MCS）または Provisioning Services（PVS）で、構成済みのマスターイメージとインストール済みの Microsoft Message Queuing（MSMQ）を使用して複数の VDA を作成すると、一定の状況下において、これらの VDA の QMId が同じになる可能性があります。これは、次のようなさまざまな問題が発生する原因となる場合があります：

- 録画契約が承認されていても、セッションが録画されない場合があります。
- セッションのログオフ信号が Session Recording サーバーによって受信されず、セッションのステータスが常に［ライブ］になってしまう可能性があります。

解決策は VDA ごとに固有の QMId を作成することですが、方法は展開方法によって異なります。

Session Recording Agent がインストールされたデスクトップ OS の VDA を、PVS 7.7 以降または MCS 7.9 以降のバージョンを使用して静的デスクトップモードで作成する場合（たとえば、すべての変更が別の Personal vDisk または VDA のローカルディスクで永続的になるように構成する場合）、追加の操作は不要です。

サーバー OS の VDA が MCS または PVS とデスクトップ OS の VDA を使用して作成され、ユーザーがログオフする

とすべての変更が削除されるように構成されている場合は、GenRandomQMID.ps1 スクリプトを使用してシステム起動時に QMId を変更します。電源管理方法を変更して、ユーザーがログインを試行する前に十分な数の VDA が実行されているようにします。

GenRandomQMID.ps1 スクリプトを使用するには、以下の手順に従ってください:

1. PowerShell の実行ポリシーが **RemoteSigned** か **Unrestricted** に設定されていることを確認します。

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

2. スケジュールされたタスクを作成し、トリガーを［システム起動時］に設定して、PVS または MCS マスターイメージマシンで SYSTEM アカウントを使って実行します。

3. スタートアップタスクとしてコマンドを追加します。

   ```
   powershell .exe -file C:\\GenRandomQMID.ps1
   ```

GenRandomQMID.ps1 スクリプトの概要:

1. レジストリから現在の QMId を削除します。
2. HKEY_LOCAL_MACHINE\Software\Microsoft\MSMQ\Parameters に SysPrep = 1 を追加します。
3. CitrixSmAudAgent や MSMQ などの関連サービスを停止します。
4. ランダムな QMId を生成するために、先ほど停止したサービスを開始します。

```
# 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
         }


 }
```



```
21
22    }
```

Session Recording Player のインストール

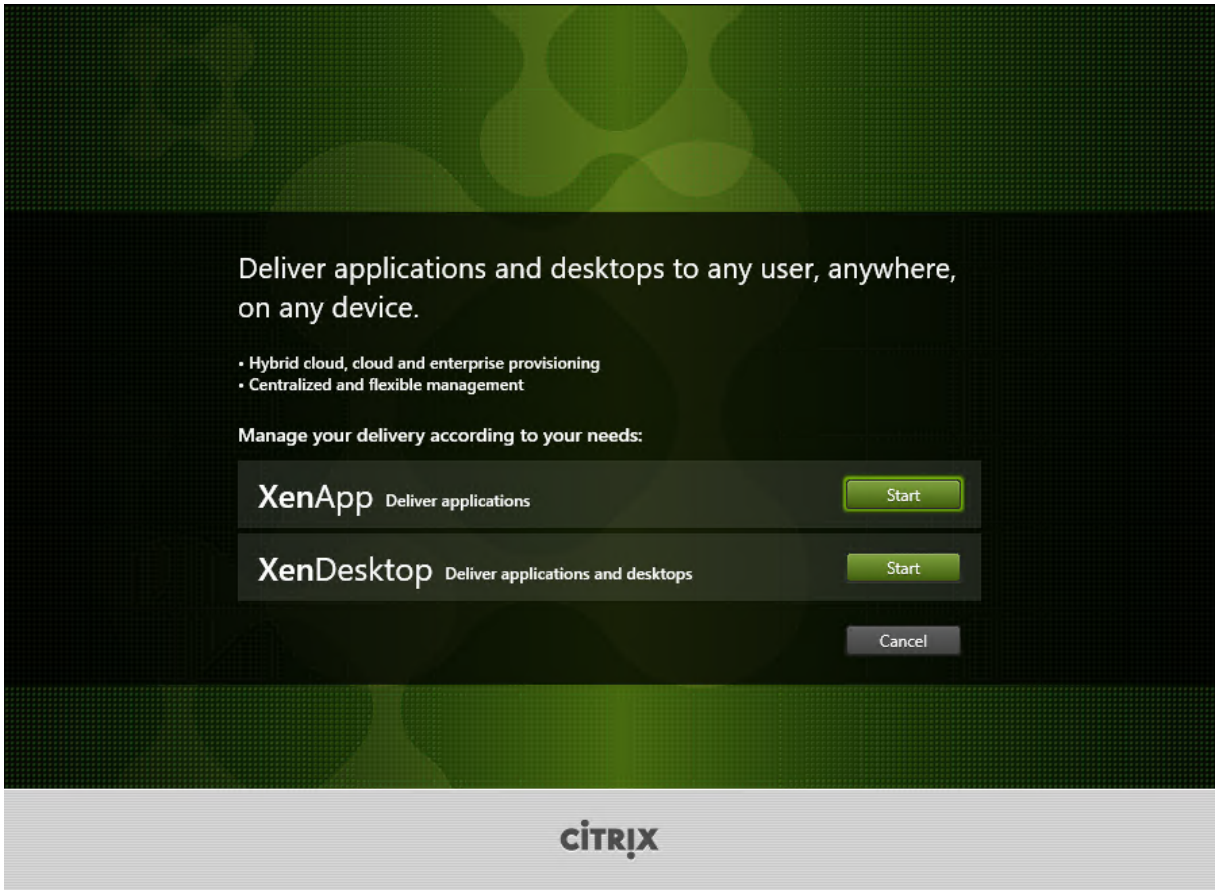
Session Recording サーバーに、またはセッションの録画を見るユーザーのドメイン内の 1 つ以上のワークステーションに Session Recording Player をインストールします。

手順 **1**：製品ソフトウェアをダウンロードしてウィザードを起動する

ローカルの管理者アカウントを使って、Session Recording Player コンポーネントのインストール先マシンにログオンします。DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

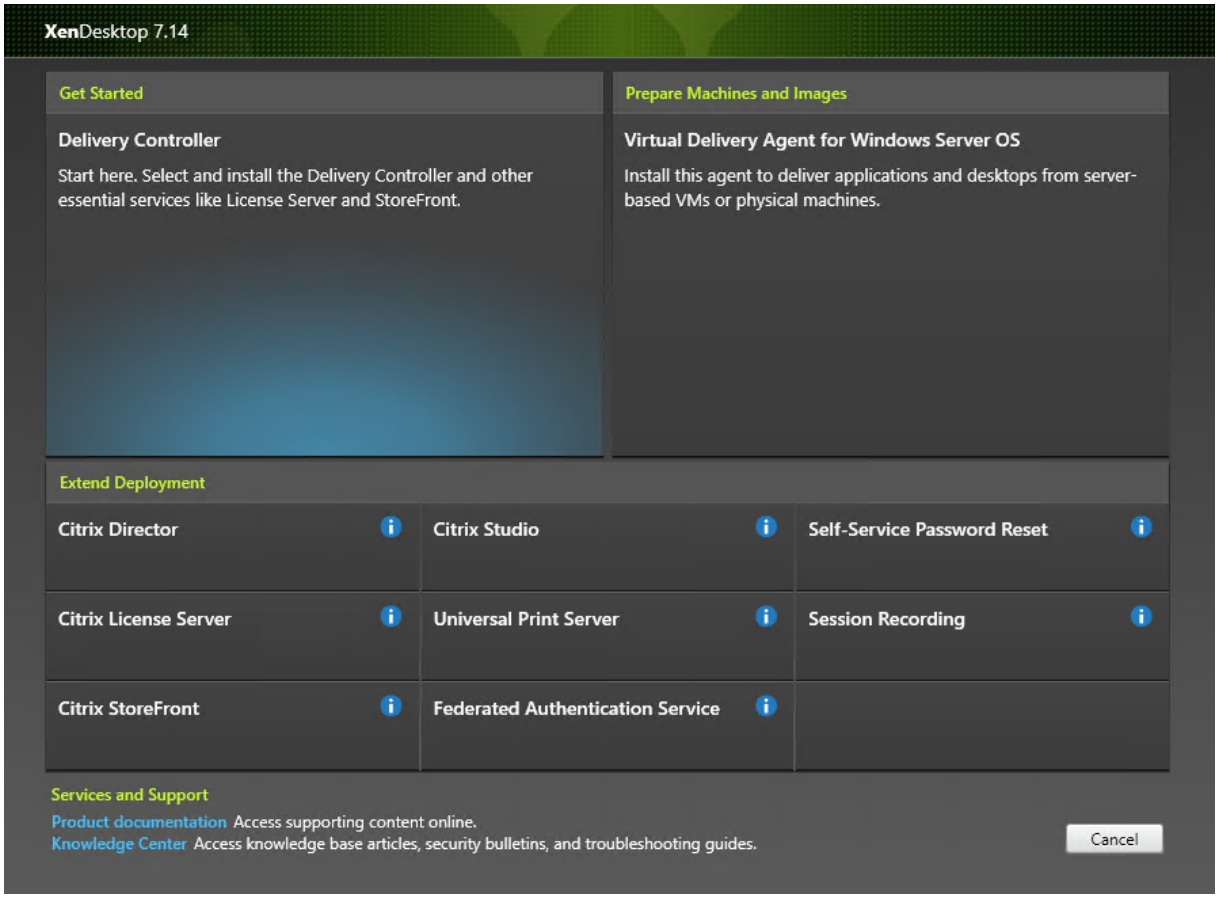
インストールウィザードが起動します。

手順 **2**：インストールする製品を選択する



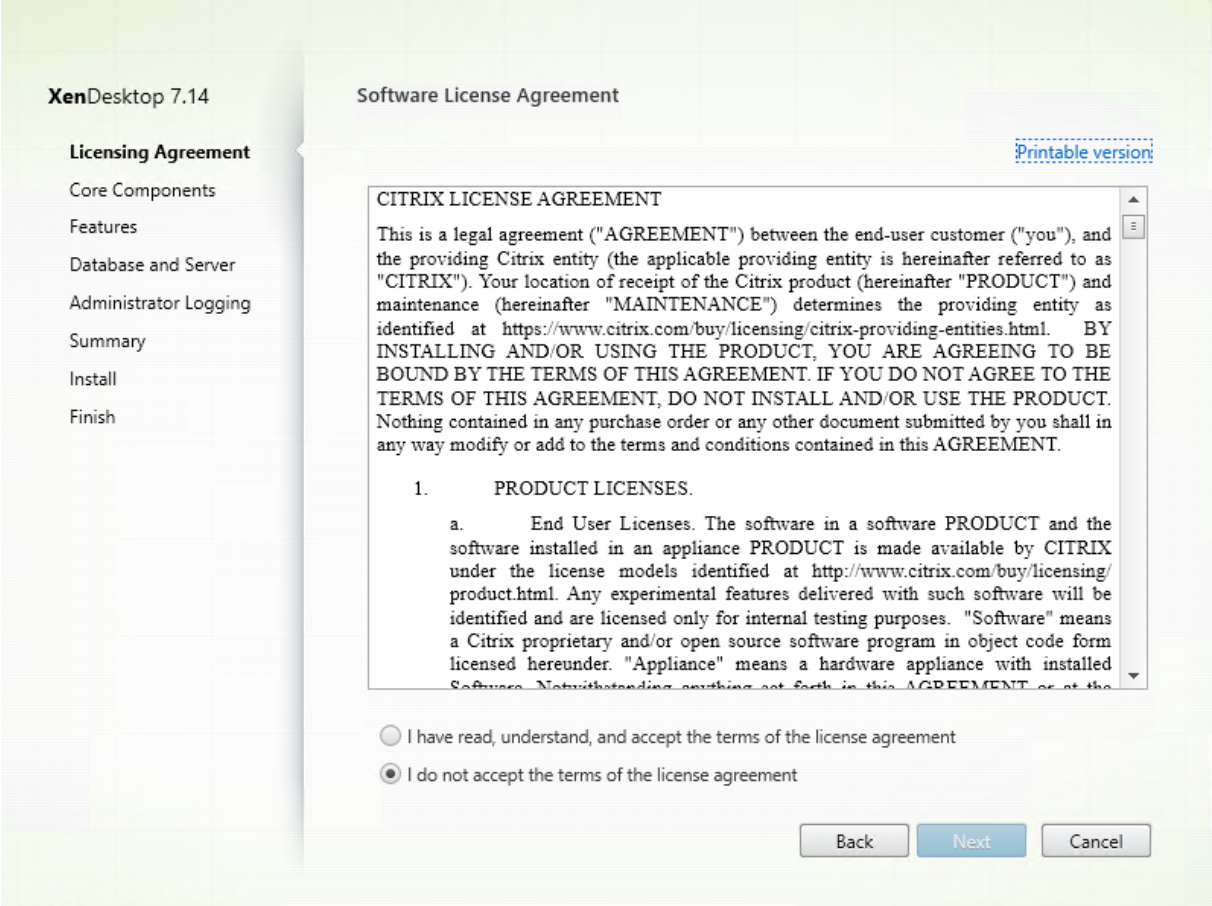
XenApp または **XenDesktop** の横にある ［開始］をクリックして、必要な製品をインストールします。

手順 **3**：**Session Recording** を選択する



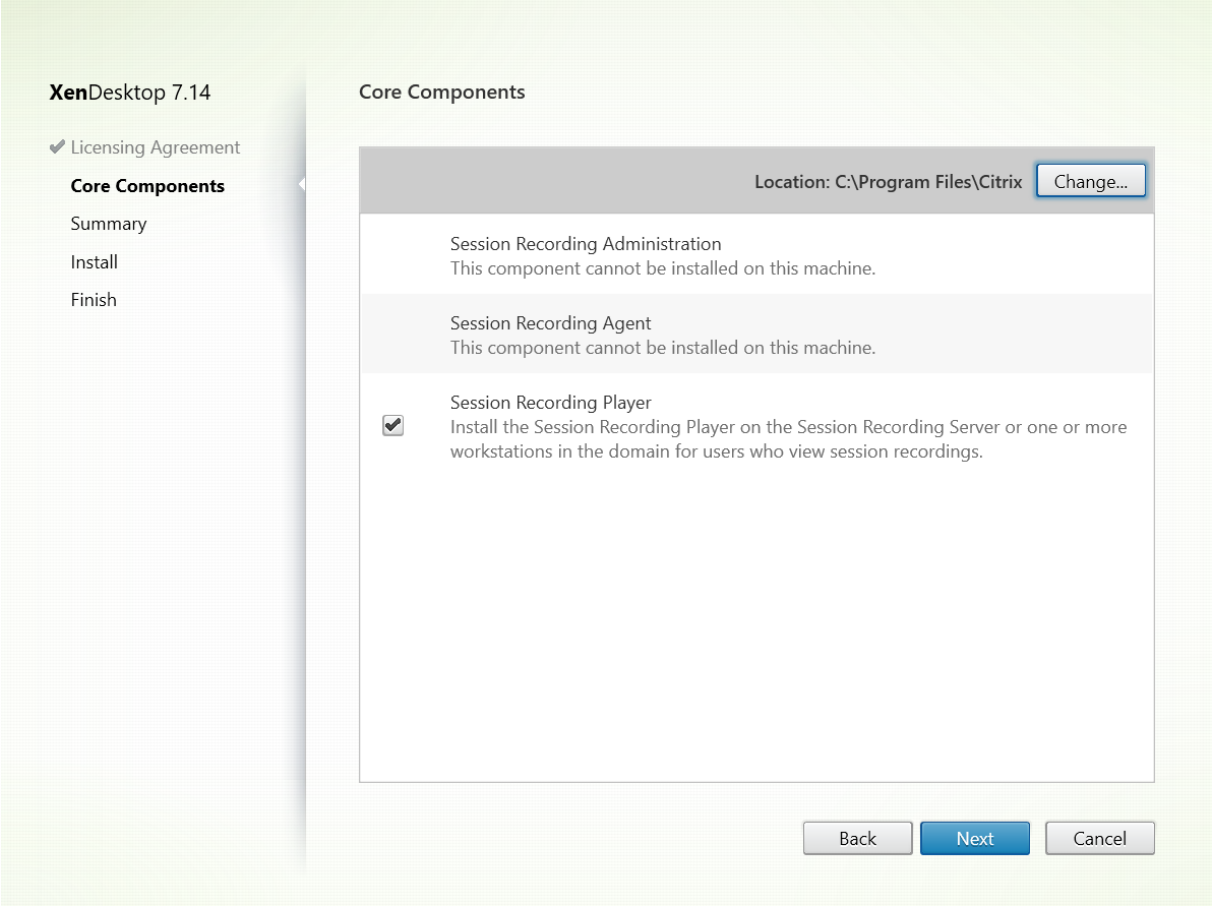
Session Recording エントリを選択します。

手順 **4**：ライセンス契約書を読み、同意する



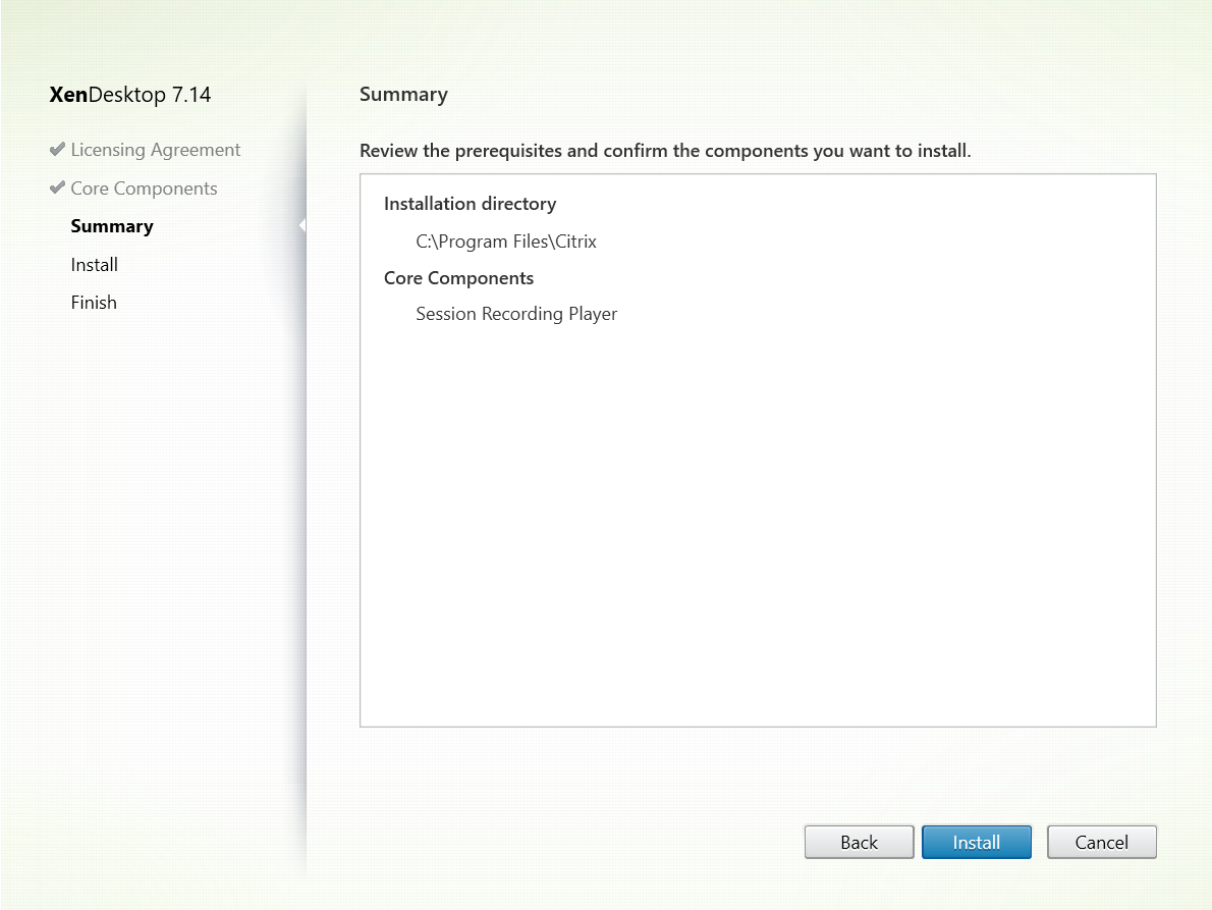
［ソフトウェアライセンス契約］ページでライセンス契約を読み、同意して ［次へ］をクリックします。

手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



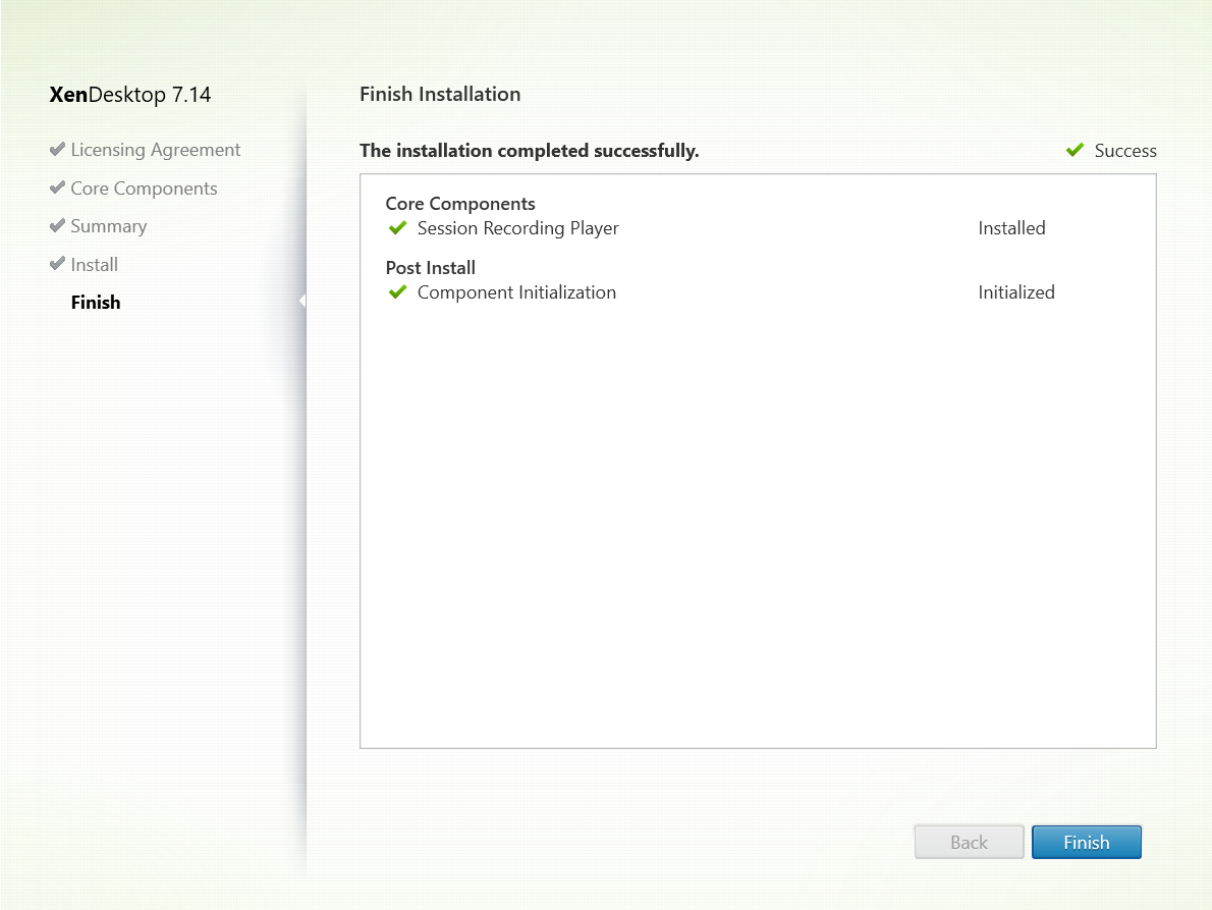
［**Session Recording Player**］を選択して ［次へ］をクリックします。

手順 **6**：インストール前に前提条件を確認する



［概要］ページにインストールの選択が表示されます。［戻る］をクリックして前のウィザードページに戻り、選択を変更できます。または、［インストール］をクリックしてインストールを開始します。

手順 **7**：インストールを完了する



［インストールの完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックして Session Recording Player のインストールを完了します。

インストールの自動化

Session Recording Agent を複数のサーバーにインストールするには、サイレントインストールを行うスクリプトを作成します。

次のコマンドラインでは、Session Recording Agent をインストールし、インストール情報を取得するためにログファイルを作成します。

64 ビットシステム：

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注: XenApp および XenDesktop ISO の SessionRecordingAgentx64.msi ファイルは、\layout\image-full\x64\Session Recording の下にあります。

32 ビットシステム:

msiexec /i SessionRecordingAgent.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注: XenApp および XenDesktop ISO の SessionRecordingAgent.msi ファイルは、\layout\image-full\x86\Session Recording の下にあります。

各項目の意味は次の通りです:

yourservername は、Session Recording サーバーをホストするコンピューターの NetBIOS 名または FQDN です。指定しない場合のデフォルト値は **localhost** です。

yourbrokerport は、Session Recording Broker との通信に Session Recording Agent で使用されるポートを表す HTTP または HTTPS です。指定しない場合のデフォルト値は HTTPS です。

yourbrokerport は、Session Recording Broker との通信に Session Recording Agent で使用されるポートを表す整数です。指定しない場合のデフォルト値は 0 で、選択したプロトコルのデフォルトのポート番号を使用するよう Session Recording Agent に指示します。具体的には、HTTP では 80、HTTPS では 443 です。

/l*v スイッチにより詳細モードでログが記録されます。

yourinstallationlog は、セットアップログを作成する場所です。

/q スイッチによりサイレントモードでインストールされます。

Session Recording のアップグレード

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。Session Recording 7.6（またはそれ以降のバージョン）を、最新リリースの Session Recording にアップグレードすることができます。

メモ:

- Session Recording Administration を 7.6 から 7.13 以降にアップグレードし、Session Recording Administration で［変更］を選択して管理者ログサービス追加した場合、［管理者ログの構成］ページに SQL Server インスタンスの名前が表示されません。［次へ］をクリックすると、次のようなメッセージが表示されます: `Database connection test failed. Please enter correct Database instance name.`この問題を回避するには、SmartAuditor サーバーの次のレジストリフォルダーにローカルホストのユーザーの読み取りのアクセス許可を追加します: HKEY_LOCAL_MACHINE:\SOFTWARE\Citrix\SmartAuditor\Server。

- マシン上にコンポーネントをインストールしただけで、Session Recording データベースをアップグレードしようとした場合は、失敗することがあります。その場合は、以下のレジストリエントリが、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Database の下にあるかどうかを確認してください。ない場合は、アップグレードの前にエントリを手動で追加してください。

キー名	キー型	キー値
SmAudDatabaseInstance	文字列	Session Recording データベースのインスタンス名
DatabaseName	文字列	Session Recording データベースのデータベース名

要件、準備、および制限

注: Technical Preview バージョンからはアップグレードできません。

- Session Recording コンポーネントのアップグレードは、コンポーネントをインストールしたマシンで、Session Recording インストーラーのグラフィカルインターフェイスまたはコマンドラインインターフェイスを使用して行う必要があります。
- アップグレードを開始する前に、SQL Server インスタンスで CitrixSessionRecording という名前のデータベースをバックアップします。これにより、データベースのアップグレード後に問題が発生した場合に元の状態に復元することができます。
- Session Recording コンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。
- Session Recording 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、データベースの役割権限が必要です。この権限がない場合は
  - データベース管理者に頼んで、アップグレードのために **securityadmin** および **dbcreator** サーバー役割権限を割り当ててもらいます。アップグレードの完了後は、**securityadmin** および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、SessionRecordingAdministrationx64.msi パッケージを使用してアップグレードします。msi のアップグレード中、**securityadmin** および **dbcreator** サーバー役割権限を持つデータベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、［**OK**］をクリックし、アップグレードを続行します。
- 同時にすべての Session Recording Agent をアップグレードしない場合は、Session Recording Agent 7.6.0（またはそれ以降）を、最新リリース（現行）の Session Recording サーバーと共に使用できます。ただし、一部の新機能やバグ修正は反映されない可能性があります。
- Session Recording 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。
- デスクトップコンポジションリダイレクトモードとの互換性を維持するために、新規インストールまたはアップグレード後に［Session Recording Agent のプロパティ］の ［グラフィック調整］オプションがデフォル

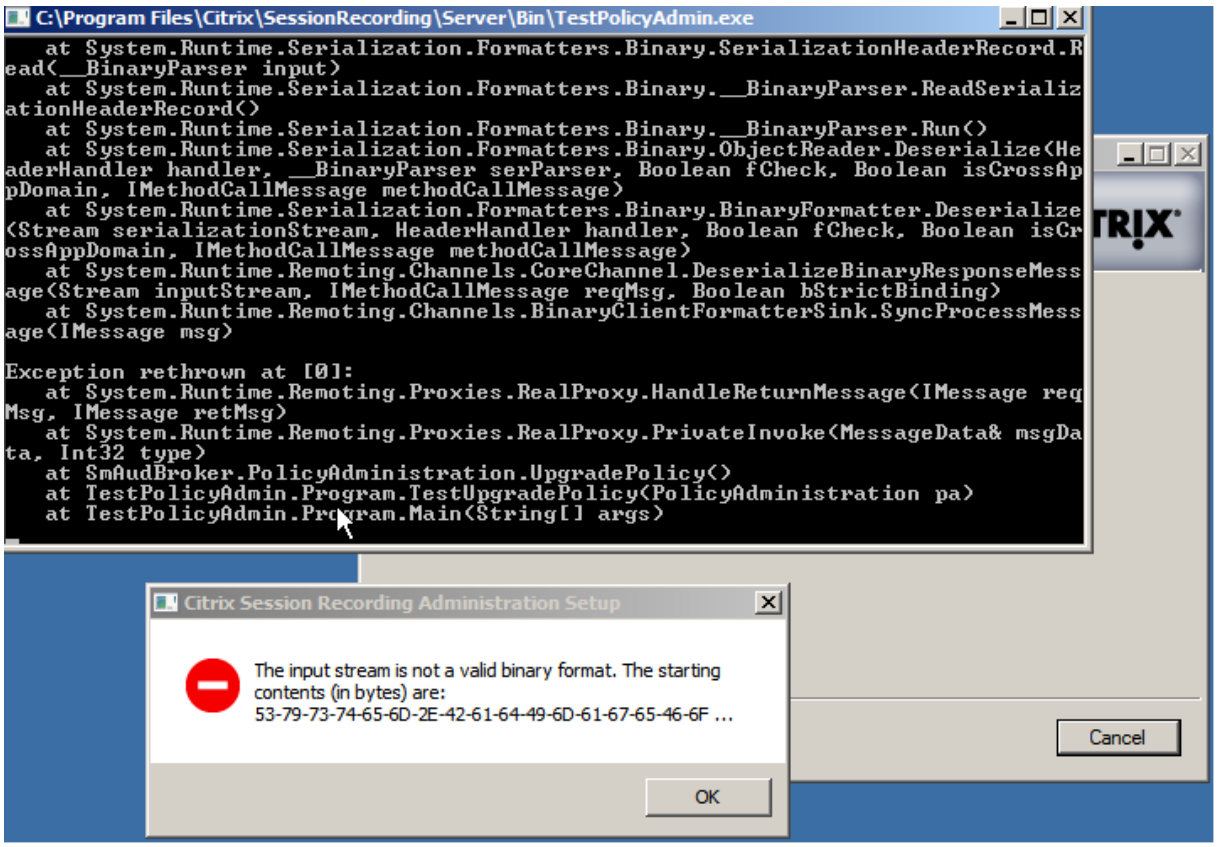
トで有効になっています。このオプションは、新規インストールまたはアップグレード後に手動で無効にできます。

- 管理者ログ機能は、この機能を含まない以前のリリースから Session Recording をアップグレードした後はインストールされません。この新しい機能を追加するには、アップグレード後にインストールを修正します。
- アップグレードプロセスの開始時にライブ録画セッションが実行されていた場合、録画を完了できる可能性はほとんどありません。
- サイトが停止する場合に備えて影響を軽減するために、後述のアップグレードの順序を確認してください。

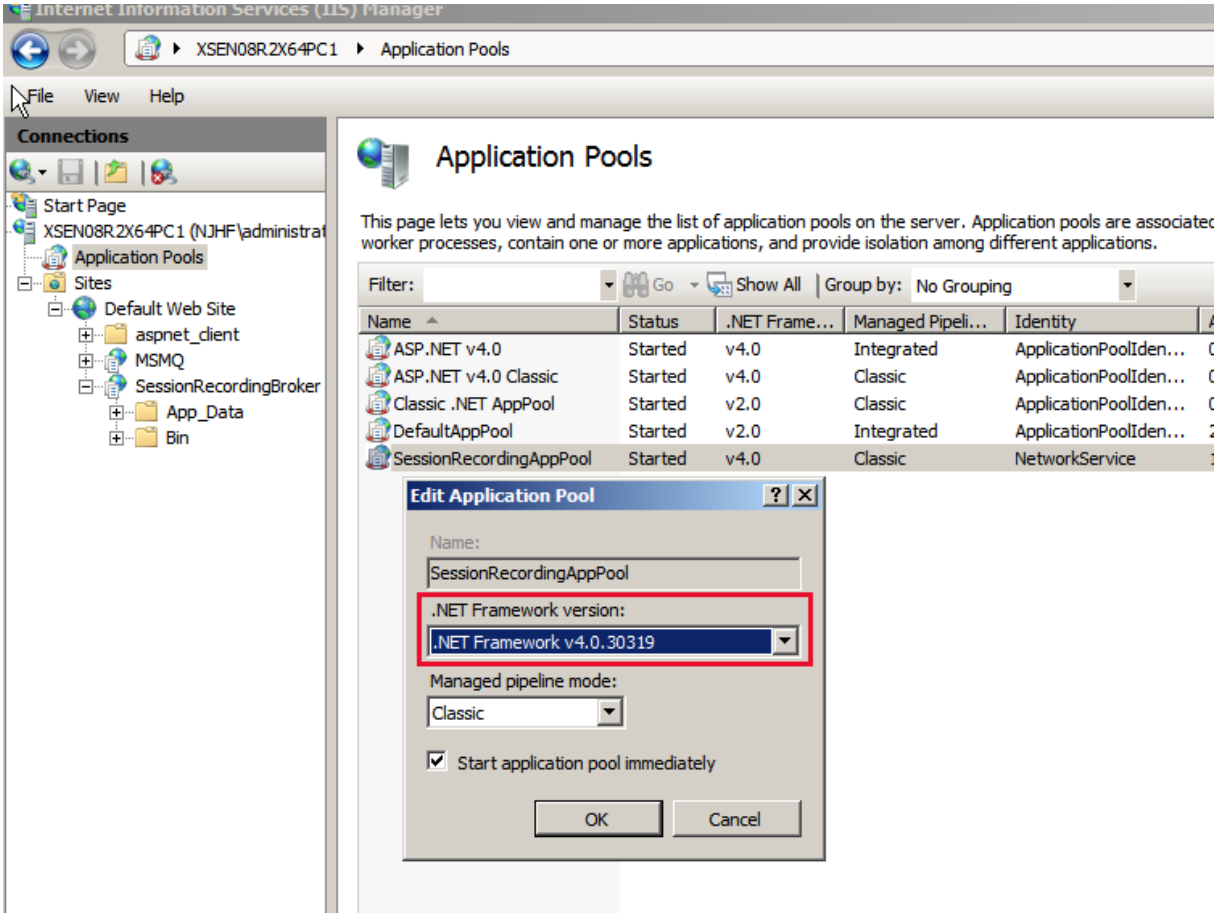
アップグレードの順序

1. Session Recording データベースと Session Recording 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 サービスと共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。

注: Windows Server 2008 R2 で Session Recording Administration コンポーネントをアップグレードすると、次のエラーが発生することがあります。



この場合は、［SessionRecordingAppPool］の［.NET Framework のバージョン］を IIS の［.NET Framework v4］に変更し、再度アップグレードしてください。



Session Recording のアンインストール

サーバーやワークステーションから **Session Recording** コンポーネントを削除するには、**Windows** のコントロールパネルのプログラムのアンインストールまたは削除オプションを使用します。Session Recording データベースを削除するには、インストール時と同じ SQL Server の役割権限 **securityadmin** および **dbcreator** が必要です。

セキュリティ上の理由により、コンポーネントがアンインストールされた後には管理者ログデータベースは削除されません。

Session Recording の構成

July 7, 2020

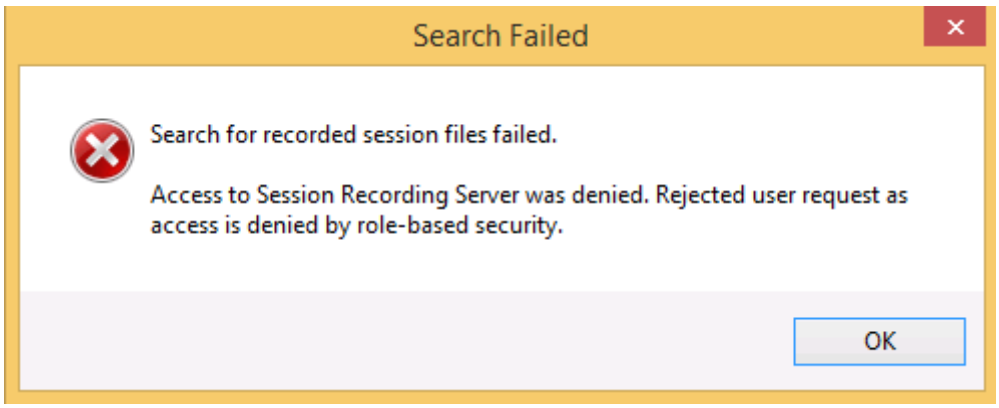
セッションの再生と録画のための **Session Recording** の構成

Session Recording コンポーネントをインストールしたら、次の手順を実行し、Session Recording を構成して、XenApp または XenDesktop セッションを録画して表示できるようにします:

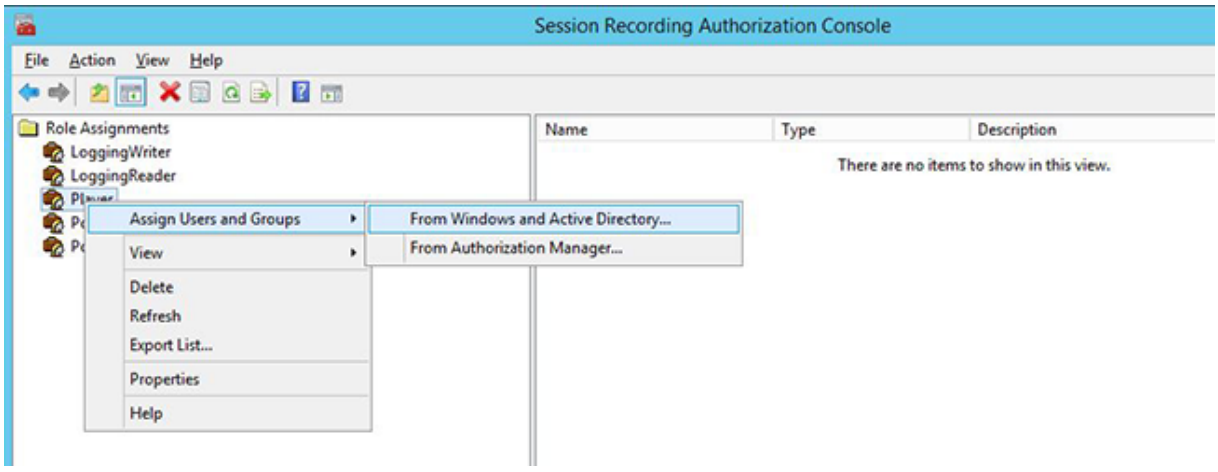
- ユーザーに録画を再生する権限を与える
- ユーザーに録画ポリシーを管理する権限を与える
- セッションを録画する録画ポリシーをアクティブに設定
- カスタムポリシーの構成
- Session Recording Player を構成して Session Recording サーバーと接続する

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 サーバー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［プレーヤー］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します。



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。

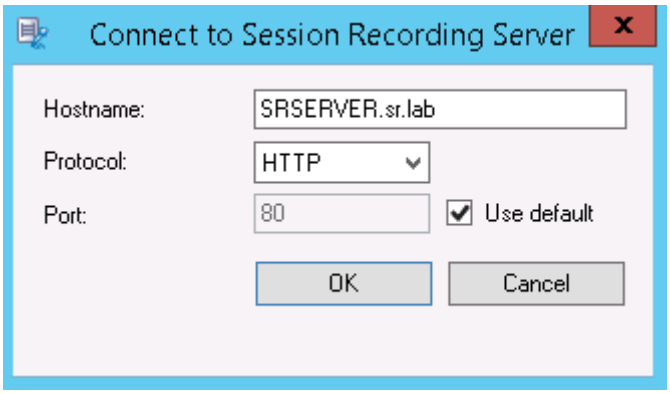
1. Session Recording サーバーをホストするマシンに管理者としてログオンします。
2. Session Recording 承認コンソールを起動して、PolicyAdministrators を選択します。
3. 録画ポリシーを管理できるユーザーとグループを追加します。

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 サーバーに接続する、すべての VDA または VDI でのセッションの録画処理が決定されます。Session Recording のデフォルト設定では、アクティブな録画ポリシーは「録画しない」ポリシーです。アクティブな録画ポリシーを変更するまで、セッションは録画できません。

重要：ポリシーには多くの規則を含めることができますが、一度に実行できるのはアクティブなポリシー 1 つだけです。

1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. [**Session Recording** サーバーへの接続] ダイアログボックスが開いたら、Session Recording サーバーをホストするコンピューターの名前、プロトコル、およびポート番号が正しいことを確認します。



4. Session Recording ポリシーコンソールで、[録画ポリシー] を展開して使用可能な録画ポリシーを表示します。チェックマークはそのポリシーがアクティブであることを示します：
   - 録画しない。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。それぞれが録画されていることを通知するウィンドウが表示されます。
   - すべてのユーザーを通知しないで録画する。このポリシーを選択すると、すべてのセッションが録画されます。録画されていることを通知するウィンドウが表示されません。

5. アクティブにするポリシーを選択します。
6. メニューバーで ［操作］>［ポリシーのアクティブ化］の順に選択します。

Session Recording では独自の録画ポリシーを作成できます。録画ポリシーを作成すると、Session Recording ポリシーコンソールの ［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。

注: Session Recording の管理者ログ機能により、録画ポリシーの変更を記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

Session Recording Player の構成

Session Recording Player でセッションを再生するには、録画されたセッションを格納する Session Recording Player との接続を設定する必要があります。Session Recording Player ごとに複数の Session Recording サーバーとの接続を設定できますが、同時に複数の Session Recording サーバーに接続することはできません。Session Recording Player に複数の Session Recording サーバーとの接続が構成される場合は、［ツール］>［オプション］の ［接続］タブのチェックボックスをオンにして、接続先の Session Recording サーバーを変更できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. Session Recording Player を起動します。
3. Session Recording Player のメニューバーで、［ツール］>［オプション］の順に選択します。
4. ［接続］タブで ［追加］をクリックします。
5. ［ホスト名］フィールドに、Session Recording サーバーをホストするコンピューターの名前か IP アドレスを入力し、プロトコルを選択します。デフォルトでは、セキュリティで保護された通信のため HTTPS/SSL を使用するように Session Recording が構成されます。SSL が構成されていない場合は、HTTP を選択します。
6. Session Recording Player が複数の Session Recording サーバーと接続できるように構成するには、Session Recording サーバーごとに手順 4 および 5 を繰り返します。
7. 接続する Session Recording サーバー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 サーバーとの接続の構成

Session Recording Agent と Session Recording サーバーの間の接続は、通常、Session Recording Agent をインストールするときに設定します。Session Recording Agent をインストールした後でこの接続を設定するには、［Session Recording Agent のプロパティ］を使用します。

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
3. ［接続］タブをクリックします。

4. [**Session Recording** サーバー] フィールドで、Session Recording サーバーの完全修飾ドメイン名を入力します。

   > 注:
   >
   > HTTPS 接続でメッセージキューを使用するには、[**Session Recording** サーバー] フィールドに完全修飾ドメイン名を入力します（デフォルトでは TCP を使用）。入力しない場合、Session Recording は失敗します。

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。

   > 注:
   >
   > HTTP および HTTPS 経由でメッセージキューを使用するには、IIS 推奨機能をすべてインストールします。

6. [メッセージの有効期間] フィールドで、通信エラーが発生したときにキューに各メッセージを保持する秒数として、デフォルトの 7,200 秒（2 時間）を受け入れるか、新しい値を入力します。この期間が経過すると、メッセージは削除され、ファイルを再生できるのはデータが失われた時点までになります。

7. [**Session Recording Broker**] で、Session Recording Broker が通信に使用するプロトコルを選択し、必要であればデフォルトのポート番号を変更します。

8. 確認メッセージが表示されるので、**Session Recording Agent** サービスを再起動して変更を受け入れます。

ユーザーへのアクセス権の付与

November 28, 2018

> 重要:
>
> 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 サーバー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。デフォルトでこのロール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、認証ユーザーがこのロールのメンバーです。
- **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 サーバーをホストするコンピューターの管理者がこのロールのメンバーです。

Session Recording では、Active Directory で定義されるユーザーおよびグループがサポートされます。

役割へのユーザーの割り当て

1. Session Recording サーバー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ロールを選択します。
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

August 24, 2021

Session Recording ポリシーコンソールを使用して、録画するセッションを決定するポリシーを作成しアクティブにします。

> 重要:
>
> Session Recording ポリシーコンソールを使用するには、Broker PowerShell スナップイン（Broker_PowerShellSnapIn_x64.msi）をインストールする必要があります。スナップインは、インストーラーによって自動的にインストールされません。XenApp および XenDesktop の ISO（\layout\image-full\x64\Citrix Desktop Delivery Controller の下にあります）でスナップインを検索し、指示に従って手動でインストールする必要があります。従わない場合、エラーが発生する可能性があります。
>
> ヒント:
>
> レジストリを編集して、Session Recording サーバーに予期しない障害が発生した場合にファイルが失われるのを防ぐことができます。Session Recording Agent をインストールしたマシンに管理者としてログオンし、レジストリエディターを開いて、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`の下に DWORD 値`DefaultRecordActionOnError` =1を追加します。

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

Session Recording には、次の 3 つのシステムポリシーがあります。

- 録画しない。これがデフォルトのポリシーです。ほかのポリシーを指定しなければ、セッションは録画されません。
- すべてのユーザーを通知して録画する。このポリシーを選択すると、すべてのセッションが録画されます。記録の発生を通知するポップアップウィンドウが表示されます。
- すべてのユーザーを通知しないで録画する。このポリシーを選択すると、すべてのセッションが録画されます。記録の発生を通知するポップアップウィンドウは表示されません。

システムポリシーは変更したり削除したりできません。

ポリシーのアクティブ化

1. Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. [**Session Recording** サーバーへの接続] ポップアップウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。[**OK**] をクリックします。
4. Session Recording ポリシーコンソールで、[**Recording** ポリシー] を展開します。
5. アクティブにするポリシーを選択します。
6. メニューバーで [操作] > [ポリシーのアクティブ化] の順に選択します。

カスタム録画ポリシーの作成

独自のポリシーを作成するときは、規則を作成して、録画対象のユーザーおよびグループ、公開アプリケーション、およびサーバーを指定します。Session Recording ポリシーコンソールにはウィザードが用意されており、このウィザードに従って規則を作成します。公開されているアプリケーションやサーバーの一覧を取得するには、サイト管理者の読み取り権限が必要です。この権限はこのサイトの Delivery Controller で設定します。

作成する規則ごとに録画操作および規則条件を指定します。録画操作は規則条件を満たすセッションに適用されます。

規則ごとに録画操作を 1 つ選択します:

- 録画しない。(規則ウィザードで [セッションを録画しない] をクリックします) この録画操作では、規則条件を満たすセッションを録画しないことを指定します。
- 通知して録画する。(規則ウィザードで [通知してセッションを録画する] をクリックします) この録画操作では、規則条件を満たすセッションを録画することを指定します。記録の発生を通知するポップアップウィンドウが表示されます。
- 通知しないで録画する。(規則ウィザードで [通知しないでセッションを録画する] をクリックします) この録画操作では、規則条件を満たすセッションを録画することを指定します。ユーザーは録画されていることに気付きません。

規則ごとに次の項目のいずれかを少なくとも 1 つ選択して、規則条件を作成します:

- ユーザーまたはグループ。規則の録画操作を適用するユーザーまたはグループの一覧を作成します。

- 公開リソース。規則の録画操作を適用する公開アプリケーションまたはデスクトップの一覧を作成します。規則ウィザードで、アプリケーションまたはデスクトップを使用できる 1 つまたは複数の XenApp および XenDesktop サイトを選択します。
- デリバリーグループまたはマシン。規則の録画操作を適用するデリバリーグループまたはマシンの一覧を作成します。規則ウィザードで、デリバリーグループまたはマシンの場所を選択します。
- **IP** アドレスまたは **IP** 範囲。規則の録画操作を適用する IP アドレスまたは IP アドレスの範囲の一覧を作成します。［**IP** アドレスまたは **IP** の範囲の選択］画面で、録画が有効または無効になった有効な IP アドレスまたは IP 範囲を追加します。

注：Session Recording ポリシーコンソールでは、1 つの規則内で複数の条件を構成できます。規則が適用される際には、「AND」と「OR」の両方の論理演算子が、最終的なアクションを計算するために使われます。一般的に、「OR」演算子は一定の条件内の項目に使われ、「AND」演算子は違った複数の条件に当てはまる項目に使われます。結果が true であれば、Session Recording ポリシーエンジンがその規則のアクションをとります。そうでなければ、次の規則に進み、処理を繰り返します。

録画ポリシーに複数の規則を作成する場合は、複数の規則条件に一致するセッションがある可能性があります。そのような場合は、優先順位が最も高い規則がセッションに適用されます。

規則により実行される録画操作によってその優先順位が決まります。

- 録画しない規則の優先順位が最も高くなります。
- 通知して録画する規則の優先順位が次に高くなります。
- 通知しないで録画する規則の優先順位が最も低くなります。

録画ポリシーの規則条件のいずれにも当てはまらないセッションがある可能性があります。そのようなセッションについては、フォールバック規則の録画操作が適用されます。フォールバック規則の録画操作は常に 「録画しない」です。フォールバック規則は変更したり削除したりできません。

カスタムポリシーを構成するには、次を実行します。

1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動して、左側のペインで ［レコーディングポリシー］を選択します。メニューバーで ［操作］>［新しいポリシーの追加］の順に選択します。
3. 新しいポリシーを右クリックして ［規則の追加］をクリックします。
4. 録画オプションの選択 - 規則ウィザードで、[セッションを録画しない]、[通知してセッションを録画する]（または ［通知しないでセッションを録画する]）を選択し、［次へ］をクリックします。
5. 規則条件の選択 - 以下のオプションの 1 つまたは任意の組み合わせを選択することができます：
   ユーザーまたはグループ
   公開リソース
   デリバリーグループまたはマシン
   IP アドレスまたは **IP** の範囲
6. 規則条件の編集 - 編集するには、下線付きの値をクリックします。前の手順で選択した条件に基づき、値に下線が引かれます。

注：［公開リソース］の下線付きの値を選択した場合、［サイトアドレス］は IP アドレス、URL、またはコントローラーがローカルネットワーク上にある場合はコンピューター名になります。［アプリケーションの名前］リストに表示名が表示されます。

7. ウィザードの指示に従って構成を終了します。

Active Directory グループの使用

Active Directory グループを使用して、Session Recording のポリシーを作成できます。個々のユーザーではなく Active Directory グループを使用すると、規則とポリシーを簡単に作成したり管理したりできます。たとえば、財務部門のユーザーが Finance という名前の Active Directory グループに含まれている場合は、規則を作成するときに規則ウィザードで Finance グループを選択することで、このグループのすべてのメンバーに適用される規則を作成できます。

ユーザーのホワイトリスト化

組織内の一部のユーザーのセッションを確実に録画対象から除外する、Session Recording ポリシーを作成できます。これはユーザーのホワイトリスト化と呼ばれます。個人情報を取り扱う社員や特定の階層の従業員など、セッションを録画するべきではないユーザーをホワイトリストに登録すると便利です。

すべての上級管理職が Executive という名前の Active Directory グループのメンバーである場合、Executive グループのセッション録画を無効にする規則を作成して、それらのユーザーのセッションが決して録画されないように設定できます。この規則を含むポリシーがアクティブな間は、Executive グループのメンバーのセッションは録画されません。組織内のほかのメンバーのセッションは、アクティブなポリシーのほかの規則に基づいて録画されます。

IP アドレスまたは **IP** の範囲規則条件の使用

ポリシー一致の規則条件として、クライアント IP アドレスを使用できます。たとえば、特定の IP アドレスを持つか、ある IP 範囲に含まれるクライアントからのセッションを記録する場合、規則ウィザードを使用して、それらのクライアントにのみ適用される規則を作成します。

新しいポリシーの作成

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 ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. ［**Session Recording** サーバーへの接続］ポップアップウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。［**OK**］をクリックします。
4. Session Recording ポリシーコンソールで、［レコーディングポリシー］を展開します。

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］をクリックして、規則ウィザードを起動します。
9. 画面の指示に従ってこのポリシーの規則を作成します。

ポリシーの変更

1. Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. ［**Session Recording** サーバーへの接続］ポップアップウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。［**OK**］をクリックします。
4. Session Recording ポリシーコンソールで、［**Recording** ポリシー］を展開します。
5. 変更するポリシーを選択します。ポリシーの規則が右ペインに表示されます。
6. 新しい規則を追加するか、規則を変更または削除します。
   - メニューバーで ［操作］ > ［新しい規則の追加］の順に選択します。ポリシーがアクティブな場合はポップアップウィンドウが開き、操作の確認を促すメッセージが表示されます。規則ウィザードを使用して新しい規則を作成します。
   - 変更する規則を選択し、右クリックして ［プロパティ］を選択します。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 ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. ［**Session Recording** サーバーへの接続］ポップアップウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。［**OK**］をクリックします。
4. Session Recording ポリシーコンソールで、［**Recording** ポリシー］を展開します。
5. 左ペインで削除するポリシーを選択します。ポリシーがアクティブな場合は、ほかのポリシーをアクティブにする必要があります。
6. メニューバーで ［操作］>［ポリシーの削除］の順に選択します。
7. ［はい］をクリックして操作を確定します。

注：事前起動されたアプリケーションセッションに関する制限事項：

- アクティブなポリシーでアプリケーション名を照合する場合、事前起動されたセッションで起動されたアプリケーションは照合されないため、セッションが録画されません。

- アクティブなポリシーですべてのアプリケーションが録画される場合、ユーザーが Citrix Receiver for Windows にログインすると、（事前起動されたセッションが確立されるのと同時に）録画に関する通知が表示され、事前起動された（空の）セッションと、今後そのセッションで起動されるすべてのアプリケーションが録画されます。

これを回避するには、録画ポリシーに従って別のデリバリーグループでアプリケーションを公開します。録画条件にアプリケーション名を使用しないでください。こうすることで、事前起動されたセッションを録画できます。ただし、通知は表示されます。

ロールオーバーの動作

ポリシーをアクティブにするとき、それまでアクティブだったポリシーはユーザーセッションが終了するまで効力を保ちます。ただし、一部の場合、ファイルがロールオーバーされると新しいポリシーが有効になります。ロールオーバーは、ファイルサイズが上限に達すると実行されます。録画ファイルのサイズの上限について詳しくは、「録画ファイルのサイズの指定」を参照してください。

次の表で、セッションの録画中に新しいポリシーを適用してロールオーバーが起きたときに生じる現象について説明します:

以前のポリシー	新しいポリシー	ロールオーバーの後のポリシー
録画しない	ほかのポリシー	変更なし。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。
通知しないで録画する	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。
通知して録画する	通知しないで録画する	録画を続行します。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

August 28, 2019

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"Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs."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 サーバーをホストするコンピューターのオペレーティングシステムの言語で表示されます。

選択した言語でカスタムの通知を作成できますが、言語ごとに作成できる通知メッセージは 1 つだけです。ユーザーには、ユーザーが選択したローカル設定の言語で通知メッセージが表示されます。

新しい通知メッセージの作成

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［通知］タブをクリックします。
4. ［追加］をクリックします。
5. メッセージで使用する言語を選択し、新しいメッセージを入力します。1 つの言語につき作成できるメッセージは 1 つです。

新しいメッセージを受け入れてアクティブにすると、［言語特有の通知メッセージ］ボックスに表示されます。

注: Session Recording の管理者ログ機能により、Session Recording のサーバーポリシー変更を記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

録画の無効化または有効化

August 24, 2021

Session Recording Agent は、セッションを録画する各 VDA for Server OS にインストールします。インストール先のサーバーで録画を有効にするかどうかの設定を、Session Recording Agent で行います。録画を有効にすると、Session Recording によりアクティブな録画ポリシーが評価されます。このポリシーにより録画対象のセッションが決定されます。

Session Recording Agent をインストールすると、デフォルトで録画が有効になります。録画しないサーバーでは Session Recording を無効にすることをお勧めします。録画をしていないときでも、サーバーのパフォーマンスが多少影響を受けるためです。

サーバーでの録画の無効化または有効化

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］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 ［このサーバー **OS VDA** でセッションを録画する］チェックボックスをオンまたはオフにし、このサーバーでセッションを録画できるようにするかどうかを指定します。
4. 確認メッセージが表示されるので、Session Recording Agent サービスを再起動して変更を受け入れます。

注： Session Recording をインストールしたときにアクティブになっているポリシーは「
録画しない」ポリシーです。どのサーバーのセッションも録画されません。録画を開始するには、Session Recording ポリシーコンソールを使用して別のポリシーをアクティブにします。

カスタムイベントの記録の有効化

Session Recording では、サードパーティ製のアプリケーションを使用して、イベントとして知られるカスタムデータを録画されたセッションに挿入することができます。これらのイベントは、Session Recording Player を使用してセッションを再生するときに表示されます。これらは録画されたセッションの一部であり、録画の後に変更することはできません。

たとえば、イベントに「ユーザーが Web ブラウザーを開きました」というテキストが含まれることがあります。というテキストが含まれることがあります。このテキストは、録画対象のセッションでエンドユーザーが Web ブラウザーを開くたびに録画に挿入されます。Session Recording Player を使用してセッションを再生するとき、Session Recording Player の［イベントとブックマーク］の一覧に表示されるマーカーの数から、ユーザーが Web ブラウザーを開いた回数がわかります。

サーバー上の録画にカスタムイベントを挿入するには

- ［**Session Recording Agent** のプロパティ］を使用して、カスタムイベントを挿入する各サーバーで設定を有効にします。サーバーは個別に有効にする必要があります。サイト内のすべてのサーバーをまとめて有効にすることはできません。
- イベント API に基づくアプリケーションを開発します。このアプリケーションを各エンドユーザーの XenApp セッションで実行し、録画にデータを挿入します。

Session Recording のインストールにはイベント記録 COM アプリケーション（API）が含まれており、サードパーティ製のアプリケーションからテキストを録画に挿入することができます。Visual Basic、C++、または C# を含む、多くのプログラミング言語で API を使用できます。詳しくは、Citrix の記事CTX226844を参照してください。Session Recording イベント API の DLL は Session Recording の一部としてインストールされます。API のファイルは、C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll. です。

サーバーでカスタムイベントの記録を有効にするには、以下の手順を実行します：

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
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

October 16, 2020

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。セッションを録画しながら表示することは、ライブでセッションを見るようなものです。ただし、XenApp または XenDesktop サーバーからデータが送信されると実際には 1〜2 秒の遅延が発生します。

録画が完了していないセッションを再生するときは、次の機能は使用できません:

- 録画が完了するまでデジタル証明書を割り当てることはできません。デジタル署名が有効な場合は、ライブセッションを再生できますが、まだ録画に署名はされていません。セッションが完了して初めて、証明書を表示できます。
- 録画が完了するまで、再生データの保護は適用できません。再生データの保護が有効な場合は、ライブセッションを再生できますが、セッションが完了するまでは暗号化されません。
- 録画が完了するまで、ファイルをキャッシュできません。

デフォルトで、ライブセッションの再生は有効になっています。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** 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. [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、Session Recording Player で表示するためにダウンロードされた録画ファイルは自動的に暗号化されます。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`.icle`拡張子で識別されます。暗号化されていないファイルは`.icl`拡張子で識別されます。Session Recording Player がインストールされている`%localAppData%\Citrix\SessionRecording\Player\Cache`にある間、ファイルは、権限を持つユーザーがファイルを開くまで暗号化されたままです。

HTTPS を使用して転送データを保護することをお勧めします。

再生データの保護は、デフォルトで有効になります。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** 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

July 3, 2019

Session Recording コンポーネントがインストールされているコンピューターに証明書をインストールする場合は、デジタル署名を Session Recording に割り当てることにより、Session Recording 環境のセキュリティを強化できます。

デフォルトで、デジタル署名は無効になっています。録画に署名する証明書を選択すると、Session Recording から Session Recording ストレージマネージャーサービスに読み取り権限が付与されます。

デジタル署名の有効化

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［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保護された通信を有効にする証明書を参照します。

デジタル署名の無効化

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［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

August 24, 2021

［Session Recording サーバーのプロパティ］を使用して、録画の格納先とアーカイブされた録画の再生時の復元先を指定します。

注：ファイルをアーカイブする、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。

録画を格納するフォルダーを指定する

デフォルトでは、録画は Session Recording サーバーをホストするコンピューターの drive:**\SessionRecordings** フォルダーに格納されます。録画を保存するフォルダーを変更したり、複数のボリューム間で負荷分散をするため、または追加の容量を活用するために、フォルダーを追加したりできます。複数のフォルダーが一覧にある場合は、録画がフォルダー間で負荷分散されていることを示します。1 つのフォルダーを複数回追加できます。負荷分散は各フォルダーを循環して行われます。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［格納場所］タブをクリックします。
4. ［ファイル格納フォルダー］ボックスの一覧を使用して、録画を格納するフォルダーを管理します。

フォルダーを選択すると、それらのフォルダーにフルコントロール権限のサービスが付与されます。

ローカルドライブ、SAN ボリューム、または UNC ネットワークパスで指定する場所にファイル格納フォルダーを作成できます。マップされたネットワークドライブのドライブ文字はサポートされません。Session Recording では、NAS（Network-Attached Storage：ネットワークアタッチトストレージ）を使用しないでください。ネットワークドライブへの録画データの書き込みに関連して、パフォーマンスおよびセキュリティ上の重大な問題が起きる可能性があります。

アーカイブされた録画の再生時の復元フォルダーを指定する

デフォルトでは、アーカイブされた録画は Session Recording サーバーをホストするコンピューターの「ドライブ名:**\SessionRecordingsRestore**」フォルダーに復元されます。フォルダーは変更できます。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［格納場所］タブをクリックします。
4. ［アーカイブ済みファイルの復元フォルダー］ボックスにアーカイブ済み録画を復元するフォルダーを入力します。

録画ファイルのサイズの指定

November 28, 2018

録画ファイルのサイズが大きくなるにつれて、ダウンロードに時間がかかり、再生中にシークスライダーを使用して再生箇所を変更するときに反応が遅くなるようになります。ファイルサイズを制御するにはファイルのしきい値を指定します。録画ファイルがこの限界に達すると、Session Recording によってファイルが閉じられ、録画を続行するために新しいファイルが開かれます。この操作をロールオーバーと呼びます。

重要：ロールオーバーの設定は、XenDesktop 7.8 および Session Recording Agent の VDI デスクトップセッシ

ョンに適用されません。この場合、各録画ファイルの最大サイズは 1GB であり、この上限に到達するとアクティビティは録画されません。

ロールオーバーのため、2 つのしきい値を指定できます:

- ファイルサイズ。ファイルが MB 単位で指定された大きさに達すると、ファイルが閉じられ、新しいファイルが開かれます。デフォルトでは、ファイルが 50MB に達するとロールオーバーが起こります。ただし、10MB から 1GB の範囲で上限を指定できます。
- 時間。セッションが時間単位で指定された時間録画されると、ファイルが閉じられ、新しいファイルが開かれます。デフォルトでは、12 時間録画するとロールオーバーが起こります。ただし、1 時間から 24 時間の範囲で上限を指定できます。

Session Recording により両方のボックスの値が確認され、ロールオーバーを実行するタイミングを決定するイベントとして、どちらのしきい値を先に超過するかが判断されます。たとえば、ファイルサイズに 17MB、時間に 6 時間を指定し、録画ファイルのサイズが 3 時間で 17MB に達したとします。この場合、17MB のファイルサイズに対応してロールオーバー処理が起動し、ファイルが閉じられ、新しいファイルが開かれます。

多くの小さなファイルが作成されないように、ファイルサイズに指定された値にかかわらず、少なくとも 1 時間（指定できる最小の値）が経過するまでロールオーバーは起こりません。この規則の例外は、ファイルサイズが 1GB を超えた場合です。

録画の最大ファイルサイズの指定

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** 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、［ロールオーバー］タブをクリックします。
4. 10 から 1,024 の間の整数を入力して、ファイルサイズの上限を MB 単位で指定します。
5. 1 から 24 の間の整数を入力して、録画時間の上限を時間単位で指定します。

ログ管理アクティビティ

August 24, 2021

Session Recording 管理者ログでは、以下のアクティビティが記録されます:

- Session Recording Policy Console または Citrix Director での録画ポリシーへの変更。
- Session Recording サーバーのプロパティにおける変更。
- Session Recording Player での録画のダウンロード。
- ポリシークエリ完了後の Session Recording によるセッションの録画。
- 権限のない管理者ログサービスへのアクセス試行。

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

管理者ログの無効化または有効化

インストール後、Session Recording サーバーのプロパティで Session Recording 管理者ログ機能を無効または有効にできます。

1. Session Recording 管理者ログがインストールされているサーバーに管理者としてログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［ログ］タブをクリックします。

Session Recording 管理者ログを無効にすると、新しいアクティビティは記録されません。既存のログを Web ベースの UI から照会できます。

［必須のブロック機能を有効にする］がオンの場合、ログが失敗すると以下のアクティビティがブロックされます。システムイベントもイベント ID 6001 で記録されます:

- Session Recording Policy Console または Citrix Director での録画ポリシーへの変更。
- Session Recording サーバーのプロパティにおける変更。

セッションの録画は必須のブロック設定による影響を受けません。

ユーザーへのアクセス権の付与

セキュリティ上の理由から、Administrator Logging のログの照会など、特定の機能を実行するために必要な権限のみをユーザーに付与します。

Session Recording サーバーをホストするコンピューターで Session Recording 承認コンソールを使用して役割を割り当てることにより、ユーザーに権限を付与します。Administrator Logging には 2 つの役割があります:

- **LoggingWriter**。管理者ログを書き込む権限を付与します。デフォルトでは、ローカル管理者および Network Service がこの役割のメンバーです。

  注: デフォルトの **LoggingWriter** メンバーシップを変更すると、ログの書き込みが失敗する原因となる可能性があります。

- **LoggingReader**。管理者ログを照会する権限を付与します。デフォルトでこのロールのメンバーになるユーザーはありません。

ユーザーに役割を割り当てるには

1. 管理者として、Session Recording サーバーをホストするコンピューターにログオンします。
2. **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ロールを選択します。
4. メニューバーで、［操作］>［**Windows** ユーザーとグループの割り当て］の順に選択します。
5. ユーザーとグループを追加してください。

管理コンソールで加えた変更は、1 分間隔の更新時に有効になります。

Administrator Logging サービスアカウントの構成

デフォルトで、管理者ログはインターネットインフォメーションサービス（IIS）の Web アプリケーションとして実行されており、ID は Network Service です。セキュリティレベルを拡張するために、この Web アプリケーションの ID をサービスアカウントまたは特定のドメインアカウントに変更できます。

1. 管理者として、Session Recording サーバーをホストするコンピューターにログオンします。
2. IIS マネージャーで、［アプリケーションプール］をクリックします。
3. ［アプリケーションプール］で、**SessionRecordingLoggingAppPool** を右クリックして ［詳細設定］を選択します。
4. 属性 **ID** を、使用する特定のアカウントに変更します。
5. **db_owner** 権限を、Microsoft SQL Server のデータベース **CitrixSessionRecordingLogging** のアカウントに付与します。
6. レジストリキー **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server** の読み取り権限をアカウントに付与します。

録画アクションの記録の無効化または有効化

デフォルトで、管理者ログではポリシークエリ完了後のすべての録画アクションが記録されます。これにより、大量のログが生成される可能性があります。パフォーマンスを向上させてストレージを確保するには、レジストリでこの種類のログを無効にします。

1. 管理者として、Session Recording サーバーをホストするコンピューターにログオンします。
2. レジストリエディターを開きます。
3. **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server** に移動します。
4. **EnableRecordingActionLogging** の値として、以下を設定します:

   0: 録画アクションの記録の無効化

   1: 録画アクションの記録の有効化

Administrator Logging データの照会

Session Recording では、すべての Administrator Logging を照会するための Web ベースの UI が提供されます。

Session Recording サーバーをホストするコンピューターで、次の処理を行います:

1. ［スタート］ボタンをクリックし、［**Session Recording** 管理者ログ］を選択します。
2. **LoggingReader** ユーザーの資格情報を入力します。

別のコンピューターで、次の処理を行います:

1. Web ブラウザーを開いて、管理者ログの Web ページにアクセスします。

   HTTPS で接続する場合: `https://servername/SessionRecordingLoggingWebApplication/`（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/SessionRecordingLoggingWebApplication/`（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。）

2. **LoggingReader** ユーザーの資格情報を入力します。

データベースの高可用性を備えた **Session Recording** のインストール

April 1, 2021

Session Recording は、Microsoft SQL Server をベースとしたデータベースの高可用性に関する次のソリューションをサポートしています。プリンシパル SQL Server またはプライマリ SQL Server のハードウェアまたはソフトウェアに障害が発生した場合、データベースが自動的にフェールオーバーするので、Session Recording が想定どおりに機能し続けます。

- Always On 可用性グループ

AlwaysOn 可用性グループ機能は、高可用性および障害回復ソリューションで、データベースのミラーリングに取って代わるエンタープライズレベルのサービスです。SQL Server 2012 で導入された Always On 可用性グループ機能によって、エンタープライズ向けのユーザーデータベースの可用性が最大化します。Always On 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、「https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server」を参照してください。

- SQL Server クラスタリング

Microsoft の SQL クラスタリングテクノロジーを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQL Server データベースミラーリングなどほかのソリューションよりも自動フェールオーバーには一般的に時間がかかります。詳しくは、「https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/windows/always-on-failover-cluster-instances-sql-server」を参照してください。

- SQL Server データベースミラーリング

データベースのミラーリングによって、アクティブなデータベースサーバーが停止しても数秒で自動的にフェールオーバーが実行されます。各データベースサーバー上に完全な SQL Server ライセンスが必要になるため、ほかの 2 つのソリューションよりも費用が高くつきます。SQL Server Express エディションを使用してデータベースをミラーリングすることはできません。詳しくは、「https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/database-mirroring-sql-server」を参照してください。

データベースの高可用性を備えた **Session Recording** のインストール方法

データベースの高可用性を備えた Session Recording をインストールするには、次のいずれかを実行します。

- 最初に Session Recording サーバーコンポーネントをインストールし、次に作成したデータベースのデータベース高可用性を構成します。
  準備した SQL Server インスタンスにデータベースがインストールされるよう構成して、Session Recording Administration コンポーネントをインストールした後で、作成したデータベースのデータベース高可用性を構成できます。
  - Always On 可用性グループおよびクラスタリングの場合は、SQL Server インスタンス名を手動で、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance の可用性グループのリスナーの名前、または SQL Server ネットワークの名前に変更する必要があります。
  - データベースのミラーリングの場合、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\Datab および HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartn にデータベースのフェイルオーバーパートナーを手動で追加する必要があります。
- 最初に空のデータベースのデータベース高可用性を構成し、次に Session Recording Administration コンポーネントをインストールします。
  想定したプライマリ SQL Server インスタンスに、Session Recording データベースおよび管理者ログデータベースとして空のデータベースを 2 つ作成し、高可用性を構成できます。次に、Session Recording サーバーコンポーネントをインストールするときに、SQL Server のインスタンス名を入力します。
  - Always On 可用性グループソリューションを使用するには、可用性グループのリスナーの名前を入力します。
  - データベースのミラーリングソリューションを使用するには、プリンシパル SQL Server の名前を入力します。
  - クラスタリングソリューションを使用するには、SQL Server のネットワーク名を入力します。

録画の表示

August 24, 2021

Session Recording Player を使用して、録画した XenApp または XenDesktop セッションを表示、検索、およびブックマークします。

ライブセッションの再生機能を有効にしてセッションを録画する場合は、完了したセッションはもちろん、進行中のセッションも数秒遅れで表示できます。

Session Recording 管理者が設定する時間やファイルサイズの上限を超えるセッションは、複数のセッションファイルに分けて表示されます。

注: Session Recording 管理者が、録画された VDA for Server OS のセッションへのアクセス権をユーザーに付与する必要があります。セッションを表示できない場合は、Session Recording 管理者に連絡してください。

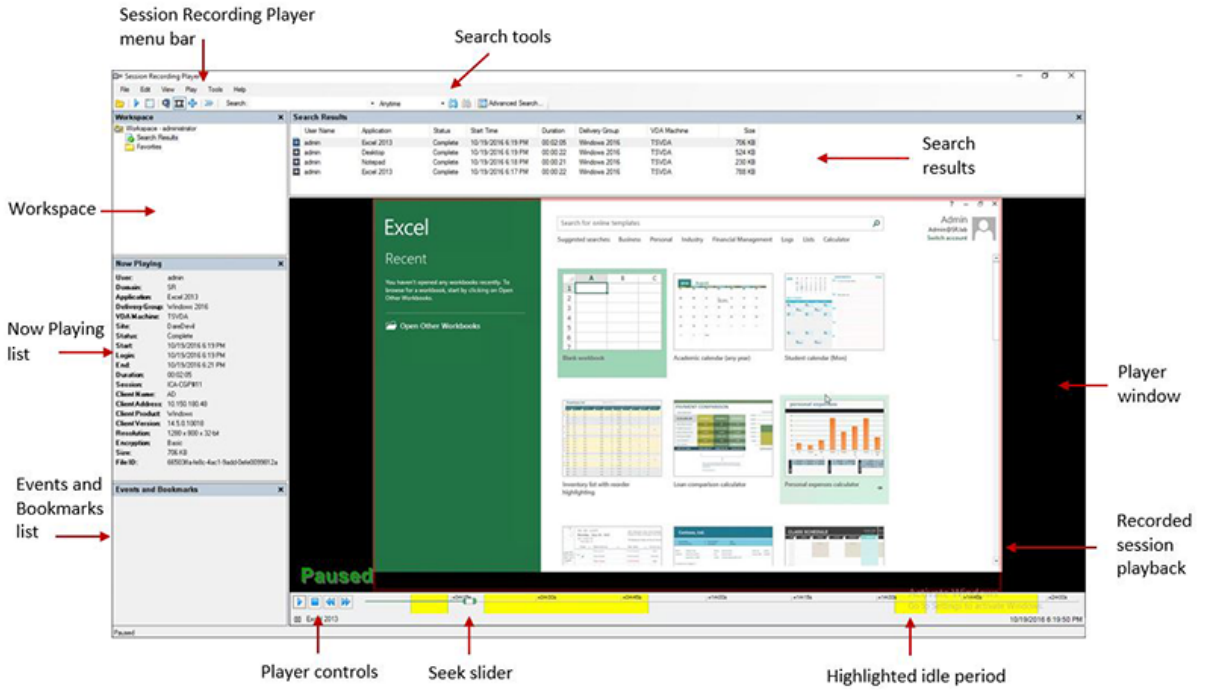
通常、Session Recording 管理者が Session Recording Player をインストールするとき、Session Recording Player と Session Recording サーバーの間の接続も設定します。この接続が未設定の場合は、初めてファイルを検索するときに設定のダイアログボックスが開きます。設定に必要な情報については Session Recording 管理者に問い合わせてください。

Session Recording Player の起動

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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 の主要な要素を示しています。これらの要素の機能について、以下で説明します。



ウィンドウ要素の表示または非表示

Session Recording Player には、表示するかどうかを切り替えるためのウィンドウ要素があります。

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］メニューの ［**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 サーバーの変更

Session Recording 管理者が Session Recording Player から複数の Session Recording サーバー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 サーバーを選択できます。Session Recording Player から同時に複数の Session Recording サーバーに接続することはできません。

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］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］ > ［オプション］ > ［接続］の順に選択します。
4. 接続する Session Recording サーバーを選択します。

録画の再生

October 22, 2021

Session Recording Player でセッションの録画を開くには、次の 3 つの方法があります:

- Session Recording Player を使用して検索を実行する。検索条件に一致するセッションの録画が、検索結果の領域に表示されます。
- ローカルディスクドライブまたは共有ドライブ上のセッションの録画ファイルに直接アクセスする。
- お気に入りフォルダーからセッションの録画ファイルにアクセスする。

デジタル署名なしで録画されたファイルを開くと、その元ファイルと整合性が検証されていないという警告が表示されます。ファイルの整合性について確信がある場合は、警告のポップアップウィンドウで ［はい］をクリックしてファイルを開きます。

注: Session Recording の管理者ログ機能により、Session Recording Player の録画ダウンロードを記録できます。詳しくは、「ログ管理アクティビティ」を参照してください。

検索結果の領域にある録画を開いて再生する

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。

3. 検索を実行します。
4. 検索結果ビューが表示されていない場合は、［ワークスペース］ペインで ［検索結果］を選択します。
5. 検索結果ビューで、再生するセッションを選択します。
6. 次のいずれかの操作を行います:
    - セッションをダブルクリックします。
    - 右クリックして ［再生］を選択します。
    - **Session Recording Player** のメニューバーで、［再生］> ［再生］の順に選択します。

ファイルにアクセスして録画を開き再生する

セッションの録画ファイルの名前は、冒頭に i_ が付く一意な英数字のファイル ID で、ファイル拡張子は.icl か.icle になります。.icl 拡張子は再生データの保護機能が無効な録画を示し、.icle 拡張子は有効な録画を示します。セッションの録画ファイルは、セッションが録画された日付が組み込まれたフォルダに保存されます。たとえば、2014 年 12 月 22 日に録画されたセッションのファイルは、2014\12\22 というフォルダパスに保存されます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. 次のいずれかの操作を行います:
    - **Session Recording Player** のメニューバーで、［ファイル］> ［開く］の順に選択し、ファイルを参照します。
    - Windows のエクスプローラーを使用してファイルを表示し、ファイルをプレーヤーウィンドウにドラッグします。
    - Windows のエクスプローラーを使用してファイルを表示し、ダブルクリックします。
    - ［ワークスペース］ペインで「お気に入り」を作成した場合は、［お気に入り］を選択し、検索結果エリアからファイルを開くのと同じ方法で、［お気に入り］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オンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** ウィンドウの［ワークスペース］ペインで ［お気に入り］フォルダーを選択します。

4. メニューバーで ［ファイル］>［フォルダー］>［フォルダーの作成］の順に選択します。新しいフォルダが［お気に入り］フォルダ配下に表示されます。
5. フォルダ名を入力し、**Enter** キーを押すか、新しい名前を反映する場所をクリックします。

［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再生

August 24, 2021

Session Recording Player でセッションの録画を開いた後は、次の方法で録画されたセッション内を移動できます。

- プレーヤーウィンドウのボタンを使用して、再生、停止、一時停止、および再生速度の変更を行います。
- シークスライダーを使用して、前後に移動します。

マーカーが録画に挿入されている場合、およびセッションの録画にカスタムイベントが含まれている場合は、マーカーおよびイベントのポイントに移動することによって、録画されたセッション内を移動することもできます。

注:

- セッションの録画の再生時に、マウスポインターが 2 つ表示される場合があります。この問題は、ユーザーが Internet Explorer を使用中に、Internet Explorer により自動的に縮小表示されたイメージをユーザーがクリックすると発生します。セッション中は 1 つのマウスポインターしか表示されませんが、セッションの録画の再生時にのみ 2 つ目のマウスポインターが表示されます。
- このバージョンの Session Recording は、XenApp の SpeedScreen マルチメディアアクセラレーション機能や［Flash 品質の調整］ポリシー設定をサポートしません。この機能が有効の場合、再生画面が黒く表示されます。
- HDX RealTime Optimization Pack を使用している場合、Session Recording で Lync Web カメラの映像を録画することはできません。
- 4096 x 4096 以上の解像度でセッションを録画すると、録画が断片化する場合があります。
- XenDesktop サイトポリシーによって従来のグラフィックモードが有効になっており、Citrix Receiver for Windows ポリシーによってディスクベースのキャッシングが有効になっている場合、Windows 7 デスクトップセッションを正しく録画できません。録画したものを再生すると、真っ黒の画面が表示されます。
  この問題を回避するには、Citrix Receiver for Windows をインストールしたマシンで、グループポリシーオブジェクトを使用してディスクベースのキャッシングを無効化します。ディスクベースのキャッシングの無効化について詳しくは、CTX123169を参照してください。
- Session Recording では、Framehawk の表示モードはサポートされません。このため、Framehawk の表示モードのセッションを正しく録画および再生することはできません。Framehawk の表示モードで録画されたセッションには、セッションアクティビティが含まれない可能性があります。

プレーヤーウィンドウのボタンの使用

Player ウィンドウのボタンを使用するか、**Session Recording Player** メニューバーの ［再生］の下のメニューアイテムを選択して、セッションの録画を操作します。プレーヤーウィンドウのボタンまたはメニューアイテムを使用して次の操作を実行します。

Player ウィンドウのボタン	機能
	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］をクリックし、［再生］をクリックすると、ファイルの冒頭から録画が再開されます。
	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

Player ウィンドウの下部にあるシークスライダーを使用して、セッションの録画内の別の位置にジャンプします。シークスライダーを録画内の表示したいポイントまでドラッグすることも、スライダーバーの任意のポイントをクリックして移動することもできます。

また、次のキーボードキーを使用してシークスライダーを制御できます:

キー	シーク操作
ホーム	冒頭へシークします。
End	末尾へシークします。
→	5 秒先へシークします。
←	5 秒前へシークします。
マウスホイールを 1 目盛り手前に動かす	15 秒先へシークします。
マウスホイールを 1 目盛り奥に動かす	15 秒前へシークします。
Ctrl+→	30 秒先へシークします。
Ctrl+←	30 秒前へシークします。

キー	シーク操作
PgDn	1 分先へシークします。
PgUp	1 分前へシークします。
Ctrl キーを押しながらマウスホイールを 1 目盛り手前に動かす	90 秒先へシークします。
Ctrl キーを押しながらマウスホイールを 1 目盛り奥に動かす	90 秒前へシークします。
Ctrl+PageDown	6 分先へシークします。
Ctrl+PageUp	6 分前へシークします。

シークスライダーの速度を調整するには、**Session Recording Player** のメニューバーで、［ツール］>［オプション］>［**Player**］の順に選択し、スライダーをドラッグしてシークの応答速度を変更します。応答速度を上げると、より多くのメモリが消費されます。録画のサイズやマシンのハードウェアによって、応答速度が低下する場合があります。

再生速度の変更

Session Recording Player を設定して、標準の 4 分の 1 倍速から 32 倍速までの速度で、セッションの録画を再生できます。速度は指数的に増加します。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［再生］>［再生速度］の順に選択します。
4. 速度を選択します。

すぐに速度が調節されます。速度を示す数字がプレーヤーウィンドウのボタンの下に表示されます。この速度を示す緑色のテキストは、プレーヤーウィンドウにも短時間表示されます。

録画されたセッションのアイドル期間のハイライト表示

録画されたセッションのアイドル期間とは、何も操作が行われていない部分です。Session Recording Player では、録画したセッションのアイドル期間を再生時にハイライトできます。このオプションは、デフォルトで ［オン］になっています。

Session Recording Player でライブセッションを再生すると、アイドル期間がハイライトされない点に注意してください。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。

3. **Session Recording Player** のメニューバーで、［表示］>［アイドル期間］と選択し、オプションボックスをオンまたはオフにします。

操作のない空白期間の省略

高速レビューモードを使用すると、録画されたセッション内で操作のない部分の再生を省略することができます。この設定により再生時間を短くできます。ただし、アニメーションを用いたマウスポインター、点滅するカーソル、秒針付きの時計など、動画による連続処理の再生は省略できません。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2.［スタート］メニューの［**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 Player 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

August 24, 2021

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、セッション再生中に、Session Recording Player を使用して録画されたセッションに挿入するマーカーです。ブックマークは、挿入すると、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。ブックマークは、Session Recording Player の **Bookmarks** キャッシュフォルダーに（たとえば C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks）「.iclb」ファイルとして、「.iclb」形式の録画ファイルと同じファイル名で保存されます。別のプレイヤーでブックマーク付きの録画ファイルを再生する場合は、「.iclb」ファイルをプレイヤー上の **Bookmarks** キャッシュフォルダーに移動します。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］の一覧にも表示できます。そのテキストラベルと録画されたセッションでの時刻と共に、時系列で一覧に表示されます。

イベントとブックマークを使用して、録画されたセッション内を簡単に移動できます。イベントまたはブックマークに移動することにより、それらが挿入されているポイントまでを省略して、録画されたセッション内を移動できます。

イベントとブックマークの一覧への表示

［イベントとブックマーク］の一覧には、現在再生中の録画されたセッションに挿入されているイベントとブックマークが表示されます。イベントのみ、ブックマークのみ、または両方を表示できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ［イベントとブックマーク］の一覧にマウスポインターを移動し、右クリックしてメニューを表示します。
4. ［イベントのみ表示］、［ブックマークのみ表示］、または ［すべて表示］を選択します。

ブックマークの挿入

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを追加する録画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。
   - テキストラベル付きのブックマークを追加するには、［コメントの追加］を選択します。ブックマークに割り当てるテキストラベルを最長 128 文字で入力します。［**OK**］をクリックします。

コメントの追加または変更

ブックマークを作成した後でコメントを追加したり、コメントを変更したりできます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを含む録画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］の一覧で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. ［コメントの編集］を選択します。
7. ウィンドウが表示されたら、新しいコメントを入力して ［**OK**］をクリックします。

ブックマークの削除

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを含む録画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］の一覧でブックマークが表示されていることを確認します。
5. ［イベントとブックマーク］の一覧でブックマークを選択し、右クリックしてメニューを表示します。

6. ［削除］を選択します。

イベントまたはブックマークへの移動

イベントまたはブックマークに移動すると、それらが挿入されているポイントまでを省略して、録画されたセッション内を移動できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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セッションの再生を開始します。
4. 次の方法で、イベントまたはブックマークに移動します：
   - プレーヤーウィンドウの下部でイベントまたはブックマークを表す丸印をクリックし、イベントまたはブックマークに移動します。
   - ［イベントとブックマーク］の一覧で、イベントまたはブックマークをダブルクリックします。次のイベントまたはブックマークに移動するには、一覧からイベントまたは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、［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

August 24, 2021

オプションを使用して、Player 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 Player 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、Player 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 Player ウィンドウの背景と区別しやすくしたりできます。

Player ウィンドウの全画面表示

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［表示］>［全画面］の順に選択します。
4. 元のサイズに戻すには、Esc キーまたは F11 キーを押します。

独立ウィンドウでの **Player** ウィンドウの表示

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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。ドラッグしてウィンドウのサイズを変更することができます。

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 **Player** ウィンドウのサイズに合わせる

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［再生］ > ［表示モード］ > ［ウィンドウに合わせる］の順に選択します。
   - ［ウィンドウに合わせる（高速描画）］を選択すると、十分な画質を維持しながら画像を縮小します。高画質オプションを使用する場合より描画が高速で行われますが、画像とテキストの明晰さは低下します。高画質モードでパフォーマンスに問題が生じる場合は、このオプションを使用します。
   - ［ウィンドウに合わせる（高画質）］を選択すると、明晰な画像とテキストを維持しながら画像を縮小します。このオプションを使用すると、高速描画オプションの場合より描画速度が遅くなることがあります。

再生するセッションの画面サイズを元のセッションのサイズに合わせる

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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。この小さなイメージで、画面のどこにいるかがわかります。
5. ［セッションに合わせる］を終了するには、表示モードのいずれかのオプションを選択します。

セッションの録画の周りに赤い枠線を表示する

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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

August 24, 2021

セッションの録画ファイルを開くたびに、録画が格納されている場所からファイルがダウンロードされます。同じファイルを頻繁にダウンロードする場合は、ファイルをワークステーションにキャッシュすることでダウンロード時間を節約できます。ワークステーションにキャッシュされるファイルは次のフォルダーに格納されます:

```
userprofile\\AppData\\Local\\Citrix\\SessionRecording\\Player\\Cache
```

キャッシュに割り当てるディスク容量を指定できます。指定した容量まで録画ファイルが蓄積されると、最も古く使用されていない録画が削除され、新しい録画のための空き領域が作成されます。ディスク領域を解放するために、いつでもキャッシュを空にすることができます。

キャッシュの有効化

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］>［オプション］>［キャッシュ］の順に選択します。
4. ［ダウンロードしたファイルをローカルコンピューターにキャッシュする］チェックボックスをオンにします。
5. キャッシュに使用されるディスク容量を制限するには、［使用するディスク容量を制限する］チェックボックスをオンにして、使用する容量をメガバイト単位で指定します。
6. ［**OK**］をクリックします。

キャッシュを空にする

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**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。

録画の検索

August 24, 2021

Session Recording Player では、クイック検索を実行することも、高度な検索を実行して検索に適用するオプションを指定することもできます。検索結果は Session Recording Player の検索結果の領域に表示されます。

> 注:
>
> 使用可能な録画されたセッションを 1 回の検索で表示できるセッション数の上限まですべて表示するには、検

> 索パラメーターを指定せずに検索を実行します。

クイック検索の実行

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. 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。
   - ［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日時を指定できます。
4. ドロップダウンリスト右側の双眼鏡のアイコンをクリックして、検索を開始します。

高度な検索の実行

高度な検索では、結果に 150,000 個を超えるエンティティが含まれている場合、返されるまでに最大 20 秒かかる場合があります。Citrix では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］メニューの ［**Session Recording Player**］を選択します。
3. ［**Session Recording Player**］ウィンドウで、ツールバーの ［高度な検索］をクリックするか、メニューバーで ［ツール］>［高度な検索］の順に選択します。
4. ［高度な検索］ダイアログボックスのタブで検索条件を定義します：
   - ［共通］タブでは、ドメインまたはアカウントの認証先、サイト、グループ、サーバー OS の VDA、アプリケーション、またはファイル ID を使用して検索できます。
   - ［日付/時刻］タブでは、日付、曜日、および時刻を使用して検索できます。
   - ［イベント］タブでは、セッションに挿入された Citrix 定義イベントとカスタムイベントを検索できます。
   - ［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。

   高度な検索のクエリは、保存しておいて後で取得することができます。［高度な検索］ダイアログボックスの［保存］をクリックして、現在のクエリを保存します。保存したクエリを取得するには、［高度な検索］ダイアログボックスの ［開く］をクリックします。保存したクエリファイルの拡張子は.isq です。

検索オプションの設定

Session Recording Player の検索オプションにより、表示される検索結果数の上限およびアーカイブ済みのファイルを検索に含めるかどうかも指定できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** メニューバーで、［ツール］>［オプション］>［検索］の順に選択します。
4. ［検索結果の表示件数の上限］ボックスに、表示する検索結果数を入力します。最大で 500 件の検索結果を表示できます。
5. アーカイブ済みのファイルを検索に含めるかどうかを設定するには、［アーカイブ済みファイルを含める］チェックボックスをオンまたはオフにします。

Session Recording のトラブルシューティング

August 24, 2021

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 ポリシーコンソールの問題。
- 通信プロトコルに関連して問題が発生する。

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

Session Recording Agent 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。次のような原因があります:

- 接続が閉じられました。**SSL/TLS** の安全なチャネルを確立できませんでした。この例外は、Session Recording サーバーで使用している証明書を署名した CA が、Session Recording Agent が動作するサーバーに信頼されていないか、Session Recording Agent が動作するサーバーに CA 証明書がインストールされていないことを示します。または、証明書の有効期限が切れているか失効している可能性があります。

解決策：正しい CA 証明書が Session Recording Agent をホストするサーバーにインストールされているか、信頼されている CA を使用していることを確かめます。

- リモートサーバーがエラーを返しました：**HTTP 403**（アクセス不可）。これは、HTTP（セキュリティで保護されていないプロトコル）を使用して接続しようとしたときに表示される、標準の HTTPS エラーです。Session Recording サーバーをホストするコンピューターでセキュリティで保護された接続のみを受け付けるため、接続が拒否されています。

  解決策：［Session Recording Agent のプロパティ］を使用して Session Recording Broker のプロトコルを **HTTPS** に変更します。

レコードポリシークエリの検証中に、**Session Recording Broker** が不明なエラーを返しました。エラーコード **5**（アクセスが拒否されました）。詳しくは、**Session Recording** サーバー上のイベントログを参照してください。このエラーは、セッションが開始され録画ポリシーの評価要求が送信されると発生します。このエラーは、Session Recording 承認コンソールの役割であるポリシークエリの役割から、デフォルトのメンバーである Authenticated Users グループが削除された結果発生します。

解決策：Authenticated Users グループをこの役割に再追加するか、各 Session Recording Agent をホストする各サーバーをポリシークエリの役割に追加します。

接続が閉じられました。維持される必要があった接続が、サーバーによって切断されました。このエラーは、Session Recording サーバーが停止しているか、要求を受け付けられないことを示します。IIS がオフラインまたは再起動中であることが原因か、サーバー全体がオフラインである可能性があります。

解決策：Session Recording サーバー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 サーバーが **Session Recording** データベースに接続できない

Session Recording サーバーから 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** サーバーへの接続確立時にネットワーク関連またはインスタンス固有のエラーが発生しました。」このエラーは、Session Recording サーバーをホストするコンピューターのイベントビューアーにおいて、ID が 2047 のアプリケーションイベントログに表示されます。

「**Citrix Session Recording** ストレージマネージャーの説明**:** データベース接続を確立しています **-** この処理の実行中に例外が見つかりました。」このエラーは、Session Recording サーバーをホストするコンピューターのイベントビューアーにおいて、アプリケーションイベントログに表示されます。

Session Recording サーバーに接続できません。**Session Recording** サーバーが実行中か確認してください。このエラーメッセージは、Session Recording ポリシーコンソールの起動時に表示されます。

解決方法:

- Microsoft SQL Server 2008 R2、Microsoft SQL Server 2012、Microsoft SQL Server 2014、または Microsoft SQL Server 2016 の Express Edition がスタンドアロンサーバーにインストールされていますが、Session Recording のサービスまたは設定が正しく設定されていません。サーバーで TCP/IP プロトコルを有効にして SQL Server Browser サービスを実行する必要があります。これらの設定を有効にする方法について詳しくは、Microsoft 社のドキュメントを参照してください。
- Session Recording 管理ツールのインストール中に、サーバーとデータベースについて誤った情報が指定されています。Session Recording データベースをアンインストールし、正しい情報を指定して再インストールします。
- Session Recording データベースサーバーが停止しています。サーバーに接続できることを確かめます。
- Session Recording サーバーまたは Session Recording データベースサーバーをホストするコンピューターで、もう一方の FQDN または NetBIOS 名を解決できません。ping コマンドを使用して、名前を解決できることを確認します。
- Session Recording データベースのファイアウォールの構成をチェックし、SQL Server の接続が許可されていることを確認します。詳しくは、Microsoft 社のhttps://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access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正常に録画されない場合は、まず Session Recording Agent と Session Recording サーバーが動作する VDA for Server OS 上のイベントビューアーで、アプリケーションイベントログを確認します。このログには有益な診断情報が含まれている可能性があります。

セッションが録画されない場合、次の問題が原因である可能性があります。

- コンポーネント間の接続と証明書。Session Recording コンポーネントの間で通信ができない場合は、セッションの録画に失敗する可能性があります。録画の問題のトラブルシューティングをするには、すべてのコンポーネントが適切に設定されていて正しいコンピューターを参照していることと、すべての証明書が有効で適切にインストールされていることを確かめます。
- 非 **Active Directory** ドメイン環境。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ユーザーが最初に開いた公開アプリケーションを照合します。同じセッション上で次のアプリケーションを開くと、最初のアプリケーションに対して有効なポリシーが、次のアプリケーションにも適用されます。セッション共有がアクティブなポリシーと競合することを防ぐには、競合するアプリケーションを別の VDAs for Server OS で公開します。
- 録画が有効になっていない。VDA for Server OS に Session Recording Agent をインストールすると、そのサーバーではデフォルトで録画が有効になります。録画を許可するアクティブな録画ポリシーを設定するまでは、録画はされません。
- アクティブな録画ポリシーによって録画が許可されない。セッションを録画するには、特定のユーザー、サーバー、または公開アプリケーションを対象に、アクティブな録画ポリシーでセッションの録画が許可されている必要があります。
- **Session Recording** サービスが実行されていない。セッションを録画するには、VDA for Server OS で Session Recording Agent サービスが実行されており、Session Recording サーバーをホストするコンピューターで Session Recording ストレージマネージャーサービスが実行されている必要があります。
- **MSMQ** が設定されていない。Session Recording Agent が動作するサーバーと Session Recording サーバーをホストするコンピューターで MSMQ が適切に設定されていない場合は、録画の問題が起きる可能性があります。

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** サーバーのプロパティ］で ［再生］タブをクリックし、［ライブセッションの再生を許可する］チェックボックスをオンにします。

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、Machine Creation Services（MCS）または Provisioning Services（PVS）で構成済みのマスターイメージとインストール済みの Microsoft Message Queuing（MSMQ）を使用して VDA を作成する場合に発生します。この状況では、VDA で MSMQ の QMId が同じになります。

これを回避するには、各 VDA に対し、一意の QMId を作成します。詳しくは、「Session Recording のインストール、アップグレード、およびアンインストール」の「**Session Recording Agent** のインストール」セクションの手順 8 を参照してください。

- 特定の録画ファイルを再生しているときに、Session Recording Player がメッセージ「再生中のファイルにより、内部システムエラー（エラーコード**: 9**）が元の録画中に発生したことが報告されました。エラーが発生した箇所までは再生できます。」を表示して内部エラーをレポートすることがあります。

  この問題は通常、グラフィック指向セッションの録画中に Session Recording Agent のバッファーサイズが不十分だったために発生します。

  これを回避するには、Session Recording Agent でレジストリ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAud の値を大きな値に変更してから、マシンを再起動します。

Session Recording データベースまたは **Session Recording** サーバー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 サーバー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「データベース接続テストに失敗しました。正しいデータベースインスタンス名を入力してください。」が表示されて接続テストが失敗します。

そのような場合は、現在のユーザーに、権限制限エラーを修正するためのパブリック SQL Server 役割権限があることを確認してください。

管理者ログ

Windows Server 2008 R2 SP1 では、管理者ログ機能をインストールする前に、まず［**.Net Framework 3.5** の機能］>［**WCF** アクティブ化］>［**HTTP** アクティブ化］をインストールしてから、.Net Framework 4.5 以降のバージョンをインストールします。これら 2 つの要件を逆の順番でインストールしないでください。順番に従わないと、管理者ログが想定どおり機能しない可能性があります。Session Recording の構成をサーバープロパティコンソールで変更しようとしたり、Session Recording ポリシーを必須のログが有効になった状態でポリシーコンソールで更新しようとしたりすると、操作がブロックされる場合があります。

この問題を解決するには、次の手順に従います。

1. ［インターネットインフォメーションサービス（IIS）マネージャー］を開いて［アプリケーションプール］ノードに移動します。
2. ［**SessionRecordingLoggingAppPool**］を右クリックして、［基本設定］ダイアログボックスを開きます。
3. .NET Framework バージョンを.NET Framework v4.0 に変更します。

コンポーネント間の接続の確認

August 24, 2021

Session Recording のセットアップ中にコンポーネント間の接続に成功しないことがあります。すべてのコンポーネントが Session Recording サーバー（Broker）と通信を行います。デフォルトでは、IIS のコンポーネントであるブローカーのセキュリティは、IIS の既定の Web サイトの証明書を使用して保護されます。あるコンポーネントから Session Recording サーバーに接続できないときは、ほかのコンポーネントから接続を試行しても失敗することがあります。

Session Recording Agent と Session Recording サーバー（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 サーバーをホストするコンピューターの、イベントビューアーのアプリケーションログに記録されます。Session Recording 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 Agent** のプロパティ］で、［接続］をクリックします。
4. ［Session Recording サーバー］の値が、Session Recording サーバーをホストするコンピューターの正しい名前であることを確認します。
5. ［Session Recording サーバー］の値として入力されているサーバーに VDA for Server OS から通信できることを確かめます。

注：アプリケーションイベントログで、エラーと警告を確認します。

Session Recording サーバー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によって、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. レジストリエディターを開きます。
3. HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server に移動します。
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 管理ツールを使って、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 ブラウザーで Session Recording Broker の Web ページにアクセスして Session Recording サーバーの IIS サイトへの接続をテストすると、問題の原因が、プロトコルの誤設定なのか、証明書の問題なのか、Session Recording Broker の問題なのかを判断するのに役立ちます。

Session Recording Agent の IIS の接続を確かめるには:

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. Web ブラウザーを開いて次のアドレスを入力します:
   - HTTPS で接続する場合: `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）
   - HTTP で接続する場合:`http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Session Recording Player の IIS の接続を確かめるには

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. Web ブラウザーを開い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。

Session Recording ポリシーコンソールの IIS の接続を確かめるには

1. Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Web ブラウザーを開いて次のアドレスを入力します:
   - HTTPS で接続する場合:`https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）
   - HTTP で接続する場合:`http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Web ブラウザーに XML ドキュメントが表示された場合は、設定したプロトコルを使用して、Session Recording ポリシーコンソールが動作するコンピューターが Session Recording サーバーをホストするコンピューターと接続していることが確かめられたことになります。

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 サーバーをホストするコンピューターにサーバー証明書を設定する必要があります。すべてのコンポーネントの Session Recording サーバーへの接続に、ルート CA（Certificate Authority：証明機関）が必要です。この証明書をインストールしないと、コンポーネント間の通信は失敗します。

IIS の接続をテストするときのように、Session Recording Broker の Web ページにアクセスすることによって、証明書をテストすることができます。各コンポーネントの XML ページにアクセスできる場合は、証明書は正しく設定されています。

ここでは、接続エラーの原因になる、証明書によくある問題について説明します:

- 無効な証明書または証明書の不足。Session Recording Agent が動作するサーバーにサーバー証明書を信頼するためのルート証明書がインストールされていない場合は、HTTPS を介して Session Recording サーバーを信頼できず、接続できません。Session Recording サーバー上のサーバー証明書がすべてのコンポーネントで信頼されていることを確かめてください。
- 名前の不一致。Session Recording サーバーをホストするコンピューターに割り当てられたサーバー証明書が、FQDN を使用して作成されている場合、Session Recording サーバーに接続するとき、接続するすべてのコンポーネントで FQDN を使用する必要があります。サーバー証明書が NetBIOS 名を使用して作成されている場合、Session Recording サーバーに接続するとき、接続するすべてのコンポーネントで NetBIOS 名を使用するように設定します。
- 期限切れまたは失効した証明書。サーバー証明書が失効している場合、HTTPS を介した Session Recording サーバーへの接続は失敗します。Session Recording サーバーをホストするコンピューターに割り当てられているサーバー証明書が有効で、失効していないことを確かめてください。録画したセッションのデジタル署名に同じ証明書を使用している場合は、Session Recording サーバーをホストするコンピューターのイベントログに、証明書が失効したことを示すエラーメッセージまたは失効日が近づいていることを示す警告メッセ

ージが記録されます。

Player で録画を検索できない

August 24, 2021

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 サーバーと通信することができません。誤ったサーバー名が入力されているか、DNS でサーバー名を解決できていないという、2 つの理由が考えられます。

  解決策: Session Recording Player のメニューバーで、[ツール] > [オプション] > [接続] の順に選択し、[**Session Recording** サーバー] ボックスの一覧のサーバー名が正しいことを確認します。サーバー名が正しい場合は、コマンドプロンプトで ping コマンドを実行し、名前を解決できるかどうかを確認します。Session Recording サーバーが停止しているかオフラインのときにセッションの録画ファイルを検索すると、「リモートサーバーに接続できません」というエラーメッセージが返されます。

- リモートサーバーに接続できません。このエラーは、Session Recording サーバーが停止しているかオフラインのときに発生します。

  Resolution: Verify that the Session Recording Server is connected.

- アクセスが拒否されました。アクセス拒否のエラーは、ユーザーにセッションの録画ファイルを検索およびダウンロードする権限がない場合に発生します。

  解決策: Session Recording 承認コンソールで、ユーザーを Player の役割に割り当てます。

- **Player** の役割が割り当てられているときにアクセスが拒否されました。このエラーは、Session Recording Player と Session Recording サーバーを同じマシンにインストールし、UAC を有効にしているときに発生します。Domain Admins または Administrators ユーザーグループに Player の役割を割り当てたときに、そのグループに含まれていない組み込みではない管理者ユーザーが Session Recording Player で録画ファイルを検索するときに役割ベースのチェックを渡せないことがあります。

  Resolutions:

  - Run Session Recording Player as administrator.
  - Assign specific users as Player role rather than the entire group.
  - Install Session Recording Player in a separate machine rather than Session Recording Server.

- セッションの録画ファイルを検索できませんでした。接続が閉じられました。**SSL/TLS** の安全なチャネルを確立できませんでした。この例外は、Session Recording サーバーで使用している証明書を署名した CA

（Certificate Authority：証明機関）がクライアントデバイスに信頼されていないか、クライアントデバイスに CA 証明書がインストールされていないために発生します。

Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.

- 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** サーバー］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 に問題があります。Session Recording サーバー（ストレージマネージャー）にキューが接続されていることを確認します。Web ブラウザーを使用して接続エラーが発生しないかテストします（MSMQ の接続プロトコルとして HTTP または HTTPS を使用している場合）。

キューが接続されていることを確認するには：

1. Session Recording Agent をホストするサーバーにログインして、発信キューを表示します。
2. Session Recording サーバーをホストするコンピューターへのキューが接続された状態であることを確認します。
   - 接続を待っている状態で、メッセージがキューにあり、プロトコルが HTTP または HTTPS の場合は（［**Session Recording Agent** のプロパティ］の ［接続］タブで選択されているプロトコルに対応します）、手順 3 を実行します。
   - 接続済みの状態で、メッセージがキューにない場合は、Session Recording サーバーをホストするサーバーに問題がある可能性があります。手順 3 を省略し、手順 4 を実行します。
3. キューにメッセージがある場合は、Web ブラウザーを起動して次のアドレスを入力します：
   - HTTPS で接続する場合：`https://servername/msmq/private$/CitrixSmAudData`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）
   - HTTP で接続する場合：`http://servername/msmq/private$/CitrixSmAudData`（ここで、*servername* は Session Recording サーバーをホストするコンピューターの名前です。）

「サーバーはセキュリティで保護された接続のみを受け付けます」というようなエラーが返される場合は、［**Session Recording Agent** のプロパティ］に一覧されている MSMQ プロトコルを HTTPS に変更します。Web サイトのセキュリティ証明書に問題があるというエラーが返される場合は、TLS のセキュアチャ

ネルのための信頼関係に問題がある可能性があります。その場合は、正しい CA 証明書をインストールするか、信頼されている CA を使用します。

4. キューにメッセージがない場合は、Session Recording サーバーをホストするコンピューターにログオンし、専用キューを表示します。**citrixsmauddata** を選択します。キューに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

August 24, 2021

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 Citrix で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

1. Session Recording サーバーをホストするコンピューターにログオンし、IIS で Session Recording Broker との接続に使用しているセキュリティで保護された接続を無効にします。
2. Session Recording Agent がインストールされている各サーバーの［**Session Recording Agent** のプロパティ］でプロトコル設定を HTTPS から HTTP に次の手順に従って変更します：
   a) 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。
   b)［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。
   c)［**Session Recording Agent** のプロパティ］で、［接続］タブを選択します。
   d)［**Session Recording Broker**］で［プロトコル］ボックスの一覧から［**HTTP**］を選択し、［**OK**］をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、［はい］をクリックします。
3. Session Recording Player の設定で、プロトコルを HTTPS から HTTP に変更します：
   a) 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。
   b)［スタート］メニューの［**Session Recording Player**］を選択します。
   c)［**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。
   d)［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 ポリシーコンソールの設定で、プロトコルを HTTPS から HTTP に変更します：
   a) Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
   b)［スタート］ボタンをクリックし、［**Session Recording** ポリシーコンソール］を選択します。
   c)［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も使用されます。

通信プロトコルを **HTTPS** に戻す

1. Session Recording サーバーをホストするコンピューターにログオンし、IIS で Session Recording Broker との接続に使用しているセキュリティで保護された接続を有効にします。
2. Session Recording Agent がインストールされている各サーバーの［**Session Recording Agent** のプロパティ］でプロトコル設定を HTTP から HTTPS に変更します。
   a) 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。
   b)［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。
   c)［**Session Recording Agent** のプロパティ］で、［接続］タブを選択します。
   d)［**Session Recording Broker**］で ［プロトコル］ボックスの一覧から ［**HTTPS**］を選択し、［**OK**］をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、［はい］をクリックします。
3. Session Recording Player の設定で、プロトコルを HTTP から HTTPS に変更します:
   a) 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。
   b)［スタート］メニューの ［**Session Recording Player**］を選択します。
   c)［**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。
   d)［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 ポリシーコンソールの設定で、プロトコルを HTTP から HTTPS に変更します:
   a) Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
   b)［スタート］ボタンをクリックし、［**Session Recording** ポリシーコンソール］を選択します。
   c)［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も使用されます。

データベースレコードの管理

August 24, 2021

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 サーバーソフトウェアをホストするサーバーの drive:\Program Files\Citrix\SessionRecording\Server\Bin フォルダーに、Session Recording と合わせてインストールされます。

クイックリファレンス

次の表に、ICLDB ユーティリティで使用できるコマンドとオプションの一覧を示します。コマンドは次の形式で入力します。

icldb [version | locate | dormant | import | archive | remove | removeall] \[/l\] \[/f\] \[/s\] \[/?\] コマンドオプション >

> 注:
>
> 詳しくは、ユーティリティ関連のヘルプを参照してください。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、**\Program Files\Citrix\SessionRecording\Server\Bin** フォルダーに移動し、「**icldb /?**」と入力します。特定のコマンドのオンラインヘルプにアクセスするには、「**icldb *command* /?**」と入力します（command は対象のコマンド名）。

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私指定することも、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。
インポート	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。

コマンド	説明
削除	セッションの録画ファイルへの参照をデータベースから削除します。このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。条件として使用する保有期間を指定します。関連付けられている物理ファイルを削除することもできます。
removeall	セッションの録画ファイルへのすべての参照を Session Recording データベースから削除し、データベースを元の状態に戻します。実際の物理ファイルは削除されません。ただし、Session Recording Player でファイルを検索することはできなくなります。このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。削除された参照はバックアップから復元しない限り元に戻せません。
version	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。

セッションの録画ファイルのアーカイブ

録画の格納場所に適切なレベルの空きディスク容量を維持するには、セッションの録画ファイルを定期的にアーカイブします。使用可能なディスク容量と標準的なセッションの録画ファイルのサイズに応じて、アーカイブ間隔は異なります。録画開始日から 2 日以上経過すると、セッションの録画ファイルはアーカイブ可能となります。これは、ライブ録画が完了前にアーカイブされないようにするためのルールです。

セッション録画をアーカイブするには、2 つの方法があります。セッションの録画ファイルが録画の格納場所にある間に、セッションの録画ファイルのデータベースレコードをアーカイブ済みのステータスで更新できます。この方法を使用すると、プレイヤーでの検索結果を減らすことができます。もう 1 つの方法は、セッションの録画ファイルのデータベースレコードをアーカイブ済みのステータスで更新し、セッションの録画ファイルを録画の格納場所から別の場所に移動して代替メディアにバックアップする方法です。ICLDB ユーティリティを使ってセッションの録画ファ

イルを移動する場合、それらのファイルは、年/月/日の元のファイルフォルダー構造のない指定されたディレクトリに移動します。

Session Recording データベース内のセッション録画レコードには、アーカイブ化に関連する 2 つのフィールドがあります：セッション録画がアーカイブされた日付と時刻を表すアーカイブ時間と、アーカイブ中に管理者が追加することのあるアーカイブメモ（オプションのテキストを含むメモ）です。この 2 つのフィールドは、セッション録画がアーカイブされたこと、およびアーカイブ時間を示します。

Session Recording Player では、アーカイブされたセッションの録画にアーカイブ済みのステータスとアーカイブ日時が示されます。ファイルが移動していなくても、アーカイブされたセッション録画は再生されます。アーカイブ中にセッションの録画ファイルが移動した場合、「ファイルが見つかりません」というエラーが表示されます。セッションを再生するには、セッションの録画ファイルを復元する必要があります。セッション録画を復元するには、Session Recording Player の録画プロパティダイアログボックスのセッション録画のファイル ID とアーカイブ時間を管理者に提供します。アーカイブされたファイルの復元については、以下の「セッションの録画ファイルの復元」セクションで詳しく説明しています。

ICLDB ユーティリティの **archive** コマンドには、次のようなパラメーターがあります：

- **/RETENTION:<days>** - セッション録画の保有期間（日数）。指定された日数を超過した録画は、Session Recording データベースでアーカイブ済みにマークされます。保有期間は 2 日以上の整数とする必要があります。
- **/LISTFILES** - セッションの録画ファイルのアーカイブ時の完全なファイルパスとファイルを一覧表示します。これはオプションのパラメーターです。
- **/MOVETO:<directory>** - アーカイブされたセッションの録画ファイルを物理的に移動する移動先ディレクトリ。あらかじめ存在するディレクトリを指定する必要があります。これはオプションのパラメーターです。ディレクトリが指定されていない場合、ファイルは元の格納場所に残ります。
- **/NOTE:<note>** - データベースレコードに追加される、アーカイブされた各セッション録画のテキストを含むメモ。このメモは二重引用符で囲んでください。これはオプションのパラメーターです。
- **/L** - Windows イベントログに、アーカイブされたセッションの録画ファイルの結果とエラーの数を記録します。これはオプションのパラメーターです。
- **/F** - プロンプトを表示せずに archive コマンドを強制的に実行します。これはオプションのパラメーターです。

Session Recording データベースにセッション録画をアーカイブし、セッションの録画ファイルを物理的に移動するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。
3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（Session Recording サーバーのインストールパス/Server/Bin）に変更します。

4. **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /L** コマンドを実行します。ここで、**days** はセッションの録画ファイルの保有期間、**directory** はアーカイブされたセッションの録画ファイルの移動先ディレクトリ、**note** はデータベースレコードに追加された、アーカイブされた各セッションの録画ファイルに関するメモです。**Y** と入力してアーカイブを確定します。

Session Recording データベースでセッション録画のアーカイブのみを行うには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。
3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（Session Recording サーバーのインストールパス/Server/Bin）に変更します。
4. **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE:<note> /L** コマンドを実行します。ここで、**days** はセッション録画の保有期間、**note** はデータベースレコードに追加された、アーカイブされる各セッション録画に関するメモです。**Y** と入力してアーカイブを確定します。

セッションの録画ファイルの復元

Session Recording データベースにアーカイブされたセッション録画を表示する場合に、そのファイルが録画の格納場所から移動されているときには、セッションの録画ファイルの復元が必要となります。アーカイブ中に録画の格納場所から移動されなかったアーカイブ済みのセッション録画は、Session Recording Player で引き続きアクセスできます。

移動されたセッションの録画ファイルを復元するには、2 つの方法があります。必要なセッションの録画ファイルをアーカイブされたファイルの復元ディレクトリにコピーするか、ICLDB ユーティリティを使用して Session Recording データベースにインポートします。Citrix では、アーカイブされたセッションの録画ファイルの復元には、最初の方法をお勧めします。アーカイブ済みファイルの復元フォルダーにコピーしたファイルは、不要になった場合、削除します。

Session Recording Broker では、セッションの録画ファイルが元の格納場所に見つからない場合、アーカイブ済みファイルの復元フォルダーを利用します。このケースは、Session Recording Player からセッションの録画ファイルの再生が要求された場合に発生します。Session Recording Broker は最初に、元の格納場所でセッションの録画ファイルを探します。ファイルが元の格納場所に見つからない場合、Session Recording Broker は次に、アーカイブ済みファイルの復元フォルダーをチェックします。ファイルが復元用フォルダーに存在する場合には、Session Recording Broker はそのファイルを再生のために Session Recording Player に送信します。ファイルが見つからない場合は、Session Recording Broker は「ファイルが見つかりません」というエラーを Session Recording Player に送信します。

アーカイブ済みのセッションの録画ファイルを ICLDB ユーティリティを使用してインポートすると、Session Recording データベースがこのファイルのセッション録画情報（新しい格納パスなど）で更新されます。ICLDB ユーティリティを使用してアーカイブされたセッションの録画ファイルをインポートしても、ファイルはセッション録画時の元の格納場所には戻されません。

注：インポートされたセッションの録画ファイルには、Session Recording データベースで消去されたアーカイブ時間とアーカイブメモが含まれています。そのため、次に ICLDB archive コマンドを実行すると、インポートされたセッションの録画ファイルが再度アーカイブされることがあります。

ICLDB import コマンドは、アーカイブされたセッションの録画ファイルを多数インポートしたり、Session Recording データベース内の誤ったまたは欠落したセッション録画データを修復または更新したり、Session Recording サーバー上でセッションの録画ファイルを 2 つの格納場所の間で移動させるのに便利です。ICLDB **import** コマンドは、ICLDB **removeall** コマンドの実行後、Session Recording データベースにセッション録画を再取り込みするのにも使用できます。

ICLDB ユーティリティの **import** コマンドには、次のようなパラメーターがあります：

- **/LISTFILES** - セッションの録画ファイルのインポート時の完全なファイルパスとファイル名を一覧表示します。これはオプションのパラメーターです。
- **/RECURSIVE** - すべてのサブディレクトリでセッションの録画ファイルを検索します。これはオプションのパラメーターです。
- **/L** - Windows イベントログに、インポートされたセッションの録画ファイルの結果とエラーの数を記録します。これはオプションのパラメーターです。
- **/F** - プロンプトを表示せずに import コマンドを強制的に実行します。これはオプションのパラメーターです。

アーカイブされたファイルの復元フォルダーを使用してセッションの録画ファイルを復元するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. Session Recording Player のプロパティで、アーカイブされたセッションの録画ファイルのファイル ID とアーカイブ時間を特定します。
3. Session Recording Player のプロパティで指定したファイル ID を使用して、バックアップ内のセッションの録画ファイルを探します。各セッション録画のファイル名は **i_<FileID>.icl** です。ここで、FileID はセッションの録画ファイルの ID です。
4. セッションの録画ファイルを、バックアップからアーカイブ済みファイルの復元フォルダーにコピーします。アーカイブ済みファイルの復元フォルダーを特定するには：
   a) ［スタート］メニューから、［スタート］>［すべてのプログラム］>［**Citrix**］>［**Session Recording** サーバーのプロパティ］の順に選択します。
   b) ［Session Recording サーバーのプロパティ］で、［格納場所］タブを選択します。［アーカイブ済みファイルの復元フォルダー］フィールドに現在の復元ディレクトリが表示されます。

ICLDB import コマンドを使用してセッションの録画ファイルを復元するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。

3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（Session Recording サーバーのインストールパス/Server/Bin）に変更します。
4. 以下のいずれかを実行します：
    - **ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>** コマンドを実行します。ここで、**directory** はセッションの録画ファイルを含む 1 つ以上のディレクトリの（スペースで区切られた）名前です。**Y** と入力してインポートを確定します。
    - **ICLDB IMPORT /LISTFILES /L <file>** コマンドを実行します。ここで、**file** は 1 つ以上のセッションの録画ファイルの（スペースで区切られた）名前です。セッションの録画ファイルの指定には、ワイルドカード文字を使用することもできます。**Y** と入力してインポートを確定します。

構成ログ

August 24, 2021

構成ログ機能では、管理者によるサイト構成の変更やそのほかの管理操作がデータベースに記録されます。このログは、以下の目的で使用できます：

- 構成変更の履歴を確認して問題の診断およびトラブルシューティングを行う。
- 変更管理の補助および構成の追跡を行う。
- 管理アクティビティのレポートを生成する。

Citrix Studio では、構成ログの基本設定を変更したり、構成ログを表示したり、HTML および CSV 形式のレポートを生成したりできます。日範囲および全文検索の結果により構成ログ表示をフィルターできます。必須ログ機能を有効にすると、ログが記録可能になるまで管理者による構成の変更が禁止されます。適切な権限を持つ管理者は、構成ログのエントリを削除できます。構成ログ機能では、ログの内容を編集することはできません。

構成ログでは、PowerShell SDK と Configuration Logging Service が使用されます。Configuration Logging Service は、サイト内のすべての Controller 上で実行されます。任意の Controller に障害が発生しても、ほかの Controller が自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効で、サイト作成時に作成されたデータベース（サイト構成データベース）が使用されます。データベースには別の場所を指定できます。構成ログデータベースでは、サイト構成データベースと同じ高可用性機能がサポートされます。

構成ログにアクセスするには、［ログ基本設定を編集］および［構成ログを表示］権限が必要です。

構成ログの言語には、作成時のロケールが適用されます。たとえば、英語で作成されたログは、管理者側のロケールには関係なく英語で表示されます。

ログの内容

構成ログには、Studio、Director、および PowerShell スクリプトから開始された構成の変更および管理アクティビティのログが記録されます。以下の項目に対する作成、編集、削除などの操作が構成ログに記録されます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者の役割とスコープ
- ホストのリソースおよび接続
- Studio で構成する Citrix ポリシー

ログが記録される管理変更の例には次のものがあります:

- 仮想マシンまたはユーザーのデスクトップの電源管理
- Studio または Director からユーザーへのメッセージ送信

次の操作はログに記録されません。

- 仮想マシンのプール管理電源オンなどの自動操作。
- グループポリシー管理コンソール（GPMC）でのポリシー操作。これらの操作のログは Microsoft のツールを使って表示できます。
- レジストリによる変更、データベースの直接的な変更、および Studio、Director、PowerShell 以外での変更。
- 展開の初期化後、最初の Configuration Logging Service インスタンスが Configuration Service に登録されたときに構成ログが有効になります。このため、構成の初期のアクティビティが記録されない場合があります（ハイパーバイザーの初期化時にデータベーススキーマが取得および適用される場合など）。

構成ログの管理

デフォルトでは、サイトの作成時に作成されたデータベース（サイト構成データベース）に構成ログが記録されます。Citrix は、以下の理由により、構成ログデータベース（および監視データベース）には別の場所を使用することを推奨しています。

- 構成ログデータベースのバックアップ方針が、サイト構成データベースのバックアップ方針と異なる場合があります。
- 構成ログ（および Monitoring Service）で収集されるデータの量によっては、サイト構成データベース用の領域が不足する場合があります。
- データベースを分散させると、単一ポイント障害の問題が解消されます。

注：構成ログをサポートしない製品エディションでは、Studio に［ログ］ノードが表示されません。

構成ログおよび必須ログの有効化および無効化

構成ログ機能はデフォルトで有効になっており、必須ログ機能は無効になっています。

1. Studio のナビゲーションペインで ［ログ］ノードを選択します。
2. ［操作］ペインの ［基本設定］を選択します。［ログ設定］ダイアログボックスが開き、データベースに関する情報と、構成ログおよび必須ログ機能の有効/無効が表示されます。
3. 望ましい操作を選択します:

構成ログを有効にするには、［有効］をクリックします。これがデフォルトの設定です。データベースに書き込みができない場合、ログ情報は破棄されますが構成内容は正しく反映されます。

構成ログを無効にするには、［無効］をクリックします。それまでに記録されたログの内容は、PowerShell SDK で読み取ることができます。

必須ログ機能を有効にするには、［データベースが切断されている場合の構成変更を禁止する］をクリックします。構成の変更や管理作業は通常ログに記録されるので、構成ログデータベースへの書き込みが可能になるまで、これらの作業はできなくなります。必須ログ機能は、構成ログが有効な場合、つまり ［有効］が選択されている場合にのみ有効にできます。Configuration Logging Service に障害が発生して、しかも高可用性が無効な場合、必須ログが有効になります。このような場合、構成ログデータベースに記録されるようなタスクは実行できなくなります。

必須ログ機能を無効にするには、［データベースが切断されていても構成変更を許可する］をクリックします。構成ログデータベースにアクセスできない場合でも、管理者は構成の変更やそのほかの管理タスクを実行できます（管理タスクが優先されます）。これがデフォルトの設定です。

構成ログデータベースの場所の変更

注：必須ログ機能が有効になっている場合、データベースの場所を変更することはできません。データベースの変更時に短時間データベースから切断されるためです。

1. サポートされるバージョンの SQL Server を使用してデータベースサーバーを作成します。
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、Studio により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。

構成ログの内容を表示

管理者が構成の変更などの管理アクティビティを開始すると、Studio や Director によって作成された高レベル操作が Studio の中央ペインの上部に表示されます。高レベル操作により 1 つまたは複数のサービスおよび SDK の呼び出しが実行されます。これは、低レベル操作です。中央ペインの上部で高レベル操作を選択すると、中央ペインの下部に低レベル操作が表示されます。

操作が完了する前に失敗すると、たとえば開始レコードに対応する停止レコードがないなど、データベースでログ操作が完結しない場合があります。このような場合、情報不足であることがログに示されます。時間の範囲を指定してログを表示する場合、未完結のログが表示される場合があります。たとえば、直近 5 日間のログを表示するときにその 5 日間に開始時間のみが含まれ、終了時間が含まれていない場合も、その操作のログが表示されます。

PowerShell コマンドレットを呼び出すスクリプトを使う場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログにより代わりの高レベルの操作が作成されます。

構成ログの内容を表示するには、Studio のナビゲーションペインで ［ログ］ノードを選択します。デフォルトでは、中央ペインにログコンテンツが時系列順に（最新のエントリが最初に）表示されます。

表示条件	表示条件の指定方法
検索結果	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。

- 委任管理権限 — 展開の構成を読み取るための権限が必要です。組み込みのすべての管理権限を実行できる管理者には、この権限があります。カスタムの役割では、［そのほかの権限］カテゴリで［読み取り専用］または［管理］権限を選択する必要があります。

  構成ログデータを削除する前にバックアップを作成するには、［ログ］カテゴリで［読み取り専用］または［管理］権限を選択する必要もあります。

- **SQL Server** データベース — データベースから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が記述されます。

イベントログ

January 25, 2021

次の記事には、XenApp および XenDesktop サービスによって記録できるイベントの一覧と説明が記載されています。

この情報は包括的ではありません。個別の特集記事で、追加のイベント情報を確認してください。

Citrix Broker Service イベント（HTML）

Citrix FMA Service SDK イベント（HTML）

Citrix Configuration Service イベント（HTML）

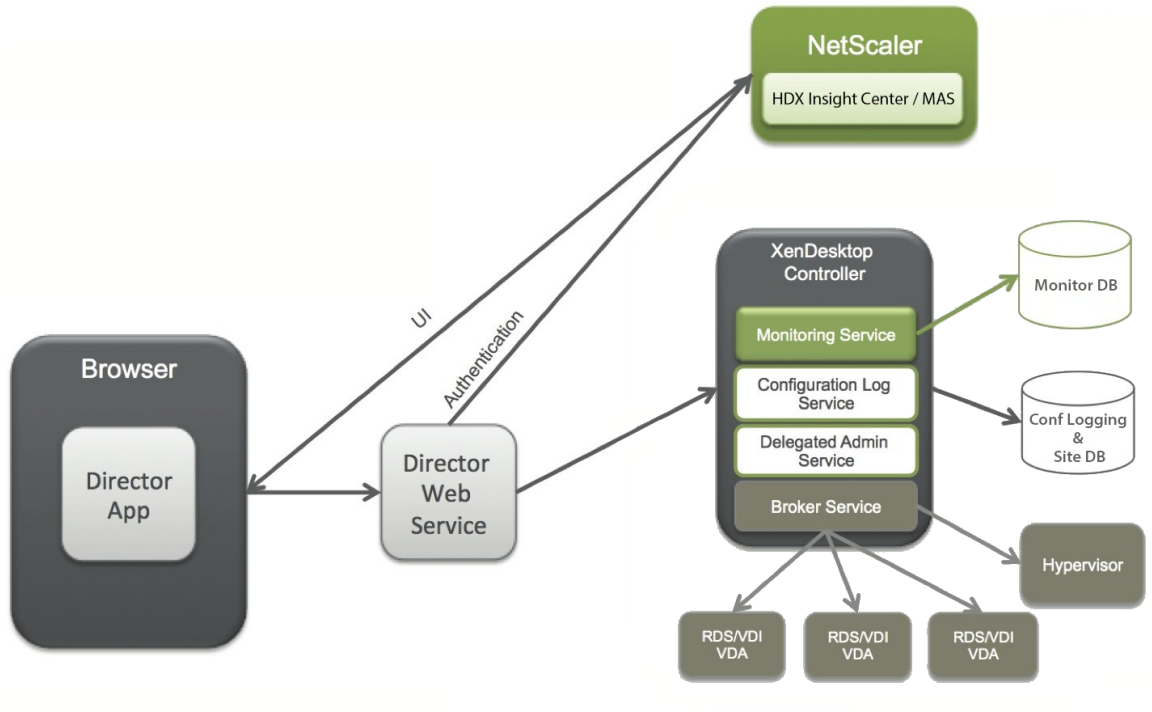
Citrix Delegated Administration Service イベント（HTML）

Director

August 24, 2021

Director について

Director は、XenApp と XenDesktop の監視およびトラブルシューティングのためのコンソールです。



Director では、以下の情報にアクセスできます。

- Broker Agent からのリアルタイムデータ。Analytics、Performance Manager、および Network Inspector の機能が統合されたコンソールを使用します。
  - Analytics には、ヘルスおよび容量のチェック機能と、NetScaler Insight Center または NetScaler MAS による履歴傾向とネットワーク解析機能が含まれており、XenApp/XenDesktop 環境のネットワークによるボトルネックを検出できます。
- 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。NetScaler Insight Center または NetScaler MAS が使用されます。
  - XenApp/XenDesktop 環境の仮想アプリケーションやデスクトップを使用するエンドユーザーのユーザーエクスペリエンスを視覚化できます。
  - ネットワークデータをアプリケーションデータやリアルタイム測定値に関連付けて効率的にトラブルシューティングを施せます。
  - XenDesktop 7 Director の監視ツールに統合されています。
- Personal vDisk データ。ディスク割り当てのランタイム監視とヘルプデスク管理者による Personal vDisk のリセットが可能になります。
  - コマンドラインツール CtxPvdDiag.exe を使用すると、ユーザーのログ情報が単一ファイルに収集され、それをトラブルシューティングに役立てることができます。

Director では、XenApp/XenDesktop サイトのリアルタイムおよび履歴ヘルス監視を提供するトラブルシューティングダッシュボードが使用されます。この機能により、リアルタイムで問題を確認して、エンドユーザーがどのような問題に直面しているのかを判断できるようになります。

Delivery Controller（DC）、VDA、その他の依存するコンポーネントについての Director の機能の互換性について詳しくは、「機能互換性マトリックス」を参照してください。

インターフェイスのビュー

Director では、管理者ごとに異なるインターフェイス（ビュー）が表示されます。Citrix 管理者の権限により、表示される内容と実行できるコマンドが異なります。

たとえば、ヘルプデスク管理者にはヘルプデスクタスク用のインターフェイスが表示されます。ヘルプデスク管理者は、問題を報告しているユーザーを Director で検索し、アプリケーションやプロセスの状態など、そのユーザーに関するアクティビティを表示できます。ヘルプデスク管理者は応答しないアプリケーションやプロセスを終了したり、ユーザーのマシン上の操作をシャドウしたり、マシンを再起動したり、ユーザープロファイルを再設定したりして問題を解決できます。

これに対して、すべての管理タスクの実行権限を持つ管理者はサイト全体を表示および管理でき、複数のユーザーやマシンに対してコマンドを実行できます。Dashboard には、セッションの状態、ユーザーのログオン、およびサイトインフラストラクチャなど、展開の主な要素に関する概要が表示されます。情報は 1 分ごとに更新されます。問題が発生すると、発生した問題の数や種類に関する詳細が自動的に表示されます。

Director 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。必須要件などについて詳しくは、このリリースのドキュメントの「システム要件」を参照してください。

このリリースの Citrix Director は、XenApp 6.5 以前の環境または XenDesktop 7 以前の環境と互換性がありません。

Director で複数のサイトを監視する場合は、Controller、Director、およびそのほかのコアコンポーネントが動作すべてのサーバーのシステムクロックが同期している必要があります。システムクロックが同期していない場合、Director にサイトの情報が正しく表示されないことがあります。

ヒント: XenApp 6.5 ファームと、XenApp 7.5 または XenDesktop 7.x サイトの両方を監視する場合は、XenApp 6.5 ファームを監視するための Director コンソールとは別のサーバー上に新しいバージョンの Director をインストールすることをお勧めします。

重要: ユーザー名とパスワードがプレーンテキストで送信されないように、Director 接続では HTTP ではなく HTTPS での接続のみを許可することを強くお勧めします。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:

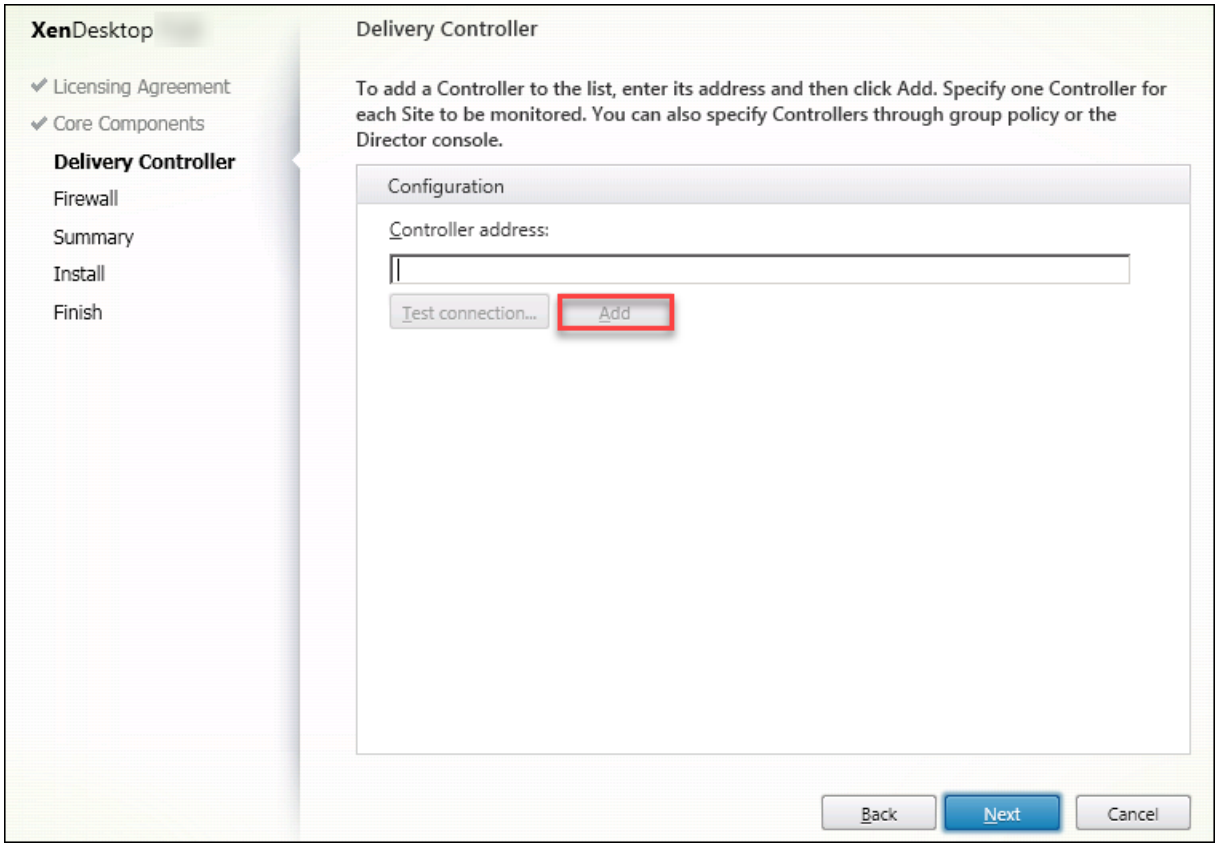
- 検索するすべての Active Directory フォレストを読み取る権限（「詳細構成」を参照）
- 委任管理者の役割を構成する（「管理権限の委任と Director」を参照）。
- ユーザーをシャドウするには、Windows リモートアシスタンスの Microsoft グループポリシーを使って管理者を構成する必要があります。また、次のように指定します：
  - VDA をインストールするすべてのユーザーデバイス上で、Windows リモートアシスタンス機能が有効である必要があります。この機能は、デフォルトで有効になっています。
  - Director をインストールするサーバーに、Windows リモートアシスタンス機能がインストールされている必要があります。この機能は、デフォルトでインストールされています。ただし、デフォルトでは無効になっています。Director を使ってエンドユーザーを支援する場合、この機能を有効にする必要はありません。セキュリティ上の理由から、この機能を無効にしておくことをお勧めします。
  - 管理者が Windows リモートアシスタンスを開始できるようにするには、適切な Microsoft グループポリシー設定を使用して管理者に必要な権限を付与します。詳しくは、CTX127388: How to Enable Remote Assistance for Desktop Director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 ISO インストーラーを使ってインストールします。このインストーラーは、前提条件をチェックし、不足しているコンポーネントをインストールして、Director の Web サイトをセットアップし、基本的な構成を行います。ISO インストーラーによるデフォルトの構成のままでも、一般的な展開を管理できます。インストール時に Director を含めなかった場合は、ISO インストーラーを再度実行して Director をインストールします。追加のコンポーネントをインストールするには、ISO インストーラーを再度実行して必要なコンポーネントを選択します。ISO インストーラーの使用について詳しくは、インストールに関するドキュメントで「コアコンポーネントのインストール」を参照してください。個々の MSI ファイルではなく、全製品 ISO インストーラーを実行して各コンポーネントをインストールすることをお勧めします。

Controller 上に Director をインストールすると、Director は localhost をサーバーアドレスとして自動的に構成され、デフォルトでローカルの Controller と通信します。

Controller 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。



注：監視対象の Controller を追加するには、［追加］をクリックします。

Director は、ここで指定したアドレスの Controller と通信します。監視する各サイトについて Controller のアドレスを 1 つずつ指定します。各サイトにあるほかのすべての Controller は自動的に検出され、指定した Controller にエラーが発生した場合はほかの Controller にフォールバックされます。

注： Director は、Controller 間で負荷分散を行いません。

Web ブラウザーと Web サーバー間の通信を保護するため、Director をホストする IIS Web サイトで TLS を実装することをお勧めします。手順については、Microsoft 社の IIS 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 Controller とは別のコンピューター上にインストールします。

1. XenApp のインストールメディアから、Director をインストールします。XenDesktop 用の Director が既にインストールされている場合は、この手順をスキップし、次の手順に進みます。
2. 「詳細構成」の「サイトを Director に追加するには」の説明に従って、各 Director サーバー上の IIS 管理コンソールで［アプリケーションの設定］の XenApp サーバーアドレスの一覧を更新します。
   XenApp サイトごとに 1 つの Controller のサーバーアドレスを指定します：そうすると、XenApp サイト

のその他の Controller は自動的にフェールオーバー用に使用されます。Director は、Controller 間で負荷分散を行いません。

重要: XenApp アドレスは Service.AutoDiscoveryAddressesXA に指定し、デフォルト設定の Service.AutoDiscoveryAddresses に指定しないでください。

3. Director WMI プロバイダーのインストーラーは DVD の **Support\DirectorWMIProvider** フォルダーに格納されています。適切なすべての XenApp サーバー（Controller およびセッションを実行するワーカー）上にこれをインストールします。

   winrm が構成されていない場合は、**winrm qc** コマンドを実行します。
4. 「権限の構成」で説明されているように、各 XenApp ワーカーサーバーが WinRM クエリを受け入れるように構成します。
5. Director と XenApp 間の通信で使用されるポート 2513 に対するファイアウォール例外を構成します。
6. Web ブラウザーと Web サーバー間の通信を保護するため、Director をホストする IIS Web サイトで TLS を実装することをお勧めします。

   手順については、Microsoft 社の IIS ドキュメントを参照してください。TLS を有効にするために Director を構成する必要はありません。

注: Director がファーム内のすべての XenApp ワーカーを見つけることができるようにするには、ファームによって使用される DNS サーバー上に XenApp サーバーがあるサブネットにリバース DNS ゾーンを追加する必要があります。

Director へのログオン

Director にログオンするには、Web ブラウザーで https または`http://<ServerFQDN>/Director`にアクセスします。

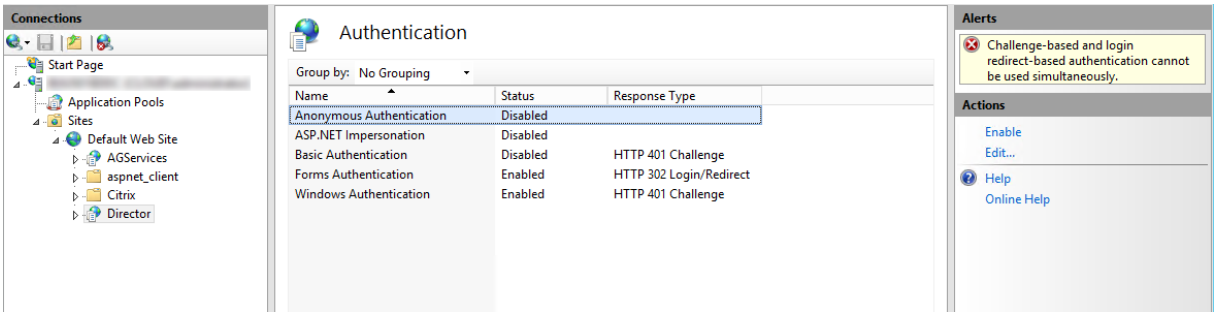
複数サイト環境でいずれかのサイトがダウンしている場合、Director へのログオンに時間がかかる場合があります。これは、ダウンしているサイトへの接続が試行されるためです。

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. [**Anonymous Authentication**] を右クリックし、[無効化] を選択します。

5.［**Windows** 認証］を右クリックし、［有効化］を選択します。



- Director マシンの Active Directory 委任アクセス許可を構成します。この作業は、Director と Delivery Controller が異なるマシンにインストールされている場合のみ必要です。
  1. Active Directory マシンで、Active Directory 管理コンソールを開きます。
  2. Active Directory 管理コンソールで、［ドメイン名］>［コンピューター］の順に移動します。Director マシンを選択します。
  3. 右クリックし、［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.［**Trust this computer for delegation to any service (Kerberos only)**］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、「システム要件」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。ログオンページで認証の種類を ［自動ログオン］または ［ユーザー資格情報］に設定できます。

Google Analytics による使用状況データ収集通知

Director がインストールされると、Director サービスは Google Analytics を使って使用状況に関するデータを匿名で収集します。［傾向］ページとそのタブの使用状況に関する統計と情報が収集されます。Director をインストールすると、データ収集はデフォルトで有効になります。

Google Analytics によるデータ収集を解除するには、Director がインストールされているマシンのレジストリキー、HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall を、「Citrix Insight Services」の「インストールとアップグレード分析」の説明に従って編集します。

注：レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall は、Citrix Insight Services だけでなく Google Analytics による使用状況に関するデータ収集も制御します。キーの値が変更されると、両方のサービスで収集は影響を受けます。

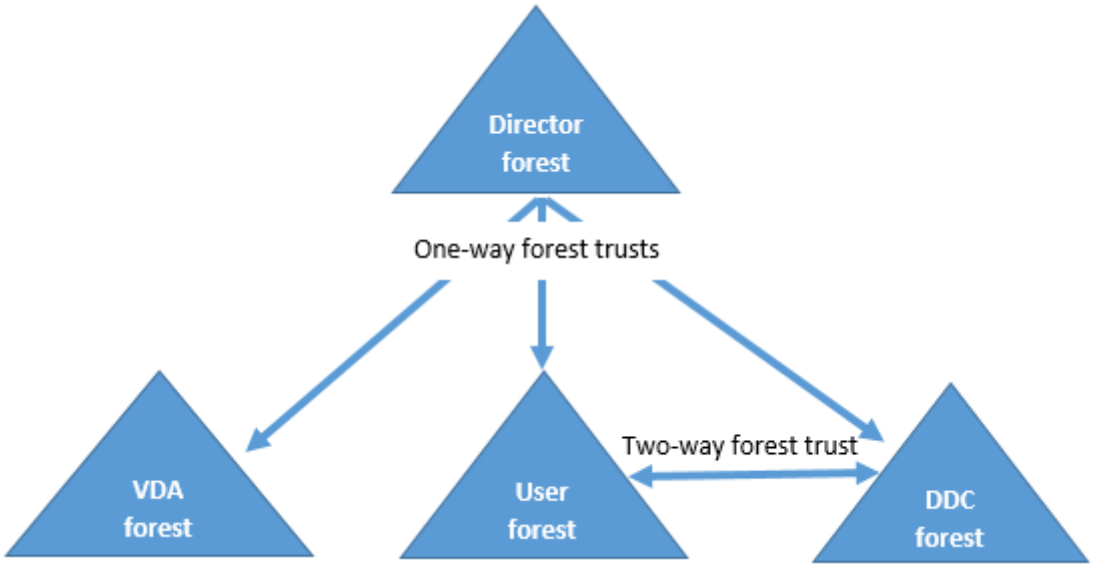
詳細な構成

August 24, 2021

Director は、ユーザー、Domain Delivery Controllers（DDC）、VDA、および Director が異なるフォレストに存在するフォレスト構成に広がるマルチフォレスト環境をサポートできます。このためには、フォレストと構成設定の間の信頼関係を適切にセットアップする必要があります。

マルチフォレスト環境で動作する **Director** の推奨構成

推奨構成では、全ドメイン認証を使用してフォレスト間の送受信フォレスト信頼関係を作成する必要があります。



Director からの信頼関係があると、管理者は異なるフォレストに存在するユーザーセッション、VDA、およびドメインコントローラーの問題のトラブルシューティングを行うことができます。

Director による複数のフォレストのサポートに必要な詳細構成は、インターネットインフォメーションサービス（IIS）マネージャー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。

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),<domain1>,<domain2>
```

リストに追加した各ドメインについて、Director によりフォレストレベルの検索が試行されます。管理者にフォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

> 注:
>
> マルチフォレスト環境では、Director はドメインローカルグループを使用して XenDesktop デリバリーグループに割り当てられた他のフォレストからのユーザーのセッションの詳細を表示しません。

Director 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* と *SiteBController* は、2 つの異なるサイトの Delivery Controller のアドレスです。

XenApp 6.5 の場合は、各 XenApp ファームの Controller のアドレスを次の設定に追加します:

```
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
```

ここで *FarmAController* および *FarmBController* は、2 つの異なるファームの XenApp Controller のアドレスです。

次の方法で XenApp 6.5 ファームの Controller 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、ユーザーが使用しているアプリケーションを保護するために、[アプリケーション] タブでアプリケーションの一覧を非表示にできます。

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス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、VDA から情報が収集されなくなるため、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
   <!--NeedCopy-->
   ```

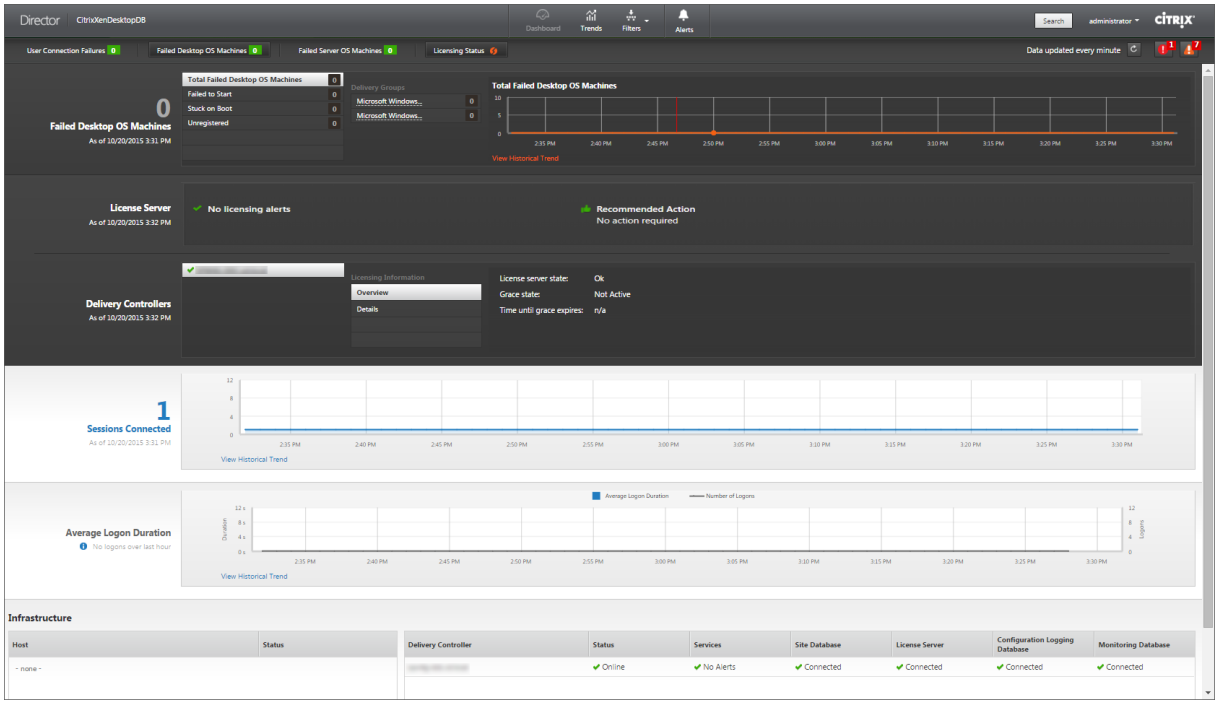
> 重要:
>
> 実行中のアプリケーションの表示を無効にするには、これらの両方の値を変更して、アクティビティマネージャーにデータが表示されなくなるようにしてください。

監視環境

August 24, 2021

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、各種のエラーのメトリックを確認します。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。

パネル	説明
ライセンスの状態	ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートメッセージとそのアラートを解決するための操作が表示されます。ライセンスサーバー 11.12.1 以降が必要です。Delivery Controller アラートには、Controller から送信されたライセンス状態の詳細が表示されます。XenApp 7.6 または XenDesktop 7.6 以降の Controller が必要です。アラートのしきい値は、Studio で設定できます。
接続セッション	すべてのデリバリーグループでの過去 60 分間の接続セッションが表示されます。
平均ログオン期間	過去 60 分間のログオン処理に関するデータが表示されます。左側にある大きなサイズの数値は、全体的な平均ログオン処理時間を示します。この平均には、XenDesktop 7.0 より前のバージョンの VDA へのログオンデータは含まれません。詳しくは、「ユーザーログオンの問題の診断」を参照してください。
インフラストラクチャ	サイトのインフラストラクチャー一覧 - ホストおよびコントローラー。XenServer または VMware のインフラストラクチャで、パフォーマンスアラートを表示できます。たとえば、XenCenter では、サーバーまたは仮想サーバーの CPU、ネットワーク I/O、またはディスク I/O の使用量が特定のしきい値を超えた場合にパフォーマンスアラートが発せられるように構成できます。アラートの送信間隔はデフォルトで 60 分ですが、必要に応じて変更できます。詳しくは、「XenServer の最新リリース」に移動し、『Citrix XenServer 管理者ガイド』の、XenCenter のパフォーマンスアラートに関するセクションを参照してください。

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。

- ユーザーマシンの電源の制御
- マシンへの接続の無効化

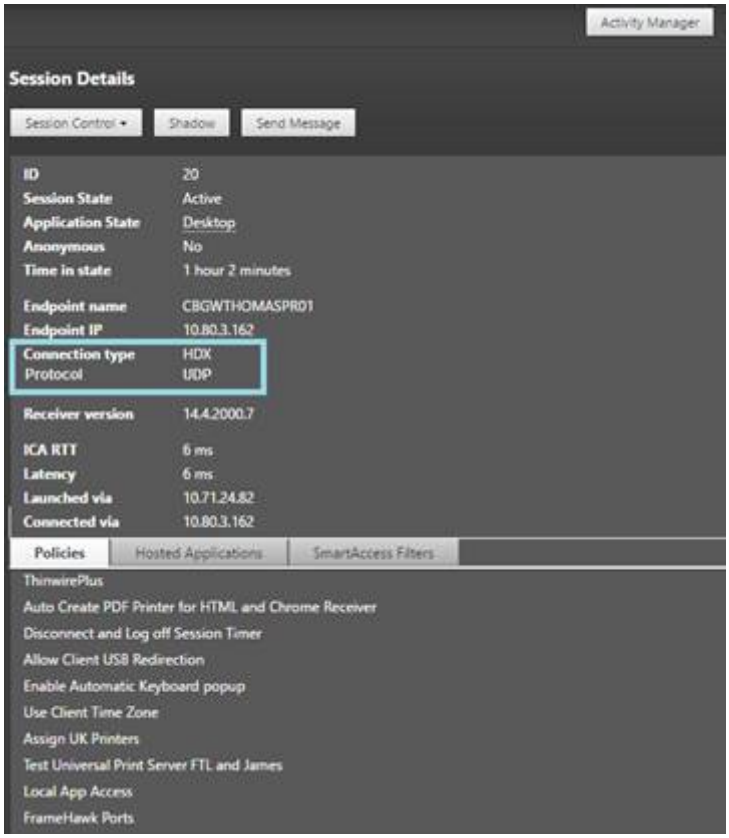
セッションの監視

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（アクション）	説明
ユーザーが接続しているマシンまたはセッションを表示する	［アクティビティマネージャー］および［ユーザーの詳細］ビューで、ユーザーが接続しているマシンまたはセッションと、そのユーザーがアクセスしているすべてマシンおよびセッションの一覧を表示します。セッションの一覧にアクセスするには、そのユーザーのビューのタイトルバーにあるセッション切り替え用のアイコンをクリックします。詳しくは、「セッションの復元」を参照してください。
すべてのデリバリーグループで接続されたセッションの総数を表示する	ダッシュボードの［接続セッション］ペインには、すべてのデリバリーグループで過去 60 分間に接続されたセッションの合計数が表示されます。その合計数をクリックすると、［フィルター］ビューが開きます。ここでは、デリバリーグループごとのセッションデータや、すべてのデリバリーグループでの特定期間での使用量を視覚的に確認できます。
アイドル状態のセッションを終了する	［セッションフィルター］ビューにすべてのアクティブなセッションの関連データが表示されます。セッションに関連付けられているユーザー、デリバリーグループ、セッション状態、しきい値の時間を超えたアイドル時間に基づいてフィルターします。フィルターされた一覧で、ログオフまたは切断するセッションを選択します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
長期間のデータを表示する	［傾向］ビューで［セッション］タブを選択し、接続されたセッションと切断されたセッションの長期間（つまり、過去 60 分より前のセッションの合計）のより具体的な利用状況データにドリルダウンします。この情報を表示するには、［履歴傾向の表示］をクリックします。

注：Virtual Delivery Agent 7 より前のバージョンの VDA、または Linux VDA を実行する場合、セッションに関する一部の情報が Director に表示されません。代わりに、利用できる情報がないというメッセージが表示されます。

［セッション詳細］パネルで、現在のセッションの HDX 接続タイプに使用されているトランスポートプロトコルを表示します。この情報はバージョン 7.13 以降の VDA で起動するセッションで利用できます。



- **HDX** 接続の種類の場合、
  - EDT が HDX 接続に使用されている場合、プロトコルは **UDP** と表示されます。
  - TCP が HDX 接続に使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP** 接続の種類の場合、プロトコルは「該当なし」と表示されます。

アダプティブトランスポートが構成されている場合、セッショントランスポートプロトコルは、ネットワーク条件に応じて、EDT（UDP 上）と TCP を動的に切り替えます。HDX セッションを EDT で確立できない場合は、TCP プロトコルにフォールバックします。

アダプティブトランスポート構成について詳しくは、「アダプティブトランスポート」を参照してください。

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、セッション、アプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. 以下のビューを選択します。
    - マシン。［デスクトップ OS マシン］タブまたは［サーバー OS マシン］タブを選択します。これらのタブには構成されたマシンの数が表示されます。また、［サーバー OS マシン］タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。
    - セッション。［セッション］ビューでセッション数を表示することもできます。アイドル時間の測定値から、しきい値時間を超えてアイドル状態にあるセッションを特定できます。
    - 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。
    - アプリケーションインスタンス。このビューは、サーバーおよびデスクトップ OS の VDA 上のすべてのアプリケーションインスタンスのプロパティを表示します。セッションのアイドル時間測定機能は、Server OS の VDA のアプリケーションインスタンスに利用できます。
2. ［フィルター基準］で、フィルター条件を選択します。
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。
6. 複数の Director サーバーからフィルターにアクセスするには、これらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
    - 共有フォルダーには、Director サーバーのアカウントを変更する権限が必要です。
    - Director サーバーは、共有フォルダーにアクセスするよう構成されている必要があります。これを行うには、**IIS** マネージャーを実行します。［サイト］**>**［既定の **Web** サイト］**>**［**Director**］**>**［アプリケーションの設定］の順に移動し、**Service.UserSettingsPath** の設定が共有フォルダーの UNC パスを反映するように変更します。
7. 後でフィルターを開くには、［フィルター］メニューでフィルターの種類（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存済みのフィルターを選択します。
8. ［マシン］ビューまたは ［接続］ビューでは、必要に応じ一覧でマシンを選択して電源制御操作を実行できます。［セッション］ビューでは、セッション制御を実行したりメッセージを送信したりできます。
9. ［マシン］ビューおよび ［接続］ビューで障害が発生したマシンまたは接続の ［エラーの理由］をクリックすると、障害の詳細な説明と、障害をトラブルシューティングするために推奨される操作が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、『Citrix Director 7.12 Failure Reasons Troubleshooting Guide』に記載されています。
10. ［マシン］ビューでマシン名のリンクをクリックすると、対応する ［マシンの詳細］ページが開きます。マシンの詳細を表示するこのページでは、電源制御が提供され、CPU、メモリ、ディスクの監視、および GPU の監視グラフが表示されます。また、［履歴使用率の表示］をクリックすると、マシンのリソース使用傾向が表示されます。詳しくは、「マシンのトラブルシューティング」を参照してください。
11. ［アプリケーションインスタンス］ビューでは、しきい値時間を超えた ［アイドル時間］に基づいてソートまたはフィルターできます。終了させるアイドル状態のアプリケーションインスタンスを選択します。ログオフまたはアプリケーションインスタンスを切断すると同一セッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
    注：［アプリケーションインスタンスフィルター］ページと［セッションフィルター］ページのアイドル時間測

定が利用できるのは、Director、Delivery Controller、VDA がバージョン 7.13 以降の場合です。

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、負荷評価、能力管理、マシン使用量、ソース使用、ネットワーク分析についての履歴傾向情報が表示されます。この情報を表示するには、［傾向］メニューをクリックします。

ズームインドリルダウン機能により、（グラフ内のデータポイントをクリックして）ある期間について着目し、その傾向に関連する詳細情報を表示させて、傾向チャートを参照できます。これにより、表示中の傾向により誰が、または何が影響を受けているかについてより詳細に把握できます。

各グラフのデフォルトの表示範囲を変更するには、［期間］フィルターを変更して適用します。

履歴傾向情報を必要とする期間を選択します。その期間を参照できるかは、Director 環境により異なります。次を参照してください:

- Platinum Edition ユーザーは、昨年（365 日）までの傾向レポートを利用できます。
- Enterprise Edition ユーザーは、先月（31 日）までの傾向レポートを利用できます。
- Platinum Edition 以外や Enterprise Edition 以外のユーザーは、過去 7 日間の傾向レポート。

注:

- すべての Director 展開環境で、期間を［先月］（現時点まで）またはそれより短く設定すると、セッション、障害、およびログオンパフォーマンスの傾向情報をグラフやテーブルとして表示できます。期間に、終了日が設定可能な［先月］、または［昨年］を選択すると、傾向情報はグラフとして表示できますが、テーブルとしては表示できません。
- Monitoring Service による傾向情報のクリーンアップ開始までのデフォルト値は、「データの粒度と保持」セクションで確認できます。Platinum Edition では、クリーンアップが開始されるまでの日数をカスタマイズできます。

利用できる傾向

セッションの傾向の表示:［セッション］タブから、同時接続セッション数に関するより詳細な情報を表示するデリバリーグループと期間を選択します。

接続エラーの傾向の表示:［エラー］タブで、接続エラー情報を表示する接続、マシンの種類、エラーの種類、デリバリーグループ、および期間を選択します。

マシン障害の傾向の表示:［失敗したデスクトップ OS マシン］タブまたは［失敗したサーバー OS マシン］タブで、障害情報を表示するエラーの種類、デリバリーグループ、および期間を選択します。

ログオンパフォーマンスの傾向の表示:［ログオンパフォーマンス］タブで、デリバリーグループと期間を選択して、サイトのログオン処理時間に関するグラフを表示し、ログオンパフォーマンスに対するログオン数の影響を確認します。このビューには、仲介処理時間や仮想マシンの起動時間などのログオンフェーズにおける平均時間も表示されます。

このデータはユーザーのログオンに関するものであり、切断セッションへの再接続は含まれません。
グラフの下のテーブルに、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、いずれかの列を基準にレポートを並べ替えることができます。
詳しくは、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向の表示：［負荷評価基準インデックス］タブで、サーバー OS マシン間で分散された負荷に関する情報を表示します。このグラフでは、対象のデリバリーグループ、サーバー OS マシン、および期間を指定できます。

ホストされたアプリケーションの使用量の表示：この機能は、組織のライセンスによっては使用できない場合があります。
［容量管理］タブから［ホストされたアプリケーションの使用量］タブを選択し、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。

リソース使用の表示：［リソース使用］タブで［デスクトップ OS マシン］または［サーバー OS マシン］を選択して、各 VDI マシンの CPU とメモリ使用量、および IOPS とディスク遅延に関する履歴傾向を取得し、容量の計画に役立てることができます。
この機能の使用には、Delivery Controller および VDA の バージョン **7.11** 以降が必要です。
平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、および最大同時セッション数を表示するグラフです。マシンにドリルダウンして、CPU を消費している上位 10 のプロセスに関するデータとチャートを表示できます。デリバリーグループ別および期間別でフィルターできます。過去 2 時間、24 時間、7 日間、月、年の CPU、メモリ使用量、最大同時セッション数のグラフを入手できます。平均 IOPS とディスク遅延は、過去 24 時間、月、年のグラフが入手可能です。

メモ：

- データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］表に表示するには、監視ポリシー

の［プロセスの監視を有効にします］設定を［許可］に設定する必要があります。このポリシーはデフォルトでは禁止されています。デフォルトではすべてのリソース使用データが収集されます。これは、ポリシーの［リソース監視の有効化］設定で無効にできます。グラフの下のテーブルは、マシンごとのリソース使用状況データを示しています。

- 平均 IOPS は、1 日の平均値を示します。最大 IOPS は、選択した期間の IOPS の平均において最も高い IOPS が算出されます。（IOPS の平均は、選択した期間に VDA で収集された IOPS の 1 時間当たりの平均です）。

ネットワーク分析データの表示：この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。この機能には、Delivery Controller バージョン **7.11** 以降が必要です。

［ネットワーク］タブで、ネットワークのユーザー、アプリケーション、およびデスクトップコンテキストビューを表示してネットワーク分析をモニターします。この機能は、Director が NetScaler Insight Center または NetScaler MAS で HDX Insight レポートを使用して ICA トラフィックを詳細に分析できます。詳しくは、「ネットワーク分析機能の構成」を参照してください。

アプリケーション障害の表示：［アプリケーション障害］タブで、VDA 上の公開アプリケーションに関連した障害が表示されます。

この機能の使用には、Delivery Controller および VDA の バージョン **7.15** 以降が必要です。Windows Vista 以降が動作するデスクトップ OS の VDA、および Windows Server 2008 以降が動作するサーバー OS の VDA がサポートされます。
詳しくは、「アプリケーション障害履歴の監視」を参照してください。

デフォルトでは、サーバー OS の VDA からのアプリケーション障害のみが表示されます。監視ポリシーを使って、アプリケーション障害の監視の設定ができます。詳しくは、「監視のポリシー設定」を参照してください。

カスタムレポートの作成：［カスタムレポート］タブには、監視データベースのリアルタイムデータおよび履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスがあります。

この機能には、Delivery Controller バージョン **7.12** 以降が必要です。

以前に保存されたカスタムレポートクエリの一覧で、［実行］をクリックするとそのレポートを CSV 形式でエクスポートでき、［**OData** のコピー］をクリックすると該当する OData クエリをコピーして共有でき、［編集］をクリックするとクエリを編集できます。
マシン、接続、セッション、またはアプリケーションインスタンスに基づいて、新しいカスタムレポートクエリを作成できます。フィールド（たとえばマシン、デリバリーグループ、または期間）に基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。

コピーした OData クエリに基づいて、新しいカスタムレポートクエリを作成できます。それには、OData Query オプションを選択し、コピーした OData クエリを貼り付けます。結果として得られたクエリを、後で実行するために保存できます。

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。

メモ：

- バージョン 7 より前の VDA に対しては、HDX 接続のログオンデータは収集されません。以前のバージョンの VDA については、チャートデータが 0 として表示されます。
- Citrix Studio で削除されたデリバリーグループは、関連データがクリーンアップされるまで Director の［傾向］フィルターで選択できます。削除されたデリバリーグループを選択すると、保存まで使用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- デリバリーグループ間でアクティブなセッションがあるマシンを移動すると、移動後のデリバリーグループの［リソース使用率］および［負荷評価基準インデックス］テーブルで両方のデリバリーグループの統合された測定値が表示されます。

レポートのエクスポート

傾向データをエクスポートして、通常使用レポートおよび能力管理レポートを生成できます。エクスポートでは、PDF、Excel、および CSV レポート形式がサポートされます。PDF と Excel 形式のレポートには、傾向がグラフとテーブルとして表示されます。CSV 形式のレポートには、処理してビューを生成したり、アーカイブしたりできる表形式のデータが含まれます。

レポートをエクスポートするには、次の手順に従います。

1. ［傾向］タブに移動します。
2. フィルターの基準と期間を設定し、［適用］をクリックします。傾向グラフとテーブルにデータが入力されます。
3. ［エクスポート］をクリックして、レポートの名前と形式を入力します。

Director は、選択したフィルター基準に基づいてレポートを生成します。フィルター基準を変更した場合は、［適用］をクリックしてから ［エクスポート］をクリックします。

注：大量のデータをエクスポートすると、Director サーバー、Delivery Controller および SQL サーバーのメモリと CPU の消費が著しく増加します。サポートされる同時エクスポート処理の数とエクスポートできるデータの量は、エクスポートのパフォーマンスを最適にするため、デフォルトの上限に設定されています。

サポートされるエクスポート上限

エクスポートされる PDF と Excel のレポートは、選択されたフィルター基準によるグラフィカルなチャートが含まれています。ただし、すべてのレポート形式の表形式のデータは、行の数またはテーブルのレコード数のデフォルト値を超えた値は切り捨てられています。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Director アプリケーションの設定をインターネットインフォメーションサービス（IIS）で構成して、デフォルトの上限を変更できます。

VHD 形式	サポートされるデフォルトのレコード数	**Director** アプリケーションの設定におけるフィールド	サポートされる最大レコード数
PDF	500	UI.ExportPdfDrilldownL	5000
Excel	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000（[セッション] タブで 10,000,000）	UI.ExportCsvDrilldownL	100,000

エクスポートできるレコード数の上限を変更するには、次の手順に従います。

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. フィールドを編集するか、新しいフィールドを追加します。

[アプリケーションの設定] でこれらのフィールドの値を追加すると、デフォルト値が上書きされます。

警告：サポートされる最大レコード数より多くフィールド値を設定すると、エクスポートのパフォーマンスが影響を受ける可能性があり、サポートもされません。

エラー処理

このセクションでは、エクスポート処理中に発生しうるエラーに対処するための情報を提供します。

- **Director** のタイムアウト

このエラーは、Director サーバーでの、または Monitor Service によるネットワーク問題や高いリソース使用率によって発生する可能性があります。

デフォルトのタイムアウト時間は 100 秒間です。Director サービスのタイムアウト時間を増やすには、インターネットインフォメーションサービス（IIS）の Director アプリケーションの設定で **Connector.DataServiceContext.Timeout** フィールドの値を設定します:

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. 値 **Connector.DataServiceContext.Timeout** を編集します。

- モニターのタイムアウト

このエラーは、Monitor Service による、または SQL サーバーでのネットワーク問題や高いリソース使用率によって発生する可能性があります。

Monitor Service のタイムアウト時間を増やすには、Delivery Controller で以下の PowerShell コマンドを実行します:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- 同時エクスポートまたはプレビュー処理上限

Director では、エクスポートまたはプレビューの 1 つのインスタンスがサポートされます。同時エクスポートまたはプレビュー処理上限エラーが発生した場合は、次のエクスポート処理を後で実行してください。

同時エクスポートまたはプレビュー処理の数を増やすことはできますが、Director のパフォーマンスに影響する可能性があり、サポートもされません:

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. 値 **UI.ConcurrentExportLimit** を編集します。

- **Director** のディスク領域不足

各エクスポート処理には、Windows Temp フォルダーに最大 2GB のハードディスク容量が必要です。容量をクリアするか、Director サーバーにハードディスク容量を追加してからエクスポートを再試行してください。

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、Director に起動に失敗したことが表示され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。

コマンド	機能
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。
一時停止	仮想マシンを一時停止して、そのときの状態をデフォルトのストレージリポジトリ上にファイルとして保存します。この方法で仮想マシンを一時停止してからそのホストサーバーをシャットダウンし、ホストサーバーを再起動してから仮想マシンを元の実行状態に戻すことができます。
再開	一時停止状態の仮想マシンを再開して、元の実行状態に戻します。
起動	シャットダウン状態の仮想マシンを起動します（「コールドスタート」とも呼ばれます）。

電源制御操作に失敗した場合、アラート上にマウスポインターを置くと問題の詳細情報がポップアップメッセージとして表示されます。

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］を選択し、オプションをオンにします。

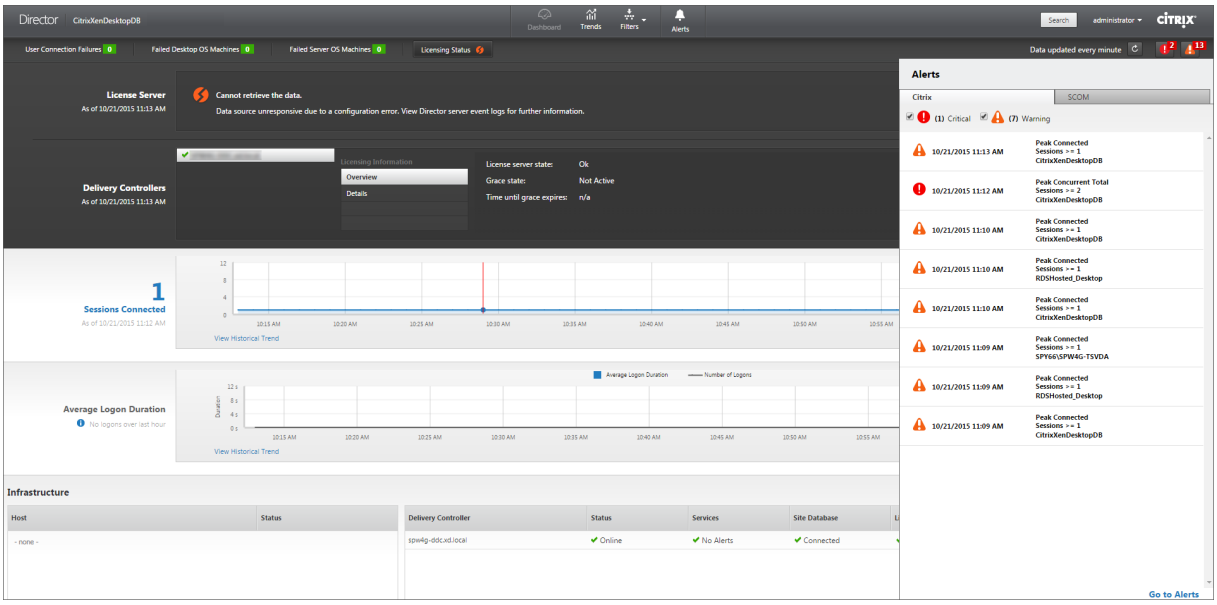
メンテナンスモードのデスクトップにユーザーが接続を試みると、デスクトップを使用できないことを示すメッセージが表示されます。管理者がメンテナンスモードを解除するまで、新しい接続は許可されません。

アラートおよび通知

August 24, 2021

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ほかの概要ビューに、警告および重大アラートシンボルと共に表示されます。アラートは、**Platinum** ライセンスを持つユーザーが使用できます。アラートは、1 分ごとに自動的に更新されます。オンデマンドで更新することもできます。

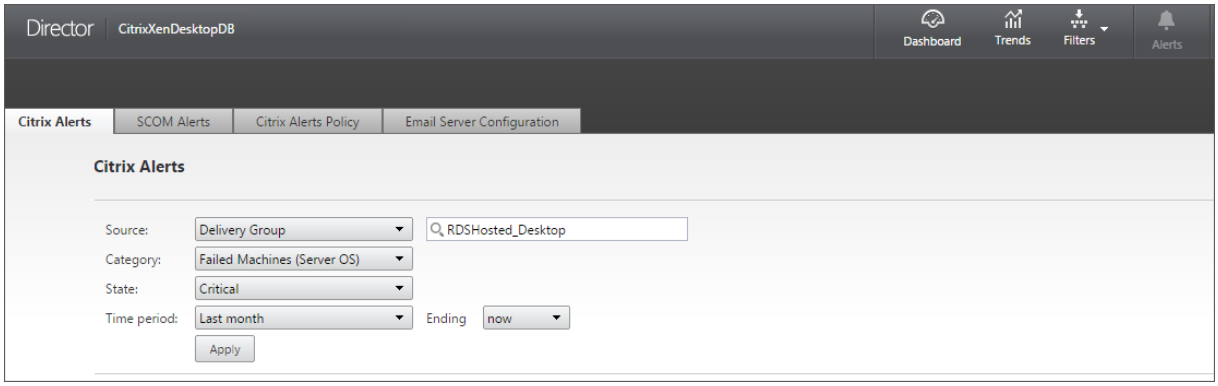


警告アラート（黄色の三角形）は、条件の警告しきい値以上になっていることを示します。

重大アラート（赤の円）は、条件の重大しきい値以上になっていることを示します。

サイドバーでアラートを選択して下部にある ［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］を選択すると、アラートに関するさらに詳細な情報を表示できます。

［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 マシンや、特定のユーザーに対するすべてのアラートを特定することができます。詳しくは、「レポートのエクスポート」を参照してください。

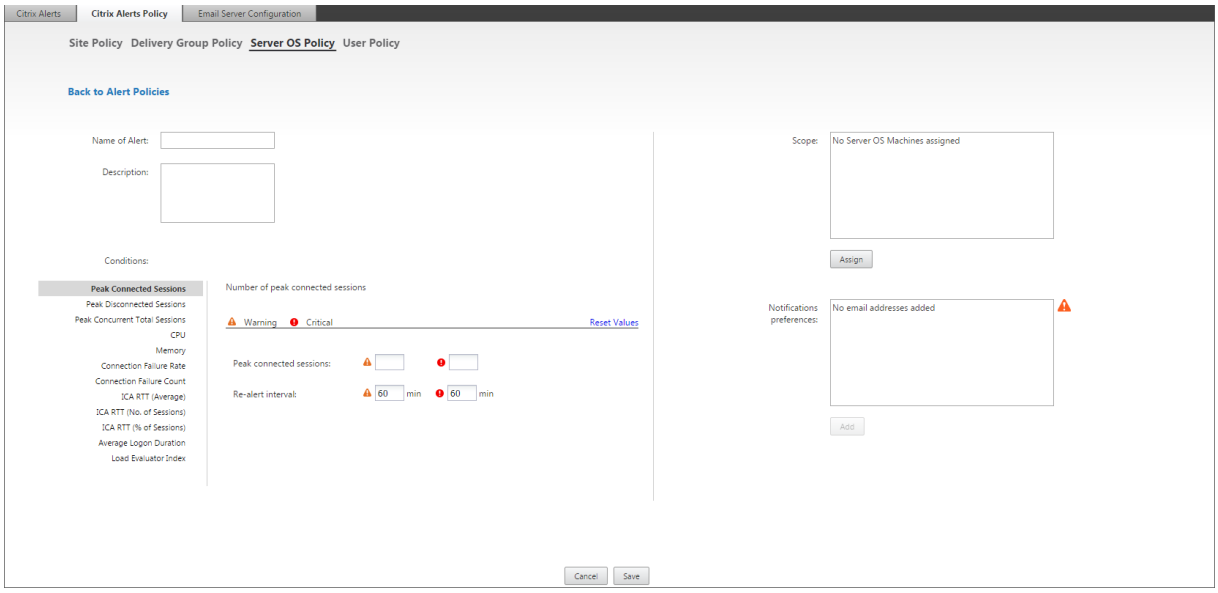


Citrix アラート：Citrix アラートは、Citrix コンポーネントで発生し、Director で監視されるアラートです。Citrix アラートは、Director 内で［アラート］>［**Citrix** アラートポリシー］の順に選択して構成できます。この構成では、設定したしきい値を超過した場合のアラートに関して、ユーザーおよびグループにメール送信する通知を設定できます。通知は、Octoblu webhook または SNMP トラップとしても構成できます。Citrix アラートのセットアップについて詳しくは、「アラートポリシーの作成」を参照してください。

SCOM アラート：SCOM アラートには、Microsoft System Center 2012 Operations Manager（SCOM）からのアラート情報が表示されます。これにより、Director 内のデータセンターの稼働状態およびパフォーマンスがより包括的に示されます。詳しくは、「SCOM アラート」を参照してください。

サイドバーを展開する前にアラートアイコンの隣に表示されているアラートの数は、Citrix アラートと SCOM アラートの合計数です。

アラートポリシーの作成



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. ［作成］をクリックします。
3. ポリシーの名前と説明を入力し、アラートをトリガーするために満たす必要がある条件を設定します。たとえば、最大接続済みセッション数、最大切断セッション数、および最大同時セッション数に対して、警告とする数および重大とする数を指定します。警告値を重大値よりも大きくすることはできません。詳しくは、「アラートポリシーの条件」を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、アラートはこの間隔で再トリガーされます。アラートポリシーで設定されている場合は、メール通知が生成されます。クリアされたアラートの場合、再アラート間隔でメール通知が生成されることはありません。
5. スコープを設定します。たとえば、特定のデリバリーグループに対して設定します。
6. お知らせ設定で、アラートがトリガーされたときのメール通知の送信先を指定します。アラートポリシーでメールお知らせ設定を行うには、［メールサーバーの構成］タブでメールサーバーを指定する必要があります。
7. ［保存］をクリックします。

Octoblu webhook 構成について詳しくは、「Octoblu webhook によるアラートポリシーの構成」を参照してください。

SNMP トラップ構成について詳しくは、「SNMP トラップによるアラートポリシーの構成」を参照してください。

スコープに 20 件以上のデリバリーグループが定義されているポリシーを作成すると、構成が完了するまでにおよそ 30 秒かかる場合があります。完了するまで、スピナーアイコンが表示されます。

最大 20 の一意のデリバリーグループに対して、50 以上のポリシー（合計で 1000 デリバリーグループターゲット）を作成すると、応答時間が遅くなることがあります（5 秒以上）。

アクティブなセッションがあるマシンをデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターで定義されたデリバリーグループアラートが誤って発信されることがあります。

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
最大接続セッション数	最大接続済みセッションの数。Director セッションの傾向ビューで、最大接続済みセッション数をチェックします。セッションの負荷に対応するのに十分な処理能力があることを確認します。必要に応じ、マシンを追加します。
最大切断セッション数	最大切断セッションの数。Director セッションの傾向ビューで、最大切断セッション数をチェックします。セッションの負荷に対応するのに十分な処理能力があることを確認します。必要に応じ、マシンを追加します。必要に応じ、切断されたセッションからログオフします。

アラートポリシーの条件	説明および推奨される操作
合計最大同時セッション数	最大同時セッションの数。Director セッションの傾向ビューで、最大同時セッション数をチェックします。セッションの負荷に対応するのに十分な処理能力があることを確認します。必要に応じ、マシンを追加します。必要に応じ、切断されたセッションからログオフします。
CPU	CPU の使用率（%）。CPU を消費しているプロセスやリソースを特定します。必要に応じてプロセスを終了します。プロセスを終了すると、保存されていないデータは失われます。すべてが想定どおりに機能している場合は、将来的に CPU リソースを追加します。注: ポリシー設定［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされると、CPU とメモリの状況に関するアラートがトリガーされます。詳しくは、「監視のポリシー設定」を参照してください。
メモリ	メモリの使用率（%）。メモリを消費しているプロセスやリソースを特定します。必要に応じてプロセスを終了します。プロセスを終了すると、保存されていないデータは失われます。すべてが想定どおりに機能している場合は、将来的にメモリを追加します。注: ポリシー設定［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされると、CPU とメモリの状況に関するアラートがトリガーされます。詳しくは、「監視のポリシー設定」を参照してください。
接続エラー率	過去 1 時間の接続エラーの率。接続の合計試行回数に対する合計エラー数の割合に基づいて計算されます。Director 接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。

アラートポリシーの条件	説明および推奨される操作
接続エラー数	過去 1 時間の接続エラー数。Director 接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。
ICA 往復時間（平均）	平均 ICA 往復時間。NetScaler HDX Insight で ICA RTT の詳細を確認して、根本原因を特定します。NetScaler が利用可能でない場合は、[Director のユーザー詳細] ビューで ICA RTT と遅延をチェックし、これがネットワークの問題か、または XD/XA の問題かを特定します。詳しくは、NetScaler Insight Center のドキュメント「HDX Insight」を参照してください。
ICA 往復時間（セッション数）	ICA 往復時間を超過しているセッションの数。NetScaler HDX Insight で、ICA RTT が高いセッションの数をチェックします。詳しくは、NetScaler Insight Center のドキュメント「HDX Insight のレポート」を参照してください。NetScaler が利用可能でない場合は、ネットワークチームと協力し根本原因を特定してください。
ICA RTT（セッションの%）	平均 ICA 往復時間を釣果しているセッションの割合(%)。NetScaler HDX Insight で、ICA RTT が高いセッションの数をチェックします。詳しくは、NetScaler Insight Center のドキュメント「HDX Insight のレポート」を参照してください。NetScaler が利用可能でない場合は、ネットワークチームと協力し根本原因を特定してください。
ICA RTT（ユーザー）	特定のユーザーが開始したセッションに適用される ICA 往復時間。1 つ以上のセッションで ICA RTT がしきい値よりも高い場合は、アラートがトリガーされます。
障害が発生したマシン（デスクトップ OS）	失敗したデスクトップ OS マシンの数。Director の [ダッシュボード] ビューおよび [フィルター] ビューに表示されるように、エラーはさまざまな理由で発生します。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。

アラートポリシーの条件	説明および推奨される操作
障害が発生したマシン（サーバー OS）	失敗したサーバー OS マシンの数。Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、エラーはさまざまな理由で発生します。Citrix Scout 診断を実行して、原因を特定します。
平均ログオン期間	過去 1 時間に行われたログオンの平均ログオン処理時間。Director のダッシュボードをチェックし、ログオンの処理時間に関する最新のメトリックを取得します。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。
ログオン処理時間（ユーザー）	過去 1 時間に行われた指定されたユーザーのログオンに関するログオン処理時間。
負荷評価基準インデックス	過去 5 分間の負荷評価基準インデックスの値。Director で、ピーク負荷（最大負荷）に達している可能性があるサーバー OS マシンをチェックします。ダッシュボード（障害）と負荷評価基準インデックス傾向レポートの両方を表示します。

Octoblu webhook によるアラートポリシーの構成

メール通知は例外として、Octoblu webhook でアラートポリシーを構成して IoT サービスを開始できます。

注：この機能の使用には、Delivery Controller バージョン 7.11 以降が必要です。

アラートを使用した IoT サービスの例としては、SMS 通知の送信によるスタッフのサポートや、カスタムインシデント解決プラットフォームとの統合による追跡通知の支援などがあります。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。webhooks のサポートのために拡張されます。

新しい Octoblu ワークフローの作成および対応する webhook URL の取得について詳しくは、『Octoblu Developer Hub』を参照してください。

新しいアラートポリシーや既存のポリシーに対して Octoblu webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

webhook URL で新しいアラートポリシーを作成する場合：


```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
```

既存のアラートポリシーに webhook URL を追加する場合:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShell コマンドのヘルプについては、たとえば次のように PowerShell ヘルプを使用します:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

PowerShell によるアラートポリシーの構成について詳しくは、Advanced Concepts の『Director 7.7: Managing and Configuring Alerts and Notifications Using Powershell』を参照してください。

アラートポリシーから生成された通知によって、webhook URL への POST コールで webhook がトリガーされます。POST メッセージには通知の情報が JSON 形式で含まれます:

```
{
 "NotificationId" : <Notification Id>,

"Target" : <Notification Target Id>,

"Condition" : <Condition that was violated>,

"Value" : <Threshold value for the Condition>,

"Timestamp": <Time in UTC when notification was generated>,

"PolicyName": <Name of the Alert policy>,

"Description": <Description of the Alert policy>,

"Scope" : <Scope of the Alert policy>,

"NotificationState": <Notification state critical, warning, healthy or
    dismissed>,

"Site" : <Site name> }

<!--NeedCopy-->
```


SNMP トラップによるアラートポリシーの構成

SNMP トラップを構成されたアラートがトリガーされると、対応する SNMP トラップメッセージが構成済みのネットワークリスナーに転送され、さらに処理されます。Citrix アラートは、SNMP バージョン 2 以降のトラップをサポートします。現時点では、トラップメッセージを 1 つのリスナーに転送できます。

注：この機能の使用には、Delivery Controller バージョン 7.12 以降が必要です。

SNMP トラップを構成するには、以下の PowerShell コマンドレットを使用します：

- 現時点の SNMP サーバー構成を取得する：

```
Get-MonitorNotificationSnmpServerConfiguration
```

- SNMP バージョン 2 のサーバー構成を設定する：

```
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
    Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
    CommunityString public -Protocol V2
```

- SNMP バージョン 3 のサーバー構成を設定する：

```
$authpass = "<authentication password>" | ConvertTo-SecureString
    -AsPlainText -Force
$privpass = "<Privacy password>" | ConvertTo-SecureString -
    AsPlainText -Force
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
    Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
    EngineId <Engine Id> -AuthPassword $authpass -PrivPassword
    $privpass -PrivPasswordProtocol <Privacy password protocol> -
    AuthPasswordProtocol <Authentication password protocol> -
    Protocol V3
<!--NeedCopy-->
```

- 既存のアラートポリシーに SNMP トラップを有効化する：

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID
    >
```

- SNMP トラップ構成を持つ新しいアラートポリシーを作成する：

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    IsSnmpEnabled $true -Description <Policy description> -Enabled
     $true
```

Director からの SNMP トラップメッセージ内の OID の構造は以下のようになります：
1.3.6.1.4.1.3845.100.1.*<UID>*

<UID> は Director に定義されたすべてのアラートポリシーに対して順次生成されます。そのため、OID はユーザー環境ごとに一意です。

- **1.3.6.1.4.1.3845.100.1** を使用すると、Director からのすべてのトラップメッセージがフィルタリングされます。
- **1.3.6.1.4.1.3845.100.1.*<UID>*** を使用すると、特定のアラートのトラップメッセージがフィルタリングされ、処理されます。

以下のコマンドレットを使用すると、ご使用の環境に定義されたアラートポリシーの UID を取得できます:

```
1 Get-MonitorNotificationPolicy
```

SNMP トラップは SCOM に転送できます。それには、SCOM を Delivery Controller とともに構成してトラップメッセージをリスンします。

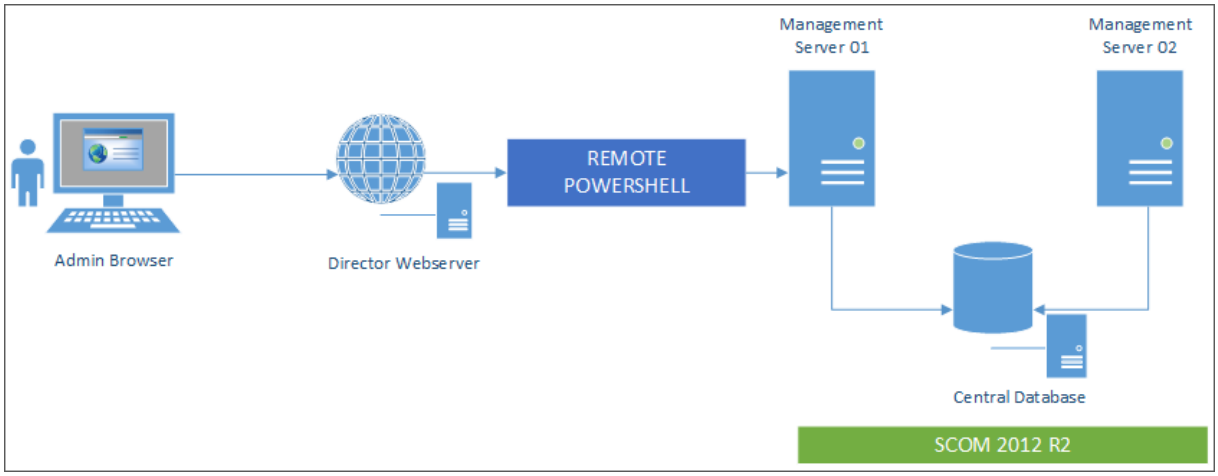
SCOM アラート統合の構成

Director との SCOM 統合により、SCOM からのアラート情報を、Director のダッシュボードおよびそのほかの概要ビューで表示できるようになります。

SCOM アラートは、Citrix アラートと共に画面上に表示されます。SCOM アラートには、サイドバーの［SCOM］タブからアクセスしてドリルダウンすることができます。

1 か月前までの過去のアラートを表示し、情報を並べ替えてフィルターし、フィルターされた情報を CSV、Excel、および PDF レポート形式にエクスポートすることができます。詳しくは、「レポートのエクスポート」を参照してください。

SCOM 統合では、リモート PowerShell 3.0 以降を使用して 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。

注:

- Director 管理者アカウントを SCOM オペレーターの役割として構成することをお勧めします。これにより、管理者が Director で完全なアラート情報を取得できるようになります。そのように構成できない場合、DirectorConfig ツールを使用して SCOM 管理者アカウントを web.config ファイルに構成できます。
- 最適なパフォーマンスのために、構成する Director 管理者の数は、1 つの SCOM 管理サーバーにつき 10 人以下とすることをお勧めします。

Director サーバーで、以下を実行します:

1. コマンド **Enable-PSRemoting** を実行して、PowerShell リモート処理を有効にします。
2. SCOM 管理サーバーを TrustedHosts 一覧に追加します。PowerShell プロンプトを開いて、次のコマンドを実行します:

    a) 最新の TrustedHosts 一覧を取得します。

```
1         Get-Item WSMAN:\localhost\Client\TrustedHosts
2 <!--NeedCopy-->
```

```
1 1.  Add the FQDN of the SCOM Management Server to the list of
      TrustedHosts. \<Old Values\> represents the existing set of entries
      returned from Get-Item cmdlet
```

```
1        Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM
             Management Server>,<Old Values>"
2 <!--NeedCopy-->
```

1. DirectorConfig ツールを使用して、SCOM を構成します。

```
1     C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
2 <!--NeedCopy-->
```

SCOM 管理サーバーで、以下を実行します:

1. SCOM 管理者の役割に、Director 管理者を割り当てます。

    a) SCOM 管理コンソールを開き、［管理］>［セキュリティ］>［ユーザーロール］の順に選択します。

b) ［ユーザーロール］では、新しいユーザー役割を作成するか、または既存のユーザー役割を変更することができます。SCOM データへのアクセス方法を定義する SCOM オペレーターの役割には 4 つのカテゴリがあります。たとえば、読み取り専用の役割には、［管理］ペインが表示されず、規則、マシン、アカウントを検出または管理することができません。オペレーターの役割は、すべての管理権限を実行できる管理者の役割です。

注：Director 管理者がオペレーター以外の役割に割り当てられている場合、以下の操作を実行できません：

- 複数の管理サーバーが構成されており、プライマリ管理サーバーを利用できない場合、Director 管理者はセカンダリ管理サーバーに接続できません。プライマリ管理サーバーは Director の web.config ファイルで構成されるサーバーであり、前述の手順 3 で DirectorConfig ツールで指定されたサーバーです。セカンダリ管理サーバーは、プライマリサーバーのピア管理サーバーです。
- 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：

```
winrm set winrm/config/winrs @{
 MaxConcurrentUsers = "20" }
```

PS：

```
Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b) MaxShellsPerUser の変更：

CLI：

```
winrm set winrm/config/winrs @{
 MaxShellsPerUser="20" }
```

PS：


```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c) MaxMemoryPerShellMB の変更:

CLI:

```
winrm set winrm/config/winrs @{
 MaxMemoryPerShellMB="1024" }
```

PS:

```
Set -Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. SCOM 統合が混在ドメイン環境で機能するよう、以下のレジストリエントリを設定します。

パス: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

値の名前: LocalAccountTokenFilterPolicy

種類: DWord

値: 1

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

SCOM 統合がセットアップされると、メッセージ「Cannot get the latest SCOM alerts. View the Director server event logs for more information」が表示されることがあります。サーバーイベントログを使用して問題を特定し、解決することができます。次の原因が考えられます。

- Director または SCOM マシンで、ネットワーク接続が失われた。
- SCOM サービスが利用できないか、ビジー状態のため応答していない。
- 構成したユーザーの権限が変更されていたため、認証に失敗した。
- SCOM データの処理中に、Director でエラーが発生した。
- Director と SCOM サーバーの PowerShell バージョンが不一致。

委任管理と **Director**

October 22, 2021

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	アクセスなし。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。

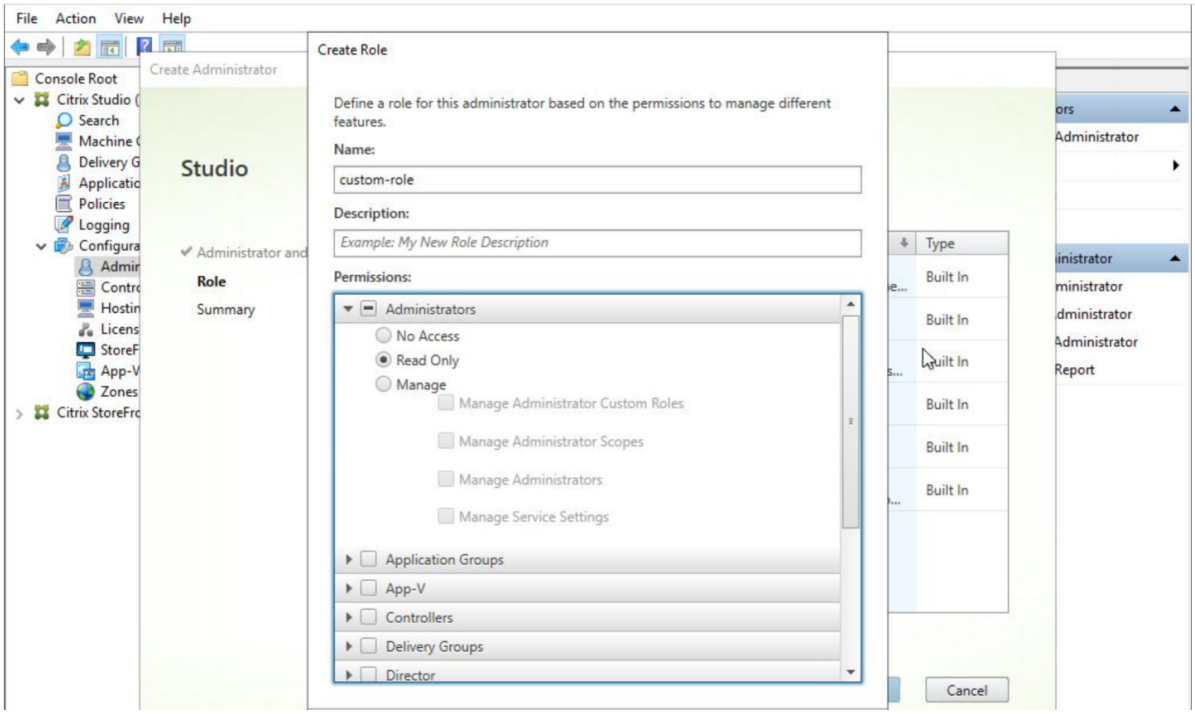
管理者の役割	Director での権限
ホスト管理者	アクセスなし。この管理者は、Director を使用したりデータを表示したりできません。

Director 管理者のカスタム役割を構成するには

Studio では、組織の要件に応じて Director 用のカスタムの役割を構成して、管理権限を柔軟に委任できます。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 - 少なくとも管理者ノードでの読み取り専用アクセス
- デリバリーグループのデータを Director で閲覧するための権限 - 少なくとも読み取り専用アクセス



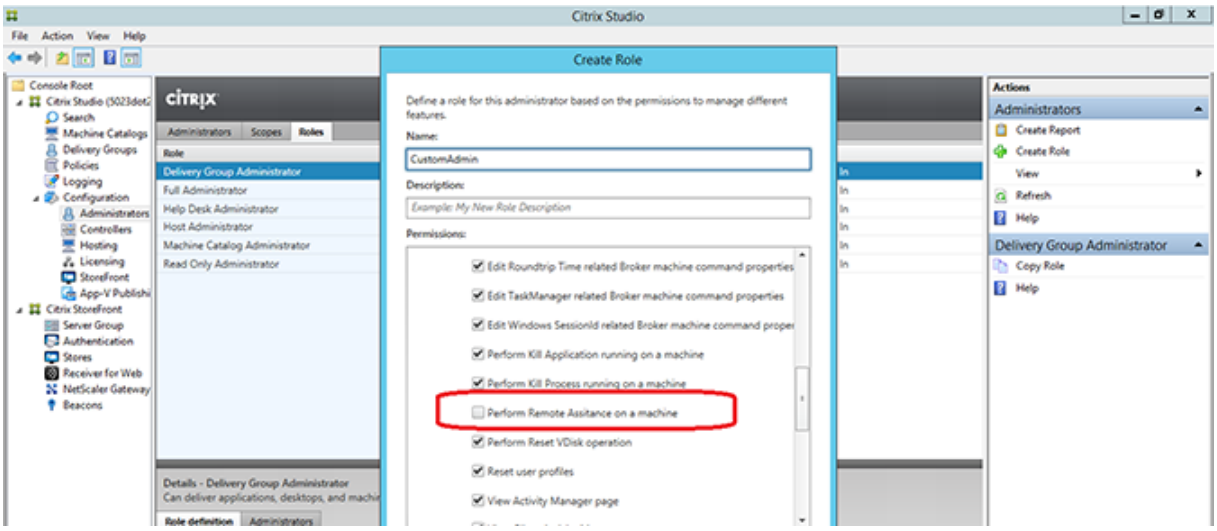
または、既存の役割をコピーしてカスタムの役割を作成し、異なるビューのための権限を追加することができます。たとえば、ヘルプデスクの役割をコピーして、［ダッシュボード］ページや［フィルター］ページを表示するための権限を追加できます。

以下の Director 用の権限を追加します。

- マシンで実行中のアプリケーションの強制終了
- マシンで実行中のプロセスの強制終了

- マシン上でのリモートアシスタンス
- vDisk のリセット操作
- ユーザープロファイルのリセット
- クライアント詳細ページの表示
- ダッシュボードページの表示
- フィルターページの表示
- マシン詳細ページの表示
- 傾向ページの表示
- ユーザー詳細ページの表示

この例では、シャドウ機能（マシン上でのリモートアシスタンス）が無効になっています。



権限は、UI で使えるようにするために、他の権限への依存関係を持つ場合があります。たとえば、マシンで実行中のアプリケーションの強制終了権限を選択すると、その役割のために権限を持つこれらのパネルのみで、［アプリケーションの終了］の機能が有効になります。以下のパネルの権限を選択することができます：

- フィルターページの表示
- ユーザー詳細ページの表示
- マシン詳細ページの表示
- クライアント詳細ページの表示

さらに、他のコンポーネントの権限の一覧から、次のデリバリーグループ権限の追加を検討します。

- デリバリーグループメンバーシップによるマシンのメンテナンスモードの有効/無効。
- デリバリーグループメンバーシップによる Windows デスクトップマシンの電源操作。
- デリバリーグループメンバーシップによるマシンのセッション管理。

Director 展開環境の保護

August 24, 2021

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
- .svc
- .woff
- .woff2
- .png
- .eot
- .svg
- .ttf
- .json
- .（リダイレクト用）

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

重要:

- Director には完全な信頼が必要です。グローバル.NET 信頼レベルを［High］またはそれ以下に設定しないでください。
- Director は個別のアプリケーションプールを保持します。Director の設定を変更するには、Director サイトを選択し変更します。

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［プロセスのメモリクォータの増加］、［セキュリティ監査の生成］、［プロセスレベルトークンの置き換え］の権限が付与されます。これはアプリケーションプールが作成された時の通常のビヘイビアーです。

通常、これらのユーザー権利を変更する必要はありません。これらの権限は Director では使用されず自動的に無効になります。

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、TLS（Transport Layer Security）プロトコルを使用して強力なデータ暗号化機能を提供します。

注:

- 実稼働環境では、Director へのすべての接続が保護されるようにしてください。
- Director からの通信を保護するには、個別に各接続を構成する必要があります。
- SSL プロトコルは、推奨されていません。代わりにより安全な TLS プロトコルを使用します。
- IPsec ではなく TLS を使用して、NetScaler との通信を保護する必要があります。

Director と XenApp および XenDesktop サーバーの（監視およびレポート機能のための）通信を保護する方法について詳しくは、「データアクセスセキュリティ」を参照してください。

Director と NetScaler の（NetScaler Insight のための）通信を保護する方法について詳しくは、「ネットワーク分析機能の構成」を参照してください。

Director とライセンスサーバーの通信を保護する方法について詳しくは、「ライセンス管理コンソールの保護」を参照してください。

Director 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

August 24, 2021

XenDesktop 7 よりも前のバージョンの VDA がある場合、Director には展開からの情報に加えて、Windows リモート管理（WinRM）によるリアルタイム状態と測定値が提供されます。

さらに、この手順を使用して XenDesktop 5.6 Feature Pack1 のリモート PC 用に WinRM を構成します。

デフォルトでは、デスクトップマシンのローカル管理者（一般的にはドメイン管理者および特権のあるそのほかのユーザー）だけが、リアルタイムデータを表示するための権限を持っています。

WinRM のインストールと構成については、CTX125243を参照してください。

ほかのユーザーがリアルタイムデータを確認できるようにするには、そのユーザーに権限を付与する必要があります。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、そのサービス ID に適切な権限のみを付与できます。

このモデルでは、Director のユーザーには WinRM を呼び出す権限を付与しません。ユーザーは Director を使ってデータにアクセスできるだけです。

IIS の Director アプリケーションプールは、サービス ID として実行するように構成されています。デフォルトでは、APPPOOL\Director 仮想アカウントが使用されます。リモート接続を実行すると、このアカウントがサーバーの Active Directory コンピューターアカウント（MyDomain\DirectorServer$ など）として表示されます。このアカウントに適切な権限を付与する必要があります。

複数の Director Web サイトが展開されている環境では、各 Web サーバーのコンピューターアカウントを、適切な権限で構成されている Active Directory セキュリティグループに追加する必要があります。

WinRM に対してユーザーの ID ではなくサービス ID を使用するように Director を設定するには、「詳細構成」の説明に従って次の設定を構成します：

```
Service.Connector.WinRM.Identity = Service
<!--NeedCopy-->
```

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アクセス許可を割り当てるには

Director が WinRM でデスクトップマシンからの情報にアクセスできるようにするには、以下の権限が必要です。

- WinRM RootSDDL の読み取りおよび実行権限
- 以下の WMI 名前空間権限：
  - root/cimv2 - リモートアクセス
  - root/citrix - リモートアクセス
  - root/RSOP — リモートアクセスおよび実行
- 以下のローカルグループのメンバーシップ：
  - パフォーマンスモニターユーザー
  - イベントログリーダー

これらの権限を自動的に付与するには、x86\Virtual Desktop Agent および x64\Virtual Desktop Agent フォルダーのインストールメディア、および C:\inetpub\wwwroot\Director\tools フォルダーに収録されている ConfigRemoteMgmt.exe ツールを使用します。すべての Director ユーザーに上記の権限を付与する必要があります。

Active Directory セキュリティグループ、ユーザー、またはコンピューターアカウントに上記の権限を付与したり、アプリケーションやプロセスを終了するための権限を付与したりするには、管理特権でコマンドプロンプトを開き、次の引数を指定してこのツールを実行します:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

ネットワーク分析機能の構成

August 24, 2021

注: この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。

Director は、NetScaler Insight Center または NetScaler MAS を統合して、ネットワーク分析機能およびパフォーマンス管理機能を提供します。

- ネットワーク分析機能では、NetScaler Insight Center または NetScaler MAS で HDX Insight レポートを使用してネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能を使用すると、Director で ICA トラフィックを高度に分析できます。
- パフォーマンス管理機能により、履歴保持および傾向に関するレポートを生成できます。データの履歴保持とリアルタイム評価により、管理者はサーバーのキャパシティとヘルスに関する傾向レポートを作成できます。

Director でこの機能を有効にすると、HDX Insight レポートにより以下の追加情報が Director に提供されます。

- ［傾向］ページの［ネットワーク］タブには、展開環境全体におけるアプリケーション、デスクトップ、ユーザーに対する遅延と帯域幅の影響が表示されます。
- ［User Details］ページには、特定のユーザーセッションに特化した遅延と帯域幅情報が表示されます。

制限事項:

- ICA セッション往復時間（RTT）には、Receiver for Windows 3.4 以降および Receiver for Mac 11.8 以降のデータが正確に表示されます。これらのバージョンよりも前のバージョンの Receiver については、正確なデータが表示されません。
- ［傾向］ビューでは、XenDesktop 7 よりも前のバージョンの VDA については HDX 接続のログオンデータが収集されません。以前のバージョンの VDA については、チャートデータが 0 として表示されます。

ネットワーク分析機能を有効にするには、Director で NetScaler Insight Center または NetScaler MAS をインストールし、構成する必要があります。Director には、NetScaler MAS Version 11.1 Build 49.16 以降が必要です。Insight Center および MAS は、Citrix XenServer で実行される仮想アプライアンスです。Director では、ネットワーク分析により、環境のトラフィック情報を収集します。

詳しくは、NetScaler MAS のドキュメントを参照してください。

1. Director がインストールされているサーバー上のコマンドラインプロンプトで、C:\inetpub\wwwroot\Director\tools にある DirectorConfig コマンドに/confignetscaler パラメーターを指定して実行します。
2. 画面上の指示に従って、NetScaler Insight Center または NetScaler MAS マシン名（完全修飾ドメイン名または IP アドレス）、ユーザー名、パスワード、および接続の種類（HTTP または HTTPS）を入力して、NetScaler Insight または NetScaler MAS との統合を選択します。
3. 変更を確認するには、いったんログオフして再ログオンします。

ユーザーの問題のトラブルシューティング

August 24, 2021

Director の［アクティビティマネージャー］ページにある［ヘルプデスク］ビューを使って、ユーザーに関する情報を確認します:

- ユーザーのログオン、接続、およびアプリケーションの状態について確認する。
- ユーザーのマシンをシャドウする。
- ICA セッションを記録する。

- 次の表に示す方法で問題のトラブルシューティングを行い、必要な場合は問題を担当の管理者に報告する。

トラブルシューティングのヒント

ユーザーの問題	提案
ログオンに時間がかかる。断続的もしくは繰り返し失敗する	ユーザーログオンの問題の診断
アプリケーションが遅いまたは応答しない	アプリケーション障害の解決
接続に失敗した	デスクトップ接続の復元
セッションが遅いまたは応答しない	セッションの復元
セッションの録画	セッションの録画
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実行

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。

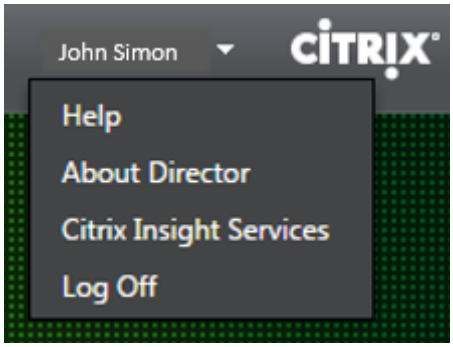
検索結果には、現在マシンを使用していないユーザーや、マシンに割り当てられていないユーザーも含まれます。

- 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 にアクセスする

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にトラブルシューティング情報をアップロードする

単一の Delivery Controller または Virtual Delivery Agent から Citrix Scout を実行し、選択したコンピューターのトラブルシューティングに必要なデータ要素や Citrix Diagnostics Facility（CDF）トレースをキャプチャします。Scout は、CIS プラットフォームにデータを安全にアップロードする機能を提供し、Citrix のテクニカルサポートのトラブルシューティングを支援します。Citrix のテクニカルサポートは CIS プラットフォームを使用して、カスタマーから報告された問題解決する時間を短縮します。

Scout は、XenApp または XenDesktop のコンポーネントと一緒にインストールされます。Windows のバージョンに応じて、Scout は、XenDesktop 7.1、XenDesktop 7.5、XenApp 7.5、XenDesktop 7.6、XenApp 7.6、XenDesktop 7.7、または XenApp 7.7 をインストール、またはこれらのバージョンにアップグレードしたときに、Windows のスタートメニュー、またはスタート画面に表示されます。

スタートメニューやスタート画面から Scout を起動するには、［Citrix］の［Citrix Scout］を選択します。

Scout の使用と構成、および一般的な問題について詳しくは、CTX130147を参照してください。

ユーザーへのメッセージの送信

August 24, 2021

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テキストを入力して再度［試行］をクリックします。

セッションの復元

August 24, 2021

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行います。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（アクション）	説明
応答していないアプリケーションまたはプロセスを終了する	［アプリケーション］タブをクリックします。応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。同様に、応答していないプロセスを選択し、［プロセスの終了］をクリックします。また、メモリや CPU リソースを過度に消費しているプロセスを終了します。
Windows セッションを切断する	［セッション制御］をクリックし、［切断］を選択します。このオプションは、仲介されたサーバー OS マシンに対してのみ使用できます。仲介されていないセッションでは無効です。
セッションからユーザーをログオフする	［セッション制御］をクリックし、［ログオフ］を選択します。

セッション障害が解決されたことを確認するために、ユーザーに再度ログオンさせます。また、ユーザーをシャドウしてセッションをより詳しく監視することもできます。

注：ユーザーデバイスで XenDesktop 7 より前のバージョンの VDA が動作している場合、Director はセッションに関する完全な情報を表示することができません。代わりに、情報を使用できないことを示すメッセージが表示されます。このメッセージは、［ユーザーの詳細］ページおよび［アクティビティマネージャー］に表示される場合があります。

Personal vDisk のリセット

August 28, 2019

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。リセットに失敗した場合は、［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。

HDX チャネルシステムレポートの実行

August 24, 2021

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。

ユーザーのシャドウ

November 28, 2018

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。

シャドウのための **Microsoft Internet Explorer** ブラウザーの構成

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。

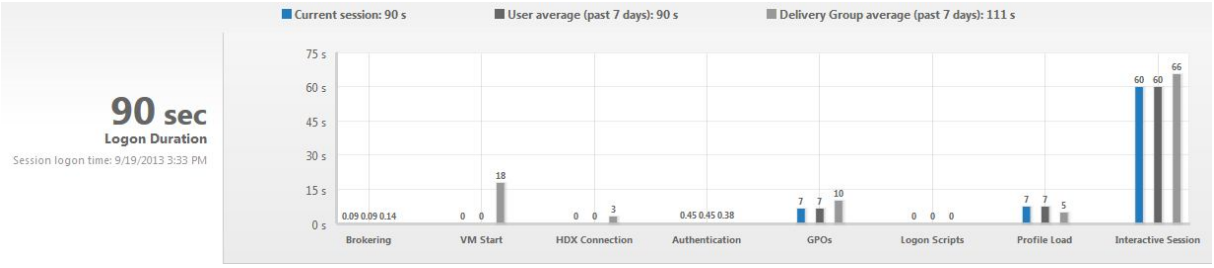
[コンピューターの構成] > [管理用テンプレート] > [Windows コンポーネント] > [Internet Explorer] > [インターネットコントロールパネル] > [セキュリティページ] > [インターネットゾーン] > [ファイルのダウンロード時に自動的にダイアログを表示]

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。

ユーザーログオンの問題の診断

January 22, 2019

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、処理時間は、ログオン時刻表示の上にある数値と、ログオン処理のフェーズのグラフとして表示されます。



ユーザーが XenApp および XenDesktop にログオンすると、Monitor Service により、ユーザーが Citrix Receiver から接続した時点から、デスクトップが使用可能になった時点までのログオンプロセスの各フェーズが追跡されます。左側の大きな数字は総ログオン時間であり、接続の確立および Delivery Controller からのデスクトップの取得にかかった時間と、仮想デスクトップの認証とログオンにかかった時間を合計して計算されます。処理時間の情報は、管理者の Web ブラウザーのローカル時刻で秒単位（または秒の小数単位）まで表示されます。

ユーザーログオンの問題のトラブルシューティングを行うには、通常は次の手順を使用します:

1. ログオン状態のトラブルシューティングを行うには、[ユーザーの詳細] ビューの [ログオン処理時間] パネルを使用します。
   - ユーザーがログオン中の場合は、ここにログオンのプロセスが表示されます。
   - ユーザーがログオン済みの場合、ユーザーがそのセッションにログオンするときにかかった時間が [ログオン処理時間] パネルに表示されます。
2. ログオンプロセスの各フェーズを調査します。

ログオンプロセスのフェーズ	説明
仲介	ユーザーに割り当てるデスクトップを決定するのに要した時間です。
仮想マシンの起動	マシンの起動を必要とするセッションの場合、これは仮想マシンの起動にかかった時間です。
HDX コネクション	クライアントから仮想マシンへの HDX 接続の設定で必要な手順を実行するためにかかった時間です。
認証	リモートセッションへの認証を実行するのにかかった時間です。

ログオンプロセスのフェーズ	説明
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。
プロファイルのロード	ユーザーまたは仮想マシンに対してプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。
対話型セッション	これは、ユーザープロファイルのロード後、キーボードやマウスの制御をユーザーに「渡す」までにかかった時間です。通常、ログオンプロセスのすべてのフェーズで最も長い時間であり、次のように計算されます：対話型セッションの処理時間 **=** デスクトップ準備完了イベントのタイムスタンプ（**VDA** の **EventId 1000**）**-** ユーザープロファイルロード完了イベントのタイムスタンプ（**VDA** の **EventId 2**）

総ログオン時間は、これらの各フェーズを厳密に合計したものではありません。たとえば、複数のフェーズが並行して発生したり、一部のフェーズで追加処理が発生したりしてログオン処理時間が合計値よりも大きくなることがあります。

注：［ログオン処理時間］グラフには、ログオンフェーズが秒単位で表示されます。1 秒未満の時間値はすべて、秒未満の値として表示されます。1 秒を超える値は、0.5 秒単位に丸められます。グラフは、Y 軸の最高値を 200 秒として表示するように設計されています。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。

トラブルシューティングのヒント

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。

セッションの録画

August 24, 2021

Director の ［ユーザーの詳細］と ［マシンの詳細］画面から、Session Recording 制御を使って、ICA セッションを録画することができます。この機能は **Platinum** ライセンスを持つユーザーが使用できます。

DirectorConfig ツールを使って Director の Session Recording を構成するには、「Session Recording のインストール、アップグレード、およびアンインストール」の「**Director** を構成して **Session Recording** サーバーを使用する」を参照してください。
ログインユーザーに Session Recording ポリシーを変更する権限がある場合のみ、Director の Session Recording 制御を使用できます。この権限は、「録画ポリシーの作成とアクティブ化」で説明されているように、Session Recording 承認コンソールで設定できます。
注：Director または Session Recording Policy Console による Session Recording の設定の変更は、次の ICA セッションの起動時から有効になります。

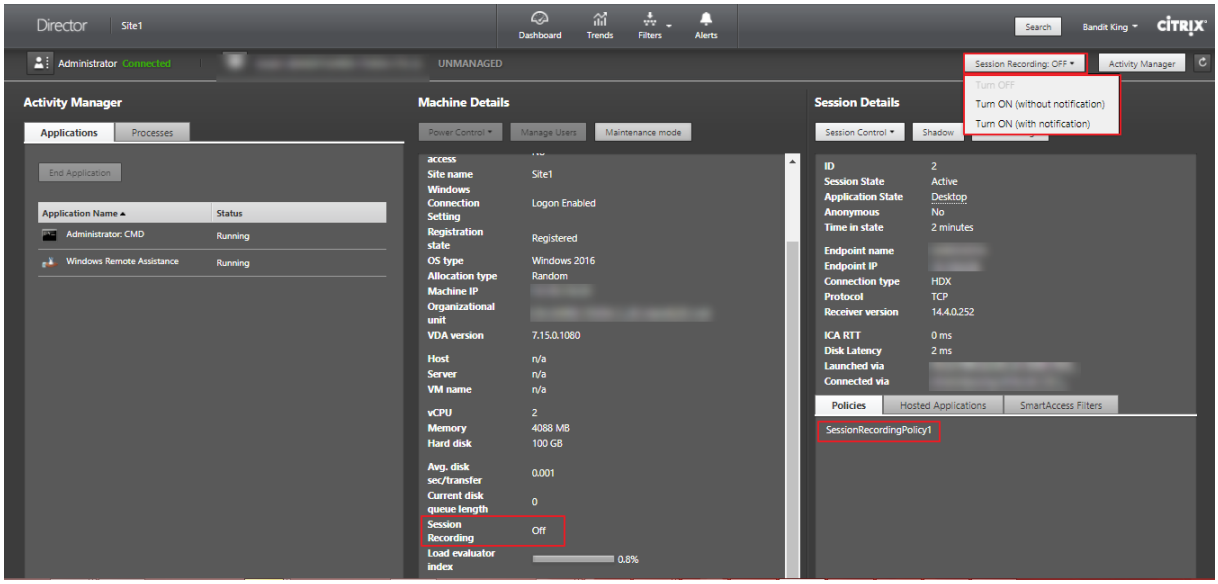
Director での **Session Recording** 制御

［アクティビティマネージャー］または ［ユーザーの詳細］画面で、特定のユーザーに対して Session Recording を有効にできます。サポートされるすべてのサーバーで特定のユーザーに対して以降のセッションが録画されます。

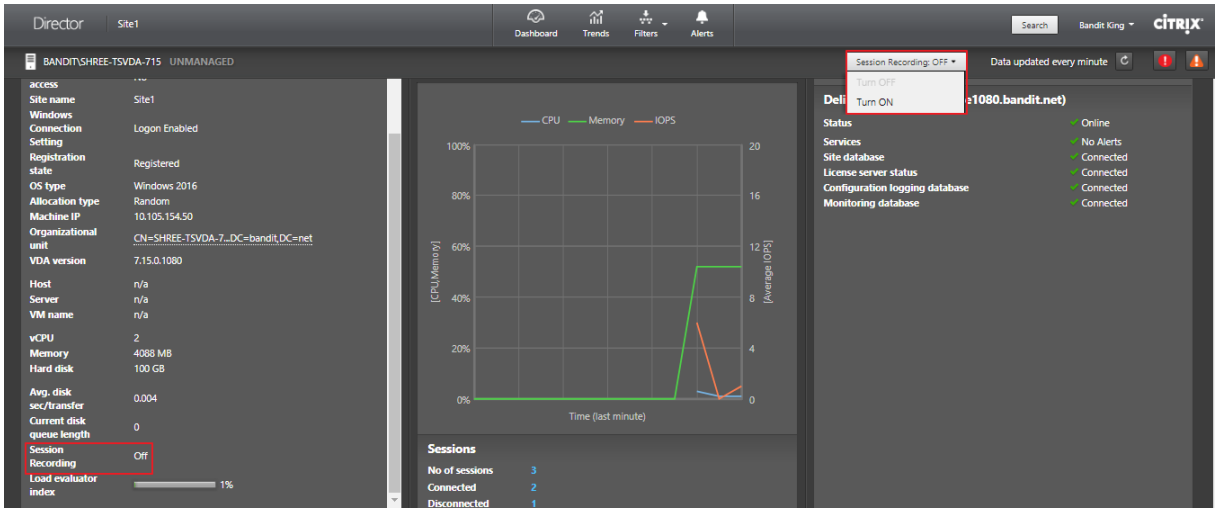
次の操作を実行できます：

- オンにする（通知あり）- ICA セッションへのログオン時に録画されているセッションについてユーザーに通知されます。
- オンにする（通知なし）- ユーザーに通知されることなく、セッションは録画されます。
- オフにする - ユーザーのセッションの録画を無効にします。

［ポリシー］パネルには、アクティブな Session Recording ポリシーの名前が表示されます。



［マシンの詳細］ページから特定のマシンに対して、Session Recording を有効にできます。そのマシンの以降のセッションが録画されます。［マシンの詳細］パネルには、そのマシンの Session Recording ポリシーの状態が表示されます。



デスクトップ接続の復元

August 24, 2021

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（アクション）	説明
マシンがメンテナンスモードでないことを確認する	[ユーザーの詳細］ページで、メンテナンスモードがオフであることを確認します。
ユーザーのマシンを再起動する	マシンを選択して［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。

アプリケーション障害の解決

August 24, 2021

［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（アクション）	説明
応答していないアプリケーションを終了する	応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。アプリケーションが終了したら、ユーザーに再度起動するように通知します。
応答していないプロセスを終了する	必要な権限がある場合は、［プロセス］タブをクリックします。アプリケーションに関連するプロセス、または CPU リソースやメモリを過度に消費しているプロセスを選択し、［プロセスの終了］をクリックします。プロセスを終了するための権限がない場合、プロセスを終了することはできません。

操作（アクション）	説明
ユーザーのマシンを再起動する	デスクトップ OS マシンでは、選択したセッションで［再起動］をクリックします。または、［マシンの詳細］ビューで電源制御を使ってマシンを再起動またはシャットダウンします。アプリケーションの状態を再確認するには、ユーザーに再度ログオンするように通知します。サーバー OS マシンでは、［再起動］オプションを使用できません。代わりに、ユーザーをログオフして、再度ログオンさせます。
マシンをメンテナンスモードにする	パッチまたはそのほかの更新などによりマシンのイメージをメンテナンスする必要がある場合は、マシンをメンテナンスモードにします。［マシンの詳細］ビューで［詳細］をクリックして、メンテナンスモードのオプションをオンにします。担当の管理者に報告します。

ユーザープロファイルのリセット

August 24, 2021

注意：プロファイルをリセットすると、そのユーザーのフォルダーやファイルは保存され、新しいプロファイルにコピーされます。ただし、多くのユーザープロファイルデータは削除されます。たとえば、レジストリはリセットされ、アプリケーション設定も削除される場合があります。

1. Director から、プロファイルをリセットするユーザーを検索し、このユーザーのセッションを選択します。
2. ［プロファイルのリセット］をクリックします。
3. ユーザーに、すべてのセッションからログオフするように指示します。
4. ユーザーに再度ログオンするように指示します。ユーザープロファイルから保存されたフォルダーやファイルが新しいプロファイルにコピーされます。
   重要：複数のプラットフォーム上（Windows 8 と Windows 7 など）にユーザーのプロファイルが存在する場合は、問題が発生したデスクトップまたはアプリケーションに最初にログオンするよう指示します。これにより、正しいプロファイルがリセットされます。
   Citrix ユーザープロファイルの場合、ユーザーのデスクトップが表示された時点でリセットされています。Microsoft の移動プロファイルの場合、フォルダーの復元処理に時間がかかる場合があります。この復元処理が完了するまで、ユーザーはログオンしていなければなりません。

注：これまでの手順では、XenDesktop（デスクトップ VDA）を使用している前提になっています。XenApp（サーバー VDA）を使用している場合は、プロファイルのリセットを実行するためにログオンする必要があります。ユーザーはいったんログオフしてから再度ログオンし、プロファイルのリセットを完了させる必要があります。

プロファイルが正しくリセットされない場合（ユーザーがそのマシンに再ログオンできなかったり一部のファイルが見つからなかったりする場合など）、管理者が手作業で元のプロファイルを復元する必要があります。

ユーザーのプロファイルのフォルダーやファイルが保存され、新しいプロファイルにコピーされます。これらのフォルダーは、以下の順番でコピーされます。

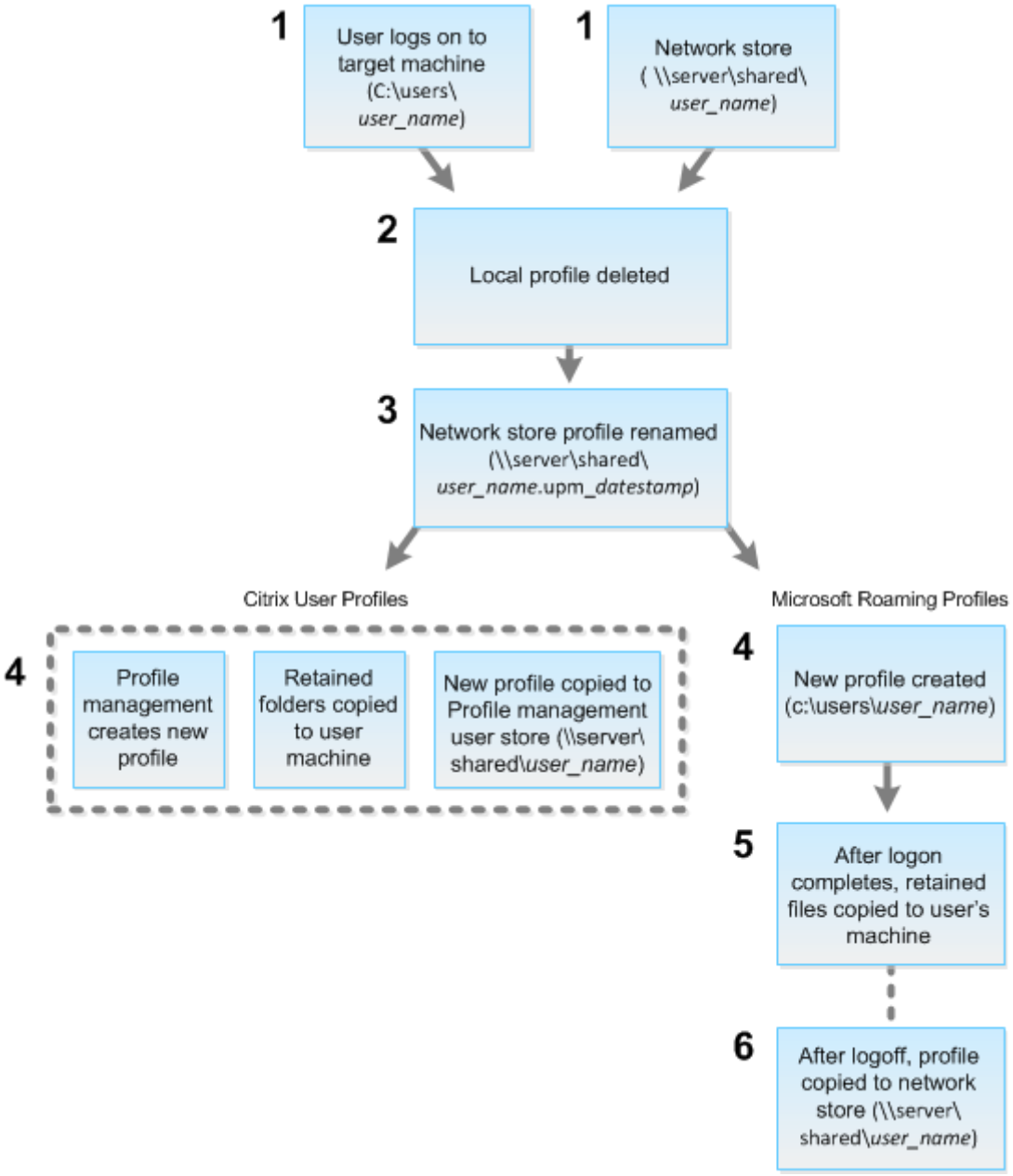
- デスクトップ
- Cookies
- お気に入り
- ドキュメント
- ピクチャ
- ミュージック
- ビデオ

注：Windows 8 以降では、プロファイルのリセット時にクッキーフォルダーはコピーされません。

リセットされたプロファイルはどのように処理されるか

いずれの Citrix ユーザープロファイルまたは Microsoft 移動プロファイルもリセットできます。ユーザーがログオフした後に管理者が Director または PowerShell SDK でリセットコマンドを選択すると、使用されているユーザープロファイルが識別され、Director により適切なリセットコマンドが発行されます。Director は Profile Management を介してプロファイルのサイズ、種類、およびログオン時間などに関する情報を取得します。

これは、ユーザーログオン後の処理を説明した図です。



1. Director からのリセットコマンドにより、プロファイルの種類が指定されます。次に、Profile Management サービスによりその種類のプロファイルのリセットが試行され、適切なネットワーク共有（ユーザーストア）が検出されます。Profile Management により処理されたユーザーのプロファイルに対して移動プロファイル用のコマンドが発行された場合は拒否されます（逆の場合も同様）。
2. ローカルプロファイルがある場合は削除されます。
3. ネットワークプロファイルの名前が変更されます。
4. 次の処理は、リセットされるプロファイルが Citrix ユーザープロファイルか Microsoft 移動プロファイルかにより異なります。
    - Citrix ユーザープロファイルの場合、Profile Management のインポート規則によって新しいプロファイルが作成され、フォルダーがネットワークプロファイルにコピーされ、ユーザーは通常どおりにロ

グオンできます。リセットに移動プロファイルが使用される場合は、移動プロファイル内のすべてのレジストリ設定がリセットプロファイル内に保持されます。
注：必要な場合は、テンプレートプロファイルが移動プロファイルよりも優先されるように Profile Management を構成することもできます。

- Microsoft 移動プロファイルの場合、Windows によって新しいプロファイルが作成され、ユーザーがログオンするとフォルダーがユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルがネットワークストアにコピーされます。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーに、すべてのセッションからログオフするように指示します。
2. ローカルプロファイルが存在する場合は削除します。
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、名前に日時と upm_datestamp 拡張子が含まれます。
4. 現在のプロファイルのフォルダー（拡張子 upm_datestamp のないもの）を削除します。
5. 元のプロファイル名を使用してアーカイブフォルダの名前を変更します。つまり、日付と時刻の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。

アプリケーションのトラブルシューティング

August 24, 2021

リアルタイムアプリケーション監視

アイドル状態の時間の指標を使用して、特定の時間制限を超えてアイドル状態であるインスタンスを識別することで、アプリケーションとセッションをトラブルシューティングできます。

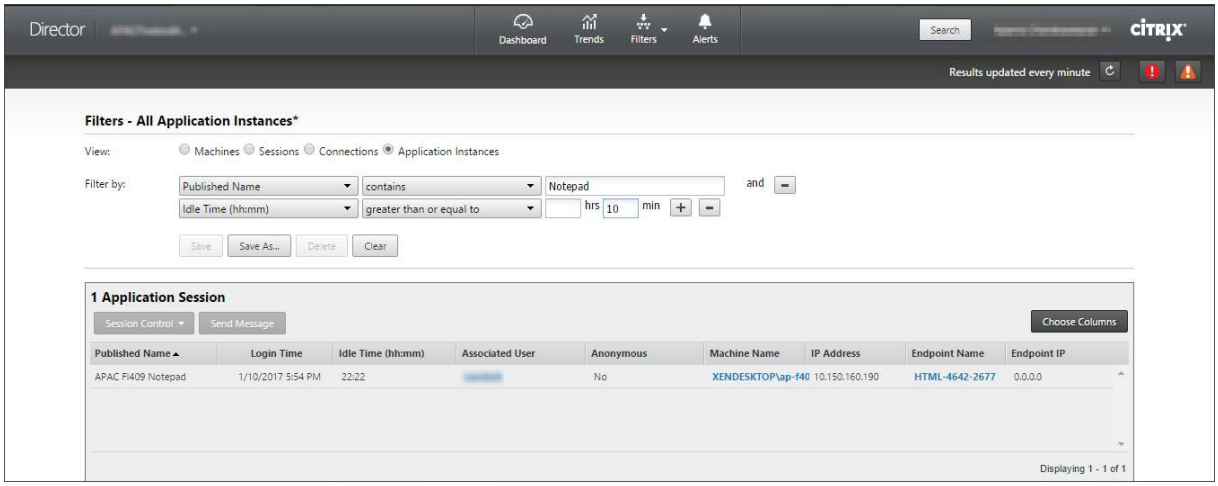
アプリケーションベースのトラブルシューティングの一般的な用途は、ヘルスケアのセクターです。このセクターでは、従業員間でアプリケーションライセンスが共有されています。このため、XenApp および XenDesktop の環境の削除、パフォーマンスの低いサーバーの再構成、またはアプリケーションの保守およびアップグレードを行うには、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

［アプリケーションインスタンス］フィルターページには、サーバー OS 上とデスクトップ OS 上にある VDA のすべてのアプリケーションインスタンスが表示されます。関連付けられたアイドル時間の測定値は、10 分間以上アイドル状態になっているサーバー OS の VDA のアプリケーションインスタンスについて表示されます。

注：アプリケーションインスタンスの測定値は、すべてのライセンスエディションのサイトで確認できます。

一定時間以上アイドル状態になっているアプリケーションインスタンスを識別して、必要に応じてログオフするか接続を切断するためにこの情報を使用します。これを行うには、［フィルター］**>**［アプリケーションインスタンス］の

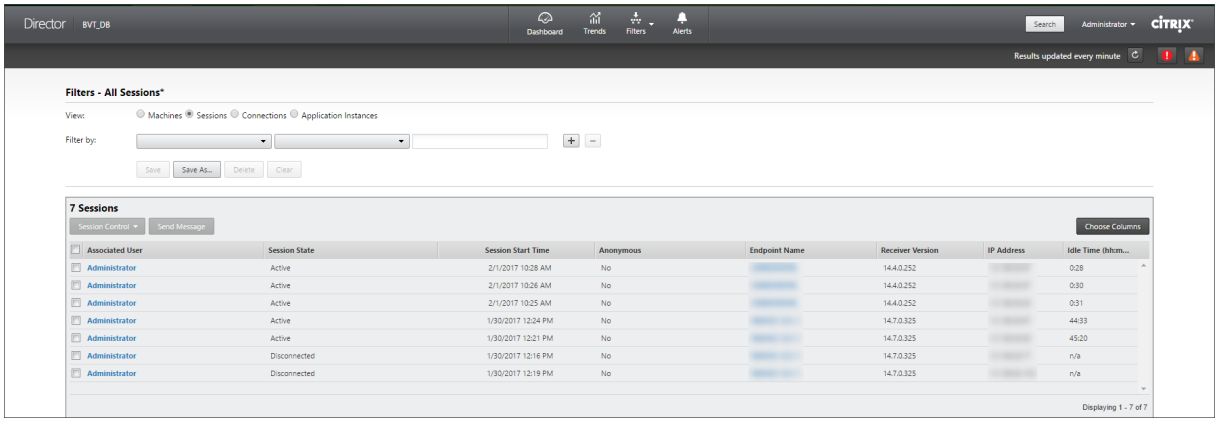
順に選択し、保存済みのフィルターを選択するか ［すべてのアプリケーションインスタンス］を選択し、独自のフィルターを作成します。



フィルターの例は次のようになります。［フィルター基準］条件として ［公開名］（アプリケーションの公開名）と［アイドル時間］を選択します。次に ［アイドル時間］に ［次のもの以上］を設定して特定の時間制限を指定、再利用のためのフィルターを保存します。フィルター後の一覧から、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、［セッション制御］ドロップダウンリストから ［ログオフ］または ［切断］を選択してインスタンスを終了します。

注：ログオフするか 1 つのアプリケーションインスタンスを切断すると、現在のセッションがログオフされるか切断されるため、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

［セッション］フィルターページでセッション状態とセッションのアイドル時間の指標を使用してアイドル状態のセッションを識別できます。［アイドル時間］列で並べ替えるか、特定の時間制限を超えてアイドル状態であるセッションを識別するフィルターを定義します。アイドル時間は、10 分間以上アイドル状態であるサーバー OS の VDA 上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次のいずれかの場合、［アイドル時間］には ［なし］と表示されます。

- アイドル状態の時間が 10 分未満の場合

- デスクトップ OS の VDA 上で起動されている場合
- バージョン 7.12 以前を実行する VDA 上で起動されている場合

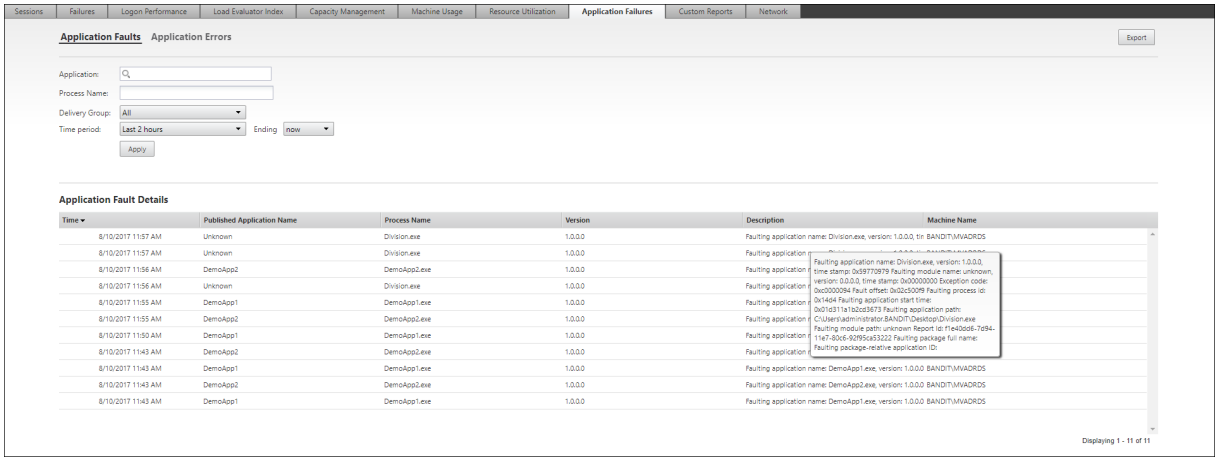
アプリケーション障害履歴の監視

［傾向］>［アプリケーション障害］タブに、VDA 上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、Platinum および Enterprise Edition では、過去 2 時間、24 時間、7 日間、および 1 か月間で使用できます。他のライセンスの種類では、過去 2 時間、24 時間、および 7 日間で使用できます。ソースに「アプリケーションエラー」がある場合は、イベントビューアーに記録されているアプリケーション障害が監視されます。［エクスポート］をクリックすると、CSV、Excel、または PDF フォーマットのレポートが生成されます。

アプリケーション障害の監視についてのグルーミング保持の設定は、Platinum および Platinum Edition 以外の両方とも、GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays がデフォルトで 1 日に設定されています。この設定は、PowerShell コマンドを使用して変更できます:

```
1 *Set-MonitorConfiguration -\<setting name\> \<value\>*
```



障害はその重要度によって［アプリケーション障害］または［アプリケーションエラー］として表示されます。［アプリケーション障害］タブには、機能またはデータの損失に関連した障害が表示されます。［アプリケーションエラー］には、即座に関連しない問題が示されます。これは、将来問題が発生する可能性がある状況を意味しています。

障害は、公開アプリケーション名、プロセス名またはデリバリーグループ、および期間によってフィルターできます。表には、障害またはエラーコードと簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

注：対応するアプリケーション名を派生できない場合、公開アプリケーション名は「不明」として表示されます。これは、通常、アプリケーションの起動がデスクトップセッションで失敗した場合、または依存している実行ファイルが原因で処理できない例外により失敗した場合に発生します。

デフォルトでは、サーバー OS の VDA でホストされたアプリケーションの障害のみが監視されています。監視グループポリシーでは次のような監視設定が変更できます：アプリケーション障害の監視の有効化、デスクトップ OS の

VDA 上のアプリケーション障害の監視の有効化、および障害の監視から除外されるアプリケーションの一覧の設定。詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

マシンのトラブルシューティング

March 25, 2020

［フィルター］>［マシン］ビューで ［デスクトップ **OS** マシン］または ［サーバー **OS** マシン］を選択して、サイトで構成されているマシンを表示します。［サーバー OS マシン］タブには負荷評価基準インデックスが表示されます。この測定値上にマウスポインターを置くと、各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。

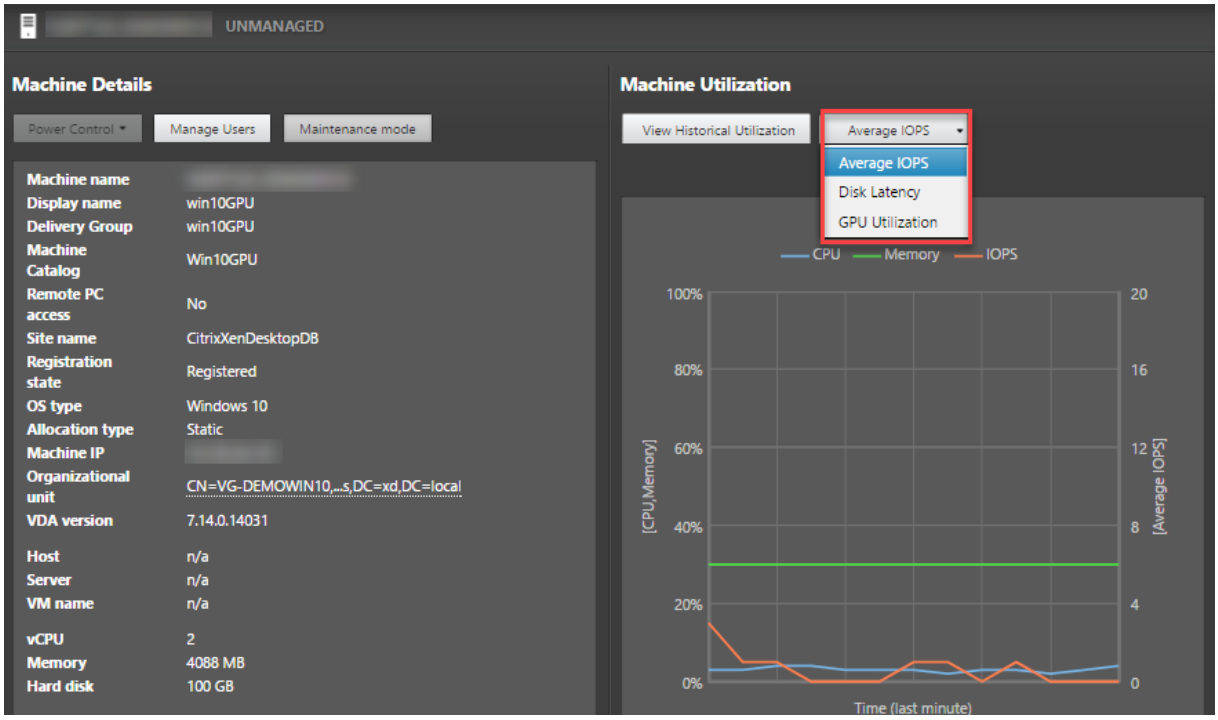
エラーが発生したマシンの ［エラーの理由］をクリックすると、エラーの詳細な説明と推奨される解決手順が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、『Citrix Director 7.12 Failure Reasons Troubleshooting Guide』に記載されています。

マシン名のリンクをクリックし、［マシンの詳細］ページに移動します。［マシンの詳細］ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用済みの HotFix の詳細の一覧が表示されます。［マシン稼働］パネルには、マシンの稼働状況を示すグラフが表示されます。

マシンごとのリアルタイムのリソース使用状況

［マシン稼働］パネルには、CPU とメモリのリアルタイムの使用状況を示すグラフが表示されます。Delivery Controller および VDA のバージョン **7.14** 以降がインストールされているサイトでは、ディスクと GPU の監視グラフも表示されます。

重要なパフォーマンス測定値としてディスク監視グラフ、平均 IOPS、ディスク遅延があり、VDA ディスク関連の問題をモニターし解決する上で役立ちます。［平均 IOPS］グラフには、ディスクの読み取りおよび書き込みの平均回数が表示されます。［ディスク遅延］を選択すると、データが要求されてディスクから返されるまでの時間をミリ秒単位で示すグラフが表示されます。



[**GPU** 使用率］を選択すると GPU、GPU メモリ、およびエンコーダーとデコーダーの使用率がパーセント値として表示され、サーバーまたはデスクトップ OS の VDA での GPU 関連の問題を解決できます。［GPU 使用率］グラフは、NVIDIA Tesla M60 GPU を搭載した 64 ビット Windows と Display Driver バージョン 369.17 以降が実行されている VDA でのみ使用できます。

VDA で GPU アクセラレーションを使用するには、HDX 3D Pro を有効にする必要があります。詳しくは、「Windows デスクトップ OS のための GPU アクセラレーション」および「Windows サーバー OS のための GPU アクセラレーション」を参照してください。

VDA が 1 つ以上の GPU にアクセスしている場合、［GPU 使用率］グラフには個々の GPU から収集された GPU 測定値の平均が表示されます。GPU 測定値は、個々のプロセスではなく VDA 全体について収集されます。

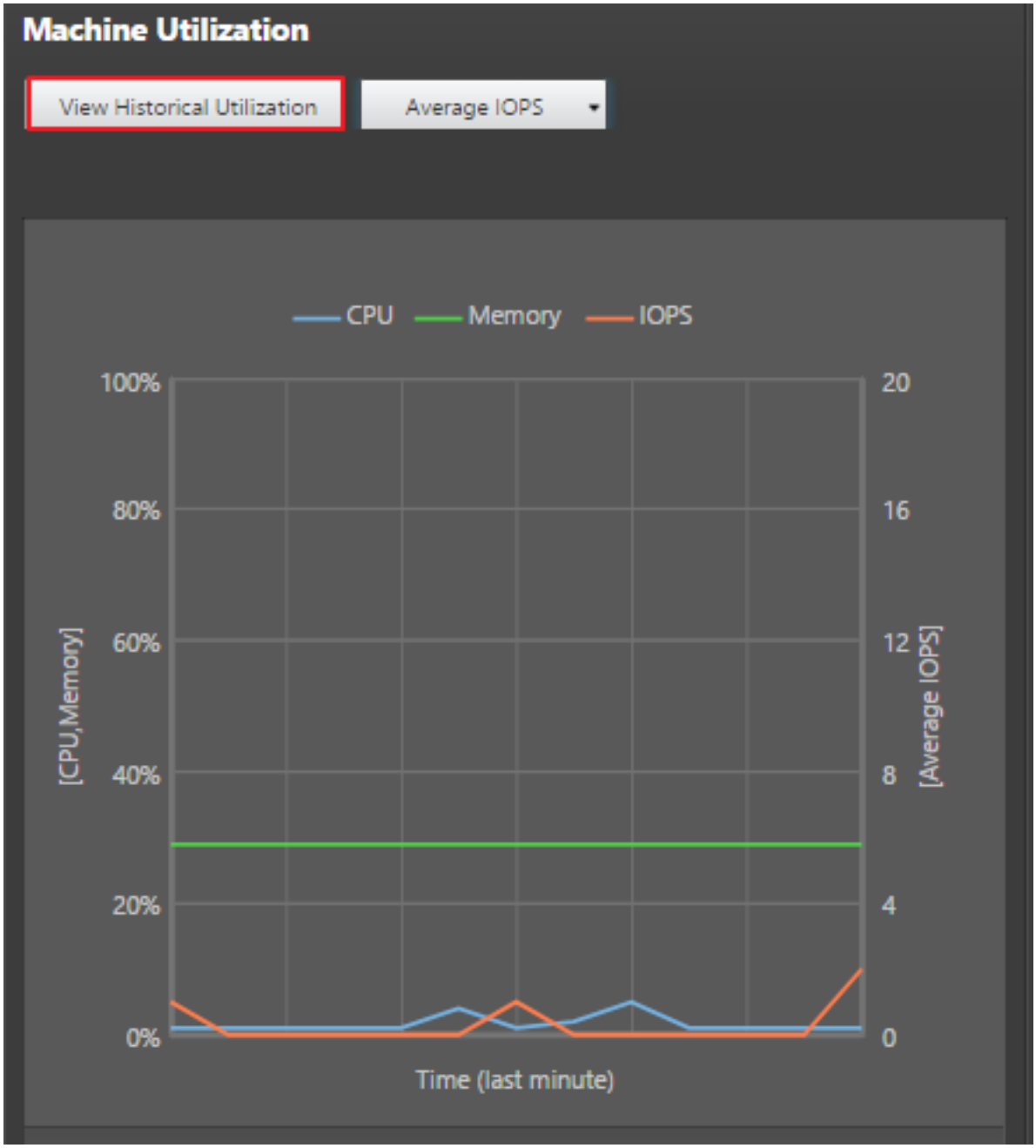
マシンごとの過去のリソース使用状況

［マシン稼働］パネルの ［履歴使用率の表示］をクリックすると、選択したマシンでの過去のリソースの使用状況を確認できます。

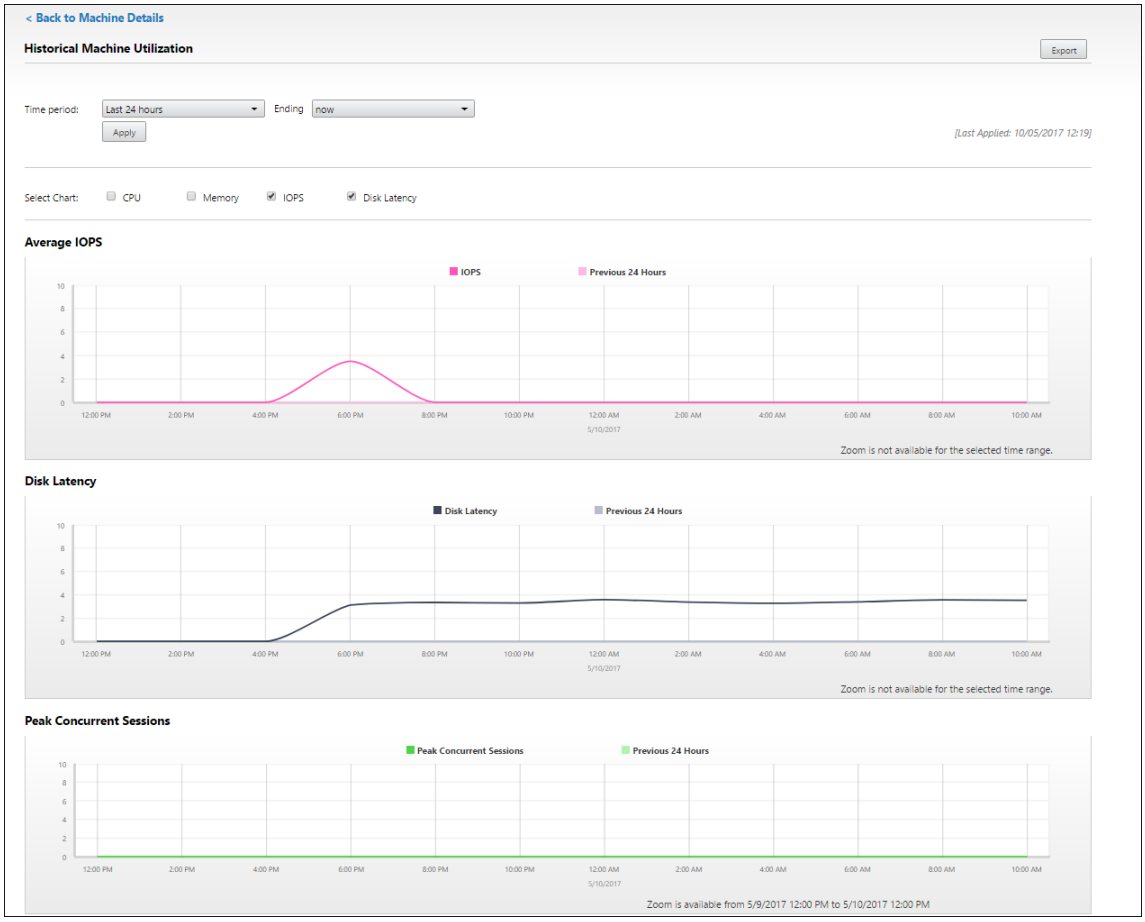
使用率グラフには、CPU、メモリ、最大同時セッション数、平均 IOPS、ディスク遅延などの重要なパフォーマンス測定が表示されます。

注：監視のポリシー設定で ［プロセス監視の有効化］を［許可］に設定して、［マシン使用率の履歴］ページの［上位 10 プロセス］テーブルでこれらのデータが収集および表示されるようにする必要があります。この設定はデフォルトでは［禁止］に設定されています。

デフォルトでは、CPU とメモリの使用率、平均 IOPS、ディスク遅延に関するデータが収集されます。この収集は、［リソースの監視を有効にします］ポリシー設定で無効にできます。



1. ［マシンの詳細］ビューの ［マシン稼働］パネルから、［履歴使用率の表示］を選択します。［マシン使用率の履歴］ページが開きます。
2. ［期間］で表示する期間を過去 2 時間、過去 24 時間、過去 7 日間、過去 30 日間、過去 1 年の使用率から選択します。
   注：現在、平均 IOPS とディスク遅延のデータについては、過去 24 時間、過去 30 日間、過去 1 年についてのみ表示できます。カスタムの終了時刻は使用できません。
3. ［適用］をクリックして、目的のグラフを選択します。
4. グラフの他のセクションにマウスを合わせると、選択した期間の詳細が表示されます。



たとえば、［過去 **2** 時間］を選択すると、基準の期間は選択した時間範囲の 2 時間前になります。過去 2 時間と基準期間の CPU、メモリ、およびセッションの傾向を表示します。

［過去 **1** か月］を選択すると、基準期間は過去 1 か月間になります。これを選択すると、先月から基準日時までの平均 IOPS およびディスク遅延が表示されます。

5. 選択した期間のリソース使用状況データをエクスポートするには、［エクスポート］をクリックします。詳しくは、「展開環境の監視」の「レポートのエクスポート」セクションを参照してください。

6. グラフの下には、CPU とメモリの使用率が上位 10 位のプロセスを示すテーブルが表示されます。選択した時間範囲のアプリケーション名、ユーザー名、セッション ID、平均 CPU、ピーク時の CPU、平均メモリ、ピーク時のメモリが表示される列から任意の列を選択してソートできます。［平均 IOPS］列と［ディスク遅延］列は並び替えできません。

   注：システムプロセスのセッション ID は「0000」と表示されます。

7. 特定プロセスのリソース消費に関する履歴傾向を表示するには、上位 10 位のプロセスから任意のプロセスを選択してドリルダウンします。

機能の互換性マトリックス

August 24, 2021

各サイトでは、VDA や Delivery Controller の以前のバージョンを使用できますが、Director の最新バージョンの機能の一部が使用できない場合があります。さらに、機能が使用できるかどうかは、サイトのライセンスエディションによって異なります。Director、Delivery Controller、VDA は同じバージョンを保有されることをお勧めします。

注： Delivery Controller のアップグレード後に Studio を開くと、サイトのアップグレードを要求するメッセージが表示されます。詳しくは、「アップグレードの順序」（「環境のアップグレード」セクション）を参照してください。

以下の表は、Director の機能と、Delivery Controller（DC）、VDA、およびライセンスエディションで必要なその他の従属コンポーネントの最小バージョンの一覧です。

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.15	アプリケーション障害の監視	DC 7.15 および VDA 7.15	すべて
7.14	アプリケーションを中心としたトラブルシューティング	DC 7.13 および VDA 7.13	すべて
7.14	ディスクの監視	DC 7.14 および VDA 7.14	すべて
7.14	GPU の監視	DC 7.14 および VDA 7.14	すべて
7.13	［セッション詳細］パネル上のトランスポートプロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリな接続およびマシンの障害の説明	DC 7.12 および VDA 7.x	すべて
7.12	Enterprise Edition での履歴データ提供期間の延長	DC 7.12 および VDA 7.x	Enterprise
7.12	カスタムレポート	DC 7.12 および VDA 7.x	Platinum
7.12	SNMP トラップによる Director 通知の自動化	DC 7.12 および VDA 7.x	Platinum
7.11	リソース使用レポート	DC 7.11 および VDA 7.11	すべて

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.11	CPU、メモリ、ICA RTT 条件に対応するアラート拡張	DC 7.11 および VDA 7.11	Platinum
7.11	エクスポートレポートの改善	DC 7.11 および VDA 7.x	すべて
7.11	Citrix Octoblu による Director 通知の自動化	DC 7.11 および VDA 7.x	Platinum
7.11	NetScaler MAS との統合	DC 7.11、VDA 7.x および MAS バージョン 11.1 ビルド 49.16	Platinum
7.9	ログオン処理時間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	予見的な監視およびアラート	DC 7.7 および VDA 7.x	Platinum
7.7	SCOM 統合	DC 7.7、VDA 7.x、SCOM 2012 R2、および PowerShell 3.0	Platinum
7.7	Windows 認証の統合	DC 7.x および VDA 7.x	すべて
7.7	デスクトップ OS およびサーバー OS の使用状況	DC 7.7 および VDA 7.x	Platinum
7.6.300	Framehawk 仮想チャネルのサポート	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合	DC 7.6 および VDA 7.x	Platinum
7	HDX Insight 統合	DC 7.6、VDA 7.x、および NetScaler Insight Center	Platinum

データの粒度と保持

August 24, 2021

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。例:

- 接続セッション（Connected Session）やマシンエラー（Machine Failure）は一定の期間の状態を示すため、その期間内の最大値として公開されます。
- ログオン期間（LogOn Duration）は時間の長さを示す指標であるため、期間内の平均として公開されます。
- ログオン数（LogOn Count）および接続障害（Connection Failure）は一定の期間に発生した数を示し、期間内の合計値として公開されます

同時データ評価

重複しているセッションは同時発生していると考える必要があります。ただし、間隔として 1 分を指定した場合、1 分以内に発生するすべてのセッションは（重複しているかしていないかに関係なく）すべて同時であるとみなされます。つまり、間隔のサイズが非常に小さいため、精度の計算に関係するパフォーマンス上のオーバーヘッドを考慮する必要はありません。2 つのセッションがその 1 時間内の別々の 1 分間に発生する場合、それらは重複しているとはみなされません。

サマリー表と生データの相関

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を集計したものが示されます。
- 生データは、セッション、接続、アプリケーション、およびそのほかのオブジェクト内で記録された個々のイベントまたは現在の状態を示します。

データを API コール間またはそのデータモデル内で関連付けるときは、以下の概念および制限事項を考慮してください。

- 未完の間隔にはサマリーデータがありません。メトリックサマリーは長時間での履歴傾向を示すためのものであり、完結した間隔のサマリーテーブルに集計されます。データ収集の開始時や終了時のサマリーデータはありません。1 日（間隔 =1440）の集計値の場合、最初と最後の未完の 1 日にはデータがないことを意味します。これらの未完の間隔に生データが存在しても、そのデータが集計されることはありません。各データ粒度の最初と最後の集計間隔は、各サマリーテーブルから最小と最大の SummaryDate を取得することで決定できます。SummaryDate 列は、間隔の開始時を示します。Granularity 列はその集計データの間隔の長さを示します。
- 時間による関連付け。前述のように、メトリック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のタイムスタンプでは UTC が使用されます。サマリーテーブルは 1 時間区切りのタイムゾーンごとに集計されます。1 時間区切りのタイムゾーンに属さない場合は、データの集計先に不整合が生じることがあります。

データの粒度と保持

Director で取得される集計データの粒度は、要求された時間（T）の関数です。以下の規則があります。

- 0 < T <= 1 時間の場合は分単位の粒度
- 0 < T <= 30 日の場合は時間単位の粒度
- T > 31 日の場合は日単位の粒度

集計データから取得されないデータを要求すると、生のセッション（Session）および接続（Connection）情報から取得されます。このデータの量はすぐに大きくなるため、専用のスケジュールでクリーンアップされます。クリーンアップにより、意味のあるデータのみが長期間保持されます。これにより、レポートに必要な粒度を維持しながら良好なパフォーマンスが提供されます。Platinum Edition では、クリーンアップが開始されるまでの日数をカスタマイズできます。

設定にアクセスするには、Delivery Controller で以下の PowerShell コマンドを実行します:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>

<!--NeedCopy-->
```

クリーンアップは以下の設定により制御されます。

	設定名	対象データ	デフォルト値（Platinum、日数）	デフォルト値（Platinum 以外、日数）
1	GroomSessionsRe	セッション終了後のセッションレコードと接続レコードの保有	90	7
2	GroomFailuresRetentionDays	MachineFailureLog レコードおよび ConnectionFailureLog レコード	90	7
3	GroomLoadIndexe	LoadIndex レコード	90	7
4	GroomDeletedRetentionDays	LifecycleState が「Deleted」である Machine エンティティ、Catalog エンティティ、DesktopGroup エンティティ、および Hypervisor エンティティ。関連する Session レコード、SessionDetail レコード、Summary レコード、Failure レコード、または LoadIndex レコードも削除されます。	90	7
5	GroomSummaries	DesktopGroupSum レコード、FailureLogSummary レコード、および LoadIndexSummary レコード。集計データ（日単位）	90	7

	設定名	対象データ	デフォルト値（Platinum、日数）	デフォルト値（Platinum 以外、日数）
6	GroomMachineHotfixLogRetentionDays	VDA および Controller マシンに適用された Hotfix	90	90
7	GroomMinuteRete	集計データ（分単位）	3	3
8	GroomHourlyRetentionDays	集計データ（時間単位）	32	7
9	GroomApplication	アプリケーションインスタンスの履歴	90	0
10	GroomNotificationLogRetentionDays	通知ログ	90	
11	GroomResourceUs	リソース使用率データ（生データ）	1	1
12	GroomResourceUsageMinuteDataRetentionDays	リソース使用率サマリーデータ（分単位）	7	7
13	GroomResourceUs	リソース使用率サマリーデータ（時間単位）	30	7
14	GroomResourceUsageDayDataRetentionDays	リソース使用率サマリーデータ（日単位）	90	7
15	GroomProcessUsa	プロセス使用率データ（生データ）	1	1
16	GroomProcessUsageMinuteDataRetentionDays	プロセス使用率データ（分単位）	3	3
17	GroomProcessUsa	プロセス使用率データ（時間単位）	7	7
18	GroomProcessUsageDayDataRetentionDays	プロセス使用率データ（日単位）	30	7
19	GroomSessionMet	セッションメトリックデータ	1	1

	設定名	対象データ	デフォルト値（Platinum、日数）	デフォルト値（Platinum 以外、日数）
20	GroomMachineMetricDataRetentionDays	インスタントマシンメトリックデータ	3	3
21	GroomMachineMe	マシンメトリックサマリーデータ	90	7
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1
23	GroomApplication	アプリケーション障害データ	1	1

注意：Monitor Service データベースの値を変更した後でその値を適用するには、このサービスを再起動する必要があります。Monitor Service データベースの値の変更は、Citrix サポート担当者からの指示があった場合のみ行ってください。

クリーンアップ保持に関する注意事項：
GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、および GroomSessionMetricsDataRetentionDays の設定はデフォルト値の 1 に制限されていますが、GroomProcessUsageMinuteDataRetentionDays はデフォルト値の 3 に制限されています。プロセス使用データが急速に増加する傾向があるため、これらの値を設定する PowerShell コマンドは無効になっています。以下は、ライセンスごとのその他の保持設定です。

- **Premium** ライセンスがあるサイト - 前述のクリーンアップ保持設定を任意の日数に更新できます。
- **Advanced** ライセンスがあるサイト - すべての設定のクリーンアップ保持は 31 日間に制限されています。
- その他すべてのサイト - すべての設定のクリーンアップ保持は 7 日間に制限されています。

例外：

- GroomApplicationInstanceRetentionDays は、Premium ライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premium ライセンスサイトでは 31 日間の制限があります。

データを長期間保持すると、テーブルのサイズについて以下の影響が発生することがあります：

- 時間単位のデータ。時間単位のデータを 2 年などの長期間保持すると、1000 個のデリバリーグループがあるサイトではデータベースが以下の数式に基づいて増大します。

  「1000 個のデリバリーグループ ×24 時間/日 ×365 日/年 ×2 年＝ 17,520,000 行のデータ」集計テーブルのデータ量が多いため、パフォーマンスに大きな影響を及ぼします。ダッシュボードのデータがこのテーブルから取得されることを考慮すると、データベースサーバーに対する要求は高くなります。データ量が過度に多いと、パフォーマンスが大きく低下します。

- セッションとイベントのデータ。各セッションの開始時および接続/再接続時に収集されるデータです。大規模サイト（100,000 ユーザーなど）では、このデータの量が急速に増加します。たとえば、これらのテーブルでは 2 年間で 1TB 以上のデータが保持され、高性能なエンタープライズレベルのデータベースが必要になります。

Citrix Director の失敗の原因とトラブルシューティング

August 24, 2021

次の表に、さまざまな失敗のカテゴリ、理由、および問題を解決するために必要なアクションを示します。詳しくは、「列挙型、エラーコード、および説明」を参照してください。

接続失敗エラー

カテゴリ	理由	問題	操作（アクション）
-	[0] Unknown。このエラーコードはマッピングされていません。	Monitoring Service は、Broker Service によって共有された情報からは、報告された起動または接続エラーの理由を判別できません。	コントローラーで CDF ログを収集し、シトリックスサポートに連絡してください。
[0] なし	[1] None	なし	-
[2] MachineFailure	[2] SessionPreparation	Delivery Controller から VDA へのセッション準備要求が失敗しました。考えられる原因: Delivery Controller と VDA 間の通信の問題、準備要求の作成中に Broker Service で発生した問題、または VDA が要求を受け入れない結果となるネットワークの問題。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。

カテゴリ	理由	問題	操作（アクション）
[2] MachineFailure	[3] RegistrationTimeout	VDA の電源は入っていますが、Delivery Controller を使用した登録を試行中にタイムアウトしました。	Citrix Broker Service が Delivery Controller 上で実行されており、Desktop Service が VDA 上で実行されていることを確認します。停止している場合は、起動してください。
[1] ClientConnection-Failure	[4] ConnectionTimeout	VDA がセッションの起動のために準備された後、クライアントがその VDA に接続しませんでした。セッションは正常に仲介されましたが、クライアントが VDA に接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定。	Director コンソールをチェックして、クライアントに現在アクティブな接続があるかどうかを確認します。これは、ユーザーに影響がないことを確認するためです。セッションが存在しない場合は、クライアントと VDA のイベントログでエラーを確認します。クライアントと VDA 間のネットワーク接続の問題を解決します。
[4] NoLicensesAvailable	[5] Licensing	ライセンス要求に失敗しました。考えられる原因：ライセンスの数が不足しているか、ライセンスサーバーが 30 日以上ダウンしています。	ライセンスサーバーがオンラインかつ到達可能な状態であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作していると思われる場合はライセンスサーバーを再起動します。環境に必要な数のライセンスがあることを確認し、必要があれば追加でライセンスを割り当てます。

カテゴリ	理由	問題	操作（アクション）
[1] ClientConnection-Failure	[6] Ticketing	チケット作成中にエラーが発生しました。VDA へのクライアント接続が、仲介された要求と一致しません。起動要求チケットは Broker によって準備され、ICA ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDA が Broker を使用して ICA ファイル内の起動チケットを検証します。考えられる原因：ICA ファイルが破損しているか、ユーザーが不正な接続を試みています。	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーが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ことを確認します。これが 1 回限りの問題であるかどうかを判断するために、アプリケーションまたはデスクトップを再起動するようにユーザーに指示します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしている VDA が登録済みであることを確認します。登録されていない場合は、VDA のイベントログを確認し、登録の問題を解決します。
[1] ClientConnection-Failure	[7] Other	クライアントが最初に VDA に接続を試行してから接続シーケンスが完了する前に、VDA でセッションが終了したことが報告されました。	起動前にユーザーがセッションを終了していないことを確認します。セッションを再起動してください。問題が解決しない場合は、CDF ログを収集してシトリックスサポートに連絡してください。

カテゴリ	理由	問題	操作（アクション）
[1] ClientConnection-Failure	[8] GeneralFail	セッションを起動できませんでした。考えられる原因：ブローカーの起動中または初期化中に、仲介される起動が要求されたか、起動の仲介フェーズ中に内部エラーが発生しました。	Citrix Broker Service が実行されていることを確認して、セッションの起動を再試行します。
[5] 構成	[9] MaintenanceMode	VDA、または VDA が属するデリバリーグループが、メンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。必要がなければ、対象のデリバリーグループまたはマシンでメンテナンスモードを無効にして、再接続するようユーザーに指示します。
[5] 構成	[10] ApplicationDisabled	アプリケーションが管理者によって無効にされているため、エンドユーザーがアプリケーションにアクセスできません。	アプリケーションが実稼働環境で使用されるためのものである場合は、アプリケーションを有効にして再接続するようユーザーに指示します。
[4] NoLicensesAvailable	[11] LicenseFeature Refused	使用中の機能が既存のライセンスでカバーされていません。	シトリックスの営業担当者に連絡して、Citrix Virtual Apps and Desktops の既存のライセンスエディションおよびライセンス種類でカバーされている機能を確認してください。

カテゴリ	理由	問題	操作（アクション）
[3] NoCapacityAvailable	[13] SessionLimitReached	すべての VDA が使用中であるため、追加のセッションをホストする容量はありません。考えられる原因: すべての VDA が使用中である（シングルセッション OS VDA の場合）、またはすべての VDA が設定した最大同時セッション数に達しています（マルチセッション OS VDA の場合）。	メンテナンスモードの VDA があるかどうかを確認します。さらに容量を解放する必要がない場合は、メンテナンスモードを無効にします。Citrix ポリシー設定で ［セッションの上限数］の値を増やすと、サーバーの VDA ごとにさらにセッションを追加できます。マルチセッション OS VDA を追加できます。シングルセッション OS VDA を追加できます。
[5] 構成	[14] DisallowedProtocol	ICA および RDP プロトコルは許可されていません。	Delivery Controller で PowerShell コマンドの「**Get-BrokerAccessPolicyRule**」を実行し、［**Allowed-Protocols**］の値にすべての必要なプロトコルがあることを確認します。この問題は、構成に誤りがある場合にのみ発生します。

カテゴリ	理由	問題	操作（アクション）
[5] 構成	[15] ResourceUnavailable	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できる VDA がない可能性があります。考えられる原因：アプリケーションまたはデスクトップが公開されていないか、アプリケーションまたはデスクトップをホストしている VDA が負荷上限に達しているか、アプリケーションまたはデスクトップがメンテナンスモードに設定されています。	アプリケーションまたはデスクトップが公開されていることと、VDA がメンテナンスモードになっていないことを確認します。マルチセッション OS VDA が負荷限界に達しているかどうかを確認します。達している場合は、追加でマルチセッション OS VDA をプロビジョニングします。接続に使用できるシングルセッション OS VDA があることを確認します。必要に応じて、追加でシングルセッション OS VDA をプロビジョニングします。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICA セッションがアクティブであり、別のエンドポイントに接続されています。ただし、［アクティブセッションの再接続］が無効になっているため、クライアントがアクティブセッションに接続できません。	Delivery Controller で、［アクティブセッションの再接続］が有効になっていることを確認します。**HKEY_LOCAL_MACHINE\Software\C** で、レジストリの **DisableActiveSessionReconnect** の値が 0 に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントが特定のセッションに再接続しようとしましたが、セッションが終了しています。	ワークスペースコントロールの再接続を再試行します。

カテゴリ	理由	問題	操作（アクション）
[2] MachineFailure	[18] SpinUpFailed	セッション起動のために VDA の電源をオンにしようとしてもオンにならない。これはハイパーバイザーで報告された問題です。	まだマシンの電源がオフになっている場合は、Citrix Studio からマシンを起動してみます。起動に失敗した場合は、ハイパーバイザーの接続とアクセス権限を確認してください。VDA が PVS でプロビジョニングされたマシンである場合は、PVS コンソールでマシンが実行されていることを確認します。そうでない場合は、マシンに Personal vDisk が割り当てられていることを確認し、ハイパーバイザーにログインして VM をリセットします。
[2] MachineFailure	[19] Refused	Delivery Controller がエンドユーザーからの接続を準備するための要求を VDA に送信しますが、VDA はアクティブにこの要求を拒否します。	ping を使用して、Delivery Controller と VDA が正常に通信できることを確認します。正常に通信できていない場合は、ファイアウォールまたはネットワークルーティングの問題を解決します。

カテゴリ	理由	問題	操作（アクション）
[2] MachineFailure	[20] ConfigurationSetFailure	Delivery Controller が、セッション起動中の VDA にポリシー設定やセッション情報などの必要な構成データを送信しませんでした。考えられる原因: Delivery Controller と VDA 間の通信の問題と VDA 間の通信の問題、構成セット要求の作成中に Broker Service で発生した問題、または VDA が要求を受け入れない結果となるネットワークの問題。	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションのインスタンス数上限に達しました。アプリケーションの追加のインスタンスを VDA で開くことができません。この問題は、アプリケーションの上限機能に関連しています。	ライセンスで可能な限り、アプリケーション設定の［同時に実行されるインスタンスの上限数］をより高い値に設定できます。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーがアプリケーションで複数のインスタンスを開こうとしていますが、アプリケーションがユーザーごとに 1 つのインスタンスのみを許可するよう構成されています。この問題は、アプリケーションの上限機能に関連しています。	デフォルトでは、アプリケーションのインスタンスはユーザーごとに 1 つだけ許可されます。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定の［ユーザーごとに **1** つのインスタンスに制限します］をオフにします。

カテゴリ	理由	問題	操作（アクション）
[1] ClientConnection-Failure	[23] Communication error	Delivery Controller が、接続を準備する要求などの情報を VDA に送信しようとしていますが、通信の試行中にエラーが発生しました。これは、ネットワークの中断によって発生した可能性があります。	すでに開始されている場合は、VDA でデスクトップサービスを再起動して登録プロセスを再開し、VDA が正常に登録されることを確認します。アプリケーションイベントログの詳細を確認し、VDA 用に構成された Delivery Controller が正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable。Monitoring Service が「[12] NoDesktopAvailable」をこのエラーコードに変換します。	セッションの起動に割り当てられた VDA が、無効または使用できない状態になっています。考えられる原因：VDA の電源状態が不明または使用できない、最後のユーザーのセッション以降 VDA が再起動しなかった、現在のセッションで有効にする必要があるセッション共有が無効になっている、または VDA が配信グループまたはサイトから削除された。	VDA がデリバリーグループにあることを確認します。ない場合は、適切なデリバリーグループに追加します。十分な数の VDA がデリバリーグループに存在し、ユーザーの要求により公開済みの共有デスクトップまたはアプリケーションを起動する準備ができた状態であることを確認します。VDA をホストしているハイパーバイザーがメンテナンスモードになっていないことを確認します。

カテゴリ	理由	問題	操作（アクション）
[2] MachineFailure	[101] MachineNot-Functional。Monitoring Service が [12] NoDesktopAvailable をこのエラーコードに変換します。	VDA が動作していません。考えられる原因: VDA がデリバリーグループから削除された、VDA が登録されていない、VDA の電源の状態が使用不可になっている、または VDA で内部の問題が発生しています。	VDA がデリバリーグループにあることを確認します。ない場合は、適切なデリバリーグループに追加します。Citrix Studio で VDA が電源オンとして表示されていることを確認します。複数のマシンの電源の状態が不明な場合は、ハイパーバイザーへの接続の問題またはホストの障害を解決します。VDA をホストしているハイパーバイザーがメンテナンスモードになっていないことを確認します。これらの問題が解決されたら、VDA を再起動します。

マシンエラーの種類

エラーコード	エラーコード ID	問題	操作（アクション）
不明	-	-	-
Unregistered	3	-	-
MaxCapacity	4	ハイパーバイザーの読み込みインデックスは最大容量に達しています。	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーに容量を追加します。ハイパーバイザ ― を追加します。

エラーコード	エラーコード ID	問題	操作（アクション）
StuckOnBoot	2	VM の起動シーケンスが完了しませんでした。ハイパーバイザーと通信していません。	VM がハイパーバイザーで正常に起動したことを確認します。オペレーティングシステムの問題など、VM 上の他のメッセージを確認します。ハイパーバイザーツールが VM にインストールされていることを確認します。VDA が VM にインストールされていることを確認します。
FailedToStart	1	ハイパーバイザーで VM の起動中に問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除の理由（エラーの種類が **Unregistered** または **Unknown** の場合に適用されます）

エラーコード	エラーコード ID	問題	操作（アクション）
AgentShutdown	0	VDA が正常にシャットダウンされました。	既存の電源管理ポリシーに基づいて、VDA のオフ状態を予期していない場合は VDA の電源をオンにします。イベントログでエラーを確認します。
AgentSuspended	1	VDA が休止状態またはスリープモードです。	VDA の休止状態モードを解除します。Citrix Virtual Apps and Desktops VDA の電源設定で、休止状態を無効にすることができます。

エラーコード	エラーコード ID	問題	操作（アクション）
IncompatibleVersion	100	Citrix のプロトコルバージョンが一致しないため、VDA が Delivery Controller と通信できません。	VDA と Delivery Controller のバージョンを揃えます。
AgentAddressResolutionFailed	101	Delivery Controller が、VDA の IP アドレスを解決できませんでした。	Active Directory（AD）に VDA マシンアカウントが存在することを確認します。存在しない場合は、作成します。DNS の VDA の名前と IP アドレスが正確であることを確認します。正確でない場合は、修正します。広範囲に及ぶ場合は、Delivery Controller の DNS 設定を検証します。`nslookup`コマンドを実行して、Delivery Controller から DNS 解決を確認します。
[Cloud]:AgentAddressR	101	Delivery Controller が、VDA の IP アドレスを解決できませんでした。	Active Directory（AD）に VDA マシンアカウントが存在することを確認します。存在しない場合は、作成します。DNS の VDA の名前と IP アドレスが正確であることを確認します。正確でない場合は、修正します。

エラーコード	エラーコード ID	問題	操作（アクション）
AgentNotContactable	102	Delivery Controller と VDA の間で通信の問題が発生しました。	ping を使用して、Delivery Controller と VDA が正常に通信できていることを確認します。通信できていない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。

エラーコード	エラーコード ID	問題	操作（アクション）
[Cloud]: AgentNotContactable	102	Delivery Controller と VDA の間で通信の問題が発生しました。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。シトリックスサポートに連絡してください。
AgentWrongActiveDirectoryOU	103	Active Directory 検出の構成ミスが発生しました。VDA レジストリで構成済みのサイト固有の OU（サイトコントローラー情報が AD に格納されている場所）は、別のサイト用です。	Active Directory の構成が正しいことを確認します。またはレジストリ設定を確認します。
EmptyRegistrationRequest	104	VDA から Delivery Controller に送信された登録要求が空でした。これは、VDA ソフトウェアのインストールが破損していることが原因である可能性があります。	VDA でデスクトップサービスを再起動して、登録プロセスを再起動し、アプリケーションのイベントログで VDA が正しく登録されていることを確認します。
MissingRegistrationCapabilities	105	このバージョンの VDA は Delivery Controller と互換性がありません。	VDA をアップグレードするか、VDA を削除してから再インストールします。

エラーコード	エラーコード ID	問題	操作（アクション）
MissingAgentVersion	106	このバージョンの VDA は Delivery Controller と互換性がありません。	この問題がすべてのマシンに影響を与えている場合は、VDA ソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDA が、その機能をブローカーに伝達できません。これは、VDA のバージョンと Delivery Controller のバージョンに互換性がないことが原因である可能性があります。登録機能が、バージョンごとに異なり、登録要求と一致しない形式になっています。	VDA と Delivery Controller のバージョンを揃えます。
NotLicensedForFeature	108	使用を試みている機能のライセンスがありません。	Citrix ライセンスのエディションを確認します。または、VDA を削除してから再インストールします。
[Cloud]: NotLicensed-ForFeature	108	使用を試みている機能のライセンスがありません。	シトリックスサポートに連絡してください。
UnsupportedCredentiaversion	109	VDA と Delivery Controller が、同じ暗号化メカニズムを使用していません。	VDA と Delivery Controller のバージョンを揃えます。

エラーコード	エラーコード ID	問題	操作（アクション）
InvalidRegistrationReques	110	VDA がブローカーに登録要求を行いましたが、登録要求の内容が破損しているか無効です。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。
SingleMultiSessionMisr	111	VDA のオペレーティングシステムの種類が、マシンカタログまたはデリバリーグループと互換性がありません。	正しいマシンカタログの種類に、または同じオペレーティングシステムのマシンを含むデリバリーグループに、VDA を追加します。
FunctionalLevelTooLowFor	112 Catalog	マシンカタログが、インストールされている VDA のバージョンよりも高い VDA の機能レベルに設定されています。	VDA のマシンカタログの機能レベルが、VDA の機能レベルと一致していることを確認します。マシンカタログをアップグレードまたはダウングレードして、VDA の機能レベルと一致させます。
FunctionalLevelTooLow	113	デリバリーグループが、インストールされている VDA のバージョンよりも高い VDA の機能レベルに設定されています。	VDA のデリバリーグループの機能レベルが、VDA の機能レベルと一致していることを確認します。マシンカタログをアップグレードまたはダウングレードして、VDA の機能レベルと一致させます。

エラーコード	エラーコード ID	問題	操作（アクション）
PowerOff	200	VDA が正常にシャットダウンされませんでした。	VDA の電源がオンになっているはずである場合は、Citrix Studio から VDA を起動して、起動と登録が正しく実行されることを確認してください。起動または登録の問題をトラブルシューティングします。シャットダウンの根本的な原因を特定するために、VDA のイベントログをバックアップしてから確認します。
AgentRejectedSettingsl	203	Citrix ポリシーなどの設定が変更または更新されましたが、VDA への更新の送信中にエラーが発生しました。これは、更新がインストールされている VDA のバージョンと互換性がない場合に発生することがあります。	必要な場合は、VDA をアップグレードします。適用された更新が、現在の VDA のバージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	ブローカーが、VDA で実行されているセッションの監査を完了しませんでした。	広範囲にわたる問題の場合は、Delivery Controller の Citrix Broker Service を再起動します。
[Cloud]: SessionPrepareFailure	206	ブローカーが、VDA で実行されているセッションの監査を完了しませんでした。	シトリックスサポートに連絡してください。

エラーコード	エラーコード ID	問題	操作（アクション）
ContactLost	207	Delivery Controller と VDA との接続が切断されました。これは、ネットワークの切断が原因である可能性があります。	Citrix Broker Service が Delivery Controller 上で実行されており、Desktop Service が VDA 上で実行されていることを確認します。停止している場合は、起動してください。すでに開始されている場合は、VDA でデスクトップサービスを再起動して登録プロセスを再開し、VDA が正常に登録されることを確認します。アプリケーションイベントログの詳細を確認し、VDA 用に構成された Delivery Controller が正確であることを確認します。ping を使用して、Delivery Controller と VDA が正常に通信できていることを確認します。通信できていない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	Delivery Controller と VDA との接続が切断されました。これは、ネットワークの切断が原因である可能性があります。	デスクトップサービスが VDA で実行されていることを確認します。停止していた場合は、開始します。

エラーコード	エラーコード ID	問題	操作（アクション）
BrokerRegistrationLimitReached	201	Delivery Controller が、構成済みの同時に登録できる VDA 数の上限に達しました。デフォルトでは、Delivery Controller は同時に 10,000 個の VDA の登録を許可します。	Delivery Controller をサイトに追加するか、新しいサイトを作成することができます。**HKEY_LOCAL_MACHINE\Software\C** レジストリキーを使用して、Delivery Controller に同時に登録できる VDA の数を増やすことができます。詳しくは、Knowledge Center の記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ（CTX117446）」を参照してください。この数を増やすと、Delivery Controller 用により多くの CPU とメモリーリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーが、VDA に送信するための一連の設定と構成を構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA は未登録になります。	Delivery Controller のイベントログでエラーを確認してください。ログで特定の問題が明らかにならない場合は、Broker Service を再起動します。Broker Service を再起動したら、影響を受ける VDA で Desktop Service を再起動し、VDA が正常に登録されたことを確認します。

エラーコード	エラーコード ID	問題	操作（アクション）
[Cloud]: SettingsCreationFailure	208	ブローカーが、VDA に送信するための一連の設定と構成を構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA は未登録になります。	影響を受ける VDA で Desktop Service を再起動し、VDA が正常に登録されたことを確認します。シトリックスサポートに連絡してください。
SendSettingsFailure	204	ブローカーが、設定と構成のデータを VDA に送信しませんでした。ブローカーでデータを収集できるが送信はできないという場合、登録が失敗します。	単一の VDA に限定される場合、VDA の Desktop Service を再起動して再登録を強制し、アプリケーションイベントログで VDA が正常に登録されたことを確認します。表示されたエラーのトラブルシューティングを行います。コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	シトリックスサポートに連絡してください。
DesktopRestart	201	不明なエラーが発生しました。	シトリックスサポートに連絡してください。

エラーコード	エラーコード ID	問題	操作（アクション）
DesktopRemoved	202	不明なエラーが発生しました。	シトリックスサポートに連絡してください。
SessionAuditFailure	205	不明なエラーが発生しました。	シトリックスサポートに連絡してください。
UnknownError	300	不明なエラーが発生しました。	シトリックスサポートに連絡してください。
RegistrationStateMisma	302	不明なエラーが発生しました。	シトリックスサポートに連絡してください。
不明	-	不明なエラーが発生しました。	シトリックスサポートに連絡してください。

SDK および API

October 22, 2021

このリリースでは、複数の SDK および API を使用できます。詳しくは、開発者用のドキュメントを参照してください。そこから以下についてのプログラミングのための情報にアクセスできます:

- Delivery Controller
- Monitor Service OData
- StoreFront

Citrix Group Policy SDK により、グループポリシーの設定およびフィルターを表示して構成できます。PowerShell プロバイダーを使用して、マシン、ユーザー設定、およびフィルターに対応する仮想ドライブを作成します。このプロバイダーは、New-PSDrive に対する拡張として表示されます。Group Policy SDK を使用するには、Studio または XenApp/XenDesktop SDK のいずれかをインストールする必要があります。詳しくは、「グループポリシー SDK」を参照してください。

Delivery Controller SDK

この SDK は、Delivery Controller または Studio と一緒にインストールされる多くの PowerShell スナップインで構成されています。

権限：シェルまたはスクリプトを実行するには、Citrix 管理者の権限が必要です。Controller のローカル管理者グループのメンバーには、XenApp または XenDesktop のインストールに必要な完全な管理権限が自動的に付与されますが、ローカル管理者アカウントを使うのではなく、適切な権限を持つ Citrix 管理者を作成することをお勧めします。Windows Server 2008 R2 を実行している場合、ローカル管理者グループのメンバーとしてではなく、Citrix 管理者としてシェルまたはスクリプトを実行する必要があります。

コマンドレットにアクセスして実行するには:

1. PowerShell のシェルを開きます。Studio を開き、［**PowerShell**］タブを選択して ［**PowerShell** の起動］をクリックします。
2. スクリプト内で SDK コマンドレットを使用するには、PowerShell 実行ポリシーを設定する必要があります。PowerShell 実行ポリシーについて詳しくは、Microsoft 社のドキュメントを参照してください。
3. Windows PowerShell コンソールで **Add-PSSnapin** コマンドレットを使って、必要なスナップインを PowerShell 環境に追加します。

V1 および V2 は、スナップインのバージョンを示します（XenDesktop 5 スナップインは V1、XenDesktop 7 スナップインは V2 です。たとえば、XenDesktop 7 スナップインをインストールするには、コマンド Add-PSSnapin Citrix.ADIdentity.Admin.V2 を実行します）。すべてのコマンドレットをインポートするには、コマンド Add-PSSnapin Citrix.*.Admin.V*を実行します。

スナップインを追加した後、コマンドレットおよび関連ヘルプにアクセスできるようになります。

注: 最新の XenApp および XenDesktop PowerShell コマンドレットヘルプを確認するには、次の手順に従います:

1. PowerShell コンソールから、次のコマンドを実行して Citrix スナップインを追加します: Add –PSSnapin Citrix.*.Admin.V*
2. 「PowerShell Integrated Scripting Environment（ISE）」の手順に従います。

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、string 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。

XenApp および **XenDesktop 7.15 LTSR** の **Citrix VDI** ベストプラクティス

August 24, 2021

Citrix VDI ハンドブックとベストプラクティス

Citrix VDI ハンドブックとベストプラクティス（PDF ダウンロード）

ビジネス環境では、PC の更新、パッチ、アップデートなどのダウンタイム、オフィスの外で作業をする場合などに生産性の低下に悩まされることがあります。アプリケーションとデスクトップの仮想化は、アプリやデスクトップをロ

ーカルデバイスではなくデータセンターで集中管理します。これによって、IT 部門はアプリやデスクトップをオンデマンドで、どのようなデバイスにも、どこにでも配信できます。

以下はデスクトップ仮想化ユーザーのご意見です:

実際の例

「リモートワーカーであるため、ネットワークに VPN 接続して会社のイントラネットにアクセスするたびに苦労していました。また、自宅のブロードバンド接続でのアクセスは遅すぎるため、データはローカルデバイスに保存していました。同僚は同様に作業してウィルスでデータを失ったので、私はラッキーな方です。

気分や天候によっては、アプリケーションやデータをさまざまなエンドポイントにコピーする必要があり、デバイスと場所の変更は困難でした。これが安全な方法ではないのは承知していましたが、柔軟性を重視した結果でした。

仮想デスクトップに移行して以来、必要なデバイスを使用できるようになりました。場所を選ばずに作業ができるようにもなりました。何よりも、データやアプリケーションをすべての個人用デバイスにコピーする必要がなくなりました」

残念なことに、一部の組織ではこれを実現するために苦労することがあります。では、成功する組織と失敗する組織の違いはなんでしょうか。

デスクトップ仮想化やその他のテクノロジ関連プロジェクトで、成功と失敗を分ける要素を比較すると、その差はほんのわずかなことです。

根拠の欠如 - 確固たるビジネス上の根拠がない限り、デスクトップ仮想化は、単にデスクトップを配信する新しい方法にすぎません。ビジネス上の根拠は、プロジェクトチームにとって達成すべき目標となります。

方法論の欠如 - デスクトップ仮想化ソリューションを展開する上で苦労することが多いのは、適切な前提条件を理解も実装もしないで、すぐに実行に移そうとするからです。構造化された方法論は、プロジェクトにつなげることができます。

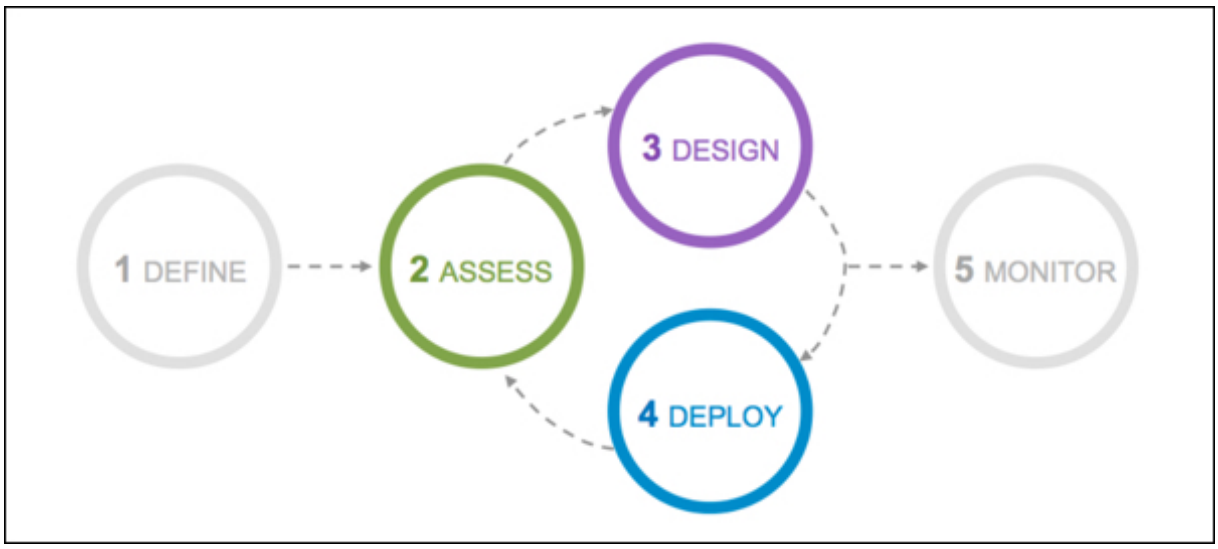
経験の不足 - デスクトップ仮想化プロジェクトに参加する人員の多くが経験不足で、結果的に設計に確信が持てません。事業計画担当者は再検討を始めることになり、プロジェクトが滞ります。

このハンドブックは、時間に追われ、組織上の課題にも悩まされている企業のデスクトップ仮想化に関する懸念を取り除くために、適切で、実現可能かつ効果的なテクノロジーを選択し、課題を解決する方法を提案することを目的としています。

シトリックスが数千のデスクトップ仮想化プロジェクトを成功に導いた方法論、経験、ベストプラクティスをご紹介します。

方法論

Citrix VDI ハンドブックは、Citrix Consulting の方法論をご説明します。これは、数千のデスクトップ仮想化プロジェクトを成功に導いた、実証済みの方法論です。各フェーズには、確認すべき重要な質問、使用すべきツール、成功につながるヒントに関する手順が含まれています。Citrix Consulting の方法論は、5 つのフェーズに分かれています。



1. 定義 – 概括的なプロジェクトロードマップの作成、アクティビティの優先度の設定、ストレージおよびハードウェア要件の見積りによって、デスクトップ仮想化の事例を構築します。
2. 評価 – 主要なビジネスの推進要因を評価し、それに従って作業の取り組みの優先度が設定されます。また、問題の可能性や、プロジェクトのユースケースを特定するために、現在の環境をレビューします。この情報は、シトリックス製品の展開、アップグレード、拡張の方向性を決めるために使用します。
3. 設計 – 評価フェーズで特定された主要なビジネスの推進要因と成功基準を満たすために必要なアーキテクチャを定義します。環境のスケーラビリティ、冗長性、高可用性などのトピックにも対応します。
4. 展開 – 展開フェーズでは、設計フェーズで定義されたようにインフラストラクチャをインストールし、構成します。インフラストラクチャのすべてのコンポーネントに対して、ユーザーが環境にアクセスできるようになる前に、綿密にユニットテストおよび回帰テストを実行する必要があります。
5. 監視 – 稼働環境を維持するために必要なアーキテクチャ上および運用上のプロセスを定義します。

Citrix Consulting の方法論では、プロジェクトの主な段階ごとに評価、設計、展開プロセスを繰り返します。これによって、各段階の完了時に、具体的な形で組織の環境が改善されます。たとえば、優先度の高いユーザーグループは評価、設計、展開フェーズを他のユーザーグループより早いペースで移動できます。

> 注
>
> VDI ハンドブックは、Citrix Consulting の方法論の評価、設計、監視フェーズの内容を提供します。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States