Citrix Virtual Apps and Desktops

Contents

Citrix Virtual Apps and Desktops 7 2003

May 3, 2021

このリリースについて

この Citrix Virtual Apps and Desktops リリースには、新しいバージョンの Windows Virtual Delivery Agent（VDA）といくつかのコアコンポーネントの新しいバージョンが含まれています。次の操作を実行できます:

- サイトをインストールまたはアップグレードする

  このリリースの ISO を使用して、コアコンポーネントと 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

  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、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。

  必ずVDA を 1912 以降にアップグレードするを確認してください。

  VDA をバージョン 7.9 以降からこのバージョンにアップグレードした後は、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。**7.9**（またはそれ以降）の値はデフォルトの機能レベルのままであり、このリリースでも有効です。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。

インストールとアップグレードの手順については、以下を参照してください:

- 新しいサイトを構築する場合は、「インストールと構成」の手順に従います。
- サイトをアップグレードする場合は、「環境のアップグレード」を参照してください。

Citrix Virtual Apps and Desktops 7 2003

> 重要:
>
> Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、その VDA をバージョン 1912 以降にアップグレードすることはできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから新しくインストールする必要があります。
>
> この手順は、Personal vDisk をインストール済みで使用したことがない場合でも適用されます。
>
> ご使用中の環境が影響を受けるかを判断し、必要な手順について知るには、「VDA を 1912 以降にアップグレードする」を参照してください。

最新リリースのホストサポートの変更点

Citrix Virtual Apps and Desktops 7 2003 では、最新リリースは次のホストで VDA（アプリとデスクトップの配信用マシン）をサポートしません：

- Amazon Web Services（AWS 上の VMWare Cloud を含む）
- CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
- Microsoft Azure（Azure Resource Manager および Azure Classic を含む）

サポートする内容：

- 最新リリース（CR）の場合、Citrix Virtual Apps and Desktops 7 は各リリースのシステム要件ドキュメントに記載されたホストおよび仮想化リソースをサポートします。

  たとえば、最新の CR でサポートされているホストは、そのリリースの「システム要件」に記載されています。

- 長期サービスリリース（LTSR）の場合、引き続き対象リリースごとに記載されたホストがサポートされます。一部の LTSR は、CR でのサポートが停止された VDA を 1 つまたは複数のクラウドホストでサポートしています。

  たとえば、Citrix Virtual Apps and Desktops 7 1912 LTSR（およびその累積更新プログラム）はそのリリースの「システム要件」に記載されているホストをサポートします。

推奨事項：

オンプレミス製品ではなく Citrix Cloud で Citrix Virtual Apps and Desktops サービスを使用することをお勧めします。詳しくは、「Citrix Virtual Apps and Desktops のオンプレミスから Citrix Cloud への移行」を参照してください。

引き続きオンプレミスで Citrix Virtual Apps and Desktops 7 CR リリースを使用する場合：

- サポートされていないホストがタスクフローに残ったままになり、Citrix Virtual Apps and Desktops で表示されることがあります。サポート対象外のホストを選択できても選択しないでください。

  > 重要：
  >
  > サポートされていないホストでサイトまたは VDA をインストールするか、バージョン 2003 以降にアップグレードすると、その展開もサポート対象外になります。サポートされていない展開の VDA は、Delivery Controller に登録することはできません。未登録の VDA で、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ことはできません。

- サポートされていないホストでマスターイメージを準備したり、マシンを作成（プロビジョニング）したり、接続を作成したりしないでください。マシンをプロビジョニングする場合、シトリックスツールを使用するかサードパーティツールを使用するかは関係ありません。
- アップグレードするリリースでサポートされているマスターイメージやホストへの接続を使用（または作成して使用）してください。
- サポートされているホスト上でマスターイメージを使用するマスターカタログを作成します。カタログ内のマシン（VDA）は、サポートされているホスト上に存在する必要があります。

- デリバリーグループ（および使用しているアプリケーショングループ）にサポートされているホストのカタログが含まれていることを確認します。

詳しくは、「CTX 270373」を参照してください。

アップグレード：サポートされている **SQL Server** バージョンの変更の影響

サポートされているデータベースのバージョン変更は、Citrix のアップグレードに影響を与えることがあります。

- サイトデータベース：SQL Server 2008 R2、2012、2014 は、サイトデータベースでサポートされなくなりました（これには、監視データベースおよび構成ログデータベースが含まれます）。
- ローカルホストキャッシュデータベース：SQL Server バージョン 2014 は、ローカルホストキャッシュデータベースでサポートされなくなりました。

使用中の Citrix コンポーネントにアップグレードする前に、SQL Server のバージョンのアップグレードが必要なことがあります。詳しくは、「SQL Server のバージョンチェック」を参照してください。

インストールとアップグレード：**Personal vDisk** をインストールおよびアップグレードすることができなくなりました

Personal vDisk（PVD）コンポーネントは、インストールおよびアップグレードすることができなくなりました。

- PVD は、VDA インストーラーのグラフィックインターフェイスに表示されなくなりました。
- コマンドラインで/`baseimage`オプションを追加すると、コマンドが失敗します。
- インストールメディアには、PVD ソフトウェアが含まれなくなりました。

ユーザー個人設定レイヤー機能の使用をお勧めします。

インストールとアップグレード：**Windows Server 2012 R2** で **Controller**、**Studio**、**Director**、**VDA**、ユニバーサルプリントサーバーをサポートすることができなくなりました

Windows Server 2012 R2 マシンで Delivery Controller、Studio、Director、VDA またはユニバーサルプリントサーバーをインストールしたり、アップグレードすることはできなくなりました。サポートされる OS 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。

インストールとアップグレード：**StoreFront** のインストールおよびアップグレード方法の変更

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。同じマシンで StoreFront とその他のコアコンポーネントのインストールを選択することができました。

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。

インストールとアップグレード：インストールメディアで **32** ビット **Studio** インストーラーが利用できなくなりました

Citrix Virtual Apps and Desktops インストールメディアには、32 ビット Studio インストーラーが含まれなくなりました。サポートされる OS については、「システム要件」を参照してください。

インストールとアップグレード：必要な**.NET** バージョンの変更

コンポーネントの前提条件である Microsoft .NET Framework がインストールされていない場合は、自動的に Microsoft .NET Framework 4.8 以降がインストールされるようになりました。これは、以前のリリースよりも新しい.NET バージョンです。システム要件では、どのコンポーネントにこの前提条件が必要かを参照できます。

インストールとアップグレード：セルフサービスパスワードリセットは廃止されました

セルフサービスパスワードリセットコンポーネントは、廃止済みです。

Citrix Scout のデータマスキング

Citrix Scout のデータマスキング機能を使用すると、シトリックスにアップロードする前に診断ファイル内の機密データをマスキングすることができます。詳しくは、「データマスキング」を参照してください。

Virtual Delivery Agent（VDA）2003

マルチセッション OS 対応 Windows VDA およびシングルセッション OS 対応 VDA のバージョン 2003 には、（この記事で前述の VDA のインストールおよびアップグレードの項目に加えて）次の拡張機能が含まれています：

> 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。

MTU Discovery

Citrix のプロトコル Enlightened Data Transport（EDT）に、MTU Discovery 機能が導入されました。MTU Discovery を使用すると、EDT でセッションのペイロードサイズを自動的に判断して設定させることができます。こ

の機能により、ICA セッションは、標準以外の最大伝送ユニット（MTU）または最大セグメントサイズ（MSS）要件を持つネットワークに調整できます。この調整機能によって、パフォーマンスの低下や ICA セッションの確立失敗となる可能性のある、パケットのフラグメンテーションが防止されます。この更新には、Windows 向け Citrix Workspace アプリ 1911 以上が必要です。Citrix Gateway を使用している場合、Citrix ADC ファームウェアの最小バージョンは 13.0.52.24 または 12.1.56.22 です。詳しくは、「EDT MTU Discovery」を参照してください。

新しいプロキシ構成オプションを使用してブラウザーコンテンツリダイレクトのルーティングを強化

VDA のプロキシ設定に構成オプションが追加されました。次のオプションから選択できます:

- 直接または透過型 – VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングして、コンテンツをホストする Web サーバーに直接転送します。
- 明示的なプロキシ（以前使用）– VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングして、指定された Web プロキシに直接転送します。
- PAC ファイル - VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングし、指定された PAC ファイルを検証して決定された Web プロキシに直接転送します。

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。

［操作時は低品質］の強化

［操作時は低品質］機能は、自動画像検出で強化されました。以前の［操作時は低品質］は、損失を前提としたアプローチでした。このアプローチでは、すべての動画は H.264（または H.265）でエンコードされ、次に動きが停止すると徐々に無損失へとシャープ化されます。ただし、無損失のままが望ましい場合もあります。新しい自動画像検出機能は、各フレームに対していくつかの簡単な画像解析を実行します。この機能は、フレームを無損失で送信する、つまり損失を前提とした手順を省略するかどうかを決定します。

損失を前提とした設定に戻すには、VDA でレジストリキーを設定します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

値の名前：BTLLossyThreshold

種類：REG_DWORD

データ：0

マルチストリーム仮想チャネルのストリーム割り当て

以前のリリースでは、マルチストリーム ICA を使用する場合、レジストリ設定を使用して仮想チャネルの割り当てを変更する必要がありました。このリリースには、仮想チャネルを割り当てるためのポリシー設定が含まれています。詳しくは、「マルチストリーム仮想チャネルの割り当て設定」を参照してください。

マルチセッション **OS VDA** で **Electron** ベースのアプリのサポートを強化

Electron ベースのアプリがサポートされるようになりました。Electron はデスクトップ GUI アプリケーション開発用のオープンソースフレームワークです。たとえば、Microsoft Teams や Slack などです。

アプリケーションの起動前にプリンターの作成を待機する

Citrix Virtual Apps で、プリンターの作成を待機する機能が利用できるようになりました。Delivery Controller 上で実行されている PowerShell コマンドレットを使用すると、アプリが起動する前に、すべてのプリンターが作成されるように指定することができます。詳しくは、「プリンターの自動作成を待機する」を参照してください。

Citrix セッションとローカルエンドポイント間でファイルをドラッグアンドドロップ（評価専用）

Citrix セッションとローカルエンドポイント間でのファイルのドラッグアンドドロップ機能は、評価専用で利用できます。ファイル、ファイルのグループ、ディレクトリ、ディレクトリのグループ、またはファイルやディレクトリの組み合わせを、セッションの同じクライアントとの間でドラッグアンドドロップできます。この機能は、デスクトップセッションまたはシームレスアプリに適用できます。これにはデスクトップ、Explorer ウィンドウ、一部のアプリケーションが含まれます。この機能は、すべてのアプリケーションをサポートしているわけではありません。たとえば、圧縮（zip 形式）フォルダーからドラッグすることはできますが、このフォルダー内にドラッグすることはできません。

> 重要：
>
> この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。この機能は評価専用で、デフォルトで無効です。

既知の制限：

- クライアントデスクトップからデスクトップセッション内の Firefox や Internet Explorer のブラウザーウィンドウにファイルをドラッグすることはできません。
- 圧縮されたフォルダー、アプリケーションショートカット、シームレスアプリケーションからクライアントデスクトップへのメッセージにドラッグアンドドロップしたり、クライアントから急いでドラッグされた場合にシームレス Outlook メッセージにドラッグアンドドロップしたりすることはできません。

ドラッグアンドドロップを有効にするには、ホストで次のレジストリ設定を追加します：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CtxDNDSvc\

値の名前：Enabled

種類：REG_DWORD

値：0 以外

このレジストリ値を有効にし、必要な Citrix Workspace アプリのバージョンを使用している場合、以降のセッションログイン後にドラッグアンドドロップが有効になります。

損失耐性モード

> 重要:
>
> この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。利用可能になった際、VDA のこのバージョンでサポートされます。

損失耐性モードは、新しい透過型プロトコルを使用して劣悪なネットワーク環境でユーザーエクスペリエンスを向上させます。詳しくは、「損失耐性モード」を参照してください。

Citrix ライセンスサーバー 11.16.3

Citrix ライセンスサーバー 11.16.3 には、新機能、解決された問題、および既知の問題があります。

Citrix フェデレーション認証サービス 2003

Citrix フェデレーション認証サービス（FAS）2003 には、新機能が含まれます。

関連コンポーネント

関連コンポーネントのドキュメントについては、以下を参照してください:

- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- ライセンス
- Linux Virtual Delivery Agent
- Profile Management
- Citrix Provisioning
- Citrix SCOM Management Pack
- セルフサービスパスワードリセット
- Session Recording
- StoreFront
- Workspace Environment Management

詳細情報

- 新しいお知らせ内容や廃止バージョンのアップデートについては、随時「廃止」を参照してください。
- 2018 年に導入された製品名およびバージョン番号の変更について詳しくは、「新しい名前と番号」を参照してください。

Citrix Virtual Apps and Desktops 7 2003

May 3, 2021

このリリースについて

この Citrix Virtual Apps and Desktops リリースには、新しいバージョンの Windows Virtual Delivery Agent（VDA）といくつかのコアコンポーネントの新しいバージョンが含まれています。次の操作を実行できます:

- サイトをインストールまたはアップグレードする

  このリリースの ISO を使用して、コアコンポーネントと 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

  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、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。

  必ずVDA を 1912 以降にアップグレードするを確認してください。

  VDA をバージョン 7.9 以降からこのバージョンにアップグレードした後は、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。**7.9**（またはそれ以降）の値はデフォルトの機能レベルのままであり、このリリースでも有効です。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。

インストールとアップグレードの手順については、以下を参照してください:

- 新しいサイトを構築する場合は、「インストールと構成」の手順に従います。
- サイトをアップグレードする場合は、「環境のアップグレード」を参照してください。

Citrix Virtual Apps and Desktops 7 2003

> 重要:
>
> Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、その VDA をバージョン 1912 以降にアップグレードすることはできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから新しくインストールする必要があります。
>
> この手順は、Personal vDisk をインストール済みで使用したことがない場合でも適用されます。
>
> ご使用中の環境が影響を受けるかを判断し、必要な手順について知るには、「VDA を 1912 以降にアップグレードする」を参照してください。

最新リリースのホストサポートの変更点

Citrix Virtual Apps and Desktops 7 2003 では、最新リリースは次のホストで VDA（アプリとデスクトップの配信用マシン）をサポートしません：

- Amazon Web Services（AWS 上の VMWare Cloud を含む）
- CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
- Microsoft Azure（Azure Resource Manager および Azure Classic を含む）

サポートする内容：

- 最新リリース（CR）の場合、Citrix Virtual Apps and Desktops 7 は各リリースのシステム要件ドキュメントに記載されたホストおよび仮想化リソースをサポートします。

  たとえば、最新の CR でサポートされているホストは、そのリリースの「システム要件」に記載されています。

- 長期サービスリリース（LTSR）の場合、引き続き対象リリースごとに記載されたホストがサポートされます。一部の LTSR は、CR でのサポートが停止された VDA を 1 つまたは複数のクラウドホストでサポートしています。

  たとえば、Citrix Virtual Apps and Desktops 7 1912 LTSR（およびその累積更新プログラム）はそのリリースの「システム要件」に記載されているホストをサポートします。

推奨事項：

オンプレミス製品ではなく Citrix Cloud で Citrix Virtual Apps and Desktops サービスを使用することをお勧めします。詳しくは、「Citrix Virtual Apps and Desktops のオンプレミスから Citrix Cloud への移行」を参照してください。

引き続きオンプレミスで Citrix Virtual Apps and Desktops 7 CR リリースを使用する場合：

- サポートされていないホストがタスクフローに残ったままになり、Citrix Virtual Apps and Desktops で表示されることがあります。サポート対象外のホストを選択できても選択しないでください。

  > 重要：
  >
  > サポートされていないホストでサイトまたは VDA をインストールするか、バージョン 2003 以降にアップグレードすると、その展開もサポート対象外になります。サポートされていない展開の VDA は、Delivery Controller に登録することはできません。未登録の VDA で、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ことはできません。

- サポートされていないホストでマスターイメージを準備したり、マシンを作成（プロビジョニング）したり、接続を作成したりしないでください。マシンをプロビジョニングする場合、シトリックスツールを使用するかサードパーティツールを使用するかは関係ありません。
- アップグレードするリリースでサポートされているマスターイメージやホストへの接続を使用（または作成して使用）してください。
- サポートされているホスト上でマスターイメージを使用するマスターカタログを作成します。カタログ内のマシン（VDA）は、サポートされているホスト上に存在する必要があります。

- デリバリーグループ（および使用しているアプリケーショングループ）にサポートされているホストのカタログが含まれていることを確認します。

詳しくは、「CTX 270373」を参照してください。

アップグレード：サポートされている **SQL Server** バージョンの変更の影響

サポートされているデータベースのバージョン変更は、Citrix のアップグレードに影響を与えることがあります。

- サイトデータベース：SQL Server 2008 R2、2012、2014 は、サイトデータベースでサポートされなくなりました（これには、監視データベースおよび構成ログデータベースが含まれます）。
- ローカルホストキャッシュデータベース：SQL Server バージョン 2014 は、ローカルホストキャッシュデータベースでサポートされなくなりました。

使用中の Citrix コンポーネントにアップグレードする前に、SQL Server のバージョンのアップグレードが必要なことがあります。詳しくは、「SQL Server のバージョンチェック」を参照してください。

インストールとアップグレード：**Personal vDisk** をインストールおよびアップグレードすることができなくなりました

Personal vDisk（PVD）コンポーネントは、インストールおよびアップグレードすることができなくなりました。

- PVD は、VDA インストーラーのグラフィックインターフェイスに表示されなくなりました。
- コマンドラインで/`baseimage`オプションを追加すると、コマンドが失敗します。
- インストールメディアには、PVD ソフトウェアが含まれなくなりました。

ユーザー個人設定レイヤー機能の使用をお勧めします。

インストールとアップグレード：**Windows Server 2012 R2** で **Controller**、**Studio**、**Director**、**VDA**、ユニバーサルプリントサーバーをサポートすることができなくなりました

Windows Server 2012 R2 マシンで Delivery Controller、Studio、Director、VDA またはユニバーサルプリントサーバーをインストールしたり、アップグレードすることはできなくなりました。サポートされる OS 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。

インストールとアップグレード：**StoreFront** のインストールおよびアップグレード方法の変更

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。同じマシンで StoreFront とその他のコアコンポーネントのインストールを選択することができました。

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。

インストールとアップグレード：インストールメディアで **32** ビット **Studio** インストーラーが利用できなくなりました

Citrix Virtual Apps and Desktops インストールメディアには、32 ビット Studio インストーラーが含まれなくなりました。サポートされる OS については、「システム要件」を参照してください。

インストールとアップグレード：必要な**.NET** バージョンの変更

コンポーネントの前提条件である Microsoft .NET Framework がインストールされていない場合は、自動的に Microsoft .NET Framework 4.8 以降がインストールされるようになりました。これは、以前のリリースよりも新しい.NET バージョンです。システム要件では、どのコンポーネントにこの前提条件が必要かを参照できます。

インストールとアップグレード：セルフサービスパスワードリセットは廃止されました

セルフサービスパスワードリセットコンポーネントは、廃止済みです。

Citrix Scout のデータマスキング

Citrix Scout のデータマスキング機能を使用すると、シトリックスにアップロードする前に診断ファイル内の機密データをマスキングすることができます。詳しくは、「データマスキング」を参照してください。

Virtual Delivery Agent（VDA）2003

マルチセッション OS 対応 Windows VDA およびシングルセッション OS 対応 VDA のバージョン 2003 には、（この記事で前述の VDA のインストールおよびアップグレードの項目に加えて）次の拡張機能が含まれています：

> 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。

MTU Discovery

Citrix のプロトコル Enlightened Data Transport（EDT）に、MTU Discovery 機能が導入されました。MTU Discovery を使用すると、EDT でセッションのペイロードサイズを自動的に判断して設定させることができます。こ

の機能により、ICA セッションは、標準以外の最大伝送ユニット（MTU）または最大セグメントサイズ（MSS）要件を持つネットワークに調整できます。この調整機能によって、パフォーマンスの低下や ICA セッションの確立失敗となる可能性のある、パケットのフラグメンテーションが防止されます。この更新には、Windows 向け Citrix Workspace アプリ 1911 以上が必要です。Citrix Gateway を使用している場合、Citrix ADC ファームウェアの最小バージョンは 13.0.52.24 または 12.1.56.22 です。詳しくは、「EDT MTU Discovery」を参照してください。

新しいプロキシ構成オプションを使用してブラウザーコンテンツリダイレクトのルーティングを強化

VDA のプロキシ設定に構成オプションが追加されました。次のオプションから選択できます:

- 直接または透過型 – VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングして、コンテンツをホストする Web サーバーに直接転送します。
- 明示的なプロキシ（以前使用）– VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングして、指定された Web プロキシに直接転送します。
- PAC ファイル - VDA 経由でブラウザーコンテンツリダイレクトのトラフィックをルーティングし、指定された PAC ファイルを検証して決定された Web プロキシに直接転送します。

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。

［操作時は低品質］の強化

［操作時は低品質］機能は、自動画像検出で強化されました。以前の［操作時は低品質］は、損失を前提としたアプローチでした。このアプローチでは、すべての動画は H.264（または H.265）でエンコードされ、次に動きが停止すると徐々に無損失へとシャープ化されます。ただし、無損失のままが望ましい場合もあります。新しい自動画像検出機能は、各フレームに対していくつかの簡単な画像解析を実行します。この機能は、フレームを無損失で送信する、つまり損失を前提とした手順を省略するかどうかを決定します。

損失を前提とした設定に戻すには、VDA でレジストリキーを設定します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

値の名前：BTLLossyThreshold

種類：REG_DWORD

データ：0

マルチストリーム仮想チャネルのストリーム割り当て

以前のリリースでは、マルチストリーム ICA を使用する場合、レジストリ設定を使用して仮想チャネルの割り当てを変更する必要がありました。このリリースには、仮想チャネルを割り当てるためのポリシー設定が含まれています。詳しくは、「マルチストリーム仮想チャネルの割り当て設定」を参照してください。

マルチセッション **OS VDA** で **Electron** ベースのアプリのサポートを強化

Electron ベースのアプリがサポートされるようになりました。Electron はデスクトップ GUI アプリケーション開発用のオープンソースフレームワークです。たとえば、Microsoft Teams や Slack などです。

アプリケーションの起動前にプリンターの作成を待機する

Citrix Virtual Apps で、プリンターの作成を待機する機能が利用できるようになりました。Delivery Controller 上で実行されている PowerShell コマンドレットを使用すると、アプリが起動する前に、すべてのプリンターが作成されるように指定することができます。詳しくは、「プリンターの自動作成を待機する」を参照してください。

Citrix セッションとローカルエンドポイント間でファイルをドラッグアンドドロップ（評価専用）

Citrix セッションとローカルエンドポイント間でのファイルのドラッグアンドドロップ機能は、評価専用で利用できます。ファイル、ファイルのグループ、ディレクトリ、ディレクトリのグループ、またはファイルやディレクトリの組み合わせを、セッションの同じクライアントとの間でドラッグアンドドロップできます。この機能は、デスクトップセッションまたはシームレスアプリに適用できます。これにはデスクトップ、Explorer ウィンドウ、一部のアプリケーションが含まれます。この機能は、すべてのアプリケーションをサポートしているわけではありません。たとえば、圧縮（zip 形式）フォルダーからドラッグすることはできますが、このフォルダー内にドラッグすることはできません。

> 重要：
>
> この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。この機能は評価専用で、デフォルトで無効です。

既知の制限：

- クライアントデスクトップからデスクトップセッション内の Firefox や Internet Explorer のブラウザーウィンドウにファイルをドラッグすることはできません。
- 圧縮されたフォルダー、アプリケーションショートカット、シームレスアプリケーションからクライアントデスクトップへのメッセージにドラッグアンドドロップしたり、クライアントから急いでドラッグされた場合にシームレス Outlook メッセージにドラッグアンドドロップしたりすることはできません。

ドラッグアンドドロップを有効にするには、ホストで次のレジストリ設定を追加します：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CtxDNDSvc\

値の名前：Enabled

種類：REG_DWORD

値：0 以外

このレジストリ値を有効にし、必要な Citrix Workspace アプリのバージョンを使用している場合、以降のセッションログイン後にドラッグアンドドロップが有効になります。

損失耐性モード

> 重要:
>
> この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。利用可能になった際、VDA のこのバージョンでサポートされます。

損失耐性モードは、新しい透過型プロトコルを使用して劣悪なネットワーク環境でユーザーエクスペリエンスを向上させます。詳しくは、「損失耐性モード」を参照してください。

Citrix ライセンスサーバー 11.16.3

Citrix ライセンスサーバー 11.16.3 には、新機能、解決された問題、および既知の問題があります。

Citrix フェデレーション認証サービス 2003

Citrix フェデレーション認証サービス（FAS）2003 には、新機能が含まれます。

関連コンポーネント

関連コンポーネントのドキュメントについては、以下を参照してください:

- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- ライセンス
- Linux Virtual Delivery Agent
- Profile Management
- Citrix Provisioning
- Citrix SCOM Management Pack
- セルフサービスパスワードリセット
- Session Recording
- StoreFront
- Workspace Environment Management

詳細情報

- 新しいお知らせ内容や廃止バージョンのアップデートについては、随時「廃止」を参照してください。
- 2018 年に導入された製品名およびバージョン番号の変更について詳しくは、「新しい名前と番号」を参照してください。

解決された問題

April 26, 2021

Citrix Virtual Apps and Desktops 7 1912 以降、次の問題が解決されています:

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。

  ログオフして再度ログオンした場合、または異なるユーザーがログオンした場合、Citrix Director は HDX insight データを正常に表示します。[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。

  Citrix Director コンソールのアプリケーションインスタンスで ［デリバリーグループ］および ［公開名］で絞り込んだユーザーに関してこの問題が発生します。[CVADHELP-12601]

- Delivery Controller の電源がオフになると、Citrix Director は Delivery Controller の誤った状態を表示します。その結果、誤ったアラートが Citrix Director の ［インフラストラクチャ］タブに表示されます。[CVADHELP-13835]

Citrix Provisioning

Citrix Provisioning 2003 のドキュメントでは、このリリースでの更新に関する具体的な情報を提供します。

Citrix Studio

- 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。[CVADHELP-9214]

- 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]

Delivery Controller

- Microsoft Azure Resource Manager が大量の要求を受信すると、Machine Creation Services（MCS）は要求された操作を続行する前に 10 分間待機することがあります。[CVADHELP-9976]
- Azure Managed Disks を使用してマシンカタログを作成する、マシンを追加する、マシンの電源をオンにする、またはマシンを再起動するなどの操作を試みると失敗することがあります。[CVADHELP-10108]
- Citrix Broker Service がイベント ID 1000 で予期せず終了することがあります。この問題は、LicPollEng.dll モジュールに障害がある場合に発生します。[CVADHELP-12019]
- 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]
- ユーザーセッションのアイドル時間が、Citrix Director で誤って **N/A** として表示されることがあります。[CVADHELP-13099]
- 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]
- PowerShell コマンド`Get-ApplibAppvPackage`を使用した場合、コマンドが`AppVApplications`を返されたプロパティとして認識しないことがあります。[CVADHELP-13296]
- 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。[CVADHELP-13393]

- 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]
- 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]

HDX RealTime Optimization Pack

HDX RealTime Optimization Pack 2003 のドキュメントでは、このリリースでの更新に関する具体的な情報を提供します。

ライセンス

ライセンス管理 2003 のドキュメントでは、このリリースでの更新に関する具体的な情報を提供します。

Linux VDA

Linux VDA 2003 のドキュメントでは、このリリースでの更新に関する具体的な情報を提供します。

Profile Management

Profile Management 2003 のドキュメントでは、このリリースでの更新に関する具体的な情報を提供します。

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]

シングルセッション **OS** 対応 **VDA**

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]

セッション/接続

- 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。[CVADHELP-11195]
- 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。[CVADHELP-11245]
- 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。

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

  名前：PacketIntegrityChecks

  種類：DWORD

  値：1

  [CVADHELP-13063]
- VDA が自動的に再起動すると応答しなくなることがあります。この問題は、winlogon サービスが termsvc プロセスで待機中に発生します。待機時間は、tdica.sys からのガベージコレクションスレッドによってずっと続きます。この問題はリモート PC が構成されている VDA で発生します。[CVADHELP-13228]
- 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]
- セッ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。

  デスクトップを起動できません。

  [CVADHELP-13320]
- Citrix Director 経由でリモートアシスタンスのユーザーセッションをシャドウしようとすると、セッションが切断されることがあります。Director からシャドウ操作を閉じるか終了しないと、セッションを再接続できません。この問題は、VDA バージョン 7.6.8000 で発生します。[CVADHELP-13654]

スマートカード

- 高速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、PIN 入力メッセージが 2 回表示されることがあります。[CVADHELP-12949]

システムの例外

- 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]

ユーザーエクスペリエンス

- 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。[CVADHELP-11841]

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]

マルチセッション **OS** 対応 **VDA**

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]

セッション**/**接続

- ［ブラウザーコンテンツリダイレクト］ポリシーが有効な場合、［新しいタブで開く］オプションが機能しないことがあります。この問題は、Windows 向けまたは Linux 向け Citrix Workspace アプリが接続している Microsoft Windows を実行している VDA で発生します。[CVADHELP-12800]

- 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]
- 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。

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

  名前：PacketIntegrityChecks

  種類：DWORD

  値：1

  [CVADHELP-13063]
- VDA が自動的に再起動すると応答しなくなることがあります。この問題は、winlogon サービスが termsvc プロセスで待機中に発生します。待機時間は、tdica.sys からのガベージコレクションスレッドによってずっと続きます。この問題はリモート PC が構成されている VDA で発生します。[CVADHELP-13228]
- セッ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。

  デスクトップを起動できません。

  [CVADHELP-13320]
- セッションに再接続しようとすると、デスクトップは読み込みに失敗し、灰色のウィンドウが表示される場合があります。この問題は、Microsoft Windows Server 2019 上で実行されている VDA バージョン 1909 で発生します。[CVADHELP-13376]
- 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]
- VDA をバージョン 1909.1 にアップグレードすると、`RemoteScan`のようなサードパーティアプリケーションがドキュメントをスキャンすることができなくなり応答しなくなることがあります。この問題は、twnhook.dll モジュールに障害がある場合に発生します。[CVADHELP-13937]
- 仮想キーボードが自動的に公開アプリケーション内に表示されないことがあります。[CVADHELP-14012]

スマートカード

- 高速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、PIN 入力メッセージが 2 回表示されることがあります。[CVADHELP-12949]

システムの例外

- 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]

既知の問題

April 24, 2021

Citrix Virtual Apps and Desktops 7 2003 リリースでは、次の問題が確認されています。個別に文書化されているコンポーネントおよび機能には、それぞれ既知の問題に関する記事があります。

レジストリエントリの変更を伴う回避策については、次の点に注意してください:

> 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。

インストールとアップグレード

- Citrix Virtual Apps and Desktops Metainstaller を実行する場合、［診断情報の収集］を選択せずに ［診断］ページで ［接続］をクリックすると、［**Citrix Insight Services** に接続します］ダイアログボックスを閉じた後に ［次へ］ボタンが無効になり、次のページに移動できません。［次へ］ボタンを再度有効にするには、［診断情報を収集する］を選択してすぐに選択解除します。[XAXDINST-572]
- Studio を XenApp および XenDesktop 7.15 LTSR（7.15 Studio）から Citrix Virtual Apps and Desktops 7 1912 LTSR（1912 Studio）にアップグレードし、1912 Studio をアンインストールして 7.15 Studio を再インストールすると、次のエラーで Studio を起動できません。「Cannot load windows PowerShell snap-in PvsPsSnapIn error」この問題を解決するには、7 15 Studio を再インストールする前に、`C:\Program Files\Citrix\PowerShell SDK`から PvsPsSnapIn.dll を手動で削除します。[XAXDINST-610]
- `XenDesktopServerSetup.exe`コマンドの有効なオプション一覧を要求すると、`/no_webstudio`オプションが表示されます。これは内部使用向けのオプションです。使用しないでください。

一般

- 保護されたアプリをお気に入りに追加しようとすると、次のメッセージが表示される場合があります。「現在、アプリケーションを使用できません...」［**OK**］をクリックすると、次のメッセージが表示されます「アプリケ

ーションを追加できません。」お気に入り画面に切り替えた後、保護されたアプリはここに一覧表示されますが、お気に入りから削除することはできません。[WSP-5497]

- Chrome ブラウザーでブラウザーコンテンツリダイレクトが有効になっている場合、新しいタブを開くリンクをクリックするとタブが開かないことがあります。この問題を回避するには、**Pop-ups blocked** メッセージで **Always allow pop-ups and redirects** を選択します。[HDX-23950]
- Skype for Business Web アプリケーションプラグインをインストールすると、Web カメラが列挙されないことや、Firefox 上の会議ページが自動的に更新されないことがあります。[HDX-13288]
- StoreFront からアプリケーションを起動したとき、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]
- 新しいセッションに接続してから切断し、同じセッションに再接続すると、デスクトップのアイコンがちらついて表示されることがあります。この問題を回避するには、ユーザープロファイルをリセットしてセッションからログオフし、再びログオンします。[HDX-15926、UPM-1362]
- Windows 10 1809 LTSC を使用している場合、VCLibs 依存関係のインストールに失敗します。[HDX-16754]
- ユーザーが既にホストでフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。この問題を回避するには、別の UI 要素を選択してからコンボボックスを選択します。[HDX-21671]
- ローカルアプリアクセスを有効にしました。Windows 2012 R2 VDA セッションを開始し、セッションを切断して再接続し、ローカルアプリケーションを開始して最大化すると、VDA タスクバーがアプリケーションを省略することがあります。[HDX-21913]
- メタインストーラーを使用して既存の VDA インストールを変更すると、「Enable MCSIO write cache for storage optimization」オプションを選択することで MCSIO ストレージ最適化をインストールに追加できます。インストールは MCSIO ドライバーなしで続行します。[HDX-21754]
- ネットワークで IPv4 および IPv6 アドレス指定の両方が構成されている場合、デリバリーグループが IPv4 アドレスフィルタリングのみを許可するように構成されたブローカーアクセスポリシー規則を使用している場合、デリバリーグループ内のリソースにアクセスできないことがあります。すべてのリソースフィルタリングが正しく動作するようにするには、クライアントの IPv4 および IPv6 アドレスの両方を含めるようにブローカーアクセスポリシー規則を構成します。[WADA-7776]

  たとえば、「StoreFront へのダイレクト」および「Citrix Gateway」アクセスを通じて IPv4 および IPv6 アドレスを許可する規則を設定するには、次のような PowerShell を使用します:

```
1 Set-BrokerAccessPolicyRule -Name "Apps_Direct" -
    IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
    10.0.0.1","2001::3")
2 Set-BrokerAccessPolicyRule -Name "Apps_AG" -
    IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
```



```
        10.0.0.1","2001::3")
```

規則を確認するには、次のような PowerShell を使用します:

```
Get-BrokerAccessPolicyRule -Name "Apps_Direct" | Select Name,
    IncludedClientIPFilterEnabled,IncludedClientIPs
```

規則が IPv4 および IPv6 アドレスに対して正しく設定されている場合、次の値が返されます:

```
Name         IncludedClientIPFilterEnabled IncludedClientIPs
--                  ---------------------------- ----------------
Apps_Direct                           True {
 10.0.0.1/32, 2001::3/128 }
```

Studio

- 構成ログを削除すると、Citrix Studio コンソールが予期せず終了することがあります。[STUD-9138]

Director

- VDA バージョン 2003 および 2006 の ［マシンの詳細］ページでマシンの使用履歴を表示しようとすると、(Citrix Studio で ［プロセスの監視を有効にします］を ［許可］に設定した後でも）次のエラー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。

  回避策として、レジストリ値を`HKLM\Software\Citrix\GroupPolicy\SaveRsopToFile`から **1** に設定して、Citrix Director でポリシー監視データを表示してください。[DIR-11794]

- Microsoft Edge 44 および Firefox 68 ESR の Web ブラウザーで［Citrix Director］>［マシン詳細］の［コンソール］リンクをクリックしても、マシンコンソールが起動しません。[DIR-8160]

- 過去のリリースから Director 7 1903 以降にアップグレードし、ブラウザーのキャッシュをクリアしていない（［キャッシュを無効にする］チェックボックスがオンになっていない）場合、以前に作成したカスタムレポートが失われ、Director のカスタムレポートタブに「予期されないサーバーエラー」が表示されます。過去のバージョンと最新のバージョンとで Director の UI デザインが異なる場合にこの問題が発生することがあります。キャッシュを無効にしてハードリフレッシュを実行した後に古いカスタムレポートを確認し、次に新しいカスタムレポートを作成して確認してください。[DIR-7634]

グラフィック

- ［ドラッグ中にウィンドウの内容を表示する］ポリシーを ［禁止］に設定すると、ESXi および Hyper-V で機能しません。[HDX-22002]

- Theora 圧縮形式で 64 ビット Web カメラを使用してビデオプレビューを起動すると、セッションがクラッシュすることがあります。[HDX-21443]
- Skype ユニバーサル Windows アプリ（UWA）が黒い背景で起動します。場合によっては、この背景がクライアントの画面全体を占めることがあります。[HDX-22088]
- 別のアプリケーションにフォーカスがあるときに、アプリケーションがバックグラウンドで起動することがあります。その結果、ローカルウィンドウの順序が変更されます。[HDX-21569]
- XenDesktop セッションを切断した後、XenCenter コンソールに空白の画面が表示されることがあります。この問題を回避するには、XenCenter コンソールに CTLR+ALT+DEL を送信して、コンソール画面を表示します。[HDX-17261]
- DPI がクライアント上で変更され、セッションが再接続されたときに、Windows マルチセッション OS 2016 または 2019 で実行されているセッションで DPI が一致しないことがあります。この問題を解決するには、DPI に応じてセッションウィンドウのサイズを変更します。[HDX-17313]
- これらの問題は、ADM ハードウェアエンコーディングに関連します。[HDX-20476]:
  - Windows 向け Citrix Workspace アプリを使用すると、ピクセル化が発生する場合があります。回避策として、Windows 向け Citrix Workspace アプリがインストールされているクライアントで次のレジストリ設定を行います:

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRenc
    （32 ビット）

    HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\M
    （64 ビット）

    値の名前：MaxNumRefFrames

    種類：DWORD

    値：5
  - 4k 解像度を使用すると、最適なパフォーマンスが得られないことがあります。この問題により、フレームレートは 1 秒あたり 7〜10 フレームのみになります。また、エンコーディングの時間が長くなります。
  - 選択的 H.264 グラフィックモードを使用している場合、ビデオの最初の 2〜5 秒間でビデオが途切れることがあります。RapidFire SDK は、このユースケースを想定して設計されていません。

印刷

- 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、「CTX213540」を参照してください。[HDX-5043、335153]

- 印刷ダイアログウィンドウで、通常使うプリンターが正しくマークされていないことがあります。この問題は、通常使うプリンターに送信される印刷ジョブには影響しません。[HDX-12755]

App-V

- Delivery Controller を Citrix Virtual Apps and Desktops 7 2003 にアップグレードすると、App-V アプリケーションに関連した以前の Delivery Controller の構成が削除できない場合、別途クリーンアップ手順が実行されていない限りアップグレードに失敗します。この問題が発生した場合は、クリーンアップを実行し問題が解決されたことを確認するための手順についてシトリックスサポートに連絡してください。[APPV-274]
- 100 を超えるアプリケーションを単一のデリバリーグループで公開する場合、App-V アプリケーションの起動に失敗する場合があります。この制限を増やすには、適切なバインド要素で MaxReceivedMessageSize プロパティを使用して、最大受信可能メッセージサイズを増やします。Delivery Controller または VDA 上の Broker Agent の構成でこれを行います。[APPV -11]

サードパーティの問題

- Chrome は、Web ページ関連のツールバー、タブ、メニュー、ボタンに対してのみ UI オートメーションをサポートします。Chrome のこの問題によって、タッチデバイスの Chrome ブラウザーでは自動キーボード表示機能が動作しない場合があります。この問題を回避するには、`chrome --force-renderer-accessibility`を実行するか新しいブラウザータブを開いて`chrome://accessibility`を入力し、特定のページまたは全ページでネイティブの **Accessibility API** を有効にします。さらに、シームレスアプリの公開時に、Chrome で`--force-renderer-accessibility`スイッチを公開できます。[HDX-20858]
- Microsoft Windows 10 バージョン 1809 の問題により、Surface Pro と Surface Book のペンを使用すると、若干動作が不安定になることがあります。[HDX-17649]
- Enlightened Data Transport(EDT)使用時に Azure 上で実行されている VDA がフリーズし、セッションの再接続が必要になることがあります。回避策としては、Azure 環境で、edtMSS=1350 と OutbufLength=1350 を設定します。詳しくは、「CTX231821」を参照してください。[HDX-12913]
- Web ブラウザーコンテンツのリダイレクトでは、YouTube HTML5 ビデオプレーヤーを使用して YouTube 動画を開始すると、全画面モードが動作しないことがあります。ビデオの右下隅にあるアイコンをクリックすると、ビデオのサイズが変更されず、黒い背景がページの全領域に残されます。回避策として、全画面ボタンをクリックし、シアターモードを選択します。[HDX-11294]

廃止

April 27, 2021

この記事の告知は、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。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。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」を参照してください。長期サービスリリース（LTSR）サービスオプションについて詳しくは、「https://support.citrix.com/article/CTX205549」を参照してください。

廃止と削除

廃止または削除されるプラットフォーム、Citrix 製品、機能を以下の表に示します。

廃止されたアイテムはすぐには削除されません。これらの項目は Citrix Virtual Apps and Desktops 7 2003 で引き続きサポートされますが、将来のリリースでは削除されます。

削除された項目は、Citrix Virtual Apps and Desktops で削除されたか、サポートされなくなりました。太字はこのリリースでの変更を示します。

項目	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（Windows ライセンスサーバー 11.16.3 ビルド 30000）。	**2003**		Citrix Licensing Manager を使用します。
Azure および AWS パブリッククラウド（AWS 上の VMware Cloud を含む）の接続。	**2003**	**2003**	Citrix Cloud で Virtual Apps and Desktops サービスを使用することを検討してください。
Windows 10 バージョン 1709 以前での Citrix Indirect Display Driver（IDD）グラフィックアダプターのサポート。	**2003**	**2003**	Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。

項目	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
GRID 9 以前のディスプレイドライバーを使用した NVIDIA GPU（NVENC）によるハードウェアエンコーディング。	**2003**	**2003**	Citrix Virtual Apps and Desktops 7 2003 以降の VDA で GRID 10 ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。
セルフサービスパスワードリセット（SSPR）機能。	**2003**		
Citrix SCOM Management Pack for XenApp and XenDesktop、Provisioning Services、および StoreFront。監視することができる製品のバージョンについては、「Citrix SCOM Management Pack ドキュメント」を参照してください。	1912		Director を使用して、展開を監視および管理します。SCOM の EOL と新しい選択肢について詳しくは、「https://support.citrix.com/article/CTX266943」を参照してください。
Microsoft .NET Framework の 4.8 より前のバージョンが VDA およびコアサーバーコンポーネントでサポート。Delivery Controller、Studio、Director、StoreFront を含みます。	1912	**2003**	.NET Framework バージョン 4.8 にアップグレードします。
Windows Server 2012 R2 の VDA。	1912	**2003**	サポートされているオペレーティングシステムに VDA をインストールします。

項目	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 Virtual Apps and Desktops プレミアムエディションの AppDNA アプリケーション移行コンポーネント。	1909	**2003**	
32 ビット（x86）マシンに Studio をインストールします。	1909	**2003**	サポートされている x64 オペレーティングシステムにインストールします。
シームレスアプリケーションでの Excel フックのサポート。これは、Microsoft Excel 2010 のブックごとに個別のタスクバーアイコンを作成するために使用されました。	1909	1909	
Windows Server 2012 R2（Service Pack を含む）上のコアサーバーコンポーネント。Delivery Controller、Studio、Director を含みます。	1906	**2003**	サポートされているより新しいオペレーティングシステムにインストールします。
Microsoft SQL Server versions 2008 R2、2012、2014（すべての Service Pack とエディションを含みます）で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をサポート。	1906	**2003**	サポートされているバージョンの Microsoft SQL Server にデータベースをインストールします。

項目	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
x86 プラットフォームにおける Windows 10 での VDA のサポート。	1906	1909 *	サポートされる x64 オペレーティングシステムに VDA をインストールします。* この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSR で引き続きサポートされています。
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	1906	
StoreFront 内で次の販売終了製品から Delivery Controller オプションを削除: VDI-in-a-Box および XenMobile（9.0 以前）。	1903	1903	
Red Hat Enterprise Linux/CentOS 7.5 での Linux VDA のサポート。	1903	1903	Red Hat Enterprise Linux のそれ以降のバージョンに Linux VDA をインストールします。
StoreFront でのデスクトップアプライアンスサイト上のデスクトップへのアクセスのサポート	1811	1912	ドメインに参加しない場合は、Desktop Lockを使用します。
Framehawk ディスプレイリモートテクノロジのサポート	1811	1903	Thinwireでアダプティブトランスポートを有効にしてください。

項目	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
すべての Citrix Virtual Apps and Desktops（および、XenApp および XenDesktop）バージョンでの Citrix Smart Scale 機能のサポート。この機能は、2019 年 5 月 31 日に製品終了となります。	1808	1906	強化された電源管理機能を Citrix Cloud で利用するには、Virtual Apps and Desktops サービスを使用することを検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、および Citrix Delivery Controller による Microsoft .NET Framework バージョン 4.5.1、4.5.2、4.6、4.6.1、4.6.2、および 4.7 のサポート。	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードします。（.NET Framework 4.7.1 がインストールされていない場合は、インストーラーによって自動的にインストールされます）。
Red Hat Enterprise Linux 7.3 での Linux VDA のサポート	7.18	1808	Red Hat Enterprise Linux のそれ以降のバージョンに Linux VDA をインストールします。
StoreFront による Citrix Virtual Apps and Desktops（旧 XenApp および XenDesktop）、Citrix Receiver、ワークスペースハブ間の TLS 1.0 および TLS 1.1 プロトコルのサポート。	7.17		Citrix Receiver を、TLS 1.2 プロトコルをサポートする Citrix Workspace アプリにアップグレードします。Citrix Workspace アプリについて詳しくは、https://docs.citrix.com/ja-jp/citrix-workspace-appを参照してください。

項目	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
ポリシー設定「付属のプリンタードライバーの自動インストール」の VDA サポート。	7.16	7.16	なし。以前の OS のみ（Windows 7、Windows Server 2012 R2 以前）で、VDA でサポートされているポリシー設定。
SUSE Linux Enterprise Server 11 Service Pack 4 での Linux VDA のサポート。	7.16	7.16	サポートされている SUSE バージョンに Linux VDA をインストールします。
VDA での Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDM ドライバーは VDA でインストールされなくなりました。
Mobility SDK/Mobile SDK（旧 Citrix Labs のもの）	7.16		モバイルエクスペリエンスのポリシー設定と、ホストされるデスクトップ/アプリのネイティブエクスペリエンスにより一時停止されます。
Windows 10 バージョン 1511（Threshold 2）および Windows 8.x と Windows 7 を含む、以前の Windows シングルセッション OS リリース用 VDA（https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/を参照）。	7.15 LTSR（および 7.12）	7.16	Windows 10 最小バージョン 1607（Redstone 1）以降の半期チャネル用シングルセッション 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。CTX224843を参照してください。

項目	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 2008 R2 および Windows Server 2012（Service Pack を含む）上の VDA。	7.15 LTSR（および 7.12）	7.16	サポートされているオペレーティングシステムに VDA をインストールします。
デスクトップコンポジションのリダイレクト（旧 DirectX コマンドリモート処理）（DCR）	7.15 LTSR	7.16	Thinwireを使用します。
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）	1903	Citrix Receiver for Web 統合エクスペリエンス。
Windows Server 2012 および Windows Server 2008 R2（Service Pack を含む）上のコアコンポーネント。Delivery Controller、Studio、Director、StoreFront、ライセンスサーバー、およびユニバーサルプリントサーバーを含みます。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにこれらのコンポーネントをインストールします。
Windows Server 2012 および Windows Server 2008 R2（Service Pack を含む）上のセルフサービスパスワードリセット（SSPR）機能	7.15 LTSR	7.18	サポートされているより新しいオペレーティングシステムにインストールします。
Windows 7、Windows 8、および Windows 8.1（Service Pack を含む）上の Studio。	7.15 LTSR	7.18	サポートされているオペレーティングシステムに Studio をインストールします。

項目	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
Flash リダイレクト	7.15 LTSR	1912	ビデオコンテンツを HTML5 ビデオとして作成します。管理コンテンツには HTML5 ビデオのリダイレクト、公開 Web サイトには Web ブラウザーコンテンツのリダイレクトを使用します。詳しくは、Flash リダイレクトの製品終了（EOL）に関する記述を参照してください。
StoreFront を含む Citrix Online Integration（Goto 製品）	7.14（および StoreFront 3.11）	StoreFront 3.12	
VDA インストール時に作成され、VDA マシンのローカル管理者グループに追加されるユーザーアカウント CtxAppVCOMAdmin は、作成されなくなります。基になる「COM」メカニズムも削除されます。	7.14	7.14	Windows サービス CtxAppVService が同じ機能を実行します。このサービスは自動的にインストールされ、構成されるため、ユーザー操作は必要ありません。
Windows Server 2008 32 ビットでのユニバーサルプリントサーバーの UpsServer コンポーネントサポート。	7.14	7.14	サポートされているより新しいオペレーティングシステムにインストールします。
Internet Explorer 8 用 Storefront および Receiver for Web	7.13	7.13	

項目	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 App-V コンポーネントをインストールしない、VDA コマンドラインでのインストールオプション/no_appv	7.13	7.13	コマンドラインインストールオプション/exclude “Citrix Personalization for App-V - VDA” を使用します。
全製品インストーラーでの新規インストール時に、Citrix.Common.Commandスナップインはインストールされなくなりました。このスナップインは、既存インストールのアップグレード時に自動で削除されます。	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部の PowerShell コマンドは、XenApp 6.5 SDK で引き続き使用できます。詳しくは、XenApp および XenDesktop バージョン 7.13 マニュアルの「削除された機能」を参照してください。
*-CtxIcon コマンドレットによって提供されていたアイコンデータを操作するための機能の一部。	7.13	7.13	Broker Service の *-BrokerIcon コマンドレットによって提供されるようになりました。
Thinwire の初期バージョン	7.12	7.16	Thinwireを使用します。Windows Server 2008 R2 で以前のバージョンの Thinwire を使用している場合は、Windows Server 2012 R2 または Windows Server 2016 に移行してから Thinwire を使用します。

項目	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 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 7.16 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。これを行うには、まず XenDesktop 7.6 LTSR（最新の CU を含む）にアップグレードしてから、最新の Citrix Virtual Desktops（旧 XenDesktop）リリースまたは LTSR バージョンにアップグレードします。
32 ビット（x86）マシンに Delivery Controller、Director、StoreFront、またはライセンスサーバーをインストールします。	7.12	7.16	サポートされている x64 オペレーティングシステムにインストールします。
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。
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	7.16	サポートされているオペレーティングシステムに VDA をインストールします。

項目	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
CloudPlatform 接続のサポート	7.12	**2003**	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）接続のサポート	7.12	**2003**	Citrix Cloud で Virtual Apps and Desktops サービスを使用することを検討してください。
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**	代わりに、Citrix App Layeringを使用してください。
Personal vDisk の機能	7.15	**2003†**	Citrix App Layering ユーザーレイヤー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。

† Citrix Virtual Apps and Desktops 7 2003 では、Personal vDisk ドライバーは VDA から削除されました。ただし Citrix Virtual Apps and Desktops 7 2003 Delivery Controller で以前の VDA を使用する場合、Personal vDisk の機能は引き続きサポートされます。

システム要件

April 26, 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。定期的に更新が行われます。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（ホストシステム、Citrix Workspace アプリ、および Citrix Provisioning）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。

インストールの前に、「インストールの準備」の内容を確認してください。

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

の必須ソフトウェアの一部は、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、Knowledge Center のCTX119253を参照してください。

Windows Server 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、Nano Server のインストールは記載がない限りサポートされていません。Server Core は、Delivery Controller および Director に対してのみサポートされています。

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。

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および StoreFront（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および StoreFront（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、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、Citrix Virtual Apps 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）。

さらに、以下の情報を参照してください:

- 「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ガイダンスが含まれています。
- 「Citrix Virtual Apps and Desktops の単一サーバーのスケーラビリティ」では、単一の物理ホストでサポートされるユーザーまたは仮想マシンの数について説明します。

Microsoft Visual C++ 2017 ランタイム

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 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き
- Windows Server 2016 の Standard Edition、Datacenter Edition、および Server Core オプション付き

要件:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft インターネットインフォメーションサービス（自動的にインストールされ、現在開発中の Citrix Orchestration Service によってインストールされている機能が使用）。
- Windows PowerShell 3.0 以降。
- Microsoft Visual C++ 2017 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。
  - 新規インストール：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 Express 2017 と累積更新プログラム（CU）16 がインストールされます。

  - アップグレードの場合、既存の SQL Server Express バージョンはアップグレードされません。
- SQL Server 2016 SP2 の Express、Standard、および Enterprise 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 Microsoft SQL Server Express LocalDB 2017 と累積更新プログラム（CU）16 がインストールされます。これは、サイトデータベースのデフォルトの SQL Server Express とは異なるインストールです（Controller をアップグレードする場合、既存の Microsoft SQL Server Express LocalDB バージョンはアップグレードされません。LocalDB バージョンをアップグレードする場合は、「データベースのアクション」のガイダンスに従ってください）。

詳しくは、次の記事を参照してください：

- データベース
- Knowledge Center のCTX114501にサポートされている最新のデータベース一覧を表示
- 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 Server 2019、Standard、および Datacenter エディション。
- Windows Server 2016、Standard、および Datacenter エディション。
- Windows 10（64 ビットのみ）

要件：

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- 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 3.0 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 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き

- Windows Server 2016 の Standard Edition、Datacenter Edition、および Server Core オプション付き

要件:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- 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］ページ）、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 の互換モードはサポートされていません。Director へのアクセスには、Web ブラウザーの推奨設定を使用してください。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。

シングルセッション **OS** 対応 **Virtual Delivery Agent**（**VDA**）

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（x64 のみ）、最小バージョン 1607。
  - エディションのサポートについては、Knowledge Center のCTX224843を参照してください。

  - バージョン 1709 に関するシトリックスの既知の問題については、Knowledge Center のCTX229052を参照してください。

要件:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2017 Runtime（32 および 64 ビット）

リモート PC アクセスでは、この VDA を社内の物理 PC 上にインストールします。この VDA では、Windows 10 での Citrix Virtual Desktops 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 シングルセッション OS のほとんどのエディションには、メディアファンデーション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。

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

Windows Server 2019 または Windows Server 2016 マシンでは、コマンドラインインターフェイスを使用して Windows シングルセッション OS 対応 VDA をインストールし、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。

Windows 7 マシンに VDA をインストールする方法については、「以前のオペレーティングシステム」を参照してください。

マルチセッション **OS** 対応 **Virtual Delivery Agent**（**VDA**）

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 2019、Standard、および Datacenter エディション。
- Windows Server 2016、Standard、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 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2017 Runtime（32 および 64 ビット）

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

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media リダイレクトなど）では、VDA のインストール先マシンに Microsoft Media Foundation をインストールする必要があります。マシンに Media Foundation がインストールされていない場合は、マルチメディアアクセラレーション機能がインストール

されません。Citrix ソフトウェアのインストール後にマシンから Media Foundation を削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。ほとんどの Windows Server バージョンでは、メディアファンデーション機能はサーバーマネージャーを介してインストールされます。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:

- 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。

Windows 2008 R2 マシンに VDA をインストールする方法については、「以前のオペレーティングシステム」を参照してください。

ホスト/仮想化リソース

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 では、最新リリースは次のホストで VDA（アプリとデスクトップの配信用マシン）をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

サポートされているホスト/仮想化リソースは以下のとおりです（アルファベット順）。該当する場合は、*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。最新のバージョン情報と既知の問題へのリンクは、Knowledge Center のCTX131239に記載されています。

一部のホストプラットフォームまたは一部のプラットフォームバージョンでのみサポートされている機能もあります。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。

- **Citrix Hypervisor**（旧称 **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。

  詳しくは、「Citrix Hypervisor 仮想化環境」を参照してください。

- **Microsoft 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。

- **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。

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

HDX

オーディオ

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

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 機能と Citrix Workspace アプリの詳細については、機能マトリックスを参照してください。

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 3D Pro

Windows シングルセッション OS 対応 VDA は、実行時に GPU ハードウェアの存在を検出します。

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 Hypervisor、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。HDX 3D Pro は、Microsoft Azure NV シリーズおよび Amazon AWS EC2 G3 のクラウドインスタンスでもサポートされています。

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

GPU（Graphical Processing Unit）:

- 無損失圧縮を含む CPU ベース圧縮の場合、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、GRID 10 ドライバーでサポートされる NVIDIA GRID GPU 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」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。
- 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 仮想化ソリューション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 に関する記事またはwww.citrix.com/xenapp/3dを参照してください。

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 2019
- Windows Server 2016

要件:

- Microsoft Visual C++ 2017 Runtime（x86 および x64）
- Microsoft .NET Framework 4.8（最小）

マルチセッション 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

Citrix ライセンスサーバー 11.16 以降のみがサポートされています。詳しくは、「ライセンス」を参照してください。

本リリースで Citrix Provisioning を利用する場合（旧称 Provisioning Services）は、Citrix Provisioning バージョン 7.x が、XenApp 7.x または XenDesktop 7.x のライフサイクルおよび Citrix Virtual Apps and Desktops のライフサイクルの対象となります。バージョンの互換性について詳しくは、製品マトリクスを参照してください。

サポートされる StoreFront のバージョンについては、「StoreFront のシステム要件」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 Citrix Virtual Apps and Desktops 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。

GPMC を使用してドメイン GPO を編集する場合は、Delivery Controller を含むすべてのマシンでグループポリシーの管理機能（Windows Server Manager）を有効にします。

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。

最新の 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。詳しくは「Windows 向け Citrix Workspace アプリのドキュメント」を参照してください。

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

この機能でサポートされている Web 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。

このバージョンの Citrix Virtual Apps and Desktops 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。

このバージョンの Citrix Virtual Apps and Desktops には、HDX RealTime Connector 2.9 LTSR 以降が必要です。詳しくは、「HDX RealTime Optimization Pack のドキュメント」を参照してください。

製品の技術概要

June 7, 2021

Citrix Virtual Apps and Desktops の仮想化ソリューションで、IT 担当者は仮想マシン、アプリケーション、ライセンス、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。

Citrix Virtual Apps and Desktops では次のことが可能です:

- 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。

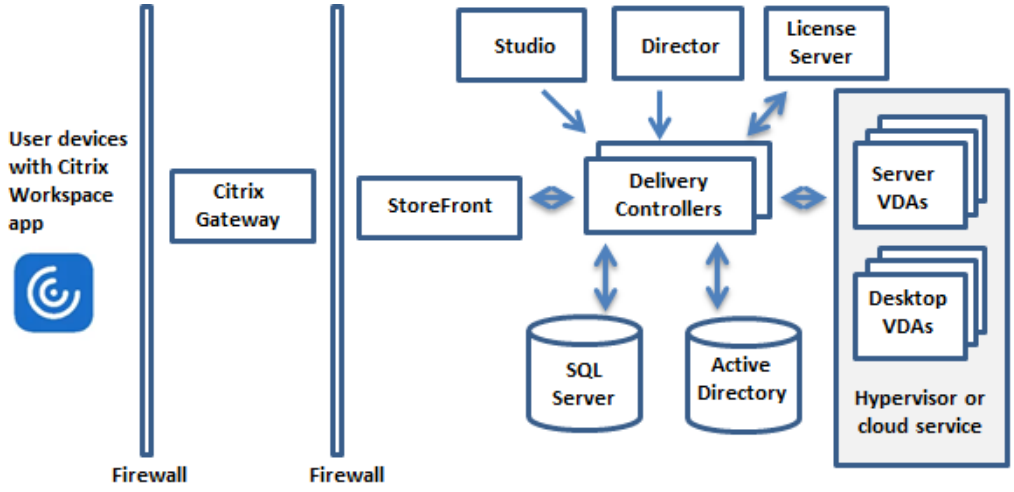
Citrix Virtual Apps and Desktops では「FlexCast Management Architecture（FMA)」と呼ばれる共通の統合アーキテクチャが使用されます。FMA により、単一サイトで複数のバージョンの Citrix Virtual Apps または Citrix Virtual Desktops を実行でき、プロビジョニング機能が統合されます。

製品名の変更について確認する。

主要コンポーネント

この記事は、Citrix Virtual Apps and Desktops を初めてご使用の方に役立ちます。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、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またはクラウドサービスが含まれる場合、Controller サービスがそれ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、接続の使用を最適化したり、接続の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

各サイトには、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との間の接続を確立して管理します。また、VDA は Citrix ライセンスがユーザーまたはセッションで使用可能であることを確認し、セッションに対して構成されている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 はシングルセッションおよびマルチセッションの Windows オペレーティングシステムで利用できます。マルチセッション Windows Server OS 対応 VDA 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。シングルセッション Windows OS 対応 VDA 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 Workspace アプリ

Citrix Workspace アプリは、ユーザーデバイスや他のエンドポイント（仮想デスクトップなど）にインストールされ、ドキュメント、アプリケーション、およびデスクトップへの迅速かつ安全なセルフサービスアクセスをユーザーに提供します。また、Citrix Workspace アプリにより、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可能になります。デバイス固有の Citrix Workspace アプリ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 HTML5 向け Citrix Workspace アプリを使用してアクセスすることもできます。

Citrix Studio

Studio は、Citrix Virtual Apps and Desktops の展開を設定および管理する管理コンソールです。Studio 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。

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 Citrix Virtual Apps または Citrix Virtual Desktops サイトに接続して監視することができます。

Director には次のものが表示されます:

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

Director では、Citrix Gateway デバイスでキャプチャされた ICA パフォーマンスおよびヒューリスティックデータを使用してデータから分析を作成し、管理者に提示します。

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。各サイトには、ライセンスファイルを格納および管理するためのライセンスサーバーが 1 つ以上必要です。

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、Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops は、さまざまなハイパーバイザーとクラウドサービスをサポートします。

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。

詳しくは、次のトピックを参照してください:

- ネットワークポート。
- データベース。
- Citrix Virtual Apps and Desktops コンポーネントの Windows サービス:「ユーザー権利の構成」
- サポートされるハイパーバイザーとクラウドサービス: システム要件

追加のコンポーネント

Citrix Virtual Apps and Desktops 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。

Citrix Provisioning

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

Citrix Gateway

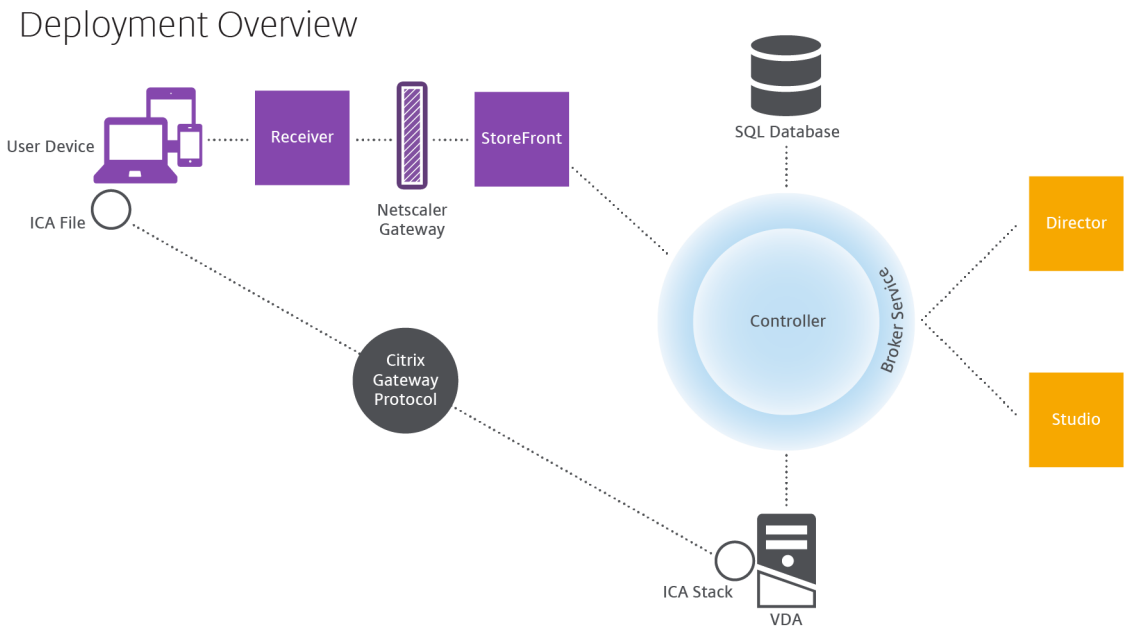
ユーザーが社内ファイアウォールの外側から接続する場合、Citrix Virtual Apps and Desktops で Citrix Gateway（旧 Access Gateway および NetScaler Gateway）テクノロジを使用して接続を TLS で保護できます。Citrix Gateway や VPX 仮想アプライアンスは非武装地帯（DMZ）に配置する SSL VPN アプライアンスであり、企業ファイアウォールを介した安全な単一アクセスポイントを提供します。

Citrix SD-WAN

支店など遠隔地のユーザーが WAN を介して仮想デスクトップに接続する環境では、Citrix 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リピータは、広域ネットワークにわたりパフォーマンスを向上させます。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。Citrix SD-WAN では、さまざまなユーザー操作に優先順位を割り当てることができます。たとえば、ネットワーク上で大きなファイルや印刷ジョブを送信する操作に高い優先度を割り当てて、遠隔地のユーザーがストレスなく作業できるようにします。HDX WAN の最適化によりトークン化された圧縮およびデータ重複排除が提供され、帯域幅消費が減少してパフォーマンスが向上します。

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。

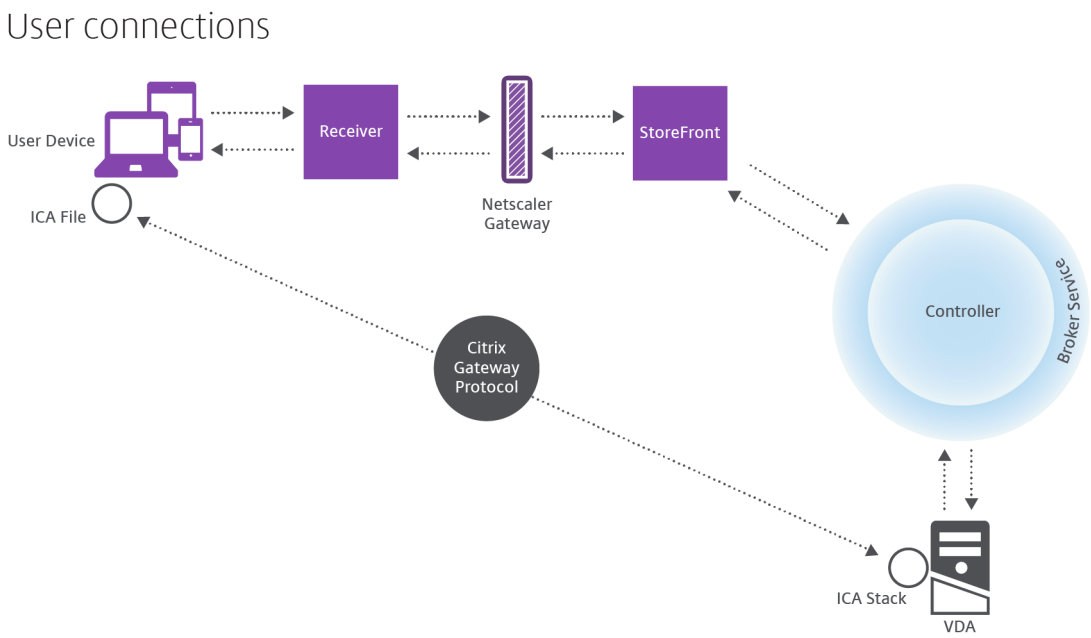
ユーザーが Controller に直接アクセスすることはありません。ユーザーと Controller 間の通信の中継点として VDA が機能します。ユーザーが StoreFront を使用してログオンすると、その資格情報は Controller 上の Broker Service にパススルーされます。Broker Service は、設定されているポリシーに基づいてプロファイルと利用可能なリソースを取得します。

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 Workspace アプリ、または StoreFront 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 Workspace アプリ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 Workspace アプリ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 は接続を受け入れ、同じ経路で Citrix Workspace アプリに情報を返送します。必要なパラメーターのセットが StoreFront 上で収集されます。収集されたパラメーターは、Citrix Workspace アプリ 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 Workspace アプリに送信されます。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。

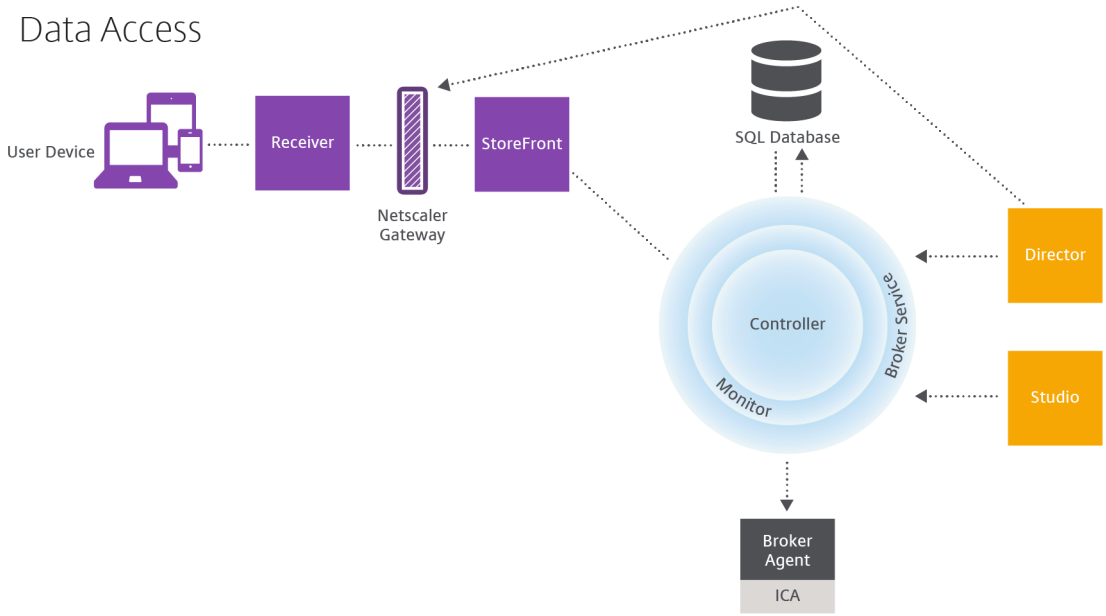
ICA ファイルがユーザーデバイスにコピーされ、VDA 上で実行される ICA スタックとの直接接続が確立されます。この接続により、管理インフラストラクチャ（Citrix Workspace アプリ、StoreFront、および Controller）がバイパスされます。

Citrix Workspace アプリと 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、Citrix Virtual Apps and Desktops の各セッションにより提供されるデータに Studio や Director でアクセスできます。Studio 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 Citrix 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

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を使用して）利用可能なアプリケーションやデスクトップ、およびどのユーザーがそれらにアクセスできるかを指定するデリバリーグループを作成します。また、アプリケーショングループを作成して、アプリケーションのコレクションを管理できます。

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、そのカタログにあるマシンのプロビジョニング方法を以下から指定できます：Citrix ツール（Citrix Provisioning または MCS）または他のツール。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。

- マルチセッション **OS**：マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps 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」とも呼ばれます）および Citrix Virtual Apps 公開デスクトップ（「サーバーでホストされるデスクトップ」とも呼ばれます）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。
- シングルセッション **OS**：シングルセッションオペレーティングシステム使用の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できるシングルセッション OS を実行しているデスクトップ）、VM でホストされるアプリケーション（シングルセッション 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 Workspace アプリを実行している任意のデバイスから社内の物理 PC にアクセスできるようにします。オフィス PC は、Citrix Virtual Desktops の展開によって管理され、ユーザーデバイスをホワイトリストで指定する必要があります。

詳しくは、「Citrix Virtual Apps and Desktops のイメージ管理」および「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。

詳細情報

Citrix Virtual Apps and Desktops の図

Active Directory

April 26, 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。この検出方法の詳細については、「Active Directory の組織単位ベースの検出」およびCTX118976を参照してください。

> 注:
>
> サイトの構成後、コンピューター名や Delivery 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 フォワーダーまたは条件付き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。以下の情報を使用して、レジストリキーを VDA および Delivery Controller に追加します。

> 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。

VDA で次を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

- 値の名前：SupportMultipleForest
- 種類：REG_DWORD
- データ：0x00000001 (1)

すべての Delivery Controller で次を構成します：HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest。

- 値の名前：SupportMultipleForest
- 種類：REG_DWORD
- 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。

VDA の場合、レジストリキーHKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDsを検索します。

- 値の名前：ListOfSIDs
- 種類：REG_SZ
- データ：Controller のセキュリティ識別子（SID）。（SID は、Get-BrokerControllerコマンドレットの結果に含まれています。）

適切な外部の信頼が構成済みの場合、VDA 上で以下の変更を行います：

1. ファイルProgram Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config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. テキストallowNtlm="false"を検索して、テキストをallowNtlm="true"に変更します。
5. ファイルを保存します。

レジストリキーListOfSIDs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

信頼の種類	推移性	Direction	このリリースでのサポート
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

April 26, 2021

Citrix Virtual Apps サイトおよび Citrix Virtual Desktops サイトでは、次の 3 つの SQL Server データベースを使用します:

- 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。

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、プライマリゾーンには必ずサイトデータベースを格納してください。すべてのゾーンのコントローラーは、このデータベースと通信します。

高可用性

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

- **AlwaysOn** 可用性グループ機能（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、「SQL Server での Windows Server フェールオーバークラスタリング」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。この機能は、すべての Controller との通信に障害がある場合にのみ使用します。ほかの高可用性ソリューションの代替策ではありません。詳しくは、「CTX 127564」を参照してください。

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」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、「CTX 137161」を参照してください。
- 必要に応じて、高可用性機能を構成します。
- ミラーリングを構成するには、まず、完全復旧モデルを使用するようにデータベースを設定します（デフォルトは簡易モデル）。プリンシパルデータベースをファイルにバックアップして、それをミラーサーバーにコピーします。ミラーデータベースで、バックアップファイルをミラーサーバーに復元します。その後、プリンシパルサーバーでミラーリングを開始します。

データベース管理者は、SQLCMD コマンドラインユーティリティ、または SQL Server Management Studio を SQLCMD モードで使用し、高可用性 SQL Server データベースインスタンスで各 xxx_Replica.sql スクリプトを実行します（高可用性機能が構成されている場合）。その後、プリンシパル SQL Server データベースインスタンスで各 xxx_Principal.sql スクリプトを実行します。SQLCMD について詳しくは、Microsoft のドキュメントを参照してください。

すべてのスクリプトが正常に終了したら、データベース管理者は、Citrix 管理者に 3 種類のプリンシパルデータベースアドレスを渡します。

Studio には、サイトの作成の続行を促すプロンプトが表示され、［データベース］ページに戻ります。渡されたアドレスを入力します。データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表

示されます。

データベースのセットアップに必要な権限

データベースを作成し、初期化（または、データベースの場所を変更）するには、ローカル管理者およびドメインユーザーでなければなりません。また、特定の SQL Server 権限も必要です。以下の権限は、Active Directory のグループメンバーシップで明示的に構成または取得できます。Studio を使用する管理者にこれらの権限がない場合、SQL Server ユーザーの資格情報を入力する必要があります。

操作	目的	サーバーロール	データベースロール
データベースの作成	空のデータベースを作成します	dbcreator	
スキーマの作成	サービス固有のすべてのスキーマを作成して、サイトに最初の Controller を追加します	securityadmin*	db_owner
Controller の追加	サイトに Controller（2 つ目以降）を追加します	securityadmin*	db_owner
Controller（ミラーサーバー）の追加	ミラー化されたデータベースのミラーロールのデータベースサーバーに Controller ログインを追加します	securityadmin*	
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。

優先データベース権限スクリプト

エンタープライズ環境では、データベースのセットアップに、役割（権限）が異なる（securityadminまたはdb_owner）チームが処理する必要があるスクリプトが含まれます。

PowerShell を使用して、優先データベース権限を指定できるようになりました。（この機能は、すべてのタスクを含む単一のスクリプトのみをサポートする Studio では使用できません）

デフォルト以外の値を指定すると、個別のスクリプトが作成されます。1 つのスクリプトには、securityadminの役割が必要なタスクが含まれています。もう 1 つのスクリプトは、db_ownerの権限のみが必要で、データベース管理者に連絡することなく Citrix 管理者が実行できます。

get-*DBSchemaコマンドレットの-DatabaseRightsオプションで有効な値は以下のとおりです：

- SA：データベースと Delivery Controller のログインを作成するスクリプトを生成します。これらのタスクにはsecurityadminの権限が必要です。
- DBO：データベースでユーザー役割を作成し、ログインを追加してから、データベーススキーマを作成するスクリプトを生成します。これらのタスクにはdb_ownerの権限が必要です。
- Mixed：（デフォルト）必要な権限に関わらず、1 つのスクリプトにすべてのタスクを含めます。

詳しくは、コマンドレットのヘルプを参照してください。

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。
- SQL Server の高可用性ソリューションを使用する場合、サイトデータベースのサイズ評価および接続文字列の構成を行います。

配信方法

April 26, 2021

Citrix Virtual Apps and Desktops では、さまざまな配信方法が提供されます。1 つの配信方法で、すべてのニーズを満たせることはまずありません。

はじめに

適切なアプリケーション配信方法を選択することで、スケーラビリティ、管理性、ユーザーエクスペリエンスを高めることができます。

- アプリのインストール：アプリケーションが、ベースのデスクトップイメージに含まれます。インストールプロセスでは、レジストリが変更されるとともに、dll ファイルや exe ファイルなどすべてのファイルがイメージドライブにコピーされます。詳しくは、「マシンカタログの作成」を参照してください。
- アプリのストリーム配信（**Microsoft App-V**）：アプリケーションはプロファイル化され、オンデマンドでネットワーク上のデスクトップへ配信されます。アプリケーションファイルとレジストリの設定は仮想デスクトップのコンテナ内に配置され、ベースオペレーティングシステムや別の設定から隔離されます。これによって、互換性の問題を解決しやすくなります。詳しくは、「App-V」を参照してください。

- アプリのレイヤー化（**Citrix App Layering**）：レイヤーごとに、アプリケーション、エージェント、またはオペレーティングシステムを 1 つ配置します。管理者は、OS レイヤーを 1 つ、プラットフォームレイヤー（VDA、Citrix Provisioning エージェント）を 1 つ、アプリケーションレイヤー複数を統合することで、展開可能な新しいイメージを簡単に作成できます。レイヤー化では 1 つのレイヤーに存在する OS、エージェント、アプリケーションが 1 つになるため、定期的なメンテナンスを簡単に行えます。レイヤーを更新すると、そのレイヤーを含む展開済みイメージがすべて更新されます。詳しくは、「Citrix App Layering」を参照してください。
- **Windows** アプリのホスト：アプリケーションをマルチユーザー Citrix Virtual Apps ホストにインストールし、デスクトップではなくアプリケーションとして展開します。ユーザーは、アプリがリモートで実行されていることを意識することなく、VDI デスクトップまたはエンドポイントデバイスからホストされている Windows アプリへシームレスにアクセスできます。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。
- ローカルアプリ：アプリケーションをエンドポイントデバイスに展開します。アプリケーションがエンドポイント上で実行される場合でも、そのインターフェイスはユーザーのホストされた VDI セッション内に表示されます。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。
- リモート **PC** アクセス：リモート PC アクセスにより、従業員は物理的な社内 PC にリモートからアクセスできます。ユーザーが社内 PC にアクセスする場合、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。詳しくは、「リモート PC アクセス」を参照してください。

デスクトップについては、公開デスクトップまたは VDI デスクトップを選択します。

Citrix Virtual Apps の公開アプリケーションと公開デスクトップ

Citrix Virtual Apps and Desktops の公開アプリケーションと公開デスクトップは、マルチセッション 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：

- サーバーベースで安価に配信を行うことで、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ながら、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これにより、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マルチセッション OS マシン上にインストールされます。
- マシンは、マシンカタログを作成することで使用可能になります。
- マシンカタログのマシンはデリバリーグループにまとめられ、同じアプリケーションセットがユーザーグループに配信されます。
- マルチセッション 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:

- マルチセッション 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 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、同一のセッションでアプリケーションを複数実行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。

VM Hosted Apps

VM Hosted App は、シングルセッション 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:

- 安全で一元管理可能であり、ホストサーバーごとに複数のユーザーをサポートできるクライアントベースのアプリケーション配信ソリューションを実現する。対象ユーザーには、アプリケーションを高画質でシームレスに表示する。
- 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。

- アプリケーションの種類：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。
- シングルセッション 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に必要なサーバーリソースと、ユーザーのデータ用のストレージ容量が増大します。

ユーザーエクスペリエンス：

- マルチセッション 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：

- これらは仮想シングルセッション OS マシンであるという以外はマルチセッション OS マシンと同様です。

セッション管理と割り当て：

- シングルセッション 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。

VDI デスクトップ

シングルセッション OS マシンを使用してユーザーに Citrix Virtual Apps and Desktops VDI デスクトップを配信します。

VDI デスクトップは、仮想マシン上でホストされ、各ユーザーにデスクトップオペレーティングシステムを提供します。

VDI デスクトップでは、公開デスクトップよりも多くのリソースが必要になります。ただし、サーバーオペレーティングシステムをサポートしないアプリケーションをインストールできる点が公開デスクトップと異なります。また、

使用する VDI デスクトップの種類にもよりますが、特定のユーザーにデスクトップを割り当てることができます。このようにすることで、ユーザーは詳細な個人設定を行うことができます。

VDI デスクトップのマシンカタログを作成するときは、以下のいずれかの種類のデスクトップを作成します。

- ランダムな非永続デスクトップ（プール **VDI** デスクトップ）：ユーザーはいずれかのデスクトップにログオンするたびに、デスクトッププールのうち指定されたデスクトップに接続されます。このプールは、単一のマスターイメージに基づきます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な非永続デスクトップ：ユーザーは初回ログオン時に、デスクトッププールのデスクトップに割り当てられます（プールの各マシンは単一のマスターイメージに基づきます）。以降のログオンでは、初回ログオン時に割り当てられたデスクトップに接続されます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な永続デスクトップ：他の VDI デスクトップとは異なり、ユーザーは完全な個人設定が可能です。初回ログオン時に、デスクトッププールのデスクトップに割り当てられますそのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。デスクトップに対するユーザーの変更内容は、マシンを再起動しても保持されます。

ネットワークポート

April 26, 2021

次の表に、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の一覧を示します。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、CTX101810を参照してください。

以下のように、このポートの情報が必要な場合があります：

- 法的なコンプライアンスが必要である。
- これらのコンポーネントと他の Citrix 製品またはコンポーネントとの間にネットワークファイアウォールがある場合、ファイアウォールを適切に構成できる。
- オペレーティングシステムのホストファイアウォールではなく、アンチマルウェアパッケージなどが付属したサードパーティ製のホストファイアウォールを使用する。
- これらのコンポーネントでホストファイアウォールの構成を変更する（通常 Windows ファイアウォールサービス）。
- これらのコンポーネントの機能を再構成して、別のポートやポート範囲を使用し、構成で使用されていないポートを無効にする、またはブロックする必要がある。詳しくは、コンポーネントのドキュメントを参照してください。
- StoreFront および Citrix Provisioning（旧称 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。

以下の表には、受信ポートのみを示しています。送信ポートには、通常はオペレーティングシステムにより無関係な番号が割り当てられます。送信ポートの情報は通常、上記に記載された目的には必要ありません。

これらのポートの一部は、Internet Assigned Numbers Authority（IANA）に登録されています。こうした割り当てについて詳しくは、http://www.iana.org/assignments/port-numbersを参照してください。ただし、IANA の保有する情報には、最新の使用状況が反映されていない場合があります。

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 Workspace アプリ

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 (WebSocket 経由)	TCP	8008	HTML5 向け Citrix Workspace アプリおよび Chrome 向け Citrix Workspace アプリ 1.6 以前のみ
VDA	ICA/HDX（UDP でのオーディオリアルタイムトランスポート）	UDP	16500 から 16509	
VDA	ICA/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	

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
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

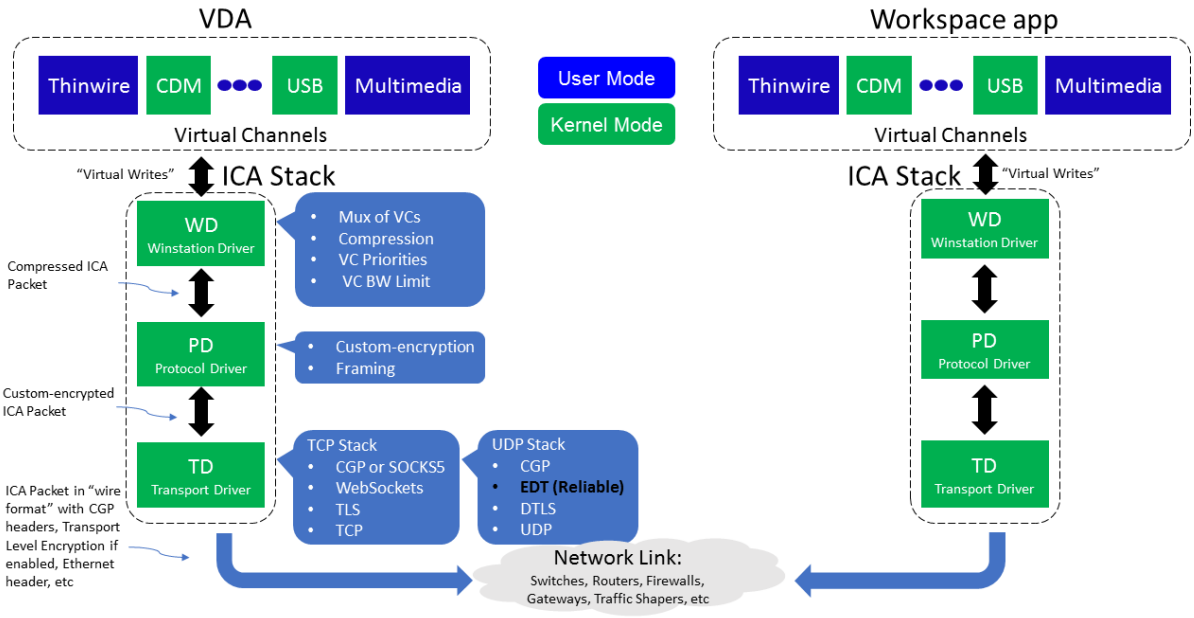
HDX

April 26, 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 では、デバイスやネットワークを問わず、一元化したアプリケーションとデスクトップを高鮮明なままユーザーに提供できます。

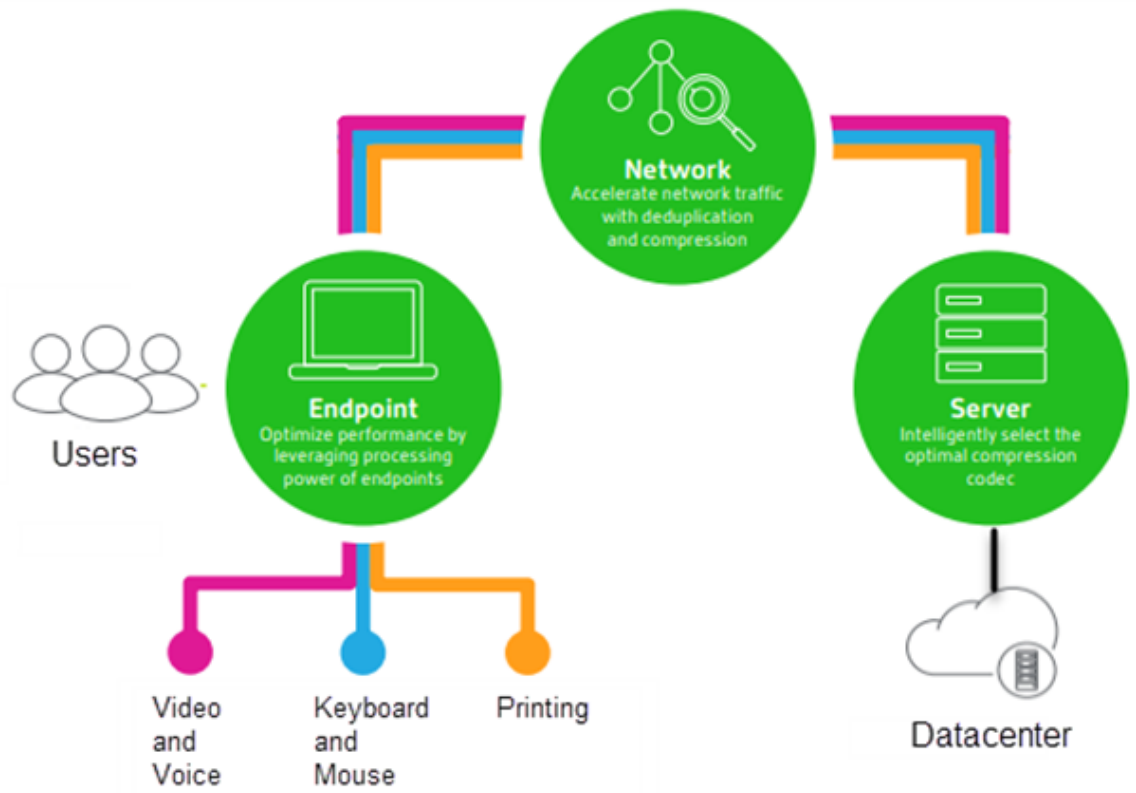


HDX は、次の 3 つの技術原則に基づいて設計されています:

- インテリジェントリダイレクト
- 連続文字圧縮
- データ重複排除

これらの原則をさまざまに組み合わせて適用することで、IT 部門およびユーザーの操作を最適化し、帯域幅の消費量を抑えてホストサーバーあたりのユーザー密度を増やすことができます。

- インテリジェントリダイレクト - 画面のアクティビティ、アプリケーションのコマンド、エンドポイントデバイス、ネットワークとサーバーの容量を調べることで、アプリケーションやデスクトップのアクティビティのレンダリング方法と表示場所を即座に決定します。レンダリングは、エンドポイントデバイスまたはホストサーバーのどちらかで行われます。
- アダプティブ圧縮 - 細いネットワーク接続でも、マルチメディアを高鮮明に表示して配信できます。HDX はまず、入力のタイプ、デバイスのタイプ、ディスプレイのタイプ（テキスト、動画、音声、マルチメディア）などのいくつかの変動要素を評価します。次に、最適な圧縮コーデックと、CPU および GPU の最適な使用率を選択します。さらに、ユニークユーザーごとにこの設定をインテリジェントにカスタマイズします。このインテリジェントな適応は、ユーザーごと、またはセッションごとでも行われます。



- データ重複排除 - 重複したネットワークトラフィックを排除することで、クライアントとサーバー間で送信される総データ量を削減します。これは、ビットマップ画像、ドキュメント、印刷ジョブ、ストリーム配信メディアなどのアクセス頻度の高いデータで繰り返されるパターンを活用して行っています。これらのパターンをキャッシュ化することで、重複したトラフィックを排除し、ネットワークで変更内容のみを送信できます。HDX では、マルチメディアストリームのマルチキャストもサポートされます。このマルチキャストでは、ソースからの単一の送信データを、ユーザーごとの 1 対 1 接続ではなく、1 つの場所にいる複数のサブスクライバーが視聴します。

詳しくは、「ユーザーワークスペースの高品位化による生産性の向上」を参照してください。

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。

データセンターでは

HDX では、サーバー側の処理能力およびスケーラビリティを利用して、クライアントデバイス側の能力に制限されずに高度なグラフィックパフォーマンスを提供できます。

Citrix Director では、ユーザーデバイスに接続している HDX チャネルの状態を監視できます。

HDX Insight

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。

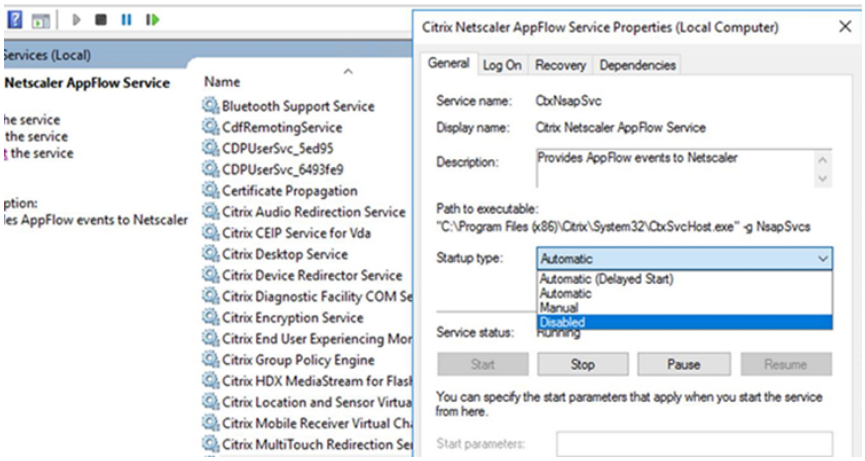
NetScaler で HDX Insight 仮想チャネルを使用して必要なすべてのデータポイントを非圧縮形式で移動できるようにすることができます。この機能を無効にした場合、NetScaler デバイスは、さまざまな仮想チャネルに分散した ICA トラフィックを暗号化解除して解凍します。単一の仮想チャネルを使用すると、複雑さが軽減され、スケーラビリティが向上し、コスト効率が向上します。

最小要件:

- Citrix Virtual Apps and Desktops 7 バージョン 1808
- XenApp および XenDesktop 7.17
- NetScaler バージョン 12.0 ビルド 57.x
- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.10
- Mac 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Mac 12.8

HDX Insight 仮想チャネルを有効または無効にする

この機能を無効にするには、Citrix NetScaler Application Flow サービスのプロパティを［無効］に設定します。有効にするには、サービスを［自動］に設定します。いずれの場合も、これらのプロパティを変更した後は、サーバーマシンを再始動することをお勧めします。このサービスは、デフォルトで有効（[自動]）になっています。



仮想デスクトップからの **HDX** 機能の体験

- Web ブラウザーコンテンツリダイレクト（4 つある HDX マルチメディアリダイレクト技術のうちの 1 つ）により、HTML5 と WebRTC 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. Chrome ブラウザーの拡張機能をダウンロードして、仮想デスクトップにインストールします。
  2. 仮想デスクトップへのマルチメディアコンテンツ配信に関する Web ブラウザーコンテンツリダイレクトのパフォーマンスを体験するには、仮想デスクトップで HTML5 動画を含むウェブサイト（YouTube など）にアクセスして、動画を再生します。ユーザーには、Web ブラウザーコンテンツリダイレクトがいつ実行されているかはわかりません。Web ブラウザーコンテンツリダイレクトが使用されているかどうかを確認するには、Web ブラウザーのウィンドウをすばやくドラッグします。ビューポートやユーザーインターフェイスの表示が遅れるか、これらの間のフレームが消失します。また、ウェブページ上で右クリックすると、メニューに［**HDX Web** ブラウザーリダイレクトについて］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 Workspace アプリで、最高の音質を選択します。詳しくは、Citrix Workspace アプリのドキュメントを参照してください。
  2. デスクトップ上のデジタルオーディオプレーヤー（iTunes など）で音楽ファイルを再生します。

HDX では、特別な構成を行わなくてもデフォルトで、一般的なユーザーに適したグラフィックおよびビデオ配信が提供されます。Citrix ポリシー設定は、一般的な使用環境で最適なユーザーエクスペリエンスが提供されるようにデフォルトで有効になっています。

- HDX は、クライアントプラットフォーム、アプリケーション、およびネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、状況の変化に応じて自動調整します。
- HDX は、2D および 3D のグラフィックおよびビデオのパフォーマンスを最適化します。
- HDX は、インターネットやイントラネット上のマルチメディアコンテンツなどをホストサーバーを介さず直接ユーザーデバイス上にストリーム配信します。このクライアント側でのコンテンツ取得に必要な条件が満たされない場合、メディア配信はサーバー側でのコンテンツ取得とマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能に関するポリシーを変更する必要はありません。

- マルチメディアリダイレクトが利用できない場合、HDX は仮想デスクトップにサーバー側でレンダリングしたビデオコンテンツを提供します。http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/などのサイトにアクセスして、高品位ビデオを含む Web サイト上のビデオをご覧ください。

ヒント:

- HDX 機能の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 マルチセッション OS マシン、Windows シングルセッション 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。

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。

HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファーを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、最初は大きい値に設定されます。値を大きくすることで、特

に高遅延のネットワークで、データをより迅速かつ効率的にクライアントに送信できます。高い双方向性、高速なファイル転送、スムーズなビデオ再生、および高いフレームレートと解像度により、優れたユーザーエクスペリエンスを実現します。

セッションの双方向性を常に測定して、ICA セッション内のデータストリームが双方向性に悪影響を及ぼしているかどうかを判別します。悪影響を及ぼしている場合、スループットを低下させて、大規模データストリームがセッションに与える影響を減らし、双方向性を回復できるようにします。

> 重要:
>
> HDX アダプティブスループットでは、このメカニズムをクライアントから VDA に移行することにより、出力バッファーの設定方法を変更しています。手動での構成は必要ありません。

この機能には以下の要件があります:

- VDA バージョン 1811 以降
- Windows 向け Workspace アプリ 1811 以降

最小要件を満たしていない展開については、「高遅延接続で HDX 帯域幅を最適化する」で手動による出力バッファの構成について参照してください。

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 Citrix Virtual Apps and Desktops 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 Workspace アプリユーザーが 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］を選択すると無効になります。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って USB デバイスのリダイレクトを無効にします。

HDX Web カメラビデオ圧縮を使用するには、以下のポリシー設定を有効にする必要があります（これらの設定項目はデフォルトで有効になっています）。

- クライアントオーディオリダイレクト
- クライアントマイクリダイレクト
- マルチメディア会議
- Windows Media リダイレクト

Web カメラで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（サービス品質）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）ストリームを使用できます。

- 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、バルク
- UDP ストリーム - ボイスおよび Framehawk ディスプレイリモート

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（サービス品質）は、セッション画面の保持機能のポートまたは CGP ポートが複数構成されている環境でのみサポートされます。

> 警告
>
> この機能を使用する場合は、トランスポートセキュリティを使用してください。IPsec（Internet Protocol Security）または TLS（Transport Layer Security）を使用することをお勧めします。TLS 接続がサポートされるのは、マルチストリーム ICA をサポートする NetScaler Gateway を通過するトラフィックのみです。企業内ネットワークでは、TLS を使用したマルチストリーム接続はサポートされません。

マルチストリーム接続の Qos（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（サービス品質）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。

リモート言語バーを表示または非表示にする

言語バーには、アプリケーションセッションでの優先される入力言語が表示されます。この機能が有効（デフォルト）になっている場合、Windows 向け Citrix Workspace アプリの ［詳細設定］**>**［言語バー］から言語バーを表示または非表示にできます。VDA 側でレジストリ設定を使用すると、言語バー機能のクライアント制御を無効にできます。この機能を無効にした場合、クライアントの UI 設定が有効にならず、ユーザーごとの現在の設定によって言語バーの状態が決まります。詳しくは、「ユーザーエクスペリエンスの向上」を参照してください。

VDA から言語バー機能のクライアント制御を無効にするには：

1. レジストリエディターで､HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI に移動します。
2. DWORD 値のキー SeamlessFlags を作成し、それを 0x40000 に設定します。

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。

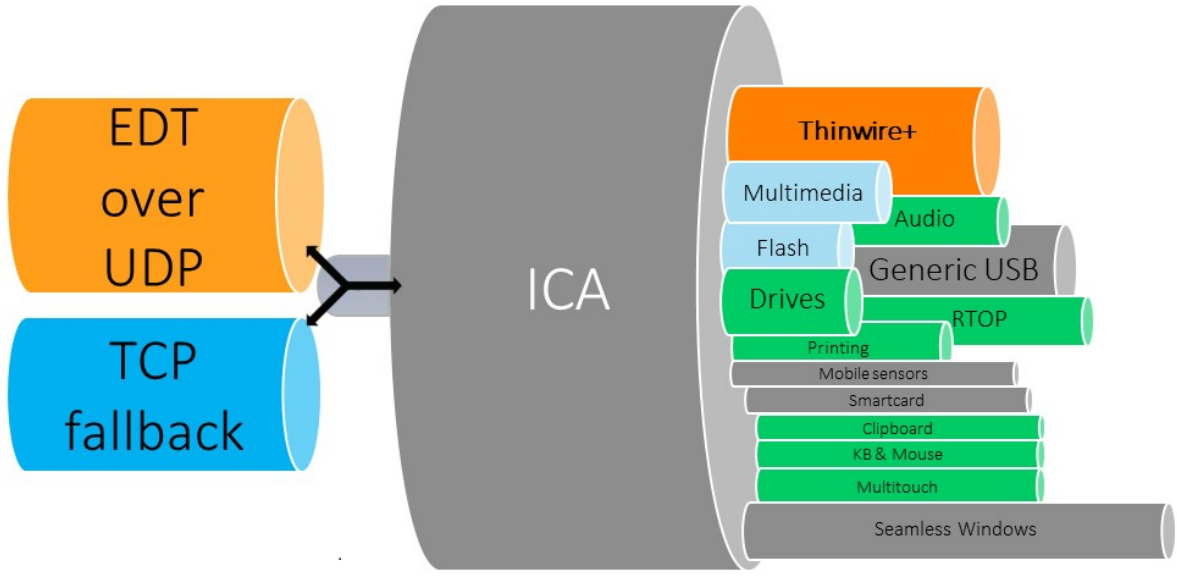
1. HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap キーの下で、DisableWindowHook の DWORD 値を 1 に設定します。
2. 通常の Unicode キーボードレイアウトマッピングを使用するには、DisableWindowHook の DWORD 値を 0 に設定します。

アダプティブトランスポート

July 27, 2021

アダプティブトランスポートは、Citrix Virtual Apps and Desktops のメカニズムであり、ICA 接続のトランスポートプロトコルとして Enlightened Data Transport（EDT）を使用する機能を提供します。EDT が使用できない場合、アダプティブトランスポートは TCP に切り替わります。

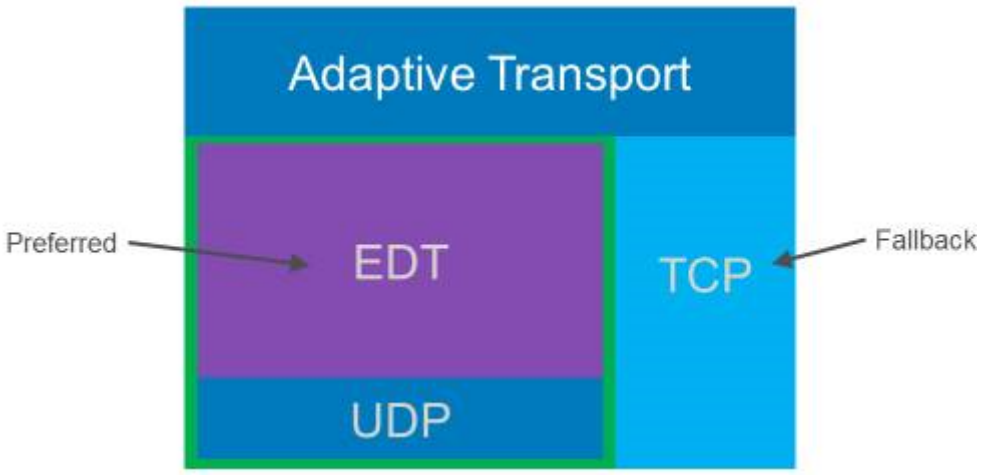
EDT は、ユーザーデータグラムプロトコル（UDP）上に構築された Citrix 独自のトランスポートプロトコルです。サーバーのスケーラビリティを維持しながら、要求の厳しい長距離接続で優れたユーザーエクスペリエンスを提供します。EDT は、信頼性の低いネットワーク上のすべての ICA 仮想チャネルのデータスループットを向上させ、より優れた、より一貫性のあるユーザーエクスペリエンスを提供します。



アダプティブトランスポートが ［優先］に設定されている場合、EDT がプライマリトランスポートプロトコルとして使用され、TCP がフォールバックに使用されます。デフォルトでは、アダプティブトランスポートは ［優先］に設定されています。テスト目的でアダプティブトランスポートを ［診断モード］に設定できます。これにより、EDT のみが許可され、TCP へのフォールバックが無効になります。

Windows、Mac、iOS 向けの Citrix Workspace アプリを使用する場合、初期接続、セッション画面の保持による再接続、自動クライアント再接続の実行中に、EDT と TCP の接続が同時に試行されます。そうすることで、基礎となる UDP トランスポートが利用できなくなり、代わりに TCP を使用する必要がある場合に、接続時間が短縮されます。アダプティブトランスポートが ［優先］に設定されていて、TCP を使用して接続が確立されている場合、アダプティブトランスポートは 5 分ごとに EDT への切り替えを試行し続けます。

Linux および Android 向けの Citrix Workspace アプリでは、最初に EDT 接続が試行されます。この接続が失敗した場合、Citrix Workspace アプリは、EDT 要求がタイムアウトした後、TCP で接続を試みます。



システム要件

アダプティブトランスポートと EDT を使用するための要件は次のとおりです:

- コントロールプレーン
  - Citrix Virtual Apps and Desktops サービス
  - Citrix Virtual Apps and Desktops 1912 以降
- Virtual Delivery Agent
  - バージョン 1912 以降（2103 以降を推奨）
  - バージョン 2012 は、Citrix Gateway Service で EDT を使用するために必要な最小バージョンです。
- StoreFront
  - バージョン 3.12.x
  - バージョン 1912.0.x
- Citrix Workspace アプリ
  - Windows：バージョン 1912 以降（2105 以降を推奨）
  - Linux：バージョン 1912 以降（2104 以降を推奨）
  - Mac：バージョン 1912 以降
  - iOS：Apple AppStore で入手可能な最新バージョン
  - Android：Google Play で利用可能な最新バージョン
- Citrix Gateway（ADC）
  - 13.0.52.24 以降
  - 12.1.56.22 以降
- ファイアウォール（VDA の観点から）
- UDP 1494 受信 – セッション画面の保持が無効になっている場合
- UDP 2598 受信 – セッション画面の保持が有効になっている場合
- UDP 443 受信 – VDA SSL が ICA 暗号化（DTLS）に対して有効になっている場合
- UDP 443 送信 – Citrix Gateway サービスを使用している場合。詳しくは、Citrix Gateway サービスのドキュメントを参照してください。

注意事項

- セッション画面の保持を有効にして、EDT MTU Discovery を使用し、Citrix Gateway および Citrix Gateway サービスで EDT を使用するようにしてください。
- 断片化を回避するために、EDT MTU が適切に設定されていることを確認してください。適切に設定されていない場合、パフォーマンスに影響が出たり、状況によってはセッションの起動に失敗したりすることがあります。詳しくは、「EDT MTU Discovery」セクションを参照してください。

- Citrix Gateway サービスで EDT を使用するための要件と考慮事項について詳しくは、「Citrix Gateway サービスの EDT サポートを備えた HDX アダプティブトランスポート」を参照してください。
- EDT をサポートするための Citrix Gateway 構成について詳しくは、「EDT および HDX Insight をサポートするように Citrix Gateway を構成」を参照してください。
- IPv6 は現在サポートされていません。

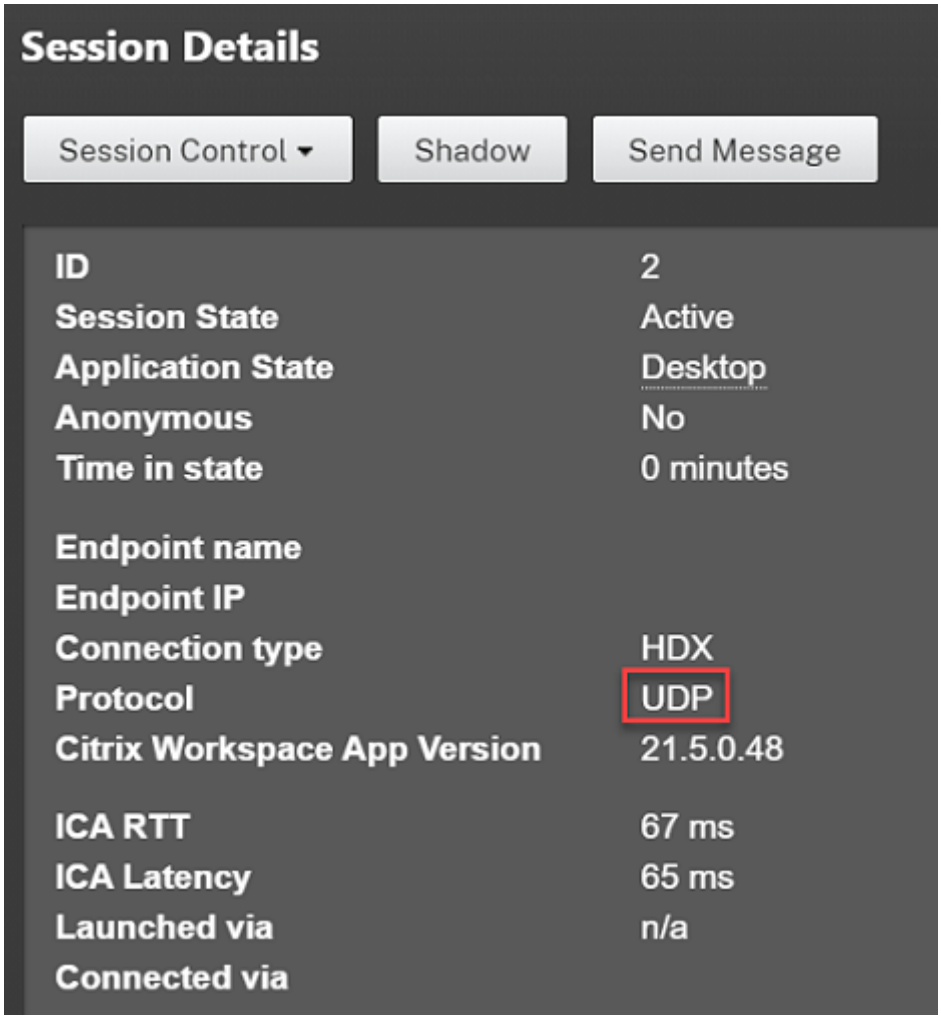
構成

アダプティブトランスポートはデフォルトで有効になっています。Citrix ポリシーの［**HDX** アダプティブトランスポート］設定を使用して、以下のオプションを構成できます。

- 優先。これがデフォルトの設定です。アダプティブトランスポートが有効になっており、TCP へのフォールバックが有効な状態で、EDT を優先トランスポートプロトコルとして使用します。
- 診断モード。アダプティブトランスポートが有効になり、EDT の使用が強制されます。TCP へのフォールバックは無効になっています。この設定は、テストとトラブルシューティングにのみ使用することをお勧めします。
- オフ。アダプティブトランスポートは無効になっており、トランスポートには TCP のみが使用されます。

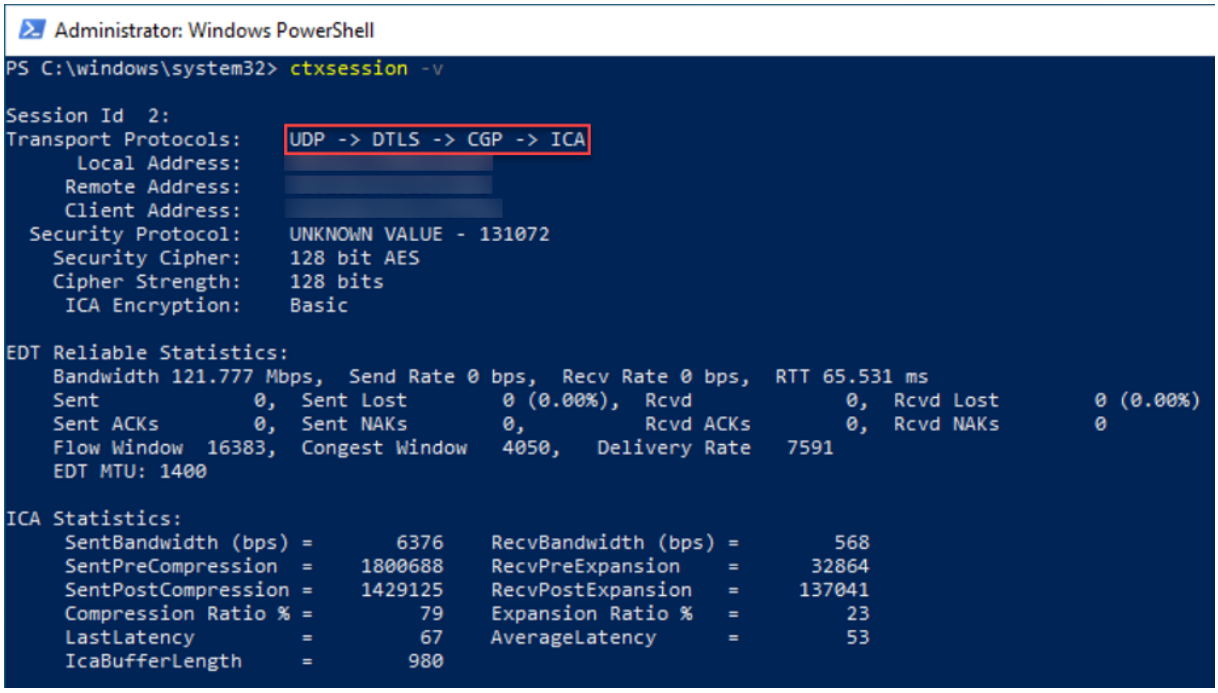
EDT がセッションのトランスポートプロトコルとして使用されていることを確認するために、VDA で Director または CtxSession.exe コマンドラインユーティリティを使用できます。

Director でセッションを検索し、［詳細］を選択します。［接続の種類］が［**HDX**］で［プロトコル］が［**UDP**］の場合、セッションのトランスポートプロトコルとして EDT が使用されています。［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］と表示されます。詳しくは、「セッションの監視」を参照してください。



CtxSession.exe ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe`を実行します。詳細な統計を表示するには、`ctxsession.exe -v`を実行します。EDT が使用されている場合、トランスポートプロトコルは次のいずれかを示します:

- **UDP > ICA**（セッション画面の保持が無効）
- **UDP > CGP > ICA**（セッション画面の保持が有効）
- **UDP > DTLS > CGP > ICA**（ICA は DTLS で暗号化されたエンドツーエンド）



EDT MTU Discovery

MTU Discovery により、セッション確立時に EDT が最大伝送単位（MTU）を自動的に決定できるようにします。これにより、パフォーマンスの低下やセッションの確立失敗となる可能性のある、EDT パケットのフラグメンテーションが防止されます。

システム要件

- VDA 最小バージョン 1912（2103 以降を推奨）
- Windows 向け Citrix Workspace アプリ 1911
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- セッション画面の保持を有効にする必要があります

クライアントプラットフォームまたはこの機能をサポートしていないバージョンを使用している場合、環境に適したカスタムの EDT MTU の構成については、「CTX231821」を参照してください。

> 重要:
>
> MTU Discovery は、マルチストリーム ICA ではサポートされていません。

VDA で EDT MTU Discovery を制御するには

MTU Discovery はデフォルトで有効になっています。この機能を無効にする場合は、**EDT MTU Discovery** レジストリ値を削除して、VDA を再起動します。詳しくは、レジストリを介して管理される HDX 機能の一覧にある「EDT MTU Discovery」の設定を参照してください。

> 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。

クライアントで EDT MTU Discovery を制御するには

ICA ファイルに **MtuDiscovery** パラメーターを追加することで、クライアント上で EDT MTU Discovery を選択的に制御できます。この機能を無効にする場合は、[アプリケーション] セクションで次のように設定します:

```
MtuDiscovery=Off
```

この機能を再度有効にするには、ICA ファイルから **MtuDiscovery** パラメーターを削除します。

> 重要:
>
> この ICA ファイルパラメータを使用するには、VDA でこの機能を有効にします。VDA でこの機能が有効になっていない場合、ICA ファイルパラメーターは無効です。

損失耐性モード

> 重要:
>
> - この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。
> - 損失耐性モードは、Citrix Gateway または Citrix Gateway サービスではサポートされていません。このモードでは、直接接続でのみ使用可能です。

損失耐性モードは、EDT Lossy トランスポートプロトコルを使用し、高遅延やパケット損失が発生しているネットワークで接続中のユーザーのユーザーエクスペリエンスを向上させます。

最初に、セッションは EDT を使用して確立されています。遅延とパケット損失のしきい値に達するかこれを上回っている場合、該当する仮想チャネルは EDT から EDT Lossy に切り替わります。他の仮想チャネルは EDT のままです。遅延とパケット損失がしきい値を下回るまで減少した場合、該当する仮想チャネルは、EDT に切り替わります。

デフォルトのしきい値は次のとおりです:

- パケット損失：5%
- 遅延：300 ミリ秒（RTT）

損失耐性モードはデフォルトで有効になっています。このモードを無効にしたり、損失耐性モードのしきい値設定を使用して、パケット損失や遅延のしきい値を調整したりできます。

システム要件

- Citrix Virtual Delivery Agent（VDA）2003
- Windows 向け Citrix Workspace アプリ 2002
- セッション画面の保持が有効。セッション画面の保持について詳しくは、「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。

既知の問題

アダプティブトランスポートと EDT には、次の問題があります:

- パケットの断片化により、パフォーマンスが低下したり、セッションの起動に失敗したりすることがあります。EDT MTU を調整して、これを回避できます。MTU Discovery を使用するか、「CTX231821」に記載された回避策を実行します。
- MTU Discovery が有効になっている場合、Windows クライアントからセッションを起動すると、灰色または黒色の画面が表示されることがあります。この問題に対処するには、Windows 2105 以降向けの Workspace アプリ、または Windows 1912 CU4 以降向けの Workspace アプリにアップグレードします。
- Linux および Android クライアント上で、Citrix Gateway または Citrix Gateway サービスを介して接続すると、TCP へのフォールバックに失敗することがあります。これは、クライアントと Gateway の間で EDT ネゴシエーションが成功し、Gateway と VDA の間で EDT ネゴシエーションが失敗した場合に発生します。この問題に対処するには、Linux 2104 以降向けの Workspace アプリ、または Android 21.5 以降向けの Workspace アプリにアップグレードします。
- 非対称ネットワークパスにより、MTU Discovery が、Citrix Gateway または Citrix Gateway サービスを介さない接続に失敗することがあります。この問題に対処するには、VDA バージョン 2103 以降にアップグレードします。
- Citrix Gateway または Citrix Gateway サービスを使用している場合、非対称ネットワークパスが原因で MTU Discovery が失敗することがあります。これは、Gateway で EDT パケットのヘッダーの Don't Fragment（DF）ビットが伝播されないことが原因です。この問題はまだ修正されていません。
- DS-Lite ネットワークを介して接続するユーザーの場合、MTU Discovery が失敗することがあります。一部のモデムでは、パケット処理が有効になっていると DF ビットを正しく処理できず、MTU Discovery が断片化を検出できなくなります。この状況では、次のオプションを使用できます:
  - ユーザーのモデムでパケット処理を無効にします。
  - 「CTX231821」で説明されているように、MTU Discovery を無効にし、ハードコードされた MTU を使用します。
  - アダプティブトランスポートを無効にして、セッションに TCP の使用を強制します。ユーザーのサブセットのみが影響を受ける場合は、他のユーザーが引き続き EDT を使用できるように、クライアント側でそれを無効にすることを検討してください。

トラブルシューティング

アダプティブトランスポートと EDT のトラブルシューティングを行うには、次のことをお勧めします:

1. 要件、注意事項、および既知の問題を十分に確認および検証します。
2. Studio または GPO に Citrix ポリシーがあり、目的の **HDX** アダプティブトランスポート設定を上書きしていないかどうかを確認します。
3. 目的の HDX アダプティブトランスポート設定を上書きする設定がクライアントにあるかどうかを確認します。上書きする設定とは、GPO 設定、オプションの Workspace アプリ管理テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルで手動で構成された **HDXoverUDP** 設定などです。
4. マルチセッション VDA マシンでは、UDP リスナーがアクティブであることを確認してください。VDA マシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳しくは、「HDX Enlightened Data Transport プロトコルの確認方法」を参照してください。
5. 内部で直接セッションを起動し、Citrix Gateway をバイパスして、使用中のプロトコルを確認します。セッションで EDT を使用する場合、VDA は Citrix Gateway を介した外部接続に EDT を使用するよう準備しています。
6. EDT が直接内部接続では機能し、Citrix Gateway を介したセッションでは機能しない場合:
   - セッション画面の保持が有効になっていることを確認します
   - Gateway で DTLS が有効になっていることを確認します
7. ネットワークファイアウォールと VDA マシンで実行されているファイアウォールの両方で適切なファイアウォール規則が構成されているかどうかを確認します。
8. ユーザーの接続に非標準の MTU が必要かどうかを確認します。有効 MTU が 1500 バイト未満の接続は、EDT パケットの断片化を引き起こし、パフォーマンスに影響を与えたり、セッションの起動に失敗したりすることがあります。この問題は、VPN、一部の Wi-Fi アクセスポイント、および 4G や 5G などのモバイルネットワークを使用している場合によく発生します。この問題に対処する方法については、「MTU Discovery」セクションを参照してください。

Citrix SD-WAN との相互運用性

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、帯域幅を大幅に削減します。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に、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、WANOP により VDA サーバーの CPU 負荷を軽減し、Citrix Virtual Apps and Desktops サーバーでより高いスケーラビリティを実現します。

現在、SD-WAN WANOP は EDT をサポートしていません。ただし、SD-WAN WANOP が使用されている場合は、アダプティブトランスポートを無効にする必要はありません。ユーザーが WANOP を有効にした SD-WAN でセッシ

ョンを起動すると、トランスポートプロトコルとして TCP を使用するようにセッションが自動的に設定されます。非 WANOP セッションは、引き続き可能な限り EDT を使用します。

Citrix ICA 仮想チャネル

April 24, 2021

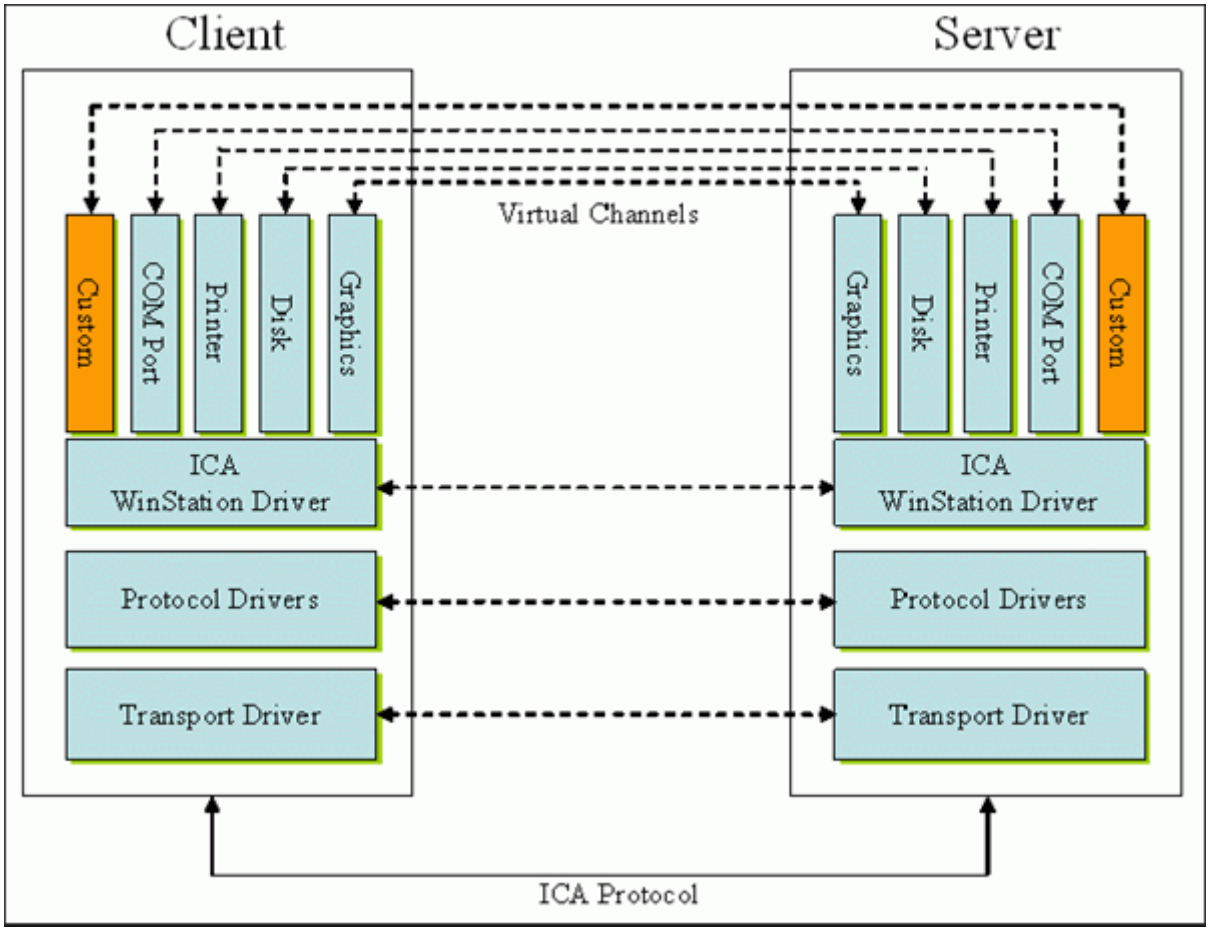
> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

ICA 仮想チャネルとは何か

Citrix Workspace アプリと Citrix Virtual Apps and Desktops サーバー間の機能および通信の大部分は、仮想チャネル経由で実行されます。仮想チャネルは Citrix Virtual Apps and Desktops サーバーを使用したリモートコンピューティング環境に不可欠な要素です。仮想チャネルは次の用途に使用されます:

- オーディオ
- COM ポート
- ディスク
- グラフィック
- LPT ポート
- プリンター
- スマートカード
- サードパーティのカスタム仮想チャネル
- ビデオ

Citrix Virtual Apps and Desktops サーバーおよび Citrix Workspace アプリの新しいバージョンとともに、追加機能を提供する新しい仮想チャネルが随時リリースされます。



仮想チャネルは、サーバー側のアプリケーションと通信するクライアント側の仮想ドライバーで構成されます。Citrix Virtual Apps and Desktops には、さまざまな仮想チャネルが含まれています。提供されている各種ソフトウェア開発キット（SDK）のいずれかを使用して、ユーザーやサードパーティベンダーが独自の仮想チャネルを作成できるように設計されています。

仮想チャネルによって、さまざまなタスクを安全な方法で実行できます。たとえば、Citrix Virtual Apps サーバー上で動作するアプリケーションとクライアント側デバイス間の通信や、アプリケーションとクライアント側環境間の通信などです。

クライアント側では、仮想チャネルは仮想ドライバーに対応します。各仮想ドライバーは、特定の機能を提供します。通常の動作に必要な仮想ドライバーやオプションの仮想ドライバーもあります。仮想ドライバーは、プレゼンテーション層のプロトコルレベルで動作します。Windows Station（WinStation）プロトコル層で提供されたチャネルを多重化することにより、いつでも複数のプロトコルをアクティブにできます。

以下の機能は、次のレジストリパスの VirtualDriver レジストリ値に含まれています：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced
\Modules\ICA 3.0
```

または

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`（64 ビット版の場合）

- Thinwire3.0（必須）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- クリップボード
- ClientComm
- ClientAudio
- LicenseHandler（必須）
- TWI（必須）
- SmartCard
- ICACTL（必須）
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> 注:
>
> レジストリキーからこれらの 1 つまたは複数の値を削除することによって、特定のクライアント機能を無効にできます。たとえば、クライアントクリップボードを削除する場合は、**Clipboard** という単語を削除します。

この一覧には、クライアント仮想ドライバーファイルと対応する機能が含まれています。Citrix Virtual Apps および Windows 向け Citrix Workspace アプリはこれらのファイルを使用します。これらは Windows ドライバー（カーネルモード）形式ではなく、ダイナミックリンクライブラリ（ユーザーモード）形式のファイルです。ただし、汎用 USB 仮想チャネルで説明する汎用 USB は例外です。

- vd3dn.dll – デスクトップコンポジションリダイレクトに使用される Direct3D 仮想チャネル
- vdcamN.dll – 双方向オーディオ
- vdcdm30n.dll – クライアント側ドライブのマッピング
- vdcom30N.dll - クライアント側 COM ポートのマッピング
- vdcpm30N.dll – クライアント側プリンターのマッピング
- vdctln.dll – ICA コントロールチャネル
- vddvc0n.dll – 動的仮想チャネル
- vdeuemn.dll - EUEM（End User Experience Monitoring：エンドユーザー状況監視）
- vdgusbn.dll – 汎用 USB 仮想チャネル
- vdkbhook.dll – 透過的なキーのパススルー
- vdlfpn.dll – UDP 経由の Framehawk ディスプレイチャネル（転送など）
- vdmmn.dll – マルチメディアのサポート
- vdmrvc.dll – Mobile Receiver 仮想チャネル
- vdmtchn.dll - マルチタッチのサポート

- vdscardn.dll – スマートカードのサポート
- vdsens.dll – センサー仮想チャネル
- vdspl30n.dll – クライアントの UPD
- vdsspin.dll – Kerberos
- vdtuin.dll – 透過的な UI
- vdtw30n.dll – クライアントの Thinwire
- vdtwin.dll – シームレス
- vdtwn.dll – Twain

一部の仮想チャネルは、他のファイルにコンパイルされています。たとえば、クリップボードマッピング機能は wfica32.exe で利用できます。

64 ビット環境との互換性

Windows 向け Citrix Workspace アプリは 64 ビット環境との互換性があります。32 ビット用にコンパイルされた大半のバイナリのように、これらのクライアントファイルには、64 ビットでコンパイル版があります:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

汎用 USB 仮想チャネル

汎用 USB 仮想チャネルの実装では、仮想チャネルドライバー vdgusbn.dll とともに 2 つのカーネルモードドライバーが使用されます。

- ctxusbm.sys
- ctxusbr.sys

ICA 仮想チャネルの動作

仮想チャネルはさまざまな方法で読み込まれます。シェル（サーバーの場合 WfShell、ワークステーションの場合 PicaShell）によって読み込まれる仮想チャネルがあります。一部の仮想チャネルは Windows サービスとしてホス

トされています。

以下は、シェルによって読み込まれる仮想チャネルモジュールの例です:

- EUEM
- Twain
- クリップボード
- マルチメディア
- シームレスなセッション共有
- タイムゾーン

以下の例のように、カーネルモードで読み込まれる場合もあります:

- ctxDvcs.sys – 動的仮想チャネル
- icausbb.sys – 汎用 USB リダイレクト
- picadm.sys – クライアント側ドライブのマッピング
- picaser.sys – COM ポートリダイレクト
- picapar.sys – LPT ポートリダイレクト

サーバー側のグラフィック仮想チャネル

XenApp 7.0 および XenDesktop7.0 以降では、`ctxgfx.exe`はワークステーションとターミナルサーバーの両方でセッションごとにグラフィック仮想チャネルをホストします。`Ctxgfx`は、対応するドライバー（RDSH の場合は`Icardd.dll`、ワークステーションの場合は`vdod.dll`と`vidd.dll`）と通信するプラットフォーム固有のモジュールをホストします。

XenDesktop 3D Pro 展開では、OEM グラフィックドライバーは VDA の対応する GPU にインストールされています。`Ctxgfx`は、OEM グラフィックドライバーと通信するための専用のアダプターモジュールを読み込みます。

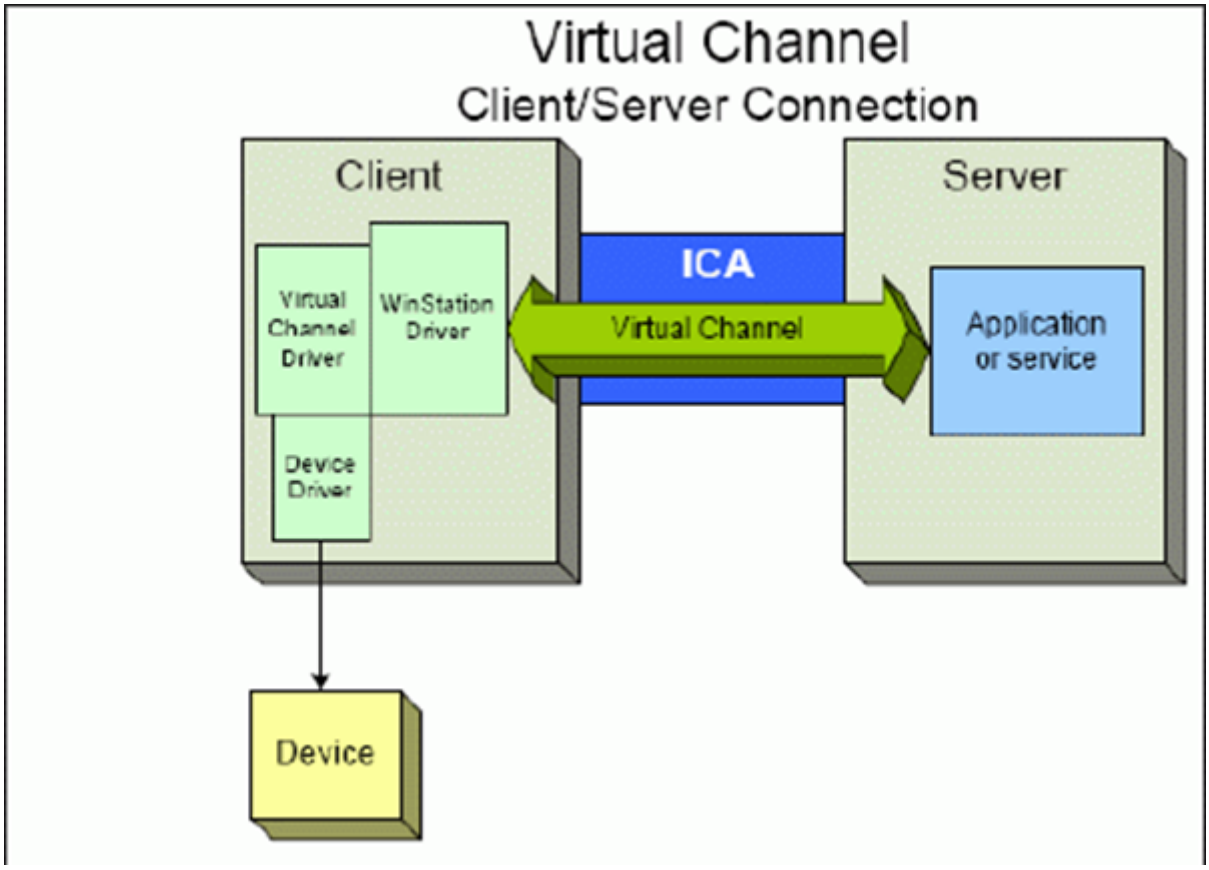
Windows サービスでの専用チャネルのホスト

Citrix Virtual Apps and Desktops サーバーでは、さまざまなチャネルが Windows サービスとしてホストされています。これによって、サーバー上のシングルセッションおよびマルチセッションで複数のアプリケーションの 1 対多の運用が可能になります。以下はこうしたサービスの例です:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix EUEM （End User Experience Monitoring: エンドユーザー状況監視）
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service（Citrix Virtual Desktops のみ）

Windows オーディオサービスを使用して Citrix Virtual Apps でオーディオ仮想チャネルがホストされます。

サーバー側では、すべてのクライアント仮想チャネルは WinStation ドライバー（Wdica.sys）経由でルーティングされます。クライアント側では、wfica32.exe に組み込まれた対応する WinStation ドライバーがクライアント仮想チャネルをポーリングします。この図は、仮想チャネルクライアント-サーバー間接続を示しています。



これは、仮想チャネルを使用したクライアント-サーバー間のデータ交換処理の概要を示します。

1. クライアントが Citrix Virtual Apps and Desktops サーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側アプリケーションが起動し、仮想チャネルのハンドルを取得して、必要に応じて仮想チャネルに関する情報を問い合わせます。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の 2 つの方法でデータを渡します：
    - サーバー側アプリケーションにクライアントへの送信データがある場合は、そのデータが直ちにクライアントに送信されます。クライアントがこのデータを受け取ると、WinStation ドライバーが ICA ストリームから仮想チャネルデータを逆多重化し、それを直ちにクライアント仮想ドライバーに渡します。
    - クライアント仮想ドライバーにサーバーへの送信データがある場合は、WinStation ドライバーが次回ポーリングを行ったときにそのデータが送信されます。サーバーがこのデータを受信すると、そのデータは仮想チャネルアプリケーションが読み込むまでキューに保持されます。サーバーがデータを受け取ったことは、サーバーの仮想チャネルアプリケーションに通知されません。

4. サーバーの仮想チャネルアプリケーションが読み取りを完了すると、アプリケーションは仮想チャネルを終了し、割り当てられているすべてのリソースが解放されます。

仮想チャネル **SDK** を使って独自の仮想チャネルを作成する

仮想チャネル SDK を使って仮想チャネルを作成するには、プログラミング知識が必要です。この方法で、クライアントとサーバー間の主要な通信パスを提供します。例として、クライアント側であるデバイス（スキャナーなど）をセッション内のプロセスとともに使用する機能を実装する場合などがあります。

> 注:
>
> - 仮想チャネル SDK では、WFAPI SDK で仮想チャネルのサーバー側を作成する必要があります。
> - Citrix Virtual Apps and Desktops および Windows 向け Citrix Workspace アプリではセキュリティが強化されているため、カスタム仮想チャネルのインストール時に追加手順が必要になります。

ICA クライアントオブジェクト **SDK** を使って独自の仮想チャネルを作成する

ICA クライアントオブジェクト（ICO）を使用した仮想チャネルの作成は、仮想チャネル SDK を使用する場合より簡単です。プログラム内で **CreateChannels** メソッドを使って名前付きオブジェクトを作成し、ICO を使用します。

> 重要:
>
> Citrix Receiver for Windows バージョン 10.00 以降（および Windows 向け Citrix Workspace アプリ）ではセキュリティが強化されているため、ICO 仮想チャネルの作成時に追加手順が必要になります。

詳しくは、「Client Object API Specification Programmer's Guide」を参照してください。

仮想チャネルのパススルー機能

Citrix から提供される仮想チャネルの大部分は、ICA セッション内またはより一般にパススルーセッションと呼ばれるセッション内で Windows 向け Citrix Workspace アプリを使用する場合でも変更なしで動作しますが、マルチホップ構成でクライアントを使用する場合はいくつか注意すべき点があります。

以下の機能は、シングルホップ構成でもマルチホップ構成でも同様に動作します:

- クライアント側 COM ポートのマッピング
- クライアントドライブマッピング
- クライアント側プリンターのマッピング
- クライアントの UPD
- EUEM（End User Experience Monitoring：エンドユーザー状況監視）
- 汎用 USB
- kerberos
- マルチメディアのサポート
- スマートカードのサポート

- 透過的なキーのパススルー
- Twain

各ホップで実行される圧縮、展開、レンダリングなどの処理に本質的に伴う遅延やその他の要因により、一部の機能ではクライアントが経由するホップが増えるとパフォーマンスが影響を受ける可能性があります。以下は影響を受ける機能です:

- 双方向オーディオ
- ファイル転送
- 汎用 USB リダイレクト
- シームレス
- Thinwire

> 重要:
>
> デフォルトでは、パススルーセッション内で動作するクライアントのインスタンスによってマップされるクライアントドライブは、接続元クライアントドライブに制限されます。

Citrix Virtual Desktops セッションと **Citrix Virtual Apps** セッション間の仮想チャネルのパススルー機能

多くの Citrix 製品は、Windows 向け Citrix Workspace アプリが Citrix Virtual Desktops サーバー上の ICA セッション内（一般的にはパススルーセッションとして知られている）で使用されている場合、操作が変更されることなく動作する仮想チャネルを提供しています。

具体的には、Citrix Virtual Desktops サーバー上で **picaPassthruHook** を実行する VDA Hook があります。これによって、クライアントを CPS サーバー上で動作していると信じさせ、一般的なパススルーモードへと設定します。

以下の標準的な仮想チャネルおよびその機能がサポートされています:

- クライアント
- クライアント側 COM ポートのマッピング
- クライアントドライブマッピング
- クライアント側プリンターのマッピング
- 汎用 USB（パフォーマンスにより制限あり）
- マルチメディアのサポート
- スマートカードのサポート
- SSON
- 透過的なキーのパススルー

セキュリティと **ICA** 仮想チャネル

使用環境でのセキュリティ確保は、仮想チャネルのプランニング、開発、実装における重要な要素です。この文書には、特定分野のセキュリティに関する参照情報が記載しています。

ベストプラクティス

仮想チャネルは接続時および再接続時に開き、ログオフ時および切断時に閉じます。

仮想チャネル機能を使用するスクリプトを作成する場合は、以下の指針に従います。

仮想チャネルの名前付け:

仮想チャネルは最大で 32 個作成できます。そのうち 17 個は、特定の用途に予約されています。

- 仮想チャネルには、7 文字以下の名前を付ける必要があります。
- 最初の 3 文字はベンダー名、それ以降の 4 文字はチャネルの種類を表します。たとえば、**CTXAUD** は Citrix のオーディオ仮想チャネルを表します。

仮想チャネルは、ASCII 文字からなる 7 文字以下の名前で参照されます。ICA プロトコルの以前のバージョンでは仮想チャネルに番号が付けられていましたが、現在のバージョンでは ASCII 名に基づいて動的に番号が付けられるため、実装が簡単になっています。社内でのみ使用する独自の仮想チャネルを開発する場合、仮想チャネルには既存の仮想チャネル名と異なる任意の 7 文字の名前を付けることができます。仮想チャネル名では、ASCII 文字の大文字、小文字、数字だけを使用できます。独自の仮想チャネルを追加する場合は、既存の命名規則に従います。あらかじめ定義されているいくつかの仮想チャネルがあります。これらの仮想チャネルはすべて、OEM 識別子 CTX から始まる名前を持ち、Citrix によってのみ使用されます。

ダブルホップのサポート:

仮想チャネル	ダブルホップがサポートされているか
オーディオ	いいえ
Web ブラウザーコンテンツのリダイレクト	いいえ
CDM	はい
CEIP	いいえ
クリップボード	はい
Continuum（MRVC）	いいえ
コントロール VC	はい
HTML5 ビデオリダイレクト（v1）	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい

仮想チャネル	ダブルホップがサポートされているか
Twain	はい
USB VC	はい
WAYCOM デバイス（USB VC 使用の K2M）	はい
Web カメラビデオ圧縮	はい
Windows Media リダイレクト	はい

関連項目

- ICA 仮想チャネル SDK
- Citrix Developer Networkには、Citrix SDK に関するあらゆる技術的なリソースおよび解説が集約されています。このネットワークでは、SDK、サンプルコード、スクリプト、拡張機能、プラグインや、SDK ドキュメントにアクセスできます。また、Citrix Developer Network フォーラムでは、各 Citrix SDK に関する技術的な議論を参照できます。

インストールと構成

April 26, 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。

Citrix Virtual Apps and Desktops を展開するには、次の手順を実行します。

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をインストールします。Citrix StoreFront をインストールすることもできます。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を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 PC 上にシングルセッション OS 対応 VDA 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ついては、「インストールの準備」を参照してください。）

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 フェデレーション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。

必要に応じて、Citrix Virtual Apps and Desktops 展開に Citrix コンポーネントをさらに統合します。

- Citrix Provisioningは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 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 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。

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

April 26, 2021

Citrix Virtual Apps and Desktops の展開では、まず次のコンポーネントをインストールします。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がいる場合には、Citrix Gateway 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。詳しくは、「Citrix Virtual Apps and Desktops と Citrix Gateway の統合」を参照してください。

製品 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 Citrix Provisioning（旧称 Provisioning Services）のマスターイメージを管理することもできます。詳しくは、「スクリプトを使用した VDA のインストール」を参照してください。

インストール前に確認する情報

- 製品の技術概要：製品およびコンポーネントについて理解を深める場合。
- 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。
- サポートされているコンポーネントをサーバーコア OS（Delivery Controller など）にインストールするには、コマンドラインを使用する必要があります。このタイプの OS ではグラフィカルユーザーインターフェイスを利用できないため、まず Studio などのツールを別の場所にインストールし、それらにコントローラーサーバーを参照させます。

Delivery Controller とマルチセッション OS 対応 VDA 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マルチセッション OS の **Virtual Delivery Agent** 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。

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。

Citrix Hypervisor では、仮想マシンの電源状態が登録されているように見える場合でも、未知として表示されることがあります。この問題を解決するには、レジストリキーの`HostTime`値を編集して、ホストとの時間同期を無効にします:

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

> ヒント:
>
> デフォルト値は`HostTime="UTC"`です。この値を、`Local`など、UTC 以外の値に変更します。この変更により、ホストとの時間同期が効果的に無効になります。

シングルセッション Windows 10 マシンでの最適化ガイダンスは、CTX216252を参照してください。

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。

この製品バージョンでサポートされていない OS に Windows VDA をインストール（またはアップグレード）しようとすると、メッセージが表示され、オプションについて記述された記事が示されます。

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は Citrix Virtual Apps and Desktops 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

- コアコンポーネント（Delivery Controller、Studio、ライセンスサーバー、Director）を全製品 ISO からインストールまたはアップグレードする場合、マシンの過去の Windows インストールから再起動が保留されていることが Citrix インストーラーで検知されると、インストーラーは終了/リターンコード 9 で停止します。マシンを再起動するように求められます。

  これは、Citrix による強制再起動ではありません。この状況は、以前マシンにインストールされた他のコンポーネントが原因で発生します。この状況が発生した場合、マシンを再起動してから、Citrix インストーラーを再起動します。

  コマンドラインインターフェイスを使用する場合、コマンドに/no_pending_reboot_checkオプションを含めて保留中の再起動のチェックを阻止できます。

- 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、Citrix Analytics 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別の Citrix プログラム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。

- Studio をインストール（またはアップグレード）すると、Google Analytics が自動的に収集され（後でアップロードされ）ます。Studio をインストールした後、レジストリキーHKLM\Software\Citrix\

DesktopStudio\GAEnabledでこの設定を変更できます。値 **1** で収集とアップロードを有効にし、**0** で収集とアップロードを無効にします。

- VDA のインストールが失敗すると、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。

VDA インストール時

Windows 向け Citrix Workspace アプリを使用可能ですが、デフォルトでは VDA をインストールしてもこのアプリはインストールされません。Windows 向け Citrix Workspace アプリおよび他の Citrix Workspace アプリは、管理者またはユーザーが Citrix Web サイトからダウンロードし、インストールできます。また、StoreFront サーバーでこれらの Citrix Workspace アプリを公開することもできます。詳しくは、StoreFront のドキュメント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 マルチセッション 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オプションを使用してください。

VDA が実装されたマシンに 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。

- 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

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。シングルセッション OS 対応 VDA では、このグループは RDP 接続のみに適用されます。マルチセッション OS 対応 VDA 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 サポートツール

各 VDA インストーラーには、VDA のパフォーマンス（全体的な正常性や接続品質など）をチェックするための Citrix ツールを含む、サポート MSI が含まれています。こうした MSI のインストールを行うかどうかは、VDA インストーラーのグラフィカルユーザーインターフェイスの ［追加コンポーネント］ページで指定します。インストールを無効にするには、コマンドラインから、`/exclude "Citrix Supportability Tools"`オプションを実行します。

デフォルトでは、サポート MSI は`c:\Program Files (x86)\Citrix\Supportability Tools\`にインストールされています。この場所は、VDA インストーラーのグラフィカルユーザーインターフェイスの ［コンポーネント］ページ、または`/installdir`コマンドラインオプションで変更できます。この場所を変更すると、サポートツールのみでなく、インストールされているすべての VDA コンポーネントの場所が変更されることに注意してください。

サポート MSI 内の現在のツール:

- Citrix Health Assistant: 詳しくは、CTX207624を参照してください。
- VDA Cleanup Utility: 詳しくは、CTX209255を参照してください。

VDA のインストール時にこのツールをインストールしない場合は、CTX の記事に、現在のダウンロードパッケージへのリンクが含まれています。

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 をバージョン 7.17（またはそれ以降のサポートされているバージョン）にアップグレードするときは、アップグレード中に再起動が行われます。これを防ぐことはできません。

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 マルチセッション 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。

> 注:
>
> VDA をバージョン 7.17 以降のサポートされているバージョンにアップグレードするときは、アップグレード

> 中に再起動が行われます。これを防ぐことはできません。

インストーラー

全製品インストーラー

ISO で提供される全製品インストーラーを使用すると、以下のことができます:

- コアコンポーネント（Delivery Controller、Studio、Director、ライセンスサーバー）のインストール、アップグレード、削除
- StoreFront のインストールまたはアップグレード
- シングルセッション OS またはマルチセッション OS 対応 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`UpsServer`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
- Session Recordingをインストールします。

（Web サイト開発などで）1 人のユーザー用にマルチセッション 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。（製品のインストールメディアでは入手できません。）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`フォルダーのドライブには、製品 ISO の VDA インストーラーを使用する場合よりも多くの空き領域が必要です。ただし、インストールの完了後、Temp フォルダーに抽出されたファイルは自動的に削除されます。または、絶対パスとともに/`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:

マルチセッション OS 対応 VDA 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マルチセッション OS 対応 VDA オプションをすべてサポートしています。

VDAWorkstationSetup.exe:

シングルセッション OS 対応 VDA 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シングルセッション OS 対応 VDA 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シングルセッション OS 対応 VDA 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.exe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 の表示に影響が生じます。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。
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook

VDAWorkstationCoreSetup.exeインストーラーには Windows 向け Citrix Workspace アプリは含まれておらず、インストールされません。

VDAWorkstationCoreSetup.exeを使用することは、全製品またはVDAWorkstationSetupインストーラーを使用することと同等であり、シングルセッション OS VDA をインストールして、次のいずれかを実行します:

- 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ます。
- コマンドラインインターフェイス: /remotepcオプションを指定します。
- 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""Citrix Supportability Tools""Citrix Files for Windows"を指定します。

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をすべてインストールできます。

VDAWorkstationCoreSetup.exeインストーラーは自動的に Web ブラウザーコンテンツリダイレクト MSI をインストールします。この自動インストールは、リリース 2003 以降でサポートされるリリースで使用できます。

Citrix インストールリターンコード

インストールログには、Microsoft の値ではなく、Citrix のリターンコードとしてコンポーネントをインストールした結果が含まれています。

- 0 = Success（成功）
- 1 = Failed（失敗）

- 2 = PartialSuccess（一部成功）
- 3 = PartialSuccessAndRebootNeeded（一部成功、再起動が必要）
- 4 = FailureAndRebootNeeded（失敗、再起動が必要）
- 5 = UserCanceled（ユーザーキャンセル）
- 6 = MissingCommandLineArgument（コマンドライン引数がない）
- 7 = NewerVersionFound（新バージョン検出）

たとえば、Microsoft System Center Configuration Manager などのツールを使用する場合、インストールログにリターンコード 3 が含まれていると、スクリプトによる VDA インストールが失敗したように見えることがあります。これは、VDA インストーラーが人を介して開始する必要がある再起動を待っているとき（たとえば、サーバーにリモートデスクトップサービスの役割の前提条件をインストールした後）に発生する可能性があります。VDA のインストールは、すべての前提条件と選択したコンポーネントがインストールされ、インストール後にマシンが再起動された後でのみ、完了したとみなされます。

代わりの方法として、インストールコマンドを CMD スクリプト（Microsoft の終了コードを返します）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。

Microsoft Azure Resource Manager 仮想化環境

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで VDA をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

はじめに

お使いの環境で 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。

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/

制限事項

Azure Resource Manager を構成する場合は、以下の制限事項を考慮します:

- Machine Creation Services を使用している場合、Azure Disk Encryption はサポートされません。

Azure のオンデマンドプロビジョニング

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure のオンデマンドプロビジョニング機能は次のことを実現します。

- ストレージコストを削減する。
- カタログ作成を高速化する。
- 仮想マシン（VM）の電源操作を高速化する。

管理者にとっては、ホスト接続と MCS マシンカタログを作成する際に、オンデマンドプロビジョニングと Studio で手順に違いはありません。相違点は、Azure でリソースを作成し管理する方法とそのタイミング、Azure Portal での VM の可視性です。

Citrix Virtual Apps and Desktops で Azure のオンデマンドプロビジョニングが使用される前は、MCS でカタログを作成すると、プロビジョニングプロセス中に Azure に VM が作成されていました。

Azure のオンデマンドプロビジョニングでは、VM は、プロビジョニング完了後、Citrix Virtual Apps and Desktops で電源投入操作が開始されたときにのみ作成されます。Azure Portal では、実行中の VM のみが表示されます。（Studio では、VM は実行中かどうかに関係なく表示されます）。

MCS カタログを作成すると、Azure Portal にリソースグループ、ネットワークセキュリティグループ、ストレージアカウント、ネットワークインターフェイス、基本イメージ、ID ディスクが表示されます。Citrix Virtual Apps and Desktops が VM の電源投入操作を開始するまで、その VM は表示されません。その後、Studio では VM のステータスがオンに変わります。

- プールされたマシンの場合、オペレーティングシステムのディスクとライトバックキャッシュは、VM が存在する場合にのみ存在します。この構成により、マシンを定期的に（たとえば、勤務時間外に）シャットダウンする場合はストレージを大幅に節約できます。
- 専用マシンでは、VM の初回電源投入時にオペレーティングシステムのディスクが作成されます。このディスクは、マシンが削除されるまでストレージに残ります。

Citrix Virtual Apps and Desktops が VM の電源切断操作を開始すると、その VM は削除されます。Azure ポータルには表示されなくなります Studio では、VM のステータスはオフに変わります。

オンデマンドプロビジョニング前に作成されたカタログ

Citrix Virtual Apps and Desktops より前に作成されていたマシンカタログは、Azure のオンデマンドプロビジョニング機能ををサポートしていました（2017 年半ば）。これらのカタログ内の仮想マシンは、実行中かどうかにかかわらず、Azure ポータルに表示されます。これらの VM をオンデマンドマシンに変換することはできません。

オンデマンドプロビジョニングの強化されたパフォーマンスとストレージコスト上の利点を活用するには、MCS を使用してカタログを作成してください。

Azure Managed Disks

Azure Managed Disks は、従来のストレージアカウントを使用する代わりに、MCS で作成したマシンカタログで使用できる柔軟なディスク記憶域システムです。

Managed Disks 機能により、ストレージアカウントの作成と管理の複雑さが解消されます。ディスクの作成と管理のために、シンプルで可用性の高いソリューションが備えられています。マスターイメージとしての Managed Disks、および VM を使用できます。Managed Disks を使用すると、マシンカタログの作成および更新時間を改善できます。詳しくは、「Managed Disks の概要」を参照してください。

デフォルトでは、マシンカタログは Managed Disks を使用します。このデフォルトはカタログを作成するときに上書きできます。

I/O 最適化構成では（VM ごとに 3 つのディスクを使用する場合）、サブスクリプションごとに最大 3,333 の VM をプロビジョニングします。I/O 最適化が構成されていない場合（VM ごとに 2 つのディスクを使用する場合）、サブスクリプションで最大 5,000 の VM ディスクをプロビジョニングできます。Managed Disks の機能では、サブスクリプションで最大 10,000 の VM ディスクを作成できます。

Managed Disks の使用

Studio でマシンカタログを作成すると、カタログ作成ウィザードの ［マスターイメージ］ページに、Managed Disks と VM および VHD が表示されます。すべての Azure リージョンが Managed Disks の機能をサポートしているわけではありません。カタログのホスト接続に表示されているリージョンについては、Managed Disks が一覧に表示されます。

カタログの作成時間は、画像とカタログが同じリージョンにある場合に最適化されます。

Managed Disks の機能は現在、Azure リージョン間におけるディスクのコピーをサポートしていません。MCS がカタログをプロビジョニングする場所以外のリージョンでイメージを選択すると、そのイメージはカタログ領域の従来のストレージアカウントの VHD にコピーされます。その後、Managed Disks に変換されて戻されます。

カタログ作成ウィザードの ［ストレージとライセンスの種類］ページで、Managed Disks の代わりに従来のストレージアカウントを使用するチェックボックスをオンにすることもできますこのチェックボックスは、Managed Disks をサポートしていない Azure リージョンでプロビジョニングしている場合は淡色表示されます。

Azure Resource Manager への接続の作成

接続を作成するウィザードについて詳しくは、「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を扱っています。

注意事項:

- サービスプリンシパルには、サブスクリプションの投稿者の役割が付与されている必要があります。
- 最初の接続を作成するときに、必要な権限付与を求めるプロンプトが Azure で表示されます。その後の接続でも認証は必要ですが、Azure では以前の同意が記憶され、このプロンプトは再表示されません。
- 認証に使用されるアカウントは、サブスクリプションの共同管理者である必要があります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべき 2 つのタイプのアカウントがあります。「職場または学校」と「個人用 Microsoft アカウント」です。詳しくは、CTX219211を参照してください。
- 既存の Microsoft アカウントは、サブスクリプションのディレクトリのメンバーとして追加して使用できますが、複雑になることがあります。たとえば、ユーザーが以前にディレクトリのリソースの 1 つにゲストアクセスを許可されていた場合などです。必要な権限を与えないディレクトリにプレースホルダーエントリが存在し、エラーが返されます。ディレクトリからリソースを削除して、明示的に追加し直します。ただし、そのアカウントがアクセスできる他のリソースに対して意図しない影響を与えるため、このオプションは注意深く実行してください。
- 特定のアカウントが実際にメンバーであるときにディレクトリゲストとして検出されるという既知の問題があります。アカウントの問題は、確立済みの古いディレクトリアカウントで発生します。アカウントをディレクトリに追加します。これにより適切なメンバーシップ値が取得されます。
- リソースグループはリソースのコンテナにすぎず、そのリージョン以外のリージョンのリソースを含んでいます。リソースグループのリージョンに表示されているリソースを利用できると期待した場合に、これらのグループが混乱を招く可能性があります。
- ネットワークとサブネットが、必要な数のマシンをホストするのに十分な大きさであることを確認してください。

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、接続の種類に ［**Microsoft Azure**］を選択します。お使いの Azure Cloud 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。接続名に指定できる文字数は 1〜64 文字であり、空白スペースのみにしたり英数字以外の文字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、表示された権限を Citrix Virtual Apps and Desktops に付与します。Citrix Virtual Apps and Desktops 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 への認証に成功すると、［新規作成］ボタンと ［既存を使用］ボタンが置き換えられます。［接続］、および緑色のチェックマークは、Azure サブスクリプションへの接続に成功したことを示します。
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。
8. 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 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、英数字以外の文字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します。
9. 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。

1. Azure Resource Manager サブスクリプションに接続します。

   ```
   Login-AzureRmAccount
   ```

2. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Select-AzureRmSubscription -SubscriptionID $SubscriptionId
   ```

3. AD テナントでアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzureRmADApplication -DisplayName $ApplicationName
    -HomePage "https://localhost/$ApplicationName"-IdentifierUris https://
   $ApplicationName -Password $ApplicationPassword
   ```

4. サービスプリンシパルを作成します。

   ```
   New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
   ApplicationId
   ```

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
   ```

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。接続名に指定できる文字数は 1～64 文字であり、空白スペースのみにしたり英数字以外の文字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によって、Azure サブスクリプションに接続されます［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。
5. 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 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、英数字以外の文字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。

6. 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情報です。

マスターイメージは、マシンカタログの仮想マシンの作成に使用されることになるテンプレートです。マシンカタログを作成する前に、Azure Resource Manager でマスターイメージを作成します。マスターイメージの一般的な情報については、「マシンカタログの作成」を参照してください。

Studio でのマシンカタログを作成する場合は、以下を確認してください。

- ［オペレーティングシステム］ページと［マシン管理］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従います。
- ［マスターイメージ］ページで、リソースグループを選択します。コンテナ内で、マスターイメージとして使用する Azure VHD まで移動（ドリルダウン）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://azure.microsoft.com/en-us/documentation/articles/storage-premium-storage/
  - https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/

  既存のオンプレミスの Windows Server ライセンスを使用するかを選択します。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。

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/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。

- (MCS を使用する場合) [リソースグループ] ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。

  リソースグループを作成する場合は、[次へ] をクリックします。

  既存のリソースグループを使用する場合は、[使用可能なプロビジョニングリソースグループ] ボックスの一覧からグループを選択します。カタログで作成しているマシンを収容するのに十分なグループを選択してください。少なすぎると、Studio にメッセージが表示されます。後でカタログにさらに VM を追加する予定がある場合は、必要最小限よりも多く選択しておくことをお勧めします。カタログが作成された後、カタログにリソースグループをさらに追加することはできません。

  詳しくは、「Azure リソースグループ」を参照してください。

- [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」のガイダンスに従います。

ウィザードを完了します。

マシンカタログを削除する

Azure Resource Manager マシンカタログを削除すると、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。

Azure リソースグループ

Azure プロビジョニングのリソースグループは、アプリケーションとデスクトップをユーザーに提供する VM をプロビジョニングする方法を提供します。Studio で MCS マシンカタログを作成するときに既存の空の Azure リソースグループを追加するか、新しいリソースグループを作成することができます。

Azure リソースグループについて詳しくは、Microsoft ドキュメントを参照してください。

要件

- 各リソースグループは、最大 240 の VM を保持できます。カタログを作成するリージョンには、十分な数の空のリソースグループがなければなりません。マシンカタログを作成するときに既存のリソースグループを使用するには、使用可能なグループを完全に選択する必要があります。このプロセスで、カタログ内に作成されるマシンの数を調整します。

  たとえば、カタログ作成ウィザードで 500 台のマシンを指定する場合は、少なくとも 3 つの使用可能なプロビジョニングリソースグループを選択します。

  マシンカタログが作成された後、そのカタログにリソースグループを追加することはできません。したがって、後でカタログに追加する可能性のあるマシンを収容するのに十分な数のリソースグループを追加しておいてください。

- ホスト接続と同じリージョンに空のリソースグループを作成します。
- MCS カタログごとに新しいリソースグループが必要な場合は、ホスト接続に関連付けられている Azure サービスプリンシパルに、リソースグループの作成と削除ができる権限が必要です。

  既存の空のリソースグループを使用する場合は、ホスト接続に関連付けられている Azure サービスプリンシパルに、それらの空のリソースグループでの投稿者の権限が必要です。

- ［新規作成］オプションを使用して Studio でホスト接続を作成すると、作成したサービスプリンシパルにサブスクリプションスコープの投稿権限が設定されます。または、［既存を使用］オプションを使用して接続を作成し、既存のサブスクリプションスコープのサービスプリンシパルの詳細を指定することもできます。［新規作成］オプションを使用して Studio でサービスプリンシパルを作成する場合、新しいリソースグループの作成と削除、または既存の空のリソースグループへのプロビジョニングに必要な権限が設定されます。
- スコープが狭いサービスプリンシパルは、PowerShell を使用して作成する必要があります。さらに、スコープが狭いサービスプリンシパルを使用するときは、PowerShell または Azure Portal を使用して、MCS が VM をプロビジョニングする各カタログ用の空のリソースグループを作成する必要があります。

  ホスト接続にスコープが狭いサービスプリンシパルを使用していて、カタログ作成ウィザードの ［マスターイメージ］ページにマスターイメージリソースグループが表示されない場合は、使用しているスコープが狭いサービスプリンシパルに、マスターイメージリソースグループを一覧表示するための`Microsoft.Resources/subscriptions/resourceGroups/read`権限がないことが原因と考えられます。ウィザードを閉じ、この権限を設定してサービスプリンシパルを更新してから（手順については、ブログの投稿を参照）、ウィザードを再起動します。Azure での更新が Studio に反映されるまで最大 10 分かかることがあります。

Azure サービスプリンシパルについて

Azure Resource Manager でマシンをプロビジョニングするには、関連する Azure リソースにアクセス許可が割り当てられたサービスプリンシパルを介して、Azure サブスクリプションへのアクセスをプラグインに付与する必要があります。サービスプリンシパルは、ユーザーアカウントと同じ基本的な目的を果たします。このサービスプリンシ

パルは、Azure リソースに対する認証とアクセス許可の資格情報を提供する Azure Active Directory ID をプラグインに提供します。ユーザーアカウントと同様に、サービスプリンシパルは役割ベースのアクセス制御（RBAC）を使用して設定されます。

権限の定義方法に応じて、サービスプリンシパルは次のように分類されます：

- サブスクリプションスコープのサービスプリンシパル
- スコープが狭いサービスプリンシパル

サブスクリプションスコープのサービスプリンシパル

サブスクリプションスコープのサービスプリンシパルは、サブスクリプション内のすべてのリソースに対する投稿者の権限を持っているため、作成と管理を容易に行うことができます。Citrix Studio では、サブスクリプションスコープのサービスプリンシパルの作成プロセスを自動化するか、PowerShell で手動で作成することができます。これらのプリンシパルにより、Azure Resource Manager プラグインで Azure リソースグループを作成し、リソースの管理を完全に自動化できます。欠点は、プラグインが管理を担当するリソースとは無関係な、サブスクリプション内のリソースに対する権限がプラグインにあることです。

投稿者の役割を使用すると、サブスクリプション内のすべてのリソースの作成、削除、読み取り、および書き込みをプラグインで行うことができます。権限は Azure Active Directory 内のオブジェクトには拡張されず、サブスクリプションスコープのサービスプリンシパルで他のユーザーまたはサービスプリンシパルにリソースへのアクセスを許可することもできません。

スコープが狭いサービスプリンシパル

スコープが狭いサービスプリンシパルを使用すると、Azure Resource Manager プラグインから、ユーザーが定義した限定されたリソースセットにアクセスできます。Azure では、リソースグループを作成するには、サブスクリプションスコープの権限が必要です。スコープが狭いサービスプリンシパルを使用する場合、プラグインではリソースグループを作成できません。サービスプリンシパルに加えて、マシンをプロビジョニングするカタログごとに、リソースグループのプールを提供する必要があります。

Citrix Studio では、スコープが狭いサービスプリンシパルまたはカタログの作成はサポートされていません。これらのタスクはいずれも PowerShell を使用して実行する必要があります。ただし、一度作成したカタログは、マシンの追加や削除など、Studio の他のカタログと同様に管理できます。ある時点で、既存のスコープが狭いサービスプリンシパルを新しいリソースグループのプールで使用する場合は、PowerShell を使用してサービスプリンシパルに権限を明示的に追加する必要があります。

Azure サブスクリプションのアクセス要件の定義

次のセクションの技法と例は、一般的な要件を示しており、固有の状況に応じて変更する必要があります。

以下の場合は、サブスクリプションスコープのサービスプリンシパルの使用を検討してください：

- 最もシンプルな管理エクスペリエンスを必要としている。

- PowerShell の使用を避けて、Citrix Studio ですべてを管理したい。
- Azure サブスクリプションが、1 つの Citrix Virtual Apps and Desktops サービス専用となっている。
- Citrix Virtual Apps and Desktops のインストールの概念実証を行っている。
- Citrix Virtual Apps and Desktops 管理者が、Azure サブスクリプションスコープで投稿者にアクセスさせている。

以下の場合は、スコープが狭いサービスプリンシパルを使用することを検討してください:

- Azure サブスクリプションが複数の無関係なサービスをホストしている。
- Azure 管理者が、役割に応じて異なるサブスクリプションの権限を持っている。
- 会社が、非常に細かいレベルでのアクセス制御を必要とするセキュリティ基準を設けている。
- スコープが狭いサービスプリンシパルを作成するための既存のプロセスがある。

> ヒント:
>
> プライマリサブスクリプションの一部として請求される子サブスクリプションを作成し、プライマリサブスクリプションのデフォルトの Azure Active Directory を参照できます。この設定で、関連のないリソースへのアクセスを制御する別のメカニズムを使用できます。

スコープが狭いサービスプリンシパルのカタログの計画

スコープが狭いサービスプリンシパルのカタログを作成する前に、ホストする初期および将来的な数の仮想マシンに必要なリソースグループの数を判断します。Machine Creation Services の制限により、カタログの作成後にリソースグループを追加することはできません。

リソースグループプールごとに **1** つのカタログのプロビジョニング

Azure Resource Manager プラグインでは、各リソースグループに必要なインフラストラクチャを作成します。リソースグループは、ストレージアカウント、セキュリティグループ、ネットワークインターフェイス、仮想マシンなどで構成されます。ストレージアカウントは、マシンがカタログに追加される場合に必要に応じて作成されます。つまり、カタログのサイズは、リソースグループプールと Azure サブスクリプションクォータのサイズによって設定された上限まで大きくなる可能性があります。ストレージアカウントを作成すると、カタログを削除しない限り削除されることはありません。どの仮想マシンも削除できるため、ストレージアカウントが空になる可能性があります。仮想マシンは使用可能なストレージアカウントにランダムに分散される傾向があるため、このような状況はまれです。ストレージアカウントを意図的に空にするには、ストレージアカウントのコンテンツを検査することによって、マシンを単純に繰り返し選択する必要があります。

Azure では、リソースグループ内の仮想マシンの数は 800 に制限されていますが、Azure Resource Manager プラグインでは異なる基準が使用されます。標準の Azure ディスクには、1 秒あたりの I/O 操作（IOPS）が 500 という制限があり、標準のストレージアカウントの IOPS 制限は 20,000 です。このため、プラグインは 40 台以下のマシン

をストレージアカウントにプロビジョニングします。この制限は、標準ストレージとプレミアムストレージの両方に適用されます。さらに、プラグインでは、1 つのリソースグループに 19 個以下のストレージアカウントを作成します。

したがって、マシンの最大数に基づいてリソースグループ数を計算する基本的な式は次のとおりです:

リソースグループの数 = 上限 (マシンの最大数/(40 * 19))

Azure Resource Manager プラグインは、リソースグループのプールを排他的に使用することを前提としています。指定されたリソースグループには、ユーザーが作成したリソースはありません。

Azure の役割ベースのアクセス制御（**RBAC**）の基礎。

Azure リソースへのアクセスは、特定のスコープでサービスプリンシパルに RBAC の役割を割り当てることによって許可されます。スコープには、サブスクリプション、リソースグループ、または特定のリソースを指定できます。リソースはコンテインメント階層に配置され、役割によって定義された権限は、適用されるスコープの下位のすべてのリソースに適用されます。サブスクリプションに適用される役割は、サブスクリプション内のすべてのリソースに適用されます。リソースグループに適用される役割は、そのリソースグループに含まれるすべてのリソースに適用されます。

Azure リソース階層が意味するのは、サブスクリプションスコープの権限を持つサービスプリンシパルだけがリソースグループを作成できるということです。プラグインのようなアプリケーションは、論理グループに対してオンデマンドでリソースグループを作成してリソースを管理できないため、最適ではありません。サブスクリプション全体に対する広範な権限を持っていない限り、これに該当します。

Azure には組み込みの役割が多数用意されており、カスタム役割の定義もサポートしています。Azure RBAC のカスタムロールの詳細については、「Azure リソースのカスタム役割」を参照してください。

サブスクリプションスコープのサービスプリンシパルの作成

この例では、サブスクリプションスコープのサービスプリンシパルを作成する方法を説明します。詳細情報を利用して、Citrix Studio で Azure 接続を作成できます。既存のサービスプリンシパルを使用するか、Azure 接続を PowerShell で手動で作成するかを選択します。

```
param(
[string]$applicationName = "SubscriptionScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

```



```
# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

スコープが狭い基本のサービスプリンシパルの作成

このセクションでは、リソースグループスのコープで権限が割り当てられる、スコープが狭い最もシンプルなサービスプリンシパルを作成するプロセスについて説明します。

Azure Resource Manager プラグインには、以下のリソースに対する権限が必要です:

1. マスターイメージ VHD
2. マシンの仮想ネットワーク
3. マシンをプロビジョニングするリソースグループ

スクリプトを簡略化するため、リソースグループのスコープで投稿者のアクセスを許可できると仮定します。Azure Resource Manager プラグインには、イメージ VHD が格納されるリソースグループ、仮想ネットワークを含むリソースグループ、およびマシンがプロビジョニングされるリソースグループプールに対する投稿者の権限があります。

```
param(
[string]$applicationName = "BasicNarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$resourceGroups
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
```



```
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $resourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

カスタム役割を使用したスコープが狭いサービスプリンシパルの作成

Azure には、組み込みの RBAC 役割の大規模なセットが付属しています。直前のセクションの投稿者の役割を Citrix で使用します。前述のように、Azure Resource Manager プラグインで、厳密に必要とされるよりもわずかに広範な権限を付与しました。このセクションでは、カスタム役割を定義して権限を絞ります。必要に応じて、より多くのカスタム役割を使用し、イメージおよびネットワークリソースに直接役割を適用して、アクセスをロックできます。

> 注:
>
> 必要な権限は変更となる可能性があります。

リソースグループのスコープで仮想ネットワークおよびマスターイメージへのアクセスを許可するカスタム役割を定義するには、以下の権限を使用します。

マスターイメージ **VHD**。

カタログ作成の場合:

- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action

今後の Citrix スタジオのサポートにて:

- Microsoft.Resources/subscriptions/resourceGroups/read

マシンの仮想ネットワーク:

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/join/action

プロビジョニングされたマシンのリソースグループ。

以下の権限を持つ別のカスタムロールを作成することもできますが、例をシンプルにするために、引き続きマシンリソースグループに対して投稿者の役割を使用します。これらのリソースグループには、Azure Resource Manager

プラグインによって作成されていないリソースは含まれていません。投稿者の役割を使用すると、プラグインに対する変更のために、サービスプリンシパルに変更を行う必要性が低くなります:

- Microsoft.Compute/virtualMachines/*
- Microsoft.Network/networkInterfaces/*
- Microsoft.Network/networkSecurityGroups/*
- Microsoft.Resources/deployments/*
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Storage/storageAccounts/*
- Microsoft.Storage/storageAccounts/listKeys/action

Citrix Virtual Apps and Desktops カスタムアクセス権役割。

先に JSON で定義してカスタム役割を作成します:

```
{

  "Name": "Citrix-Custom-Reader",
  "Description": "Grants access to Citrix XenDesktop images and virtual
      networks.",
  "Actions": [
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/listKeys/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action"
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/<YOUR-SUBSCRIPTION-ID>"
  ]
 }

<!--NeedCopy-->
```

JSON 定義を参照して役割を作成します:

```
New-AzureRmRoleDefinition -InputFile citrix-custom-reader.json
<!--NeedCopy-->
```

サービスプリンシパルを作成するときに新しいカスタム役割を使用します:

```
param(
```



```
[string]$applicationName = "NarrowScopeSP",
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string[]]$machineResourceGroups,
[Parameter(Mandatory=$true)][string]$imageResourceGroup,
[Parameter(Mandatory=$true)][string]$networkResourceGroup
)

$application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
-IdentifierUris "https://$applicationName" -Password
    $applicationPassword

New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId

# Wait for the service principal to become available
Start-Sleep -s 60

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/"

foreach ($rg in $machineResourceGroups)
{

  New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
     ServicePrincipalName $application.ApplicationId `
  -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
 }


New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $imageResourceGroup"

New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
-scope "/subscriptions/$subscriptionId/resourcegroups/
    $networkResourceGroup"

Write-Host ("Application ID: " + $application.ApplicationId)
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops の **Azure** 接続の作成。

既存のサービスプリンシパルを使用して、Citrix Studio で Citrix Virtual Apps and Desktops の Azure 接続を作成すると合理的です。PowerShell で接続を作成することも同様に合理的です。

PowerShell で接続を作成する例を以下に示します:

```
param(
[string]$connectionName = "AzureConnection",
[Parameter(Mandatory=$true)][string]$applicationId,
[Parameter(Mandatory=$true)][string]$applicationPassword,
[Parameter(Mandatory=$true)][string]$subscriptionId,
[Parameter(Mandatory=$true)][string]$subscriptionName,
[Parameter(Mandatory=$true)][string]$tenantId
)

Add-PsSnapin Citrix*

$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <Property xsi:type="StringProperty" Name="AuthenticationAuthority" Value="https://login.microsoftonline.com/"/>
 <Property xsi:type="StringProperty" Name="ManagementEndpoint" Value="https://management.azure.com/"/>
 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="core.windows.net"/>
 <Property xsi:type="StringProperty" Name="TenantId" Value="$tenantId" />
 <Property xsi:type="StringProperty" Name="SubscriptionId" Value="$subscriptionId"/>
 <Property xsi:type="StringProperty" Name="SubscriptionName" Value="$subscriptionName"/>
</CustomProperties>
"@

$connection = New-Item -ConnectionType "Custom" -CustomProperties $customProperties -HypervisorAddress @("https://management.azure.com/") `
-Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "AzureRmFactory" -Scope @() `
-SecurePassword (ConvertTo-SecureString -AsPlainText -Force $applicationPassword) -UserName $applicationId

New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```



```
28
29 <!--NeedCopy-->
```

この時点で、Studio または PowerShell のいずれかを使用して、接続にリソースを追加します。

Citrix Virtual Apps and Desktops のカタログの作成。

次の例では、Citrix PowerShell スナップインを使用して、Citrix Virtual Apps and Desktops のカタログを作成します。

スコープが狭いサービスプリンシパルでは、Azure Resource Manager プラグインでリソースグループを作成できないため、以下の操作を行う必要があります:

1. リソースグループのプールを作成します。
2. リソースグループのプール内のすべてのリソースグループに、サービスプリンシパルの権限を割り当てます。
3. プロビジョニングスキームの作成時に、リソースグループプールの各リソースグループをカスタムプロパティにリストします。

このカスタムプロパティは **ResourceGroups** という名前で、値はリソースグループ名のコンマ区切りリストとなっています。このカスタムプロパティを定義する方法の例を次の例に示します。

> 注:
>
> カスタムプロパティには、マシン用のリソースグループのみが表示されます。イメージまたは仮想ネットワークが配置されている 1 つ以上のリソースグループは含まれていません。これらが指定されている場合、Azure Resource Manager プラグインはこれらのリソースグループにマシンをプロビジョニングしようとするため、意図しない動作が発生する可能性があります。

この例では、xd-sales-1 と xd-sales-2 という名前の 2 つのリソースグループにマシンがプロビジョニングされます:

```
1  Add-PsSnapin Citrix*
2
3  # The hosting unit name is the name of the Azure connection resources
       that should be used for this catalog
4  $hostingUnitName = "AzureHostingUnit"
5  $domain = "citrix.local"
6  $controllerAddress = ("ddc." + $domain)
7  $adminAddress = ($controllerAddress + ":80")
8  $catalogName = "catalog-name"
9  $network = "network-resource-group.resourcegroup\network-name"
10 $subnet = "subnet-name"
11 $serviceOffering = "Standard_A4"
12 $template = "image-resource-group.resourcegroup\imagestorage.
       storageaccount\images.container\image-name.vhd"
13
```



```
$customProperties = @" <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Standard_LRS" />
    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="xd-sales-1, xd-sales-2" />
</CustomProperties>
"@

$identityPool = New-AcctIdentityPool -AdminAddress $adminAddress -AllowUnicode -Domain $domain `
    -IdentityPoolName $catalogName -NamingScheme "vm-#" -NamingSchemeType "Numeric" -Scope @()

$brokerCatalog = New-BrokerCatalog -AdminAddress $adminAddress -AllocationType "Random" -IsRemotePC $False `
    -MinimumFunctionalLevel "L7_9" -Name $catalogName -PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() `
    -SessionSupport "MultiSession"

Write-Host $brokerCatalog

$provScheme = New-ProvScheme -AdminAddress $adminAddress -CleanOnBoot -CustomProperties $customProperties `
    -HostingUnitName $hostingUnitName -IdentityPoolName $catalogName `
    -MasterImageVM "XDHyp:\HostingUnits$hostingUnitName\image.folder$template.vhd" `
    -NetworkMapping @{
 "0"="XDHyp:\HostingUnits$hostingUnitName\virtualprivatecloud.folder$network.virtualprivatecloud$subnet.network" }
  `
    -ProvisioningSchemeName $catalogName -Scope @() -SecurityGroup @() `
    -ServiceOffering "XDHyp:\HostingUnits$hostingUnitName\serviceoffering.folder$serviceOffering.serviceoffering"

Write-Host $provScheme

Set-BrokerCatalog -AdminAddress $adminAddress -Name $catalogName -ProvisioningSchemeId $provScheme.ProvisioningSchemeUid

Add-ProvSchemeControllerAddress -AdminAddress $adminAddress.com -ControllerAddress $controllerAddress -ProvisioningSchemeName
```



```
        $catalogName
<!--NeedCopy-->
```

この時点で、Citrix Studio のカタログページの更新、マシンの追加、他のカタログと同様のマシンの管理を行うことができます。

Studio でマシンカタログのリソースグループを構成する

カタログ作成ウィザードの ［リソースグループ］ページでは、リソースグループを作成するか、既存のグループを使用するかを選択できます。「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」を参照してください。

マシンカタログを削除したときのリソースグループへの影響:

- マシンカタログを作成するときに Citrix Virtual Apps and Desktops で新しいリソースグループを作成した場合は、後でそのカタログを削除すると、それらのグループも削除されます。
- マシンカタログを作成するときに既存のリソースグループを使用した場合は、そのカタログを削除すると、それらのリソースグループのすべてのリソースが削除されます。ただし、リソースグループは削除されません。

注意事項、制限事項、およびトラブルシューティング

既存のリソースグループを使用する場合、カタログ作成ウィザードの［リソースグループ］ページの使用可能なリソースグループの一覧は自動更新されません。したがって、このウィザードページを開き、Azure でリソースグループの権限を作成または追加した場合、その変更はウィザードの一覧に反映されません。最新の変更を確認するには、ウィザードの ［マシン管理］ページに戻ります。ホスト接続に関連付けられているリソースを再選択するか、ウィザードを閉じて再起動します。Azure での変更が Studio に反映されるまで最大 10 分かかることがあります。

1 つのリソースグループは、1 つのマシンカタログでのみ使用します。ただし、これは強制されません。たとえば、カタログを作成するときに 10 個のリソースグループを選択しましたが、カタログに 1 台のマシンしか作成しなかったとします。選択したリソースグループのうち 9 つは、カタログの作成後も空のままです。それらのリソースグループは、将来の容量拡張時に使用するかもしれないので、そのカタログに関連付けられたまま残されます。カタログが作成された後、カタログにリソースグループを追加することはできないため、将来の拡張について計画する必要があります。ただし、別のカタログが作成された場合、これらの 9 つのリソースグループが使用可能な一覧に表示されます。現在、Citrix Virtual Apps and Desktops では、どのリソースグループがどのカタログに割り当てられているかを把握していません。それを監視するのは管理者の責任です。

接続で、さまざまなリージョンの空のリソースグループにアクセスできるサービスプリンシパルが使用されている場合、それらはすべて利用可能な一覧に表示されます。マシンカタログを作成するリージョンと同じリージョンのリソースグループを選択してください。

トラブルシューティング:

- カタログ作成ウィザードの［リソースグループ］ページの一覧にリソースグループが表示されません。

  サービスプリンシパルで、一覧に表示するリソースグループに適切な権限が適用されていることが必要です。

- 以前に作成したマシンカタログにマシンを追加する場合、すべてのマシンがプロビジョニングされるわけではありません。

  カタログを作成した後でカタログにマシンを追加する場合は、最初にそのカタログ用に選択したリソースグループのマシン容量（グループあたり 240 個）を超えないようにしてください。カタログが作成された後にリソースグループを追加することはできません。既存のリソースグループが収容できる以上のマシンを追加しようとすると、プロビジョニングが失敗します。

  たとえば、300 の VM と 2 つのリソースグループを持つマシンカタログを作成したとします。リソースグループは、最大 480 の VM（240 * 2）を収容できます。200 の VM をカタログに追加すると、リソースグループの容量を超えます。現在の 300 の VM + 200 の新しい VM = 500 ですが、リソースグループは 480 しか保持できません。

詳細情報

- 接続とリソース
- マシンカタログの作成
- CTX219211：Microsoft Azure Active Directory アカウントの設定
- CTX219243：Azure サブスクリプションへの XenApp および XenDesktop アクセスの付与
- CTX219271：サイト間 VPN を使用したハイブリッドクラウドの展開

Microsoft System Center Virtual Machine Manager 仮想化環境

April 26, 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。

Citrix Provisioning（旧称 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：

- サポートされる第 1 世代デスクトップまたはサーバー OS の VM
- サポートされる第 2 世代デスクトップまたはサーバー OS の VM（セキュアブートのサポートを含む）。

ハイパーバイザーのインストールおよび構成

> 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. サーバー上に Microsoft Hyper-V Server および VMM をインストールします。

2. すべての Controller に System Center Virtual Machine Manager コンソールをインストールします。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。
3. 次のアカウント情報を確認します。

   Studio でホストを指定するために使用するアカウントは、VMM 管理者またはその Hyper-V マシンの VMM 委任管理者である必要があります。このアカウントに VMM の委任管理者の役割のみがある場合は、ホストの作成時にストレージデータが Studio の一覧に表示されません。

   Studio 統合に使用されるユーザーアカウントは、仮想マシンのライフサイクル管理（仮想マシンの作成、更新、および削除など）を実行できるように、各 Hyper-V サーバー上の Administrators ローカルセキュリティグループのメンバーでもある必要があります。

   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。

マスター仮想マシンの作成

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してください。これにより、パフォーマンスが向上します。
2. バックアップのため、マスター仮想マシンのスナップショットを作成します。

仮想デスクトップの作成

MCS を使用して仮想マシンを作成する場合、サイトまたは接続の作成時に次の手順に従います：

1. ホストの種類として［Microsoft 仮想化］を選択します。
2. アドレスとして、ホストサーバーの完全修飾ドメイン名を入力します。
3. 新しい VM を作成する権限を持つ、先にセットアップした管理者アカウントの資格情報を入力します。
4. ［ホスト詳細］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。

   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
<!--NeedCopy-->
```

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

- **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。

  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。

  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。

HCL が管理者共有からファイルを削除します。

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）。

  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。

  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。

  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。

Citrix Hypervisor 仮想化環境

April 26, 2021

Citrix Hypervisor への接続の作成

Citrix Hypervisor（旧称：XenServer）への接続の作成時には、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。

Citrix Hypervisor 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、Citrix Hypervisor 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）。

高可用性機能を構成することもできます（Citrix Hypervisor サーバーで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 Citrix Hypervisor サーバー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。

Citrix Hypervisor 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。

1 つまたは複数の Citrix Hypervisor 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)。

Citrix Provisioning（旧称 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:

- サポートされるデスクトップまたはサーバー OS の VM のレガシー BIOS。
- サポートされるデスクトップまたはサーバー OS の VM の UEFI（セキュアブートを含む)。

Citrix Hypervisor 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、Citrix Hypervisor と Studio の両方でこの機能を有効にする必要があります。

- Citrix Hypervisor のインストール時に、［シンプロビジョニングの有効化（仮想デスクトップ用に最適化されたストレージ)］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、Citrix Hypervisor のドキュメントを参照してください。
- Citrix Virtual Apps and Desktops では、IntelliCache はデフォルトで無効になっています。この設定項目は Citrix Hypervisor 接続の作成時にのみ有効にでき、IntelliCache を後で無効にすることはできません。Citrix Hypervisor 接続を追加するには、次の操作を実行します:
  - 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。

Citrix Hypervisor 接続を使用したマシンカタログの作成

GPU 対応のマシンでは、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. Citrix VM 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。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft System Center Configuration Manager 環境

April 26, 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 3.1**：Citrix Connector により、Configuration Manager と Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops による仮想環境の両方の保守、管理操作を統一することができます。詳しくは、「Citrix Connector 3.1」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、「リモート PC アクセス」を参照してください。
- **XenApp/XenDesktop** のプロパティ： XenApp および XenDesktop のプロパティ設定により、Configuration Manager で管理する Citrix 仮想デスクトップを識別できるようになります。Configuration Manager では、Citrix Virtual Apps and Desktops の旧称（XenApp および XenDesktop）が使用されます。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。
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。

プロパティ	説明
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。

VMware 仮想化環境

April 26, 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。

Citrix Provisioning（旧称 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:

- サポートされるデスクトップまたはサーバー OS の VM のレガシー BIOS。
- サポートされるデスクトップまたはサーバー OS の VM の UEFI（セキュアブートを含む）。

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。役割の作成は、さまざまな Citrix Virtual Apps and Desktops 処理をいつでも要求可能にする上で、ユーザーの権限に必要となるレベルまで細分化して行ってください。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。

以下の表に、Citrix Virtual Apps and Desktops の処理と最低限必要な VMWare 権限の間の対応関係を示します。

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]
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]

SDK	ユーザーインターフェイス
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（**Citrix Provisioning**）

「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］
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]
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]
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]

SDK	ユーザーインターフェイス
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 Delivery Controller に追加します。

1. vCenter Server を実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのホストファイル（%SystemRoot%/WINDOWS/system32/Drivers/etc/）に追加します。この手順は、vCenter Server を実行しているコンピューターの FQDN がドメイン名システムに登録されていない場合にのみ必要です。
2. 以下の 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。

   a) 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。
   b) Controller で、エクスポートした証明書の保存先に移動し、rui.crt ファイルを開きます。

   Web ブラウザーでダウンロードする。Internet Explorer で証明書をダウンロード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。

   a) 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。
   b) セキュリティに関する警告を受け入れます。
   c) 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。
   d) 証明書を表示して、［詳細］タブをクリックします。
   e)［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。
   f) エクスポートした証明書を保存します。
   g) 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** から直接インポートします。

   - 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。
   - セキュリティに関する警告を受け入れます。
   - 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。

- 証明書を表示します。

3. 各 Controller 上の証明書ストアに証明書をインポートします。

   a)［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。
   b)［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。［信頼されたユーザー］を選択し、［**OK**］をクリックします。［次へ］、［完了］の順にクリックします。

   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は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、Citrix Virtual Apps and Desktops 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

April 26, 2021

Citrix Virtual Apps and Desktops 環境で Nutanix Acropolis を使用して仮想マシンを提供する場合は、以下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。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録する。
- Nutanix Acropolis ハイパーバイザーとの接続を作成する。
- Nutanix ハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成する。

詳しくは、Nutanix サポートポータルにある『Nutanix Acropolis MCS plug-in Installation Guide』を参照してください。

Citrix Cloud Connector に Nutanix MCS プラグインをインストールする準備

Citrix Virtual Apps and Desktops の Delivery Controller に Nutanix Acropolis を統合するための前提条件:

- Citrix Cloud Connector インストーラーで AHV MCS プラグインを実行するには、Citrix Cloud Connector 仮想マシンの管理者権限が必要です。
- Citrix Cloud Connector 仮想マシンを Citrix Cloud テナントのリソースの場所に登録します。
- Connector のリソースの場所に AHV がない場合でも、Citrix Cloud テナントに登録したすべての Citrix Cloud Connector に AHV MCS プラグインをインストールします。

Nutanix プラグインのインストールと登録

Citrix Virtual Apps and Desktops コンポーネントのインストール後、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。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します。

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
<!--NeedCopy-->
```

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**］を選択します。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情報です。Nutanix に固有のフィールドのみを説明しています。

選択したスナップショットは、カタログの仮想マシンの作成に使用されるテンプレートです。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てください。

- 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、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。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

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで VDA をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

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、下記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="\*address\*"
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。デフォルト値が適切です。変更しないでください。ただし、接続を編集して変更することはできます。接続の作成時にこれらの値を変更することはできません。詳しくは、「接続の設定の編集」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は Studio の示すオプションに左右されます。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。

Studio は、Microsoft Azure で利用可能になった 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 ではこの表示を変更できません。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 要件を熟知しておいてください。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:

- 仮想マシンのサイズ
- Microsoft Virtual Machines の料金ページ
- 旧世代の仮想マシンのサイズ

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。

汎用階層: 汎用階層 VM は、B、Dsv3、Dv3、DasV4、Dav4、DSv2、Dv2、Av2、DC、および DCv2 の 10 シリーズで表示されます。これらの VM は CPU 対メモリの比率のバランスを取り、テストと開発、小規模から中規模のデータベース、および低から中程度のトラフィック量の Web サーバーに最適です。Azure VM のサイズおよび詳細については、「仮想マシンのサイズ」を参照してください。

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、「Microsoft Virtual Machines の料金ページ」を参照してください。Linux VM の料金については、「Linux Virtual Machines の料金ページ」を参照してください。

使用する VM インスタンスタイプを決定する際には、以下を考慮してください:

- コンピューティング要件を理解することは重要です。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ります。
- タスクに見合った VM を使用します。最高のパフォーマンスで始めても、必要な結果を得られないことがあり、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 インスタンスの場合、タスクに対してパフォーマンスとユーザーの操作性が適切ではありません。
- 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 VM シリーズでは、アプリケーションやユーザーが求めるパフ

ォーマンスやユーザビリティが可能です。ただし、高性能の種類の VM インスタンスのコストの高さが、本当の価値に見合う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（2,048）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 1,000 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 のデフォルトの制限により、一部の VM を超えるスケーリングは回避されます。ただし、この制限は頻繁に変更されるため、最新情報を確認してください：http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/

Microsoft Azure Virtual Network1 つあたり、サポートされている VM の数は最高 2,048 個です。

ホストされているアプリケーションの提供に必要な VM について検討します。詳しくは、「Windows 上の VM ディスクのスケーラビリティおよびパフォーマンスの目標」を参照してください。

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

April 26, 2021

コアコンポーネントとは、Citrix Delivery Controller、Citrix Studio、Citrix Director、Citrix ライセンスサーバーなどです。

(2003 より前のバージョンでは、Citrix StoreFront もコアコンポーネントに含まれていました。引き続き、[**Citrix StoreFront**] タイルをクリックするか、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。)

インストールを始める前に、本記事と「インストールの準備」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

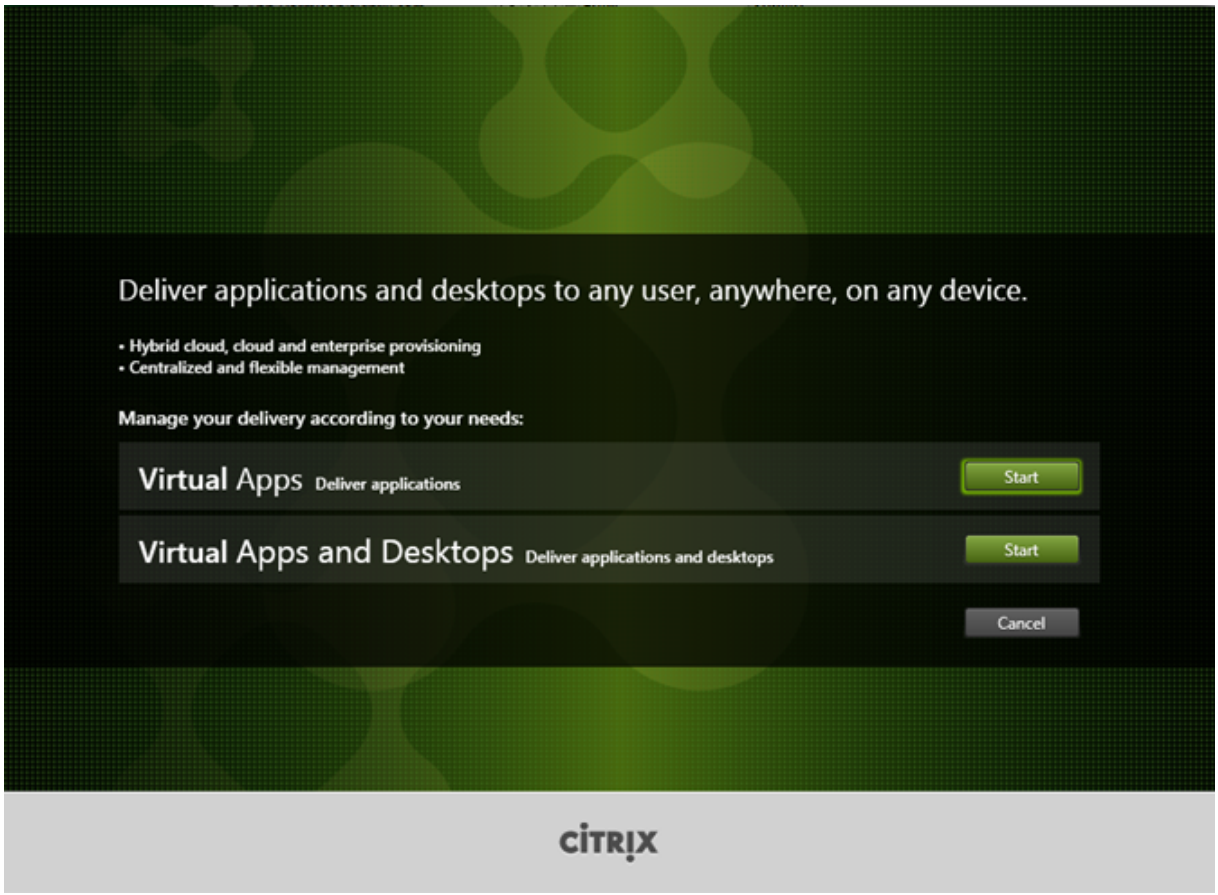
Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

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

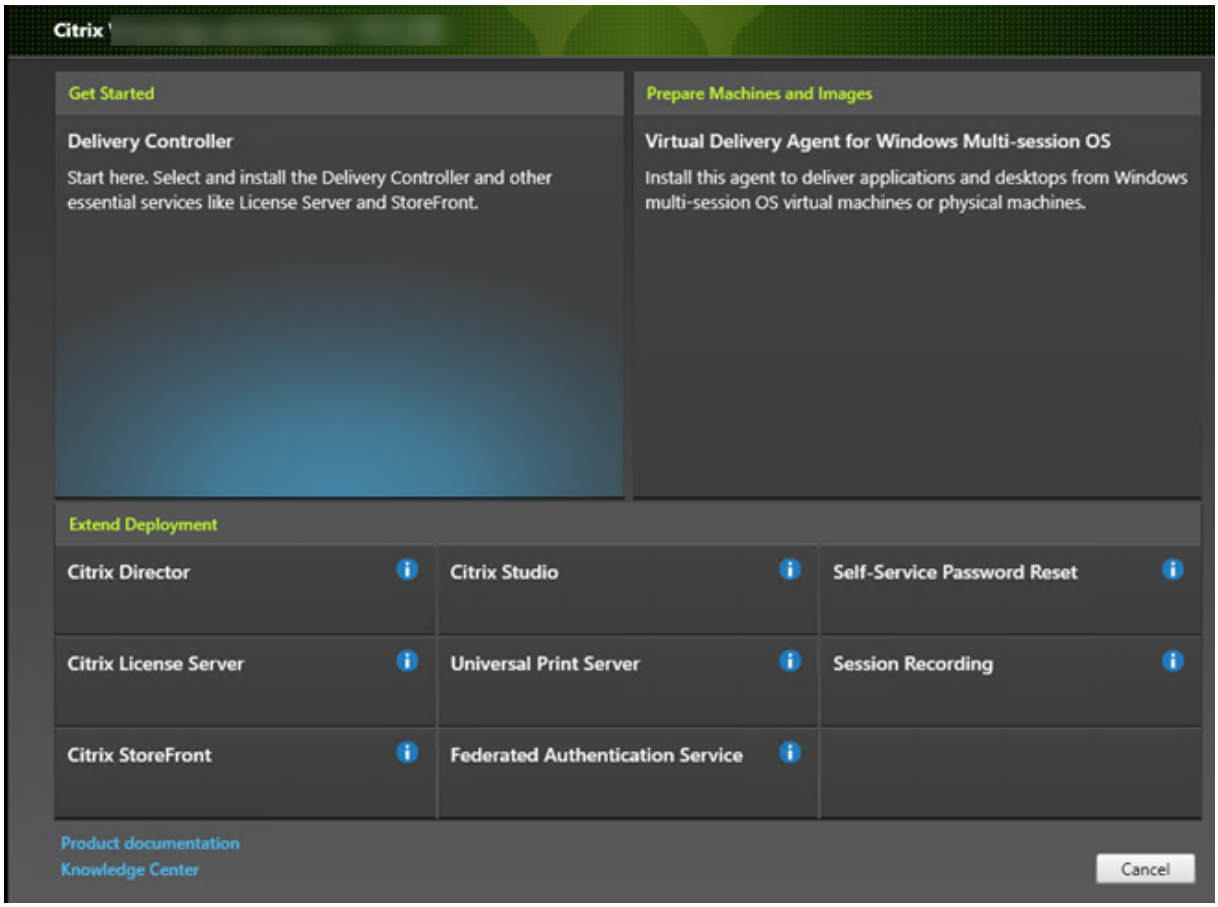


インストールする製品（Virtual Apps または Virtual Apps and Desktops）の隣にある［開始］をクリックします。

（マシンに Citrix Virtual Apps and Desktops 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を使用して Citrix Virtual Apps をインストールします。オプションを指定しない場合、Citrix Virtual Apps and Desktops 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

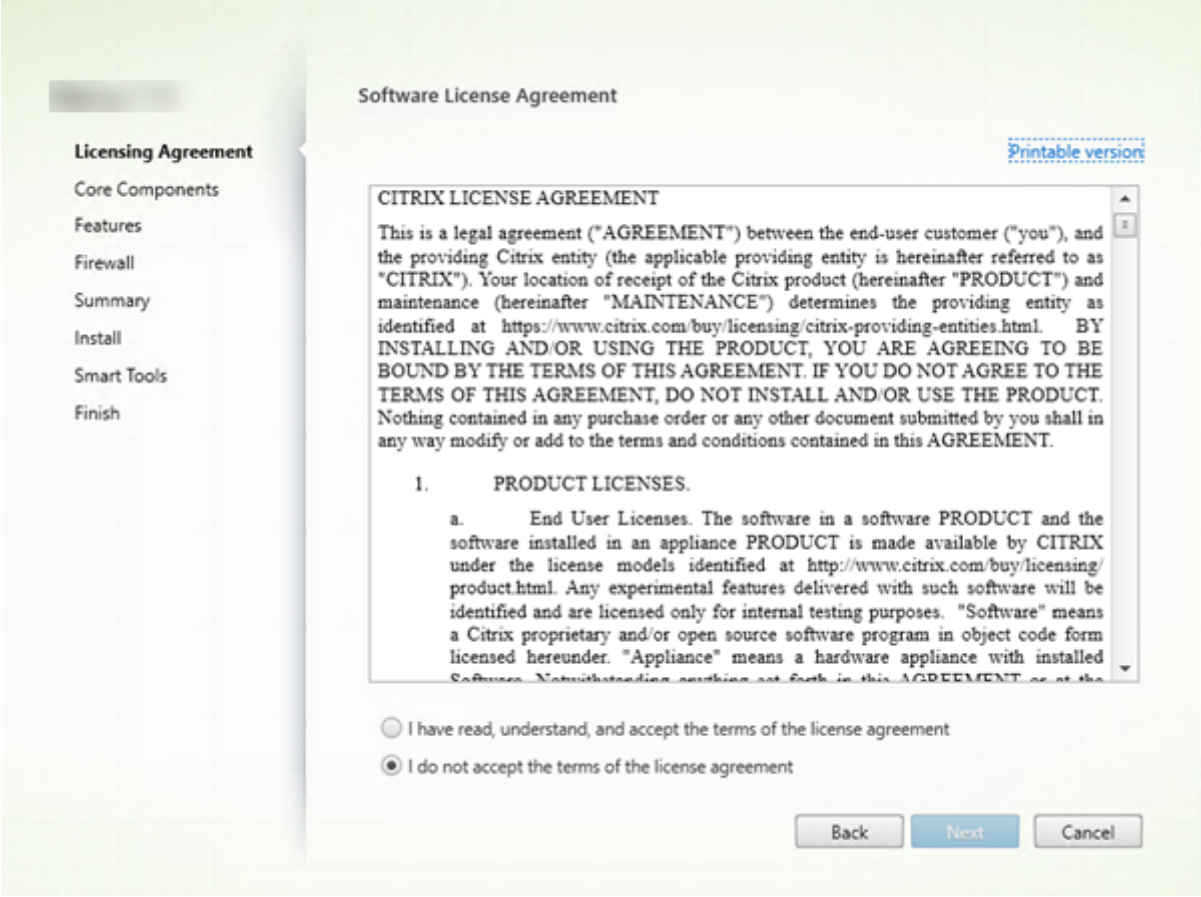


製品を初めてインストールする場合は、[**Delivery Controller**] をクリックします（後のページで、このマシンにインストールする特定のコンポーネントを選択します）。

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。

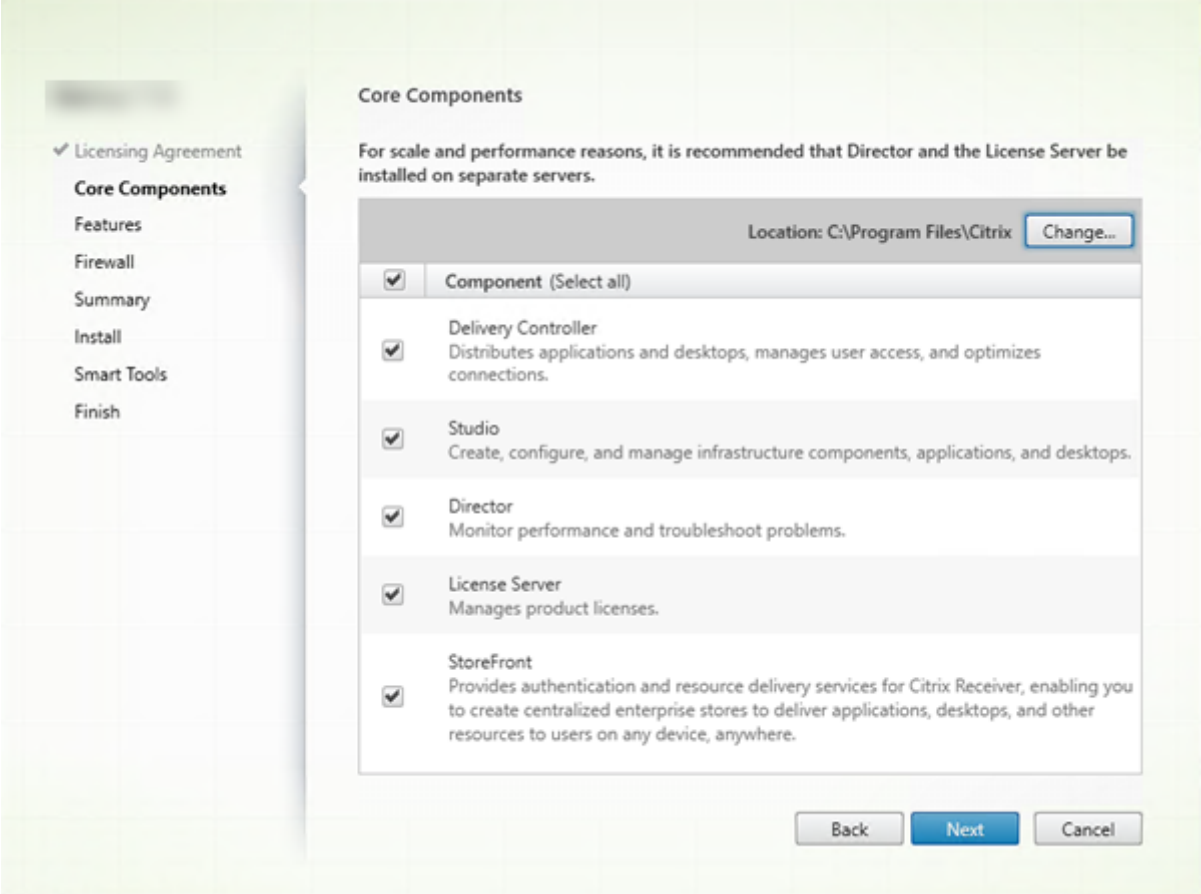
コマンドラインオプション：`/components`

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`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンの RAM が推奨容量（5GB）未満である場合、インストーラーで通知されます。推奨容量に達していないと、サイトの安定性に影響を与える可能性があります。詳しくは、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス：ダイアログボックスが表示されます。

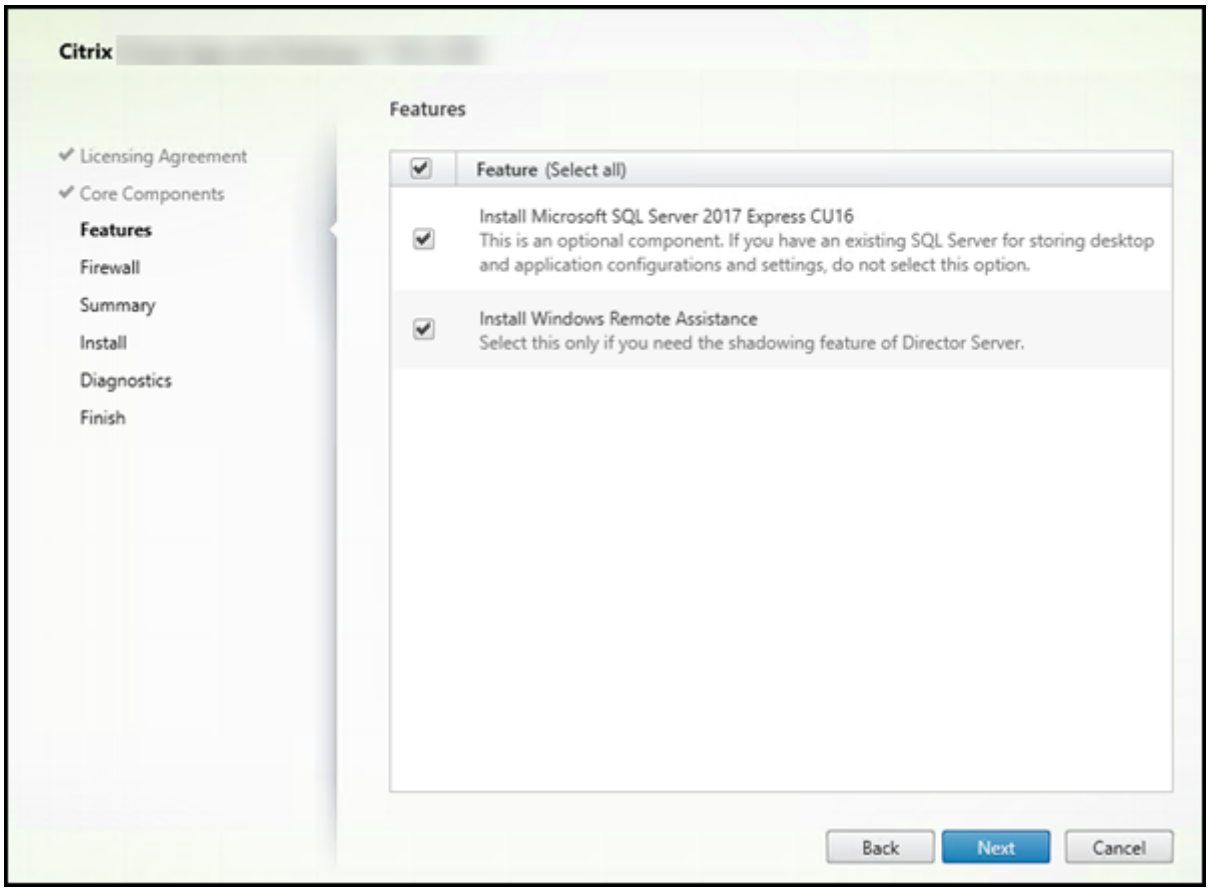
- 推奨：［キャンセル］をクリックしてインストールを停止します。マシンに RAM を追加してから、インストールを再開します。
- または、［次へ］をクリックしてインストールを続行します。サイトの安定性に問題がある可能性があります。

コマンドラインインターフェイス：インストールまたはアップグレードが終了します。インストールログに、検出された内容と使用可能なオプションを説明するメッセージが出力されます。

- 推奨：マシンに RAM を追加してから、コマンドを再実行します。
- または、`/ignore_hw_check_failure`オプションを使用してコマンドを再実行して、警告を無視します。サイトに安定性の問題がある可能性があります。

アップグレード時に、OS または SQL Server のバージョンがサポートされなくなった場合にも通知が表示されます。「環境のアップグレード」を参照してください。

手順 **6.** 機能を有効または無効にする



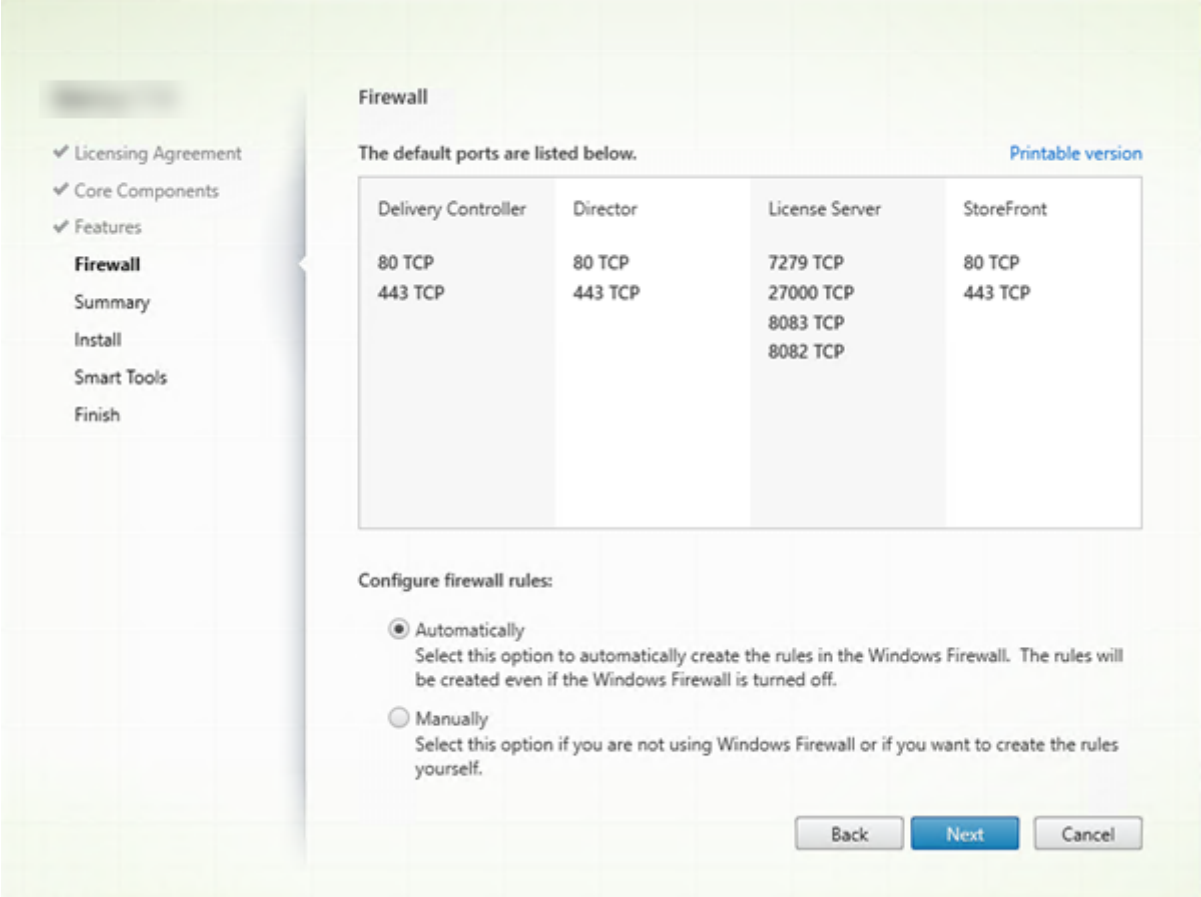
［機能］ページで次の作業を行います：

- 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。Citrix Virtual Apps and Desktops の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。
- 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



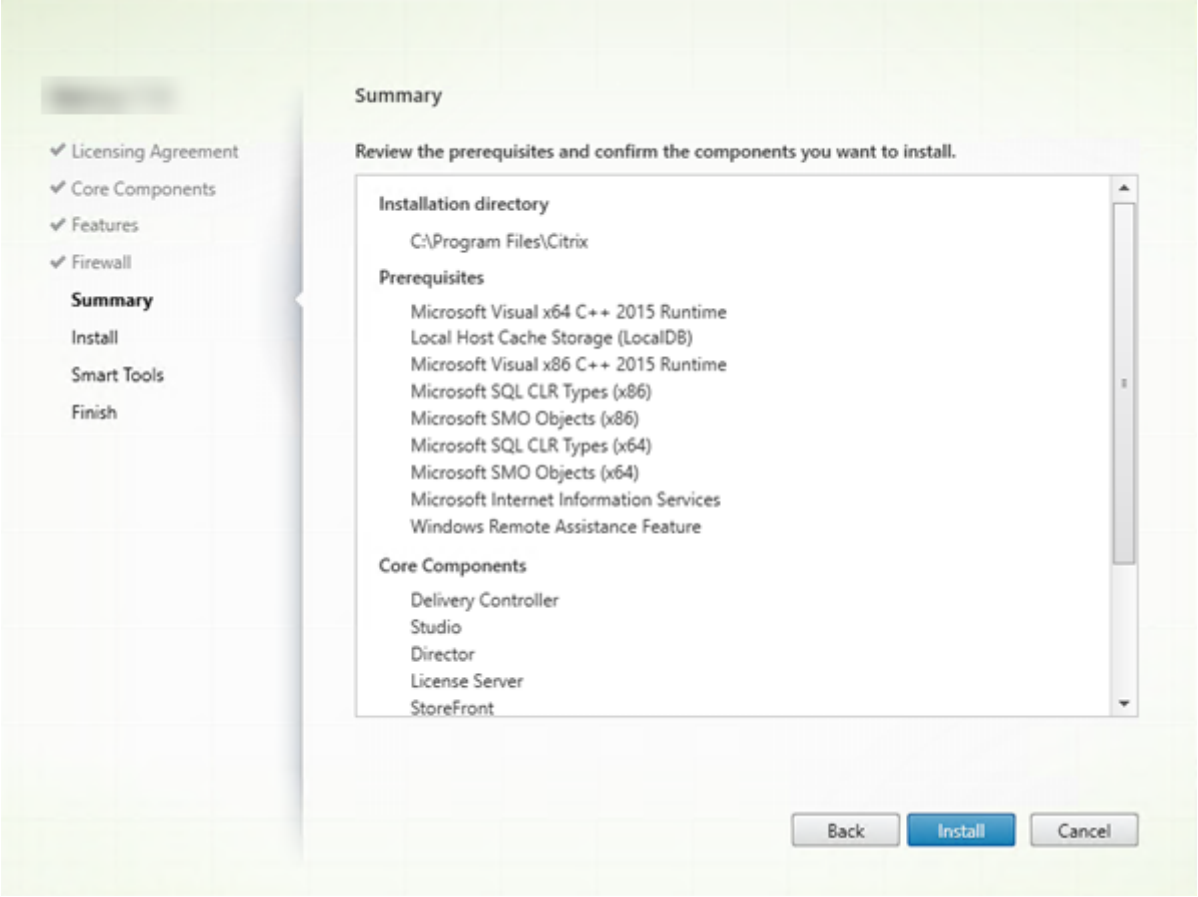
Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、デフォルトで ［ファイアウォール］ページに示されているポートが自動的に開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートの詳細については、「ネットワークポート」を参照してください。

［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`

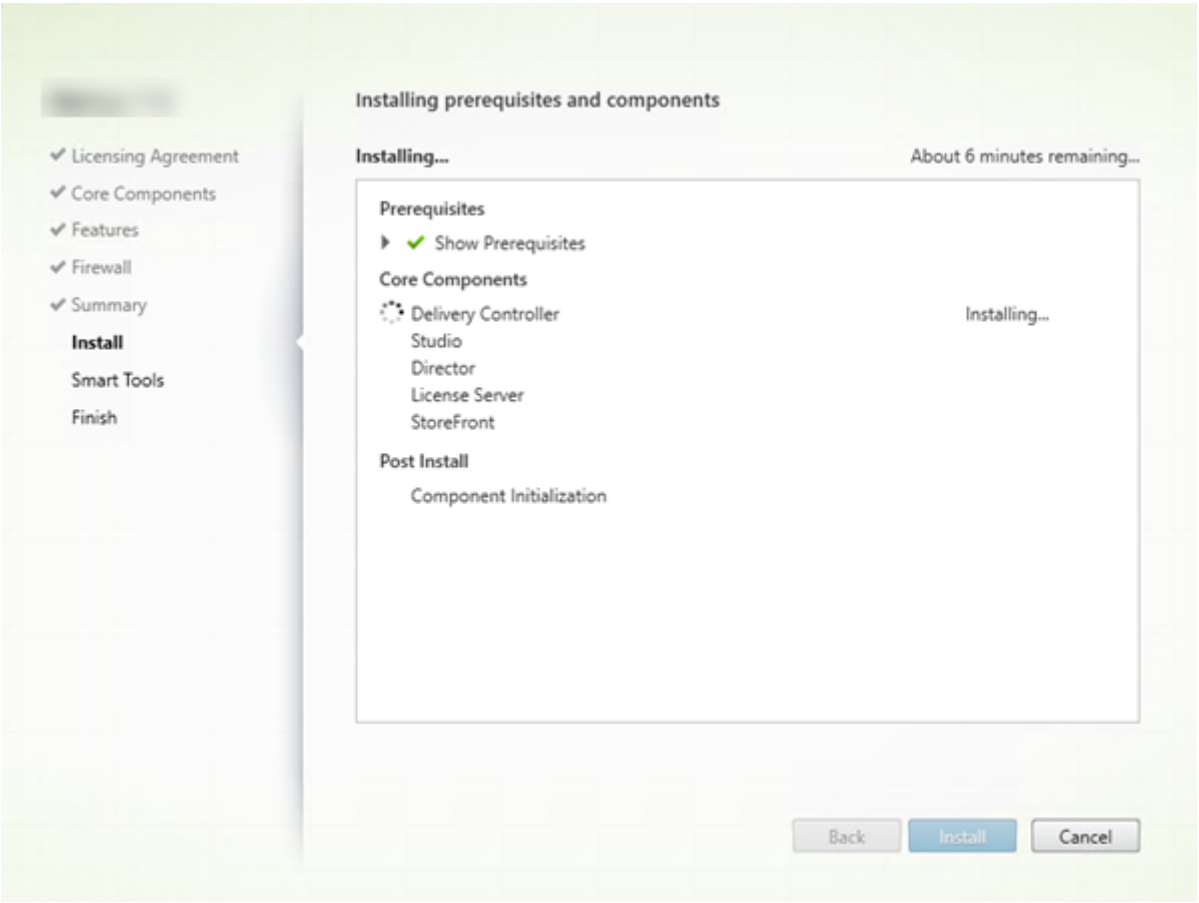
手順 **8.** インストール前に前提条件を確認する



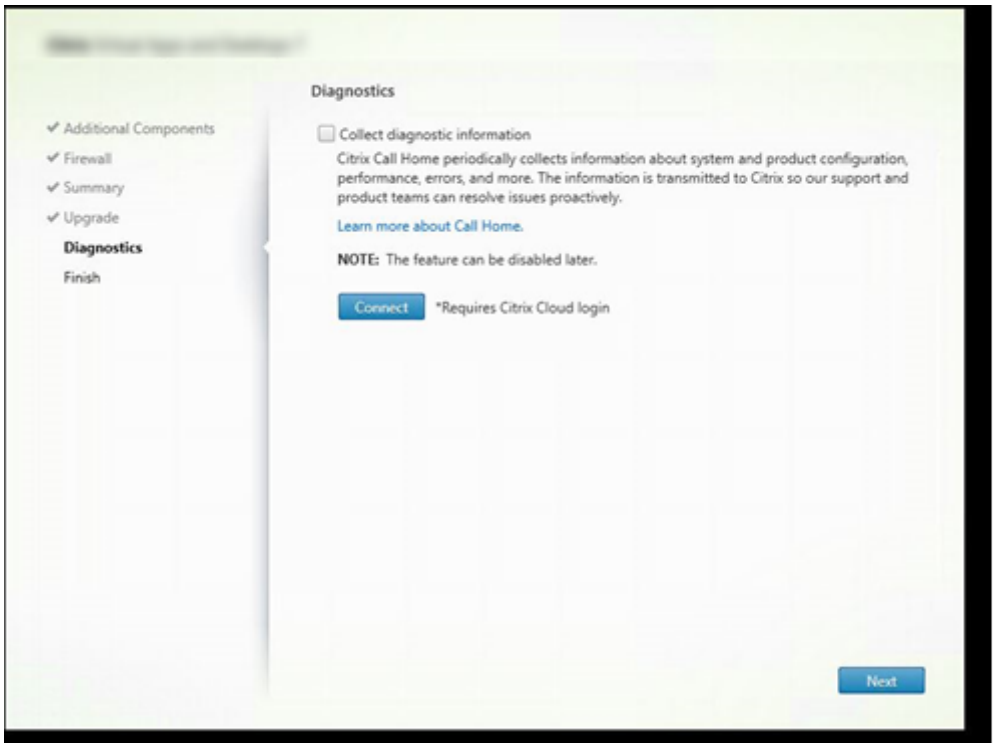
［概要］ページに、インストールされるものが表示されます。必要に応じて、［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

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.** 診断



［診断］ページで、Citrix Call Home に参加するかどうかを選択します。

このページは、グラフィカルユーザーインターフェイスで Delivery Controller をインストールするときに表示されます。StoreFront（Controller ではない）をインストールすると、このページがウィザードに表示されます。（Controller または StoreFront ではなく）その他のコアコンポーネントをインストールする場合、ウィザードにこのページは表示されません。

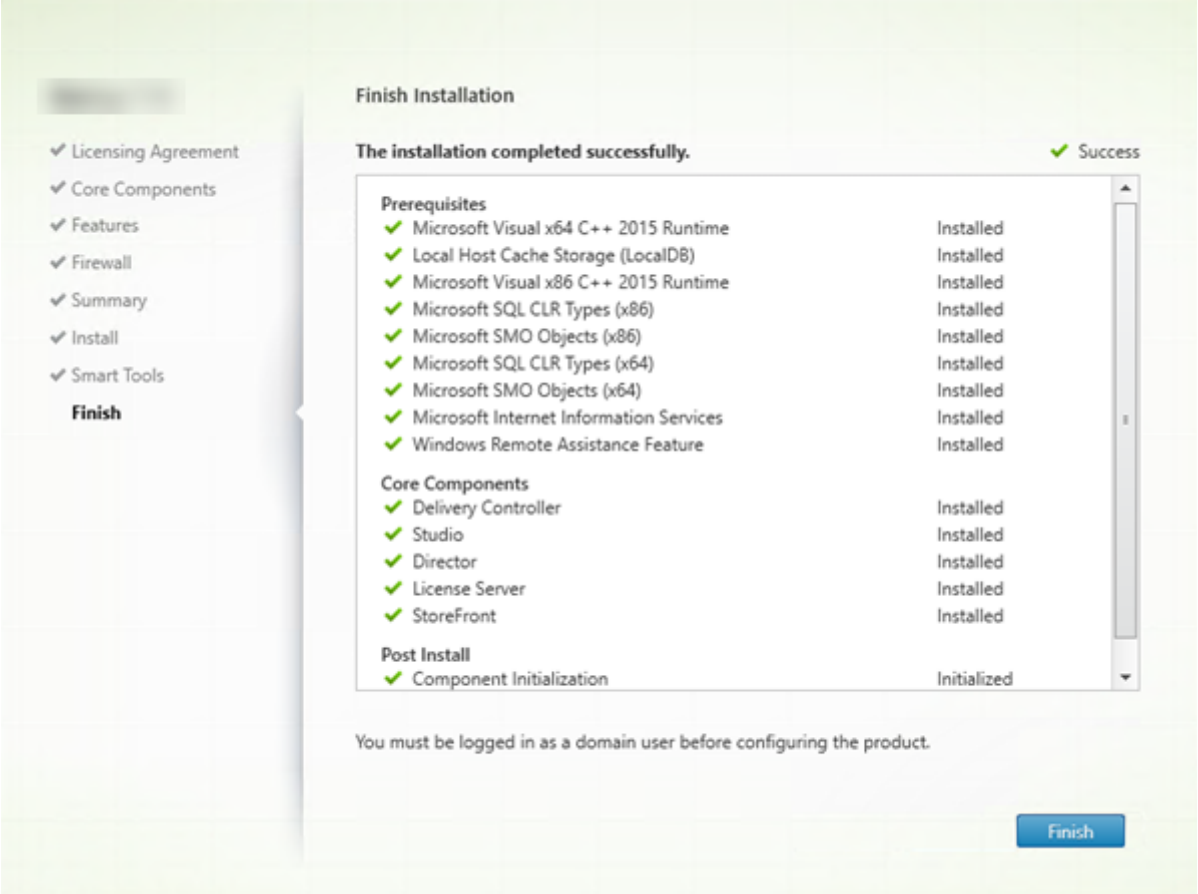
Call Home が既に有効な場合、またはインストーラーで Citrix Telemetry Service に関連するエラーが発生した場合には、アップグレード時にこのページは表示されません。

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。登録時の選択内容はインストール後に変更できます。

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。

詳しくは、「Call Home」を参照してください。

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 を使用してサイトの作成します。

サイトを作成した後、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。

1. ［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。
2. ライセンス契約に同意します。
3. Windows ファイアウォールサービスが実行されている場合、デフォルトの動作では ［ファイアウォール］ページに示される TCP ポート 7229 および 8080 が開放されます。これはファイアウォールが無効になっていても同じです。手動でポートを開放する場合は、そのデフォルト動作を無効にできます。

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、「ユニバーサルプリントサーバーをインストールするためのコマンドラインオプション」を参照してください。

- フェデレーション認証サービス。
- Session Recording。

VDA のインストール

April 26, 2021

> 重要:
>
> Personal vDisk（PvD）がインストールされている VDA をアップグレードする場合は、「VDA を 1912 以降にアップグレードする」を参照してください。

Windows マシン用には 2 種類の VDA があります：マルチセッション OS 対応 VDA とシングルセッション OS 対応 VDA 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）。

インストールを開始する前に、「インストールの準備」を確認して準備作業をすべて完了させます。

VDA をインストールする前に、コアコンポーネントをインストールしておく必要があります。VDA をインストールする前にサイトを作成することもできます。

この記事では、VDA をインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

全製品インストーラーを使用する場合:

1. まだ製品 ISO を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、Citrix Virtual Apps and Desktops 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。
2. 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。

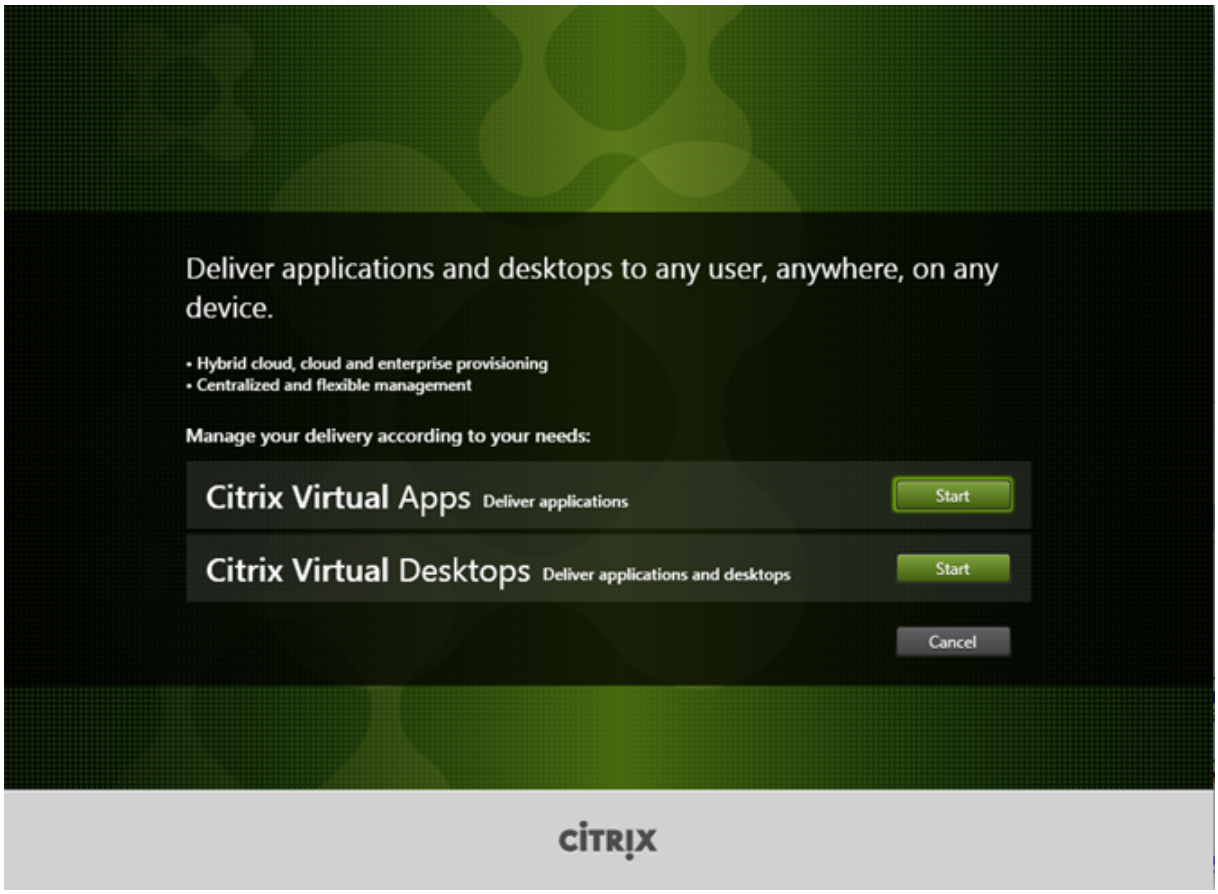
インストールウィザードが起動します。

スタンドアロンパッケージを使用する場合：

1. Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops 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`：マルチセッション OS VDA バージョン
   - `VDAWorkstationSetup.exe`：シングルセッション OS VDA バージョン
   - `VDAWorkstationCoreSetup.exe`：シングルセッション OS Core Services VDA バージョン
2. このパッケージを右クリックして、［管理者として実行］を選択します。

   インストールウィザードが起動します。

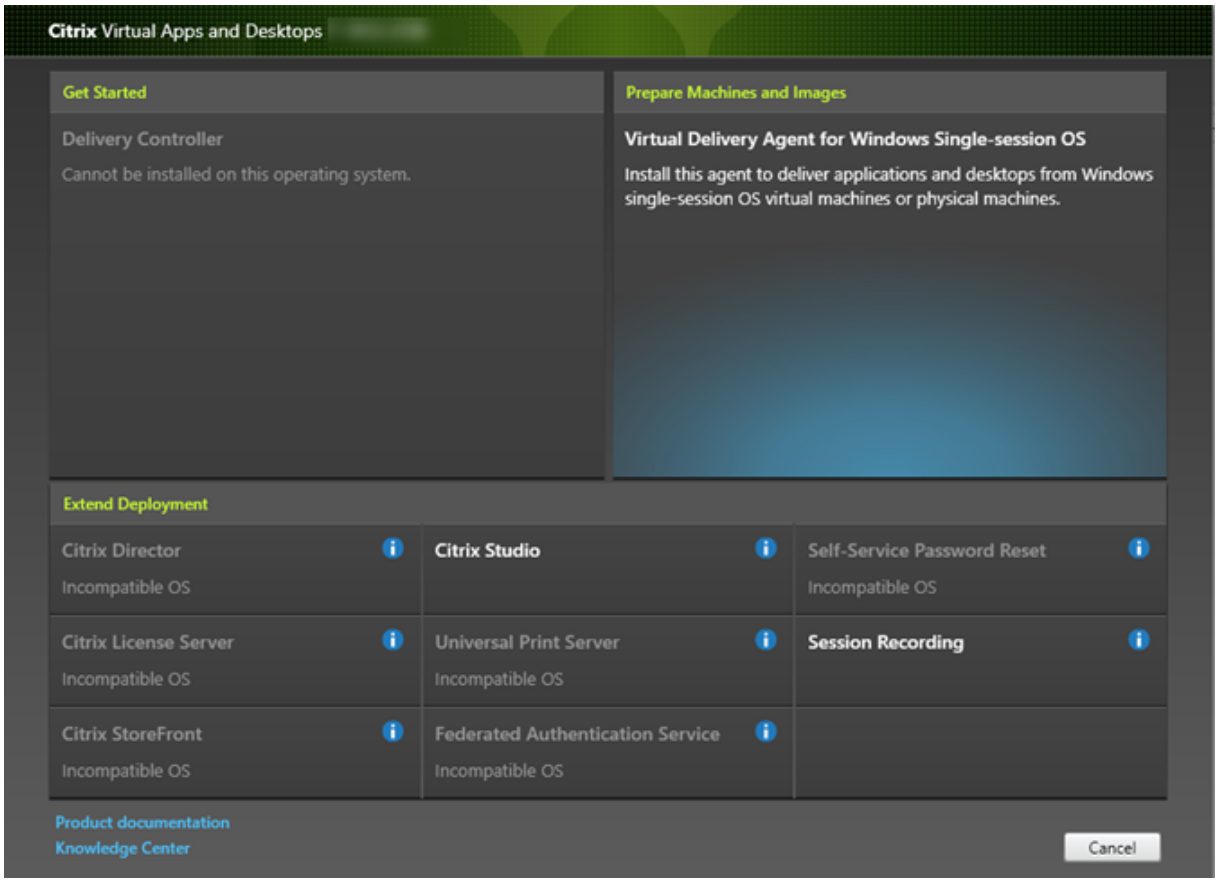
手順 **2.** インストールする製品を選択する



インストールする製品（Citrix Virtual Apps または Citrix Virtual Desktops）の横にある ［開始］をクリックします。（マシンに Citrix Virtual Apps コンポーネントまたは Citrix Virtual Desktops 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`を使用して Citrix Virtual Apps をインストールします。オプションを指定しない場合、Citrix Virtual Desktops がインストールされます。

手順 **3. VDA** を選択する

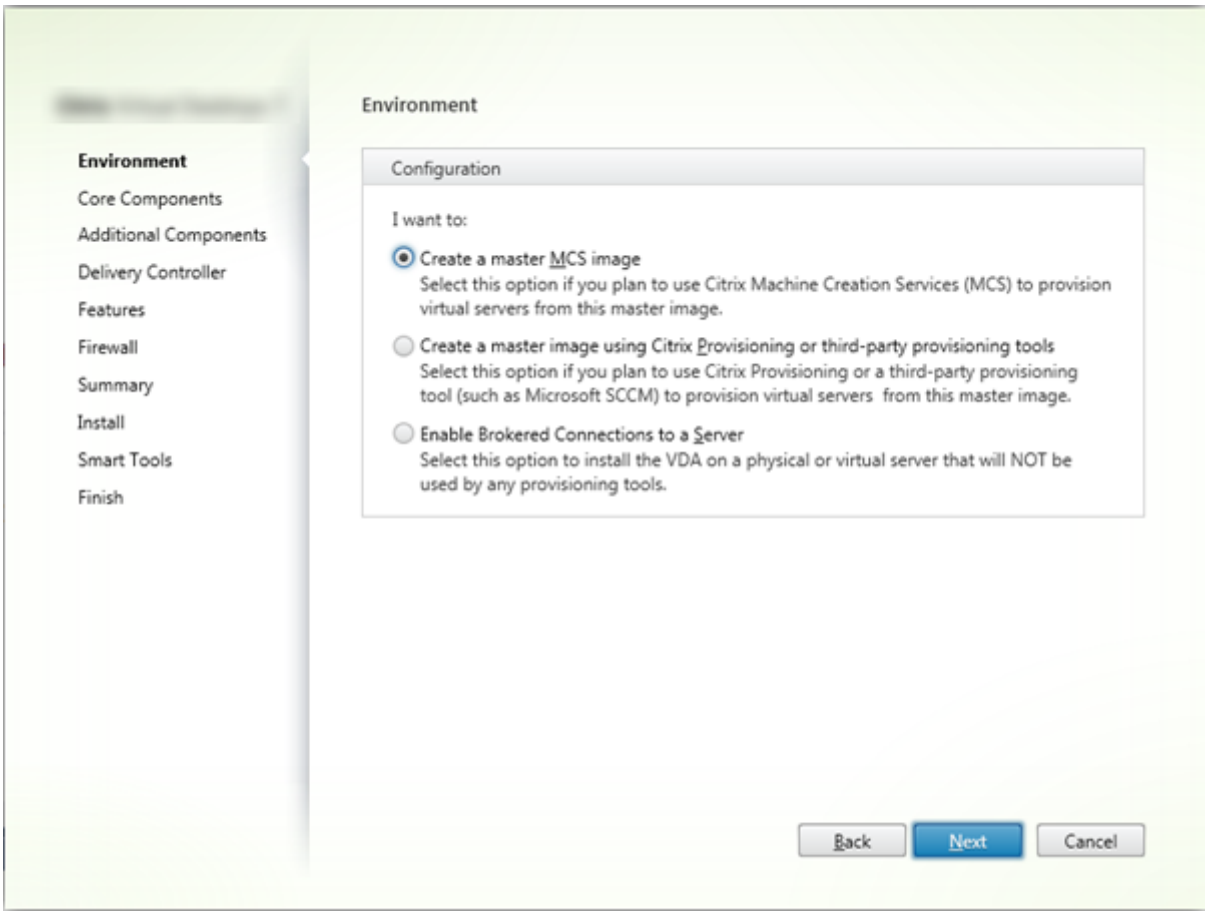


Virtual Delivery Agent エントリを選択します。インストーラーはシングルセッション OS とマルチセッション OS のいずれで実行されているかを認識しているので、適切な種類の VDA のみが提示されます。

たとえば、Windows 2016 マシンでインストーラーを実行すると、マルチセッション OS 対応 VDA のオプションが利用可能になります。シングルセッション OS 対応 VDA のオプションは提示されません。

このバージョンの Citrix Virtual Apps and Desktops でサポートされていない OS で Windows VDA をインストール（またはアップグレード）しようとすると、メッセージが表示され、選択肢についての説明が示されます。

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、つまり別のマシンのプロビジョニングでこのマシンをマスターイメージとして使用するかを選択します。

選択したオプションにより、どの Citrix Provisioning ツール（存在する場合）が自動でインストールされるか、および VDA インストーラーの［追加コンポーネント］ページのデフォルト値が決定されます。

VDA をインストールすると、複数の MSI（プロビジョニング用など）が自動的にインストールされます。これらがインストールされないようにするには、コマンドラインで/`exclude`オプションを付けてインストールを行ってください。

次のいずれかのオプションを選択します：

- マスター **MCS** イメージを作成する：仮想マシンのプロビジョニングに Machine Creation Services を使用する場合は、このオプションを選択して VM マスターイメージに VDA をインストールします。このオプションは、`TargetOSOptimizer.exe`を含む Machine Identity Service をインストールします。これはデフォルトのオプションです。

  コマンドラインオプション：/`mastermcsimage`または/`masterimage`

- **Citrix Provisioning** またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する：仮想マシンのプロビジョニングに Citrix Provisioning またはサードパーティのプロビジョニングツー

ル（Microsoft System Center Configuration Manager など）を使用する場合は、このオプションを選択して VM マスターイメージに VDA をインストールします。

コマンドラインオプション：/masterpvsimage

- （マルチセッション OS マシンでのみ表示）サーバーへの仲介接続を有効にする：別のマシンのプロビジョニングにマスターイメージとして使用しない物理マシンまたは仮想マシンに VDA をインストールするには、このオプションを選択します。

  コマンドラインオプション：/remotepc

- （シングルセッション OS マシンでのみ表示）リモート **PC** アクセスを有効にする：リモート PC アクセスで使用する物理マシンに VDA をインストールするには、このオプションを選択します。

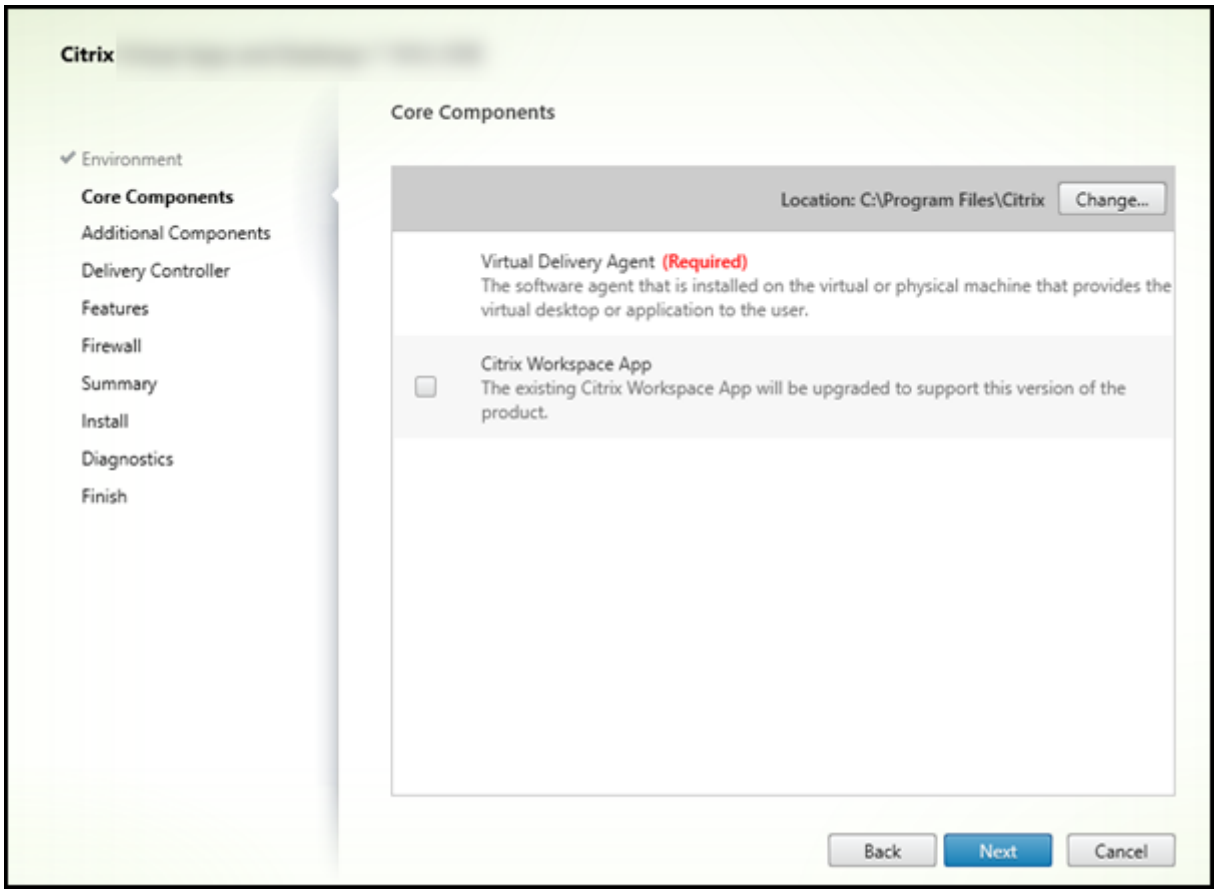
  コマンドラインオプション：/remotepc

［次へ］をクリックします。

次の場合、このページは表示されません：

- VDA のアップグレード時
- VDAWorkstationCoreSetup.exeインストーラーの使用時

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



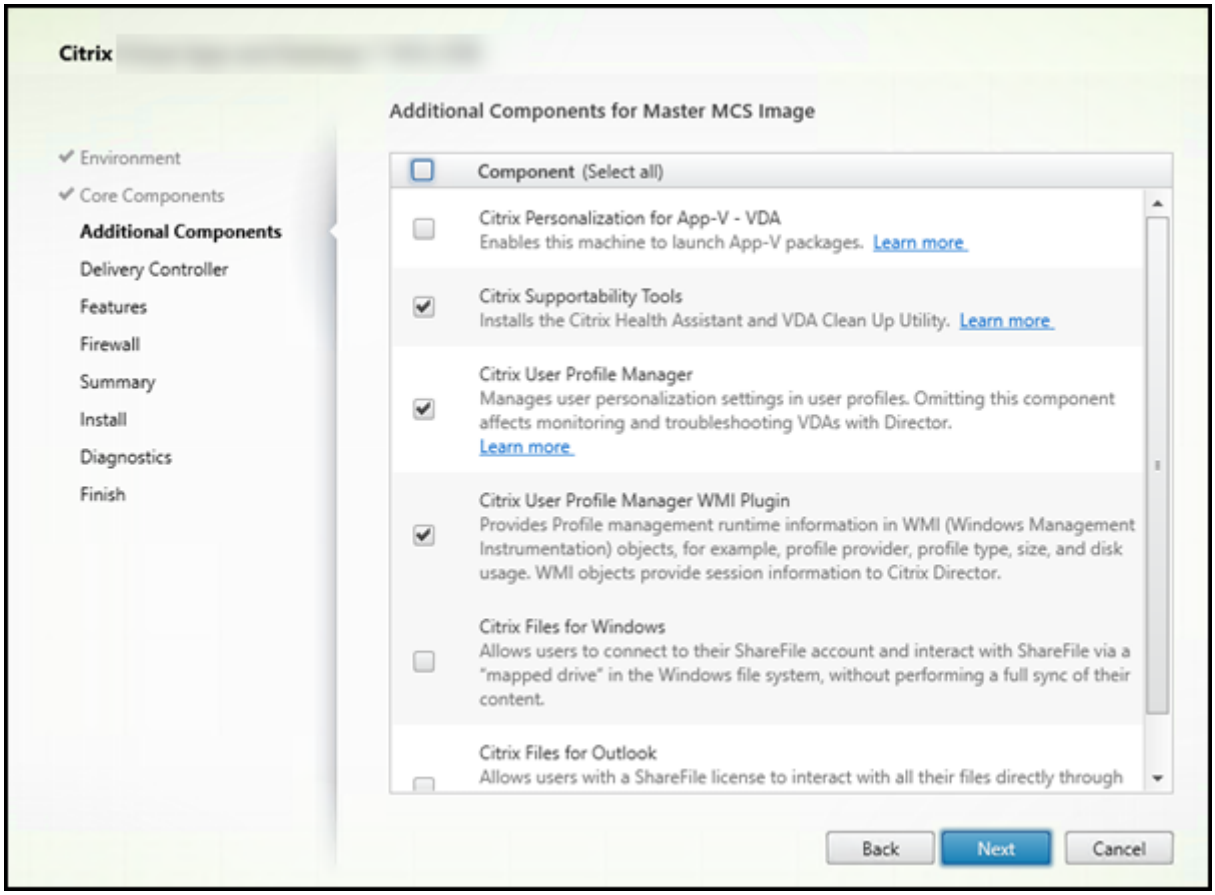
［コアコンポーネント］ページで次の作業を行います：

- 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、Windows 向け Citrix Workspace アプリは VDA とともにインストールされません。VDAWorkstationCoreSetup.exe インストーラーを使用する場合、Windows 向け Citrix Workspace アプリ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`。VDA および Windows 向け Citrix Workspace アプリをインストールする場合は`/components vda plugin`

手順 **6.** 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。コマンドラインインストールでは、`/exclude`オプションまたは`/includeadditional`オプションを指定して、使用可能なコンポーネントを 1 つまたは複数明示的に除外またはインストールすることができます。

次の表に、このページの項目のデフォルト設定を示します。デフォルトの設定は、［環境］ページで選択したオプションによって異なります。

［追加コンポーネント］ページ	［環境］ページ：［マスター MCS イメージを作成する］または［Citrix Provisioning またはサードパーティの...］を選択	［環境］ページ：［サーバーへの仲介接続を有効にする］（マルチセッション OS 対応）または［リモート PC アクセスを有効にする］（シングルセッション OS 対応）を選択
Citrix Personalization for App-V	未選択	未選択
ユーザー個人設定レイヤー	未選択	このユースケースでは無効なため表示されません。
Citrix Supportability Tools	選択済み	未選択
Citrix User Profile Manager	選択済み	未選択
Citrix User Profile Manager WMI Plugin	選択済み	未選択
Citrix Files for Windows	未選択	未選択
Citrix Files for Outlook	未選択	未選択

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。

次のチェックボックスをオンまたはオフにします：

- **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：インストールする場合は`/includeadditional "Citrix Personalization for App-V - VDA"`、インストールしない場合は`/exclude "Citrix Personalization for App-V - VDA"`

- ユーザー個人設定レイヤー：ユーザー個人設定レイヤーの MSI をインストールします。詳しくは、「ユーザー個人設定レイヤー」を参照してください。

  このコンポーネントは、シングルセッション Windows 10 マシンに VDA をインストールするときにのみ表示されます。

ユーザー個人設定レイヤーテクノロジは、Personal vDisk（PvD）および AppDisk コンポーネント（廃止済み）とともに使用することはできません。VDA をアップグレードする場合、以前に Personal vDisk をインストール済みであれば、古い VDA をアンインストールしてからこのバージョンをインストールするよう求められます。詳しくは、「VDA を 1912 以降にアップグレードする」を参照してください。

コマンドラインオプション：インストールする場合は/includeadditional "User Personalization Layer"、インストールしない場合は/exclude "User Personalization Layer"

- **Citrix** サポートツール Citrix サポートツール（Citrix Health Assistant など）を含む MSI をインストールします。

  コマンドラインオプション：インストールする場合は/includeadditional "Citrix Supportability Tools"、インストールしない場合は/exclude "Citrix Supportability Tools"

- **Citrix User Profile Manager**：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：インストールする場合は/includeadditional "Citrix User Profile Manager"、インストールしない場合は/exclude "Citrix User Profile Manager"

- **Citrix User Profile Manager WMI Plugin**：このプラグインは、プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用などの Profile Management ランタイム情報を、WMI（Windows Management Instrumentation）オブジェクトに格納して提供します。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：インストールする場合は/includeadditional "Citrix User Profile Manager WMI Plugin"、インストールしない場合は/exclude "Citrix User Profile Manager WMI Plugin"

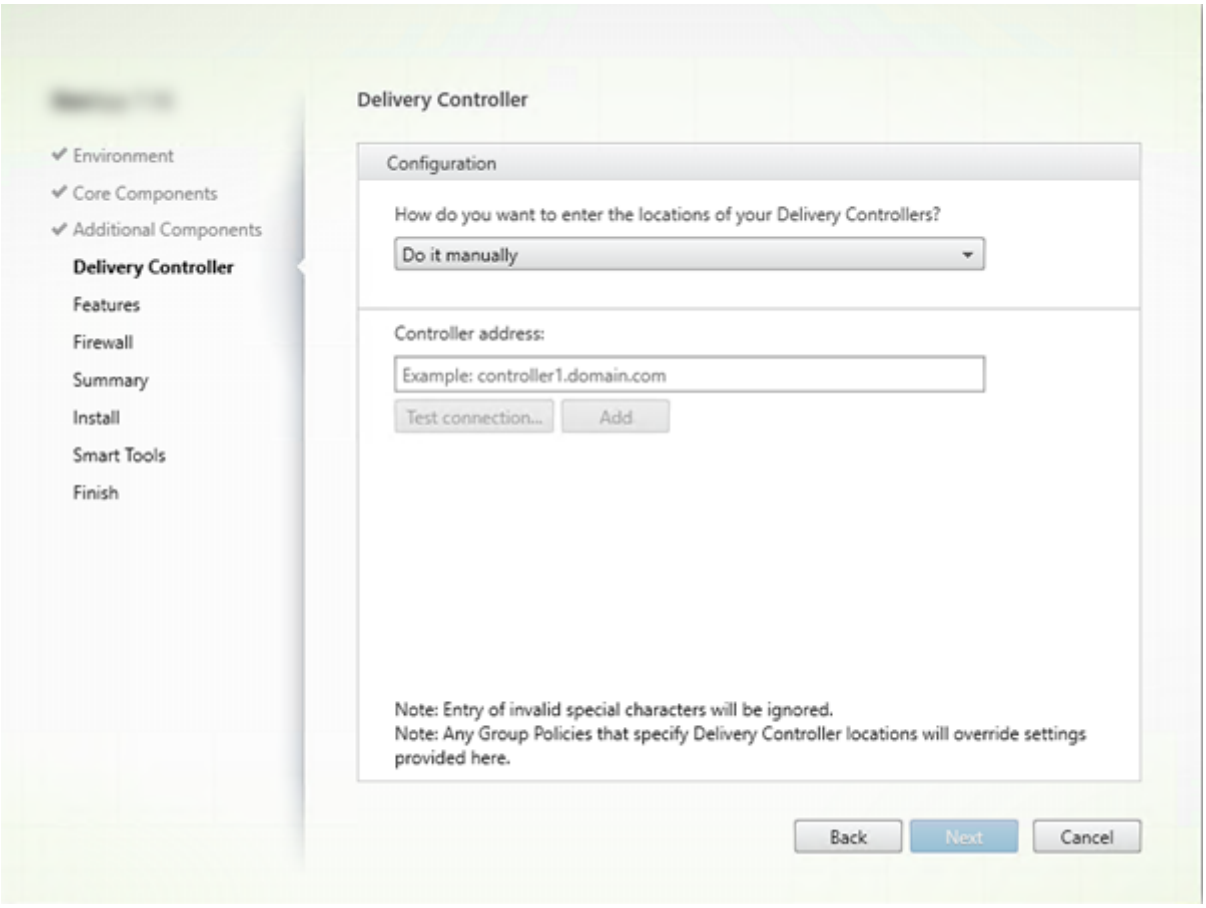
- **Citrix Files for Windows**：このコンポーネントを使用すると、ユーザーは自分の Citrix Files アカウントに接続できるようになります。これにより、コンテンツの完全同期を行わなくても、Windows ファイルシステムのマッピング済みドライブから Citrix Files にアクセスできるようになります。詳しくは、「Content Collaboration」を参照してください。

コマンドラインオプション：インストールする場合は/`includeadditional "Citrix Files for Windows"`、インストールしない場合は/`exclude "Citrix Files for Windows"`

- **Citrix Files for Outlook**： Citrix Files for Outlook によって、添付ファイルやメールを Citrix Files 経由で、ファイルサイズの制限を回避しながらセキュリティを強化して送信できます。同僚、顧客、パートナーに対して、ファイルアップロードリクエストを安全に、メールで直接送信できます。詳しくは、「Content Collaboration」を参照してください。

  コマンドラインオプション：インストールする場合は/`includeadditional "Citrix Files for Outlook"`、インストールしない場合は/`exclude "Citrix Files for Outlook"`

手順 **7. 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 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、アドレスも追加します。

- 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。

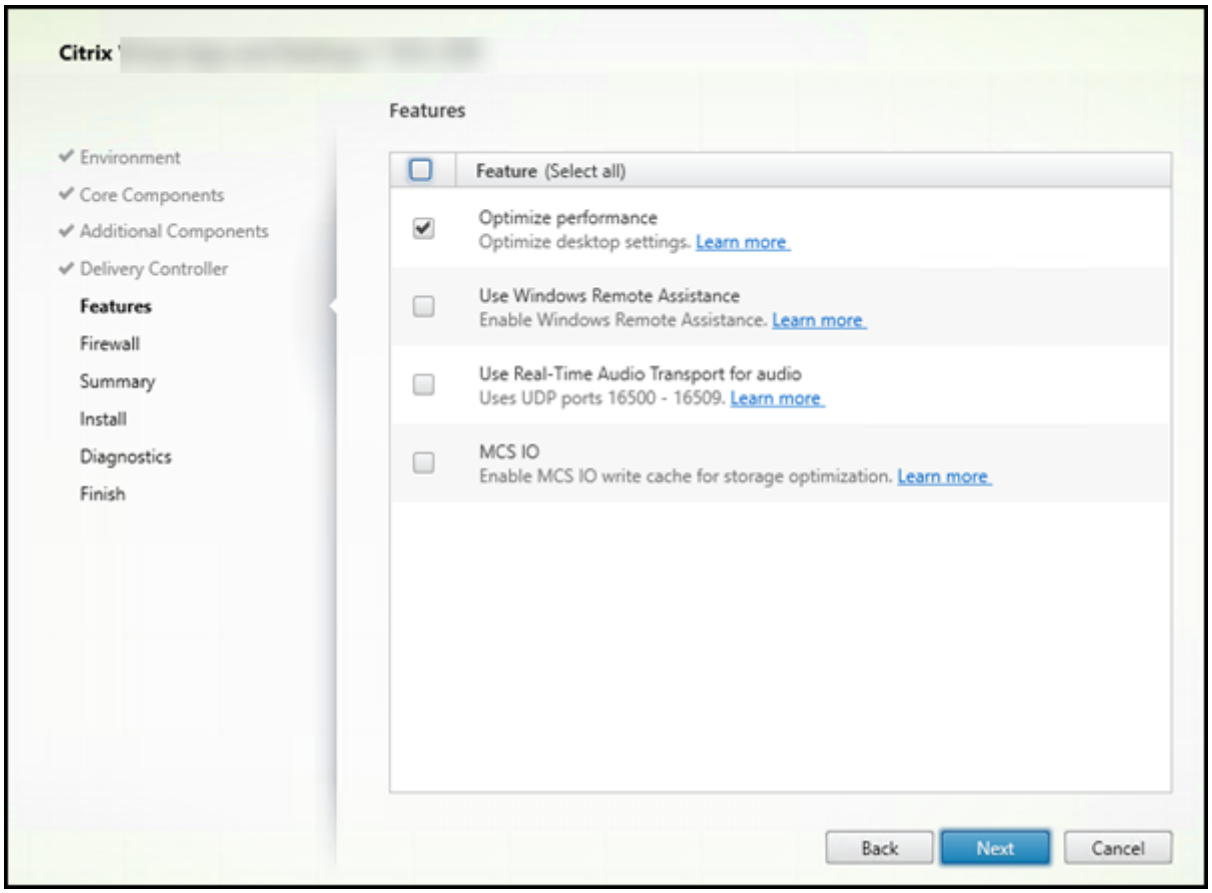
［次へ］をクリックします。［後で実行（上級）］を選択した場合、後でコントローラーのアドレスを指定することを確認するメッセージが表示されます。

そのほかの考慮事項：

- アドレスに使用できるのは、英数字のみです。
- 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、「VDA 登録」を参照してください。

コマンドラインオプション：`/controllers`

手順 **8.** 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。

- パフォーマンスを最適化する： MCS を使用し、この機能を有効にする場合（デフォルト）, 仮想マシンの最適化によってオフラインファイルが無効になり、バックグラウンド最適化（デフラグ処理）が無効になり、イベントログのサイズが縮小されます。詳しくは、「CTX125874」を参照してください。

  最適化するには、この機能を有効にするだけでなく、Machine Identity Service をインストールする必要もあります。このサービスには`TargetOSOptimizer.exe`ファイルが含まれます。Machine Identity Service は、次の場合には自動的にインストールされます：

  - グラフィカルインターフェイスの ［環境］ページで、［マスター **MCS** イメージを作成する］を選択します。
  - コマンドラインインターフェイスで、`/mastermcsimage`または`/masterimage`を指定し、`/exclude "Machine Identity Service"`は指定しません。

  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）

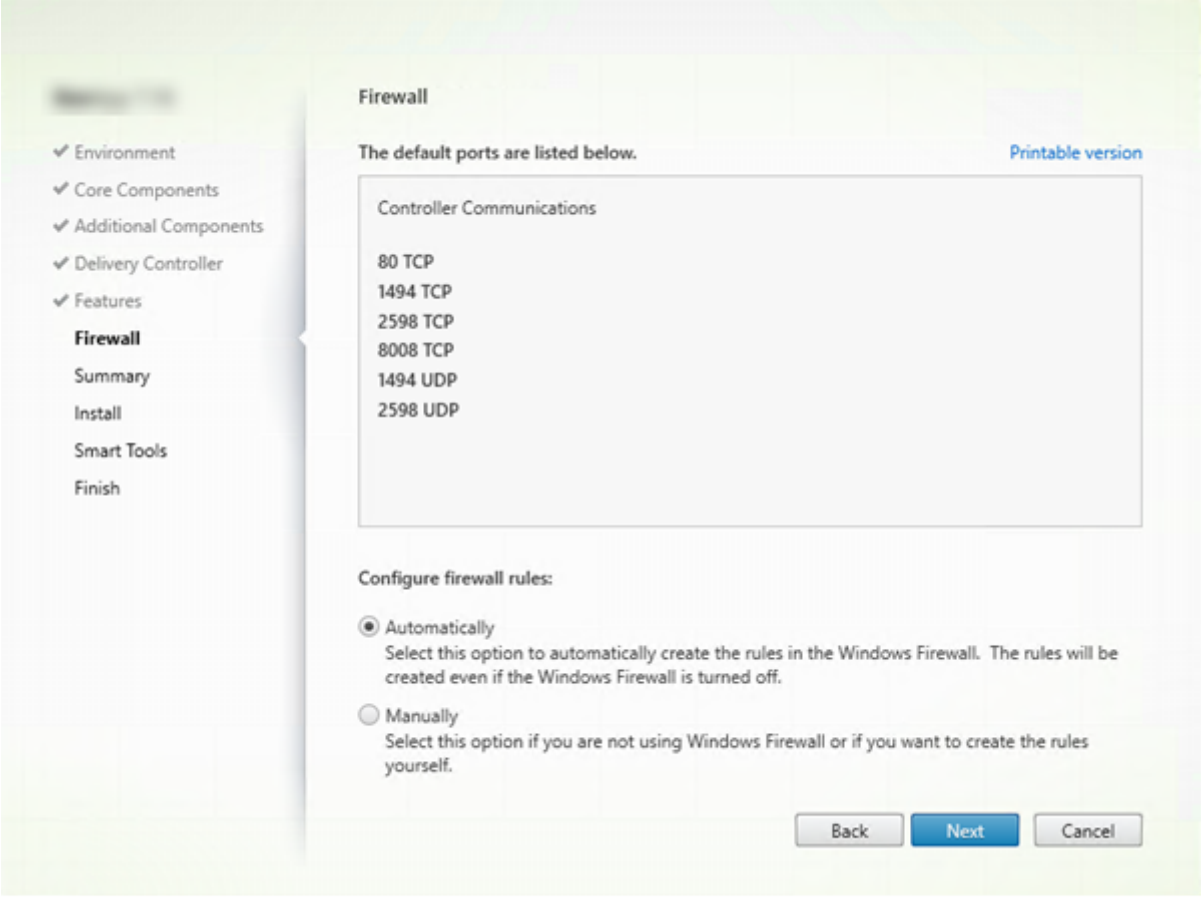
  コマンドラインオプション：`/enable_real_time_transport`

- **MCS I/O**： MCS を使用して仮想マシンをプロビジョニングする場合のみ有効になります。このオプションを選択すると、MCSIO 書き込みキャッシュドライバーがインストールされます。詳しくは、「ハイパーバイザー間で共有されるストレージ」および「一時データ用キャッシュの構成」を参照してください。

  コマンドラインオプション：`/install_mcsio_driver`

［次へ］をクリックします。

手順 **9.** ファイアウォールポート

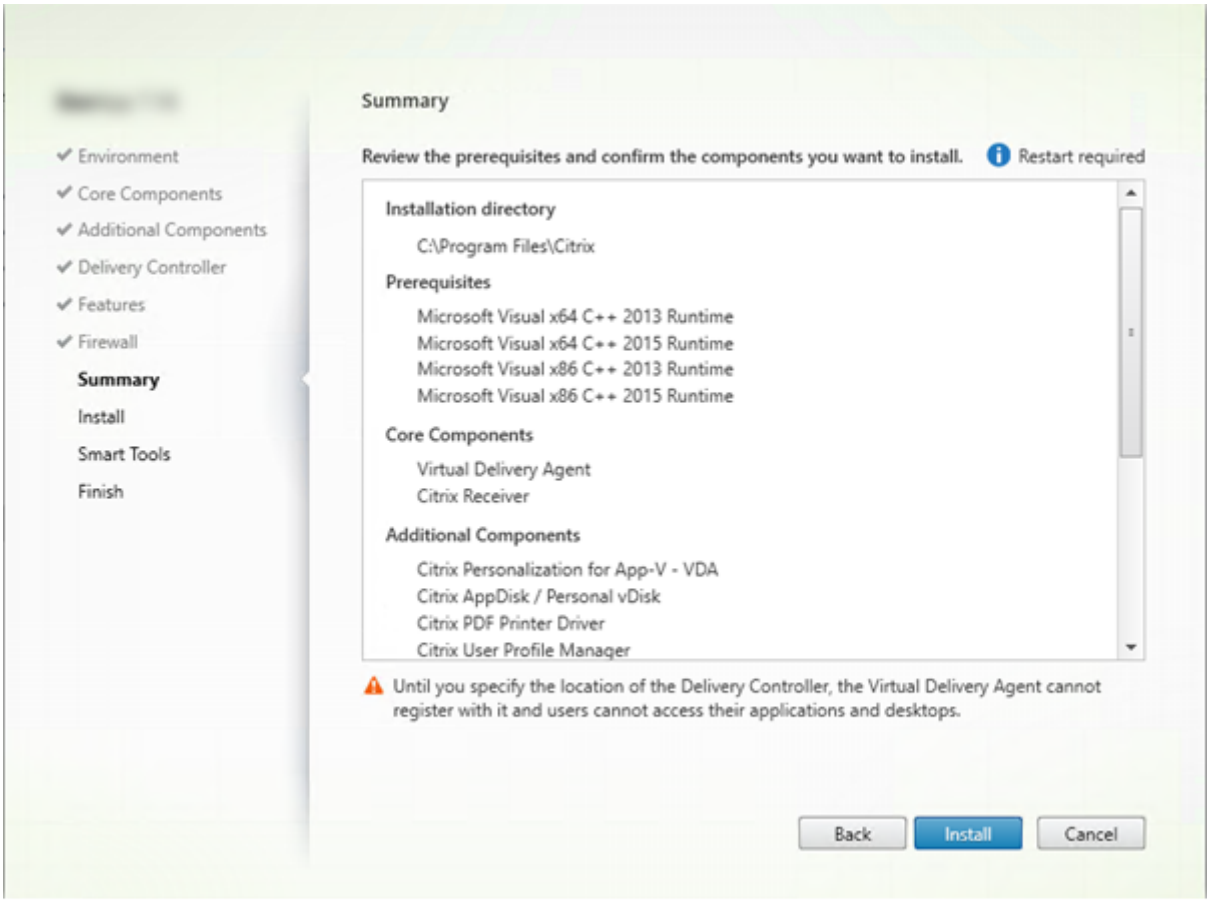


Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、［ファイアウォール］ページに示されているポートがデフォルトで開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートの詳細については、「ネットワークポート」を参照してください。

［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 **10.** インストール前に前提条件を確認する

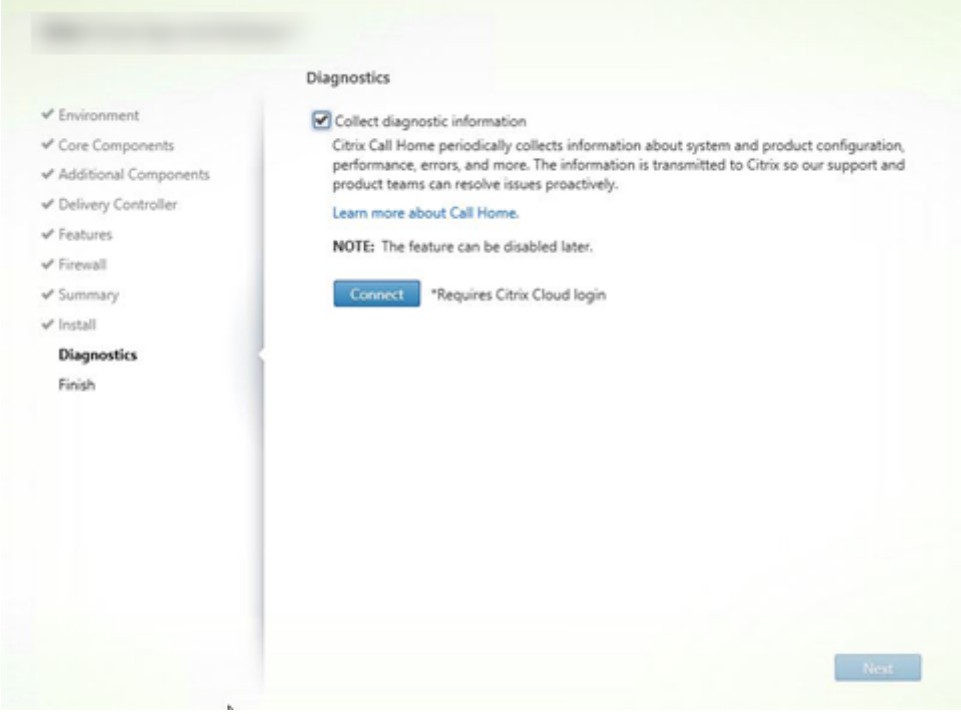


［概要］ページに、インストールされるものが表示されます。［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

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 回以上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 **11.** 診断

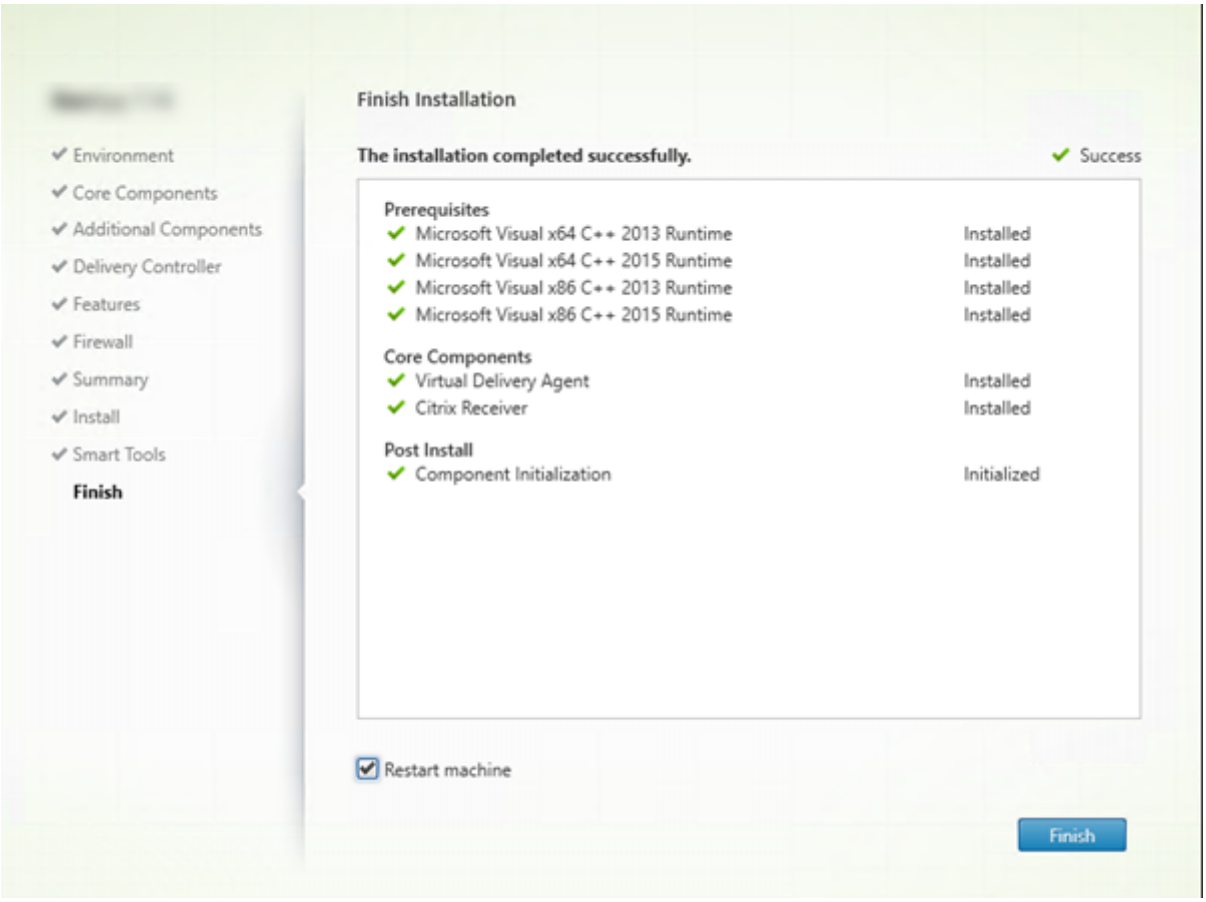


[診断] ページで、Citrix Call Home に参加するかどうかを選択します。参加することを選択する場合（デフォルト）、[接続] をクリックします。求められたら、Citrix アカウント資格情報を入力します。

資格情報が確認されたら（あるいは参加しないことを選択した場合）、[次へ] をクリックします。

詳しくは、「Call Home」を参照してください。

手順 **12.** 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。

次の手順

必要に応じて上の手順を繰り返し、他のマシンまたはイメージ上に VDA をインストールします。

すべての VDA をインストールしたら、Studio を起動します。サイトをまだ作成していない場合は、そのタスクのガイドが自動的に表示されます。それが済んだら、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

VDA のカスタマイズ

VDA をカスタマイズする場合:

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

- シトリックスがコンポーネントインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。
- デリバリーグループの Studio 表示では、[詳細] ペインの [インストール済み **VDA** のバージョン] エントリがマシンにインストールされているバージョンではないことがあります。マシンの Windows の [プログラムと機能] には、VDA の実際のバージョンが表示されます。
- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

コマンドラインを使ったインストール

April 26, 2021

> 重要:
>
> Personal vDisk（PvD）がインストールされている VDA をアップグレードする場合は、「VDA を 1912 以降にアップグレードする」を参照してください。

はじめに

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。

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。

このバージョンの Citrix Virtual Apps and Desktops でサポートされていない Windows OS バージョンで VDA をインストールまたはアップグレードしようとすると、メッセージが表示され、選択肢についての説明が示されます。また、「以前のオペレーティングシステム」も参照してください。

また、アップグレードする Citrix バージョンでサポートされていない SQL Server バージョン（サイトデータベース用）を使用するサイトをアップグレードしようとすると、メッセージが表示されます。また、「SQL Server のバージョンチェック」も参照してください。

シトリックスがコンポーネントインストールの結果を報告する方法については、「Citrix インストールリターンコード」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をインストールするには： `XenDesktopServerSetup.exe`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」に記載されているオプションを使用します。

   VDA をインストールするには： `XenDesktopVDASetup.exe`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」に記載されているオプションを使用します。

   StoreFront をインストールするには：インストールメディアの`x64 > StoreFront`フォルダーで`CitrixStoreFront-x64.exe`を実行します。

   ユニバーサルプリントサーバーをインストールするには： ユニバーサルプリントサーバーをインストールするためのコマンドラインオプションのガイダンスに従ってください。

Federated Authentication Service をインストールするには： Citrix ではグラフィカルインターフェイスを使用することをお勧めします

Sesssion Recording をインストールするには： Session Recordingのガイダンスに従ってください。

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。

1. Citrix から適切なパッケージをダウンロードします：
   - マルチセッション OS Virtual Delivery Agent：`VDAServerSetup.exe`
   - シングルセッション OS Virtual Delivery Agent：`VDAWorkstationSetup.exe`
   - シングルセッション OS Core Services Virtual Delivery Agent：`VDAWorkstationCoreSetup.exe`
2. 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、または通常どおりにパッケージを実行します。
   - インストールする前にファイルを抽出するには：
     - `/extract`に絶対パスを指定して実行します（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。存在しない場合、抽出に失敗します。
     - 次に、新しいコマンドプロンプトを開いて、抽出先フォルダー（上の例では CitrixVDAInstallMedia）から`XenDesktopVdaSetup.exe`を実行します。「VDA のインストールに使用されるコマンドラインオプション」の有効なオプションを使用します。
   - 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」の有効なオプションを使用します。

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。

  (2003 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 2003 以降では、全製品インストーラーの使用の 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** "*feature*"[,"*feature*"]

  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、それぞれを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。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合でも（RAM の不足などが原因で)、Delivery Controller のインストールやアップグレードは続行できます。詳しくは、「ハードウェアチェック」を参照してください。

- **/ignore_site_test_failure**

  Controller のアップグレード中にのみ有効です。ほとんどの場合、サイトテストの失敗は無視され、アップグレードが進行します。省略された場合（または false に設定されている場合)、サイトテストに失敗するとアップグレードを実行せずにインストーラーが失敗します。デフォルト値: false

  アップグレード中、サポートされていない SQL Server バージョンが検出されると、このオプションは無視されます。詳しくは、「SQL Server のバージョンチェック」を参照してください。

- **/installdir *directory***

  コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値：c:\Program Files\Citrix

- **/logpath *path***

  ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。デフォルト値：`TEMP%\Citrix\XenDesktop Installer`

- **/no_pending_reboot_check**

  コアコンポーネントのインストールまたはアップグレード時に、マシン上で以前の Windows インストールで保留になっていた再起動をチェックできなくなります。

- **/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**

  Citrix Virtual Apps 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、Citrix Virtual Apps and Desktops がインストールされます。

コアコンポーネントのインストールの例

次のコマンドを実行すると、Citrix Virtual Apps and Desktops、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、Citrix Virtual Apps、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（インストーラー）の 1 つ以上で使用できます：`XenDesktopVDASetup.exe`、`VDAWorkstationSetup.exe`、`VDAWorkstationCoreSetup.exe`。

オプションについて詳しくは、「VDA のインストール」を参照してください。

リリース 2003 では、`/baseimage`オプション（Personal vDisk 機能の使用が有効）は、サポートされなくなったか使用できません。同様に、`/exclude`および`/includeadditional`オプションでは、Personal vDisk または AppDisks の値を使用できなくなりました。

- **/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`：Windows 向け Citrix Workspace アプリ

  VDA および Windows 向け Citrix Workspace アプリをインストールするには、「`/components vda plugins`」と指定します。

  このオプションを指定しない場合、VDA のみがインストールされます（Citrix Workspace アプリはインストールされません）。

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。このインストーラーでは、Citrix Workspace アプリは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_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、この/enable_hdx_portsに加えて、/enable_hdx_udp_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使用するポートが 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 が使用する追加のポートを解放するには、この/enable_hdx_udp_portsに加えて、/enable_hdx_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（RealTime Audio Transport）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、それぞれ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、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:

- `Machine Identity Service`（TargetOSOptimizer.exe を含みます）
- `Citrix User Profile Manager`
- `Citrix User Profile Manager WMI Plugin`
- `Citrix Universal Print Client`
- `Citrix Telemetry Service`
- `Citrix Personalization for App-V - VDA`
- `Citrix Supportability Tools`
- `Citrix Files for Windows`
- `Citrix Files for Outlook`
- `User Personalization Layer`

インストール（`/exclude "Citrix User Profile Manager"`）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。

MCS を使用して VM をプロビジョニングする場合は、Machine Identity Service を除外しないでください。このサービスを除外すると、`TargetOSOptimizer.exe`のインストールも除外されます。

`/exclude`および`/includeadditional`の両方に同じ追加コンポーネント名を指定した場合、そのコンポーネントはインストールされません。

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。

- **/includeadditional** “*component*”[,”*component*”]

  インストールするオプションコンポーネントを 1 つ以上、それぞれ直線の二重引用符で囲みコンマ区切りで指定します。コンポーネント名の大文字と小文字は区別されます。

このオプションを使用すると、リモート PC アクセス展開を作成する場合に、デフォルトでは含まれない追加コンポーネントをインストールできます。以下の値を指定します:

- `Citrix User Profile Manager`
- `Citrix User Profile Manager WMI Plugin`
- `Citrix Universal Print Client`
- `Citrix Telemetry Service`
- `Citrix Personalization for App-V - VDA`
- `Citrix Supportability Tools`
- `Citrix Files for Windows`
- `Citrix Files for Outlook`
- `User Personalization Layer`

`/exclude`および`/includeadditional`の両方に同じ追加コンポーネント名を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *directory*

  コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値: c:\Program Files\Citrix

- **/install_mcsio_driver**

  ストレージの最適化のため、MCS I/O 書き込みキャッシュを有効にします。

- **/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。Default = 「%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`/mastermcsimage`と同等です。

  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。

- **/mastermcsimage**

  インストールするマシンを、Machine Creation Services で使用するマスターイメージに指定します。このオプションでは、`TargetOSOptimizer.exe`もインストールされます（オプティマイザーのインストーラーが含まれる`/exclude "Machine Identity Service"`を指定しない場合のみ）。このオプションは`/masterimage`と同等です。

- **/masterpvsimage**

  インストールするマシンを、Citrix Provisioning またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）で VM のプロビジョニングに使用するマスターイメージに指定します。

- **/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。

- **/nodesktopexperience**

  マルチセッション OS 対応 VDA 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**

  MCS を使用し、この機能を有効にする場合（デフォルト）, 仮想マシンの最適化によってオフラインファイルが無効になり、バックグラウンド最適化（デフラグ処理）が無効になり、イベントログのサイズが縮小されます。詳しくは、「CTX125874」を参照してください。

  最適化するには、この機能を有効にするだけでなく、Machine Identity Service をインストールする必要もあります。このサービスに`TargetOSOptimizer.exe`が含まれています。`/mastermcsimage`または`/masterimage`を指定し、`/exclude "Machine Identity Service"`を指定しないと、Machine Identity Service が自動的にインストールされます。

  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。

- **/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 アクセス展開（シングルセッション OS）または仲介接続（マルチセッション OS）でのみ有効です。シングルセッション 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（TargetOSOptimizer.exe を含む）
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - ユーザー個人設定レイヤー

  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**

  サポートされる Windows マルチセッションマシンにシングルセッション OS 対応 VDA をインストールします。Windows マルチセッションマシンにマルチセッション OS 対応 VDA をインストールするときにこのオプションを省略します。

  このオプションを使用する前に、「サーバー VDI」を参照してください。

  このオプションは、全製品 VDA インストーラーでのみ使用してください。このオプションはグラフィ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値：c:\Windows\Temp

  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。

VDA のインストールの例

フル製品インストーラーを使用して **VDA** をインストールします：

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シングルセッション OS 対応 VDA および Citrix Workspace アプリがインストールされます。この VDA はマスターイメージとなり、MCS を使用して VM をプロビジョニングします。VDA はmydomainドメインの「Contr-Main」という名前の Controller に登録されます。VDA は、ユーザー個人設定レイヤー、最適化機能、Windows リモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins
 /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /includeadditional
 "User personalization layer"/optimize /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetup スタンドアロンインストーラーでシングルセッション **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シングルセッション OS に Core Services VDA をインストールします。Citrix Workspace アプリ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
```

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 port
- /enable_hdx_ports

VDA のトラブルシューティング

- 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。
- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

ユニバーサルプリントサーバーをインストールするためのコマンドラインオプション

次のオプションはXenDesktopPrintServerSetup.exeコマンドで有効です。

- **/enable_upsserver_port**

ソフトウェア	フォルダー	ファイル名
Microsoft Visual C++ 2017 Runtime（32 および 64 ビット）	サポート **> VcRedist_2017**	vcredist_x64.exeおよびvcredist_x86.exe
Citrix Diagnostic Facility	x64 > Virtual Desktop Components	cdf_x64.msi
ユニバーサルプリントサーバーコンポーネント	x64 > Universal Print Server	UpsServer_x64.msi

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスからファイアウォールページを表示します。**Automatically** を選択すると、インストーラーは自動的に Windows ファイアウォール規則を追加し、**Manually** を選択すると管理者が手動でファイアウォールを構成できるようにします。

プリントサーバーにこのソフトウェア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」の説明に従って構成します。

詳細情報

シトリックスがコンポーネントインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。

スクリプトを使用した **VDA** のインストール

April 26, 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 Citrix Provisioning（旧称 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、完全な製品 ISO では`XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは`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。

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 ファイルに記載されています。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。例：`SET DEPLOYSHARE=\\fileserver1\share1`。
- 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`オプションはスクリプトにデフォルトで含まれており、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、展開の起動後すぐに`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。
- シトリックスがコンポーネントインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。
- デリバリーグループの Studio 表示では、［詳細］ペインの ［インストール済み **VDA** のバージョン］エントリがマシンにインストールされているバージョンではないことがあります。マシンの［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。
- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

SCCM を使用した **VDA** のインストール

April 26, 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すで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ったインストール

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

April 26, 2021

サイトとは、Citrix Virtual Apps and Desktops 展開に指定する名前のことです。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。

Controller が Server Core にインストールされている場合は、Citrix Virtual Apps and Desktops SDKの PowerShell コマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrix のカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIP では、統計情報や使用状況が匿名で収集され、Citrix に送信されます。最初のデータパッケージは、サイトを作成してから約 7 日後に Citrix に送信されます。登録内容は、サイトの作成後いつでも変更できます。Studio のナビゲーションペインで ［構成］ を選択し、［製品サポート］ タブでガイダンスに従って操作します。詳しくは、「http://more.citrix.com/XD-CEIP」を参照してください。

サイトを作成する管理者には、そのサイトのすべての管理タスクの実行権限が設定されます。詳しくは「委任管理」を参照してください。

成り行きを予想できるように、この記事を確認してからサイトを作成してください。

手順 **1. Studio** を開き、サイト作成ウィザードを開始します

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。その操作を選択します。

手順 **2.** サイトの種類と名前

［はじめに］ページで、サイトの種類を選択します：

- 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）。

手順 **3.** 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 Delivery 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。また、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。

手順 **4.** ライセンス

［ライセンス］ページでライセンスサーバーのアドレスを指定して、使用（インストール）するライセンスを決定します。

- ライセンスサーバーのアドレスを、`name:[port]`という形式で指定します。*name* は、FQDN、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、次のページに進めません。
- 接続が確立されると、［既存のライセンスを使用する］がデフォルトで選択されます。ディスプレイには、現在インストールされているライセンスに基づいて、この製品を構成できる互換性のある製品が一覧表示されます。
  - 一覧にある製品（Citrix Virtual Apps Premium または Citrix Virtual Desktops Premium など）の 1 つとしていずれかのライセンスを使用してこの製品を構成する場合は、そのエントリを選択します。
  - この製品で使用するライセンスを（Citrix Manage Licenses Tool を使用して）割り当ててダウンロードしたが、ライセンスをまだインストールしていない場合：
    * ［ライセンスファイルの参照**...**］をクリックします。
    * ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連付けられた製品が、サイト作成ウィザードの ［ライセンス］ページに表示されます。使用するエントリを選択します。
  - 必要な製品が表示されない場合、または割り当て済みライセンスやダウンロード済みのライセンスがない場合は、ライセンスの割り当て、ダウンロード、インストールを実行できます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。また、必要な製品のライセンスアクセスコードが必要です。コードはメールで届きます。
    * ［割り当ておよびダウンロード**...**］をクリックします。

* ［ライセンスの割り当て］ダイアログボックスでシトリックスから届いたライセンスアクセスコードを入力します。［ライセンスの割り当て］をクリックします。
* 新しいライセンスに関連付けられた製品が、サイト作成ウィザードの ［ライセンス］ページに表示されます。使用するエントリを選択します。

または、［**30** 日間無料のトライアルを使用する］を選択し、ライセンスを後でインストールします。詳しくは、ライセンス管理のドキュメントを参照してください。

手順 **5.** 電源管理（リモート **PC** アクセスのみ）

「手順 8. リモート PC アクセス」を参照してください。

手順 **6.** ホスト接続、ネットワーク、およびストレージ

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで VDA をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

ハイパーバイザーまたはクラウドサービスで仮想マシンを使用してアプリケーションおよびデスクトップを提供する場合、必要に応じて、ホストへの最初の接続を作成できます。その接続のストレージリソースとネットワークリソースも指定できます。サイトの作成後、この接続やリソースを変更したり、追加の接続を作成したりできます。詳しくは、「接続とリソース」を参照してください。

- ［接続］ページで指定する情報については、「接続とリソース」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。
- ストレージおよびネットワークページで指定する情報については、「ホストストレージ」、「ストレージ管理」および「ストレージの選択」を参照してください。

手順 **7.** そのほかの機能

［追加機能］ページで、サイトをカスタマイズする機能を選択できます。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：（この機能は廃止済みです）AppDisk を使用していて、AppDNA がインストールされている場合。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。
- **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。

手順 **8.** 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、「Configuration Manager とリモート PC アクセスの Wake on LAN」を参照してください。

リモート PC アクセス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 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。

手順 **9.** 概要

［概要］ページに、指定した情報が一覧表示されます。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 *site-name*）］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。

以前の展開をアップグレードすると、サイトのテストが自動的に実行されます。詳しくは、「事前サイトテスト」を参照してください。

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

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで Virtual Delivery Agent（VDA）をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

はじめに

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には、同じ種類のオペレーティングシステム（マルチセッション OS またはシングルセッション OS）がインストールされています。マルチセッション 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、Citrix 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。

> ヒント:
>
> Machine Creation Services（MCS）のストレージ最適化機能（MCS I/O と呼ばれます）を有効にする既存の展開をアップグレードする場合、追加の設定は必要ありません。VDA および Delivery Controller アップグレードにより、MCS I/O アップグレードが処理されます。

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 Citrix Provisioning（旧称 Provisioning Services）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。

次の点を考慮してください。

- MCS は、仮想マシンイメージから 1 つのシステムディスクをサポートします。このイメージに接続されている残りのデータディスクは無視されます。
- Citrix Provisioning を使用してマシンを作成する場合の手順については、Citrix Provisioning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（またはイメージのスナップショット）を提供します。カタログを作成する前に、ツールを使用してマスターイメージを作成し、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いる場合でも、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。
- 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。
- テンプレートを使用したカタログのプロビジョニングは、試験段階の機能と見なされています。この方法を使用すると、仮想マシンの準備に失敗する場合があります。そのため、テンプレートを使用してカタログを公開することができなくなります。

MCS または Citrix Provisioning 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。

> 注:
>
> MCS では、Windows 10 IoT Core および Windows 10 IoT Enterprise はサポートされていません。詳しくは、『Microsoft のサイト』を参照してください。

Citrix Provisioning ツールの技術的な詳細については、「Citrix Virtual Apps and Desktops のイメージ管理」を参照してください。

RDS ライセンスチェック

Citrix Studio は現在、Windows マルチセッション OS マシンが含まれるマシンカタログの作成時に Microsoft RDS ライセンスの有効性をチェックしません。Windows マルチセッション **OS** マシン用の Microsoft RDS ライセンスの状態を確認するには、Citrix Director にアクセスしてください。[マシンの詳細] パネルで、Microsoft RDS (Remote Desktop Services) ライセンスの状態を表示します。詳しくは、「Microsoft RDS ライセンスの正常性」を参照してください。

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 コネクタ (Citrix Cloud 展開用) に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Citrix 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可能性があることを示すメッセージが表示された場合でも、そのマシンを追加します。

詳しくは、次のトピックを参照してください:

- CTX136668: VDA 登録のトラブルシューティングガイダンス
- VDA バージョンと機能レベル
- VDA の登録方法

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。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。プールデスクトップの場合、Delivery Controller によって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。

Machine Creation Services のストレージの考慮事項

Machine Creation Services（MCS）のストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下に、適切なストレージ容量を決定するための考慮事項を示します:

容量に関する考慮事項:

- ディスク

  ほとんどの MCS 環境において、デルタ（差分）ディスクが各 VM の容量を一番多く占めます。MCS により作成される仮想マシンには、作成時にディスクが 2 つ以上割り当てられます。

  - ディスク 0 = 差分ディスク：マスター基本イメージからコピーした OS が含まれます。
  - ディスク 1 = ID ディスク：16MB - 各仮想マシンの Active Directory データが含まれます。

  製品の進化にともない、特定のユースケースや機能の消費容量に合わせたディスクの追加が必要になることがあります。例:

  - Personal vDiskを使用すると、管理者が操作を行わなくても、エンドユーザーが仮想マシンに接続されている各ディスクにアプリケーションをインストールできます。
  - AppDiskでは、エンドユーザーは、主にマルチセッション OS カタログ用の仮想マシンにアプリケーション専用ディスクを接続できます。
  - MCS ストレージ最適化では、仮想マシンごとに書き込みキャッシュ形式のディスクが作成されます。

  - 前述のデルタディスクの使用例とは対象的に、MCS には、完全なクローンを使用する機能が追加されています。

  Hypervisor の機能も、こうした要因になることがあります。例:

  - Citrix Hypervisor の IntelliCacheはローカルストレージ上に各 Citrix Hypervisor の読み取りディスクを作成します。このディスクはマスターイメージに対する IOPS を保存します。このマスターイメージは、共有ストレージの場所に保存することもできます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーごとに固有のファイルを使用するため、これが仮想マシンのオーバーヘッドとなります。ハイパーバイザーは、管理操作および一般的なログ記録でストレージを使用します。容量は、以下のオーバーヘッドを考慮して計算してください:

  - ログファイル
  - ハイパーバイザー固有のファイル。例:
    * VMware により、**VM storage** フォルダーにファイルが追加されます。VMware のベストプラクティスを参照してください。
    * 仮想マシン全体で必要なサイズを計算してください。たとえば、仮想ディスクに 20GB、仮想マシンスワップファイルに 16GB、ログファイルに 100MB を使用する仮想マシンでは、合計で 36.1GB の容量が必要になります。
  - XenServer のスナップショットおよびVMware のスナップショット。

- プロセスのオーバーヘッド

  カタログの作成と更新、およびマシンの追加を行なうと、それぞれ以下のようにストレージに影響が及びます。例:

  - カタログを初めて作成する場合、各ストレージの場所に基本ディスクをコピーする必要があります。
    * また、一時的に準備用の仮想マシンを作成する必要もあります。
  - カタログにマシンを追加する場合は、各ストレージの場所に基本ディスクをコピーする必要はありません。ただし、カタログの作成方法は、選択した機能によって異なります。このため、Personal vDisk または AppDisk を選択すると、単純なランダムプールカタログに比べて多くのスペースが必要になります。
  - カタログを更新すると、ストレージの場所ごとに基本ディスクを追加で作成できるようになります。また、カタログに含まれる仮想マシンに一定期間にわたって 2 つの差分ディスクが割り当てられるため、一時的にストレージ占有量が急増することになります。

そのほかの考慮事項:

- **RAM** のサイズ設定: I/O 最適化ディスク、書き込みキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- シン/シックプロビジョニング: シンプロビジョニング機能を備えているため、NFS ストレージが推奨されます。

Machine Creation Services（**MCS**）ストレージ最適化

MCS I/O と呼ばれる Machine Creation Services（MCS）ストレージの最適化機能の特徴:

- 書き込みキャッシュコンテナは、Citrix Provisioning と同様にファイルベースです。たとえば、Citrix Provisioning の書き込みキャッシュのファイル名は「`D:\vdiskdif.vhdx`」、MCS I/O 書き込みキャッシュのファイル名は「`D:\mcsdif.vhdx`」です。
- 書き込みキャッシュディスクへの Windows クラッシュダンプファイルの書き込みをサポートすることで、診断機能を向上させることができます。
- MCS I/O は、引き続きハードディスクへのオーバーフローありで *RAM* にキャッシュするテクノロジを利用して、複数層の書き込みキャッシュに関して最適なソリューションを提供します。この機能により、管理者は各層のコスト、RAM とディスク、パフォーマンスのバランスを取りながら、必要なワークロードに対応できます。

書き込みキャッシュの方法をディスクベースからファイルベースに更新するには、以下の変更が必要です:

1. MCS I/O では、RAM のみのキャッシュはサポートされなくなります。マシンカタログの作成中に Citrix Studio でディスクサイズを指定します。
2. 仮想マシンの初回起動時に、書き込みキャッシュディスクが自動的に作成およびフォーマットされます。仮想マシンが起動すると、書き込みキャッシュファイル`mcsdif.vhdx`はフォーマット済みボリューム`MCSWCDisk`に書き込まれます。
3. Microsoft Azure 環境を除き、ページファイルはこのフォーマット済みボリューム`MCSWCDisk`にリダイレクトされます。そのため、ディスクサイズにはディスク領域の合計容量を考慮します。この合計容量には、ディスクサイズと生成されたワークロードおよびページファイルサイズの差分が含まれます（通常は仮想マシンの RAM サイズに関連します）。Microsoft Azure のページファイルはローカルの一時ディスクを使用するよう事前構成され、MCS ストレージ最適化 I/O 機能によって`MCSWCDisk`にリダイレクトされることはありません。

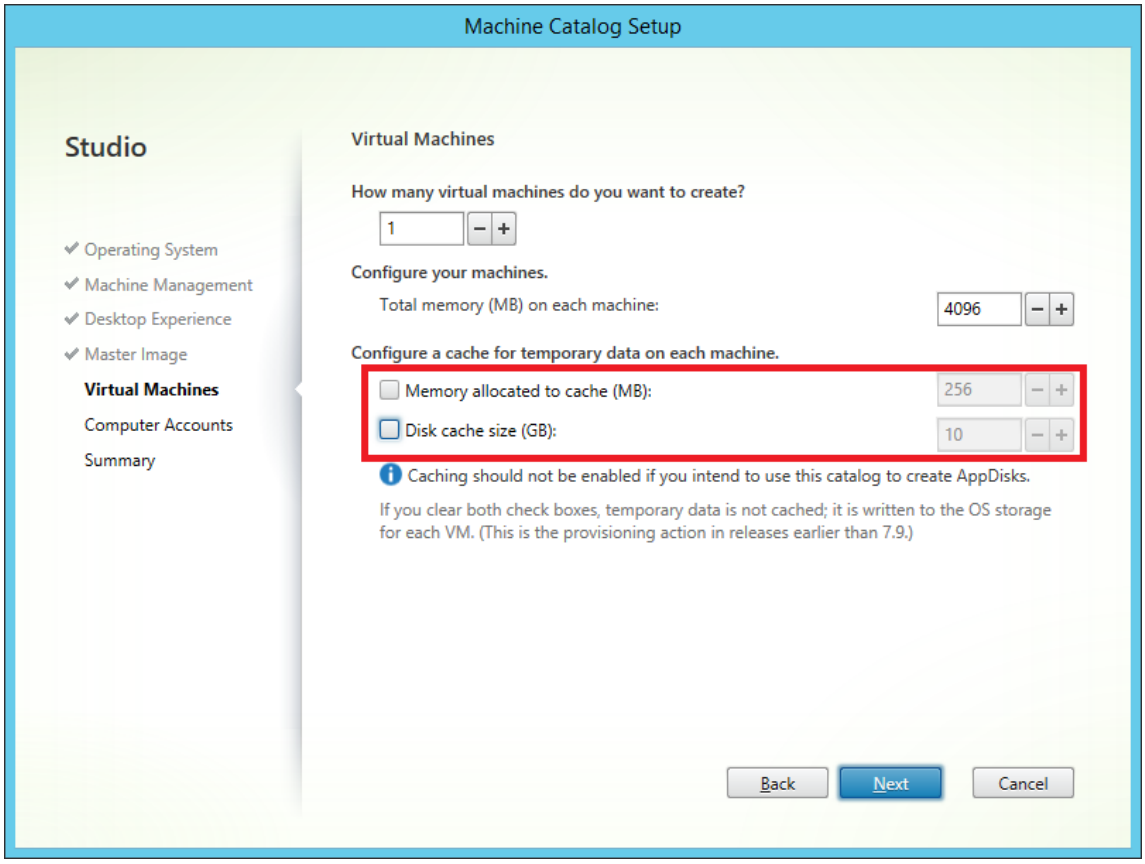
MCS ストレージ最適化の更新を有効にする

MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を最新バージョンの Citrix Virtual Apps and Desktops にアップグレードします。

> 注:
>
> MCS I/O が有効化された既存の環境をアップグレードする場合、追加の構成は必要ありません。VDA および Delivery Controller アップグレードにより、MCS I/O アップグレードが処理されます。

MCS ストレージ最適化の更新を有効にするときは、次の点を考慮してください:

- マシンカタログを作成するとき、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、Citrix Virtual Apps and Desktops バージョン 1903 の VDA を含む新しい仮想マシンスナップショットに更新すると、RAM とディスクサイズに関する既存のカタログの MCS I/O 設定が引き続き使用されます。既存の未フォーマットディスクはフォーマットされます。

> 重要:
>
> MCS ストレージ最適化は、Citrix Virtual Apps and Desktops バージョン 1912 LTSR で変更されました。このリリースでは、ファイルベースの書き込みキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O で提供される新機能は、Citrix Virtual Apps and Desktops の過去のリリースと比較して、より高い書き込みキャッシュストレージ要件が必要になることがあります。割り当てられたワークフローと追加のページファイル用の十分なディスク領域があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルのサイズは通常、システム RAM の容量に関連しています。既存のカタログのディスクサイズが不十分な場合は、マシンカタログを作成し、より大きな書き込みキャッシュディスクを割り当ててください。

Microsoft Azure 環境について

デフォルトでは、MCS I/O 書き込みキャッシュディスクは、最初の仮想マシンの起動時にプロビジョニングされ、シャットダウン後に削除されます。これは最もコスト効率の高い設定ですが、書き込みキャッシュディスクのフォーマットと追加の再起動が必要なため、仮想マシンの起動時間が長くなります。起動時間が重視されるワークロードがある環境では、PowerShell を使用して、永続的な MCS I/O キャッシュディスクの仮想マシンを作成することをお勧

めします永続的なキャッシュディスクは、電源の再投入時に削除されません。ただし、Azure ストレージアカウントでそのために必要なコストを考慮する必要があります。

PowerShell を使用して永続的なライトバックキャッシュディスクの **Azure** カタログを作成する

永続的なライトバックキャッシュディスクの Azure カタログを構成するには、PowerShell パラメーターNew-ProvScheme CustomPropertiesを使用します。このパラメーターではプロパティPersistWBCを追加することができ、MCS でプロビジョニングされたマシンをホストする Azure Resource Manager でライトバックキャッシュディスクを永続化させる方法を指定できます。PersistWBCプロパティは、UseWriteBackCacheパラメーターが指定され、WriteBackCacheDiskSizeパラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

> ヒント:
>
> Azure にはプロビジョニング用の多数のプロパティがあり、CustomPropertiesフィールドはさまざまな設定で使用されます。

以下は、PersistWBCをサポートする前にCustomPropertiesパラメーターで使用されるプロパティの例です:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

これらのプロパティを使用するときは、プロパティがCustomPropertiesパラメーターから省略されている場合にデフォルトの値が含まれるようにしてください。PersistWBCプロパティには、次の 2 つの値が設定可能です: **true** または **false**。

PersistWBCプロパティを **true** に設定すると、Citrix Virtual Apps and Desktops 管理者が Citrix Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されません。

PersistWBCプロパティを **false** に設定すると、Citrix Virtual Apps and Desktops 管理者が Citrix Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されます。

> 注:
>
> PersistWBCプロパティを省略する場合、デフォルトは **false** になり、Citrix Studio を使用してマシンをシャットダウンするとライトバックキャッシュは消去されます。

例: CustomPropertiesパラメーターを使用してPersistWBCを true に設定した場合:


```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> 重要:
>
> PersistWBCプロパティは、New-ProvScheme PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームのCustomPropertiesを変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。PersistWBCの値は Azure Resource Manager で展開されるカタログでのみ使用されます。

例: PersistWBCプロパティを true に設定するときにNew-ProvSchemeを設定してライトバックキャッシュを使用した場合:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
```

```
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

AWS 専用のホストテナントサポート

MCS を使用して、AWS 専用のホストをプロビジョニングすることができます。管理者は、PowerShell で定義されたホストテナントを持つマシンのカタログを作成できます。

Amazon [EC2] 専用ホストは、完全に専用の [EC2] インスタンス容量を搭載した物理サーバーです。既存のソケット単位または VM 単位のソフトウェアライセンスを使用することができます。

専用ホストには、インスタンスの種類に基づいて使用率が事前に設定されています。たとえば、C4 ラージインスタンスタイプの 1 つの割り当てられた専用ホストは、16 個のインスタンスの実行に限定されます。詳しくは、AWS のサイトを参照してください。

AWS ホストへのプロビジョニングの要件は次のとおりです:

- インポートされた BYOL（ライセンス持ち込み）のイメージ（AMI)。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な使用率を持つ専用ホストの割り当て。
- 自動配置を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、TenancyType パラメーターを *Host* に設定した **New-ProvScheme** コマンドレットを使用します。

詳しくは、『シトリックスの開発者用ドキュメント』を参照してください。

マスターイメージの準備

接続ホストの作成について詳しくは、「接続とリソース」を参照してください。

マ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。ホストベンダーによって、異なる用語を使用します。
- Citrix Provisioning 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。Citrix Provisioning では、イメージを指すのに MCS とは異なる用語を使用します。詳しくは、Citrix Provisioningのドキュメントを参照してください。

- ホストに、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。

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（Citrix VM 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：
>
> Citrix Provisioning 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. Citrix Provisioning 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仮想ディスクの VHD ファイルを作成します。詳しくは、Citrix Provisioning 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。

Studio でのカタログの作成

カタログ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。

- サイトは作成したがマシンカタログは作成していない場合は、カタログを作成するための説明が表示されます。
- 既存のマシンカタログがあり、別のマシンカタログを作成する場合は、**Studio** のナビゲーションペインで［マシンカタログ］を選択します。その後、［操作］ペインで ［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、以下の項目の操作を行います。選択内容によって、異なるウィザードページが表示されます。

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。いずれかを選択します。

- マルチセッション **OS**：マルチセッション OS カタログは、ホストされた共有デスクトップを提供します。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）。
- シングルセッション **OS**：シングルセッション OS カタログでは、さまざまなユーザーに割り当てることができる VDI デスクトップが提供されます。
- 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を選択します。

- Studio で電源管理されるマシン（仮想マシンやブレード PC など）。このオプションは、ホストへの接続を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 で電源管理されるように指定した場合、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。MCS は物理マシンでは使用できません。
- **Citrix Provisioning**（旧称 **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 Citrix Provisioning 仮想ディスクを使用して、デスクトップとアプリケーションを配信します。
- 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、シングルセッション 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。

2 つ目のオプションを選択し、Citrix Provisioning を使用してマシンをプロビジョニングしている場合、デスクトップへのユーザー変更の処理方法を構成できます：

- ユーザー変更を個別の Personal vDisk 上のデスクトップに保存する。（Personal vDisk は廃止済みです。）
- ユーザー変更をローカルディスク上のデスクトップに保存する。
- ユーザーがログオフしたらユーザー変更を破棄し、仮想デスクトップをクリアする。ユーザー個人設定レイヤーを使用している場合は、このオプションを選択します。

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。

［マスターイメージ］ページで、ホスト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 Citrix Provisioning 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。

デバイスコレクション

このページは、Citrix Provisioning 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。

［デバイスコレクション］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。

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 を使用する場合:

- 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。
- 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に設定されます。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、仮想ディスクサイズ（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。

Citrix Provisioning を使用する場合:

［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。

他のツールを使用する場合：

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］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、ユーザーはページ上のままで一覧から名前を削除できます。

Citrix Provisioning または他のツール（**MCS** 以外）を使う場合：

追加（または Citrix Provisioning デバイスコレクションからインポート）した各マシンに表示されるアイコンとツールチップにより、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を特定できます。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 が必要です。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メニューを使って、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

Citrix Virtual Apps and Desktops のリリースには、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、バージョン 7.17 には 7.17 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 7.9～7.16 から 7.17 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。各リリースの「新機能」には、デフォルト以外の機能レベルが必要かどうかが記載されています。

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。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、シングルセッション OS カタログにサーバーを追加しようとした場合や、ランダム割り当て用に作成されたシングルセッション 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。

> 重要:
>
> リリース 1811 では、次の機能レベルが追加されました：**1811**（またはそれ以降）。このレベルは、今後の Citrix Virtual Apps and Desktops 機能での使用を想定しています。**7.9**（またはそれ以降）の選択はデフォルトのままです。このデフォルトは、すべての環境で有効になりました。
>
> **1811**（またはそれ以降）を選択した場合、そのカタログの以前の VDA バージョンは Controller と Cloud Connector には登録できません。ただし、バージョン 1811 以降のサポート対象バージョンでカタログに VDA のみが含まれている場合は、それらはすべて登録対象です。これには、新しい Citrix Virtual Apps and Desktops リリース（バージョン 1903 および現在のリリースより前の 19XX リリースを含む）用に構成された VDA を含むカタログが含まれます。

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。

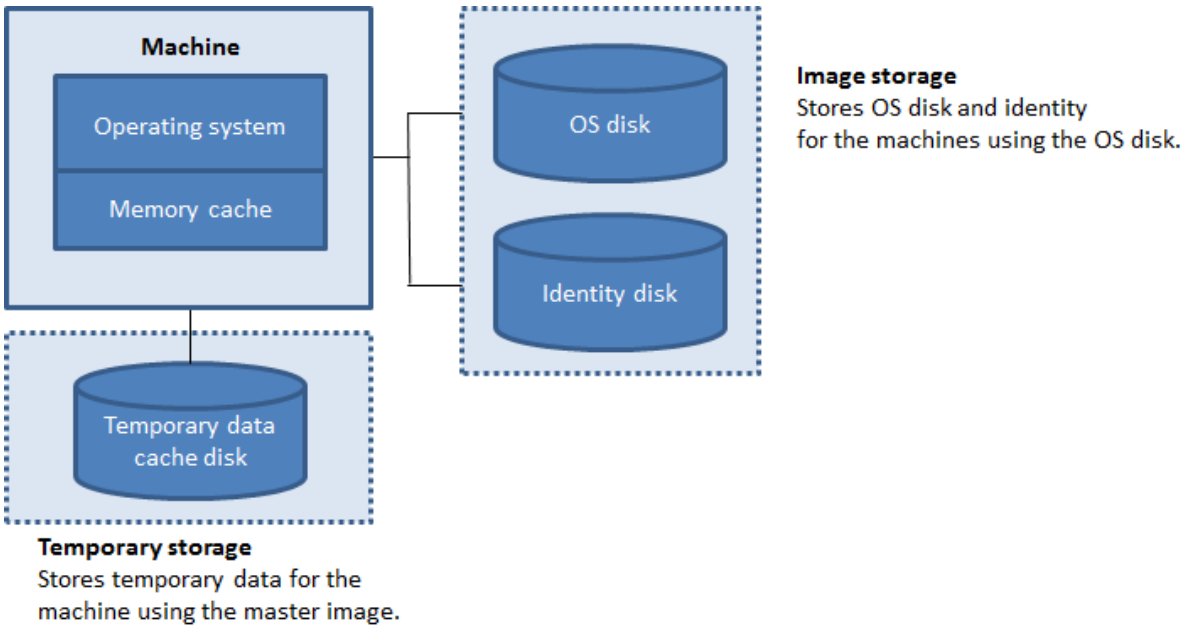
> 重要:
>
> この機能を使用するには、最新の MCS I/O ドライバーが必要です。このドライバーは、VDA のインストール時またはアップグレード時にオプションとしてインストールできます。デフォルトでは、このドライバーはインストールされません。

カタログで使用する接続を作成するときに、一時データ用に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。各マシンで一時データのキャッシュを構成する場合、次の 2 つのオプションを使用できます：［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**）]。デフォルトでは、2 つのオプションはオフになっています。[キャッシュに割り当てられたメモリ(MB)] オプションを有効にするには、[ディスクキャッシュサイズ（GB）] チェックボックスを選択します。[ディスクキャッシュサイズ] チェックボックスがオンになっていない場合、[キャッシュに割り当てられたメモリ] オプションは灰色表示になります。接続の種類によっては、これらのオプションのデフォルト値が異なる場合があります。通常は、デフォルト値で十分です。ただし、以下のデータ用に必要な容量について注意してください:

- 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。



各マシンで一時データ用のキャッシュを構成する場合、次の 3 つの点に注意してください:

- [ディスクキャッシュサイズ] チェックボックスと [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選択しない場合、一時データはキャッシュされません。各仮想マシンの差分ディスク（OS ストレージにあります）に直接書き込まれます（これはバージョン 7.8 以前のプロビジョニングアクションです）。
- [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、[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] チェックボックスと [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選択する場合、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。

> 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。
> - 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。
> - マシンの作成後は、マシンカタログのキャッシュ値を変更できません。
>
> 注:
>
> - 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す。そのため、［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を増やすことを検討してください。
> - ［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。

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。

［ネットワークインターフェイスカード］ページで、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。

［マシンアカウント］ページで、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します。

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。［コンピューターアカウント］ページで、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。

- 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。Studio はこれらのアカウントを管理します。オプションで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）。

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物理マシンまたは既存のマシンを含むカタログのユーザーアカウントに割り当てます。

Citrix Provisioning 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、Citrix Provisioning 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

［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。これらの情報は Studio に表示されます。

完了したら、［完了］をクリックしてカタログの作成を開始します。

トラブルシューティング

> 重要：
>
> Citrix Studio を使用してマシンカタログを作成すると、それ以降は`Get-ProvTask` PowerShell コマンドを使用してマシンカタログの作成に関連するタスクを取得することができなくなります。これはマシンカタログが正常に作成されたかどうかにかかわらず、取得対象のタスクが Studio によって削除されることから生じる制限です。

サポートチームが解決策を提供するのに役立つログを収集することをお勧めします。Citrix Provisioning 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、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell 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:\:Image-prep.log and PvsVmAgentLog.txt のルートから次のファイルを抽出します。
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、イメージ準備用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`。

次のステップ

最初のカタログを作成すると、Studio ではデリバリーグループの作成の手順が表示されます。

マシンカタログの管理

April 26, 2021

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。

カタログの保守には、各マシンの OS が最新状態に更新されていることを確認することも含まれます。ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更も含まれます。

- 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は、カタログで使用されるマスターイメージを更新してからマシンを更新することにより、マシンを管理できます。この方法により、多数のユーザーマシンを効率的に更新することができます。
- Citrix Provisioning で作成されたマシンの場合は、仮想ディスクを介してマシンを更新します。詳しくは、Citrix Provisioning 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。

> 注:
>
> MCS では、Windows 10 IoT Core および Windows 10 IoT Enterprise はサポートされていません。詳しくは、『Microsoft のサイト』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。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。

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。

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。

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は Azure から削除されます。保持することを指定した場合でも、この動作が発生します。

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場合、［電源管理］ページを使用して電源管理設定を変更したり、電源管理接続を選択したりします。［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。

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ります。

1. **Studio** のナビゲーションペインで ［マシンカタログ］を選択します。
2. カタログを選択し、［操作］ペインの ［移動］を選択します。
3. カタログの移動先ゾーンを選択します。

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。

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:

- シングルセッション OS カタログおよびマルチセッション 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。

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。カタログ内のマシンをロールバックして（元に戻して）、以前のバージョンのマスターイメージを使用します。デスクトップに展開した更新で問題が発生した場合は、この作業を実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。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。カタログを元に戻して使用することはできません。

Citrix Provisioning（旧称 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、新しい仮想ディスクを公開する必要があります。詳しくは、Citrix Provisioning 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

マシンカタログを更新する前に、既存のマスターイメージを更新するか、またはホストハイパーバイザー上で作成します。

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ます。仮想マシンに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ます。このスナップショットを Studio で選択します。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、Citrix Hypervisor コンソール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。
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。

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、ハイパーバイザーテンプレート (VMTemplates) を指定します。これをイメージまたはイメージのスナップショットの代わりに使用します。

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します。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］ドロップダウンメニューで、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。更新が開始される 15 分前にメッセージを表示するように選択します。または、最初のメッセージの後 5 分ごとにメッセージを繰り返すように選択します。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、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。このプロセスは、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した。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述したとおり、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、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。

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。

- Citrix Provisioning 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。Citrix Provisioning は、Citrix Virtual Apps and Desktops の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

April 26, 2021

デリバリーグループは、1 つ以上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］ページでカタログを選択して、そのカタログから使用するマシンの番号を選択します。

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。
- 複数のデリバリーグループで同じカタログを選択することができますが、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］か ［デスクトップ］を選択します。両方を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ます：この場合は、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 は廃止済みです。

AppDisk を追加するには、［追加］をクリックします。［AppDisk の選択］ダイアログボックスでは、左側の列に選択可能な AppDisk が一覧表示されます。右側の列に AppDisk のアプリケーションが一覧表示されます右の列の上にある ［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。

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）。アプリケーション資格ポリシー規則には、デフォルトではすべてのユーザーが含まれます。詳しくは、PowerShell SDK の`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。

- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront 経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーション A の使用を構成するには次のように設定します：

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- （アプリケーショングループが構成されている場合）アプリケーション A～L に管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーション A のプロパティを構成します。

認証が必要なユーザーおよび認証が不要なユーザー

ユーザーには、認証が必要なユーザーと認証が不要なユーザーの 2 種類があります（認証が不要なユーザーは「匿名ユーザー」とも呼ばれます）。いずれか一方または両方の種類のユーザーをデリバリーグループ内に構成できます。

- 認証が必要なユーザー：特定のアカウント名で指定したユーザーおよびグループメンバーは、アプリケーションとデスクトップにアクセスするときに、StoreFront または Citrix Workspace アプリで資格情報（スマートカード、またはユーザー名とパスワードなど）による認証を求められます。デリバリーグループにデスクトップ OS マシンが含まれる場合、後にそのデリバリーグループを編集することでユーザーデータ（ユーザーの一覧）をインポートできます。

- 認証が不要なユーザー（匿名ユーザー）：サーバー OS マシンを含むデリバリーグループでは、StoreFront または Citrix Workspace アプリ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、キオスクのアプリケーションでは資格情報を必須にして、Citrix アクセスポータルやツールでは不要にできます。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、Anon*XYZ*（*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）］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 Workspace アプリに同じ名前が 2 つ表示されます。

［追加］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

このページのタイトルは、[マシン] ページで選択した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] になります。
- 割り当て済みの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」になります。
- 割り当て済みの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」になります。

[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] フィールドと [説明] フィールドに、Citrix Workspace アプリで表示す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。

サイト内の最大デスクトップインスタンス数 (**PowerShell** のみ)

サイト内の最大デスクトップインスタンス数を構成するには (PowerShell のみ):

- PowerShell で、適切な BrokerEntitlementPolicyRule コマンドレットに MaxPerEntitlementInstances パラメーターを指定して実行します。たとえば、次のコマンドレットでは、「tsvda-desktop」ルールを変更して、サイト内で同時に実行できるデスクトップインスタンス数の上限を 2 に設定します。デスクト

ップインスタンスが 2 つ実行されている場合、3 人目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInstances
 2
```

- 詳しくは、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`など です。

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、Citrix Workspace アプリと Studio に表示される説明を入力することもできます。

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

April 26, 2021

はじめに

この記事では、管理コンソールで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。

手順は全般的な設定、ユーザー設定、マシン設定、セッション設定のカテゴリ別にまとめられています。タスクによっては複数のカテゴリに関係します。たとえば、「マシンへのユーザーの接続を禁止する」のタスクはマシン設定のカテゴリで説明されていますが、ユーザー設定のカテゴリにもかかわります。あるカテゴリで見つからないタスクがある場合は、関連するカテゴリを確認してください。

この他の記事にも関連情報が記載されています:

- 「アプリケーション」にはデリバリーグループでのアプリケーションの管理に関する情報が記載されています。
- デリバリーグループを管理するには、組み込みのデリバリーグループ管理者の役割が必要です。詳しくは、「委任管理」を参照してください。

一般

- 配信方法の変更
- StoreFront アドレスの変更

- デリバリーグループのアップグレード
- リモート PC アクセスのデリバリーグループの管理

デリバリーグループの配信の種類の変更

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. 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］をクリックします。
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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

StoreFront アドレスの変更

1. 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］をクリックします。
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 Workspace アプリで使用されます。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用して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、ナビゲーションペインで ［構成］**>** ［**StoreFront**］の順に選択します。

デリバリーグループのアップグレード、またはアップグレードの取り消し

デリバリーグループのアップグレードは、マシン上の VDA、およびデリバリーグループで使用されているマシンを含むマシンカタログをアップグレードしてから行ってください。

デリバリーグループのアップグレードを開始する前に、以下の操作を行います。

- Citrix Provisioning（旧称 Provisioning Services）を使用している場合は、Citrix Provisioning コンソールで VDA をアップグレードします。
- アップグレードした 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コンソールで特定されます。
- 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、アップグレードのドキュメント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. 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］をクリックします。［配信グループのアップグレード］操作は、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］をクリックします。

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。この優先度値は設定するには PowerShell SDK を使用します。

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. 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］タブをクリックし、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］をクリックします。関連付けを削除するには、［関連付けの削除］をクリックします。

ユーザー

- ユーザー設定の変更
- ユーザーの追加と削除

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. 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］をクリックします。

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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

設定	説明
説明	Citrix Workspace（または StoreFront）でユーザーに表示される説明です。
デリバリーグループの有効化	このデリバリーグループを有効にするかどうかを設定します。
タイムゾーン	
Secure ICA を有効にする	デリバリーグループのマシンとの通信を、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、「ユーザー」を参照してください。

1. 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］をクリックします。
3. ユーザーページで以下の手順を実行します：
   - 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。
   - 認証されていないユーザーによるアクセスを許可するかどうかを設定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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用して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

物理シングルセッション 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には、列見出し（順不同）としてADComputerAccount、AssignedUser、VirtualMachine、HostIdをコンマで区切って記載する必要があります。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エントリには、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を指定できます。

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. 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］をクリックします。
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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

マシン

- ユーザーへのマシン割り当ての変更
- ユーザーあたりの最大マシン数の変更
- マシンの更新
- デスクトップのタグ制約の追加、変更、または削除
- マシンの削除
- マシンへのアクセス制限
- 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）
- マシンのシャットダウンと再起動
- マシンに対する再起動スケジュールの作成と管理
- マシンの負荷管理
- マシンの電源管理

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

MCS でプロビジョニングされたシングルセッション OS マシンの割り当てを変更することができます。マルチセッション OS マシンや、Citrix Provisioning でプロビジョニングされたマシンの割り当てを変更することはできません。

1. 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］をクリックします。
3. ［デスクトップ］または ［デスクトップ割り当て規則］ページ（ページのタイトルは、デリバリーグループで使用されるマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループのユーザーあたりの最大マシン数の変更

1. 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］をクリックします。
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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループのマシンの更新

1. 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］をクリックします。
3. マシンを選択して、［操作］ペインの ［マシンの更新］をクリックします。

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、以下を指定します：

- マスターイメージを更新するタイミング：今すぐ、または次の起動時
- 再起動分散時間（グループ内のすべてのマシンの更新を開始する合計時間）
- ユーザーに再起動を通知するかどうか
- ユーザーが受け取るメッセージ

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」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. 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］をクリックします。
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. タグ制限を変更または削除するには、次のいずれかを行います：
   - 別のタグを選択する。
   - ［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限を削除する。
6. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループからのマシンの削除

マシンを削除すると、そのマシンがデリバリーグループから削除されます。この場合でも、マシンは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るため、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検討してください。

1. 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］をクリックします。
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. マシンを選択し、［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。

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。
- **SmartAccess** ポリシー式でユーザーのアクセスを制限する場合： Citrix Gateway 経由のユーザー接続を制限する SmartAccess ポリシー式を使用します。
  1. 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］をクリックします。
  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 Citrix 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、Citrix 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、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。
- 除外フィルターでユーザーのアクセスを制限する場合： 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、`VPDesktops_Direct`タグが追加されたマシンと、`VPDesktops_Test`タグ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場合、またはストアで Citrix Workspace アプリの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マルチセッション 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シングルセッション 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. 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］をクリックします。

   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］をクリックします。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］をクリックします。
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］をクリックします。

Windows リモートデスクトップ接続（RDC）の設定も、マルチセッション 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。

次のものについて、メンテナンスモードのオン/オフを切り替えることもできます:

- 接続。この接続を使用するマシンに影響が及びます。
- マシンカタログ。このカタログ内のマシンに影響が及びます。

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. 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］をクリックします。
3. マシンを選択し、［操作］ペインで以下のいずれかのエントリをクリックします（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。

セッション中はシングルセッション 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。

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と管理

再起動のスケジュールにより、デリバリーグループ内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 つのデリバリーグループに対して、1 つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響します:

- グループ内のすべてのマシン。
- グループ内の 1 つ以上のマシン（すべてではない）。マシンは、マシンに適用するタグで識別されます。これは、タグによって、タグがあるアイテム（この場合はマシン）のみにアクションが制限されるため、「タグ制限」と呼ばれます。

たとえば、すべてのマシンが 1 つのデリバリーグループに属しているとします。すべてのマシンを毎週 1 回再起動し、経理チームが使用するマシンを毎日再起動するとします。これを実現するには、すべてのマシンに対して 1 つのスケジュールを設定し、経理チームのマシンのみ別途スケジュールを設定します。

スケジュールには、再起動が開始される日時と期間が含まれます。期間は、「影響を受けるすべてのマシンを同時に起動する」か、影響を受けるすべてのマシンを再起動するのに必要な間隔のいずれかです。

スケジュールは有効または無効にできます。テストのときや、特別な間隔のとき、必要になる前にスケジュールを準備するときは、スケジュールを無効にすると役立ちます。

スケジュールは、管理コンソールからの自動パワーオンまたはシャットダウンには使用できません。再起動の場合にのみ使用できます。

スケジュールの重複

複数のスケジュールを重複させることができます。上記の例では、両方のスケジュールが経理チームのマシンに影響します。これらのマシンは、日曜日に 2 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、同じマシンを意図した回数より多く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。

- 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は高くなります。
- スケジュールの開始時間と期間が異なるほど、再起動が複数回発生する可能性が高くなります。
- スケジュールの影響を受けるマシンの数は、重複の可能性にも影響します。例では、すべてのマシンに影響がある週次スケジュールは、経理チームのマシンの日次スケジュールより大幅に高速の再起動を開始する可能性があります（それぞれに指定された処理期間により異なる）。

再起動スケジュールについて詳しくは、「Reboot schedule internals」を参照してください。

再起動スケジュールの表示

1. 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］をクリックします。
3. ［再起動スケジュール］ページを選択します。

［再起動スケジュール］ページには、構成された各スケジュールに関する次の情報が表示されます：

- スケジュール名。
- 使用されるタグ制限（ある場合）。
- マシンの再起動が発生する頻度。
- マシンのユーザーが通知を受信するかどうか。
- スケジュールが有効かどうか。テストのときや、特別な間隔のとき、必要になる前にスケジュールを準備するときは、スケジュールを無効にすると役立ちます。

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合、そのスケジュールの影響を受けるマシンにタグが追加（適用）されていることを確認してください。上記の例では、経理チームによって使用されるそれぞれのマシンにタグが適用されます。詳しくは、「タグ」を参照してください。

1 つのマシンに複数のタグを適用することもできますが、再起動スケジュールでは 1 つのタグしか指定できません。

1. 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. スケジュールによって制御されるマシンを含むグループを選択します。
3. ［マシンの表示］をクリックし、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］をクリックします。
5. タグが存在する場合は、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。

再起動スケジュールの作成

1. 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］をクリックします。
3. ［再起動スケジュール］ページで、［追加］をクリックします。
4. ［再起動スケジュールの追加］ページで次の操作を行います：
    - スケジュールの名前と説明を入力します。
    - タグ制限を使用している場合は、タグを選択します。
    - ［再起動の頻度］で、再起動の頻度を次の中から選択します：毎日、平日、週末、各週の特定の日。
    - 再起動を開始する時刻を、24 時間制で指定します。
    - ［再起動の間隔］で、すべてのマシンを同時に再起動するか、影響を受ける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。
    - ［ユーザーへ通知を送信］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選択した場合、（［通知の頻度］で）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。
    - 通知のタイトルと本文を入力します。デフォルトの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**%**>** を入れます。例：「警告：お使いのコンピューターは%m% 分後に自動的に再起動します。」この値は、繰り返されるメッセージごとに 5

分ずつ減少します。すべてのマシンを同時に再起動することを選択した場合を除き、メッセージは、再起動前の適切なタイミングで各マシンに表示されます。このタイミングは、内部アルゴリズムによって計算されます。

- スケジュールを有効にするには、チェックボックスをオンにします。スケジュールを無効にするには、チェックボックスをオフにします。

5. ［適用］をクリックすると、ウィンドウは開じずに、行った変更が適用されます。または、［**OK**］をクリックして、変更を適用してウィンドウを閉じます。

再起動スケジュールの編集、削除、有効化、無効化

1. 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］をクリックします。
3. ［再起動スケジュール］ページで、スケジュールのチェックボックスをオンにします。
   - スケジュールを編集するには、［編集］をクリックします。スケジュール設定を更新します。更新の方法については、「再起動スケジュールの作成」を参照してください。
   - スケジュールを有効または無効にするには、［編集］をクリックします。［再起動スケジュールを有効にする］チェックボックスを、オンまたはオフにします。
   - スケジュールを削除するには、［削除］をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用済みのタグには影響しません。

データベースの停止によるスケジュールされた再起動の遅延

> 注:
>
> この機能は、PowerShell のみで利用可能です。

デリバリーグループ内のマシン（VDA）に対してスケジュールされた再起動が開始される前にサイト構成データベースの停止が発生した場合、停止が終了すると再起動が開始されます。これは意図しない結果につながる可能性があります。

たとえば、デリバリーグループの再起動が生産停止時間（午前 3 時から）の間に行われるようにスケジュールしたとします。サイト構成データベースの停止が、スケジュールされた再起動が始まる 1 時間前（午前 2 時）に発生します。停止は 6 時間続きます（午前 8 時まで）。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は、元のスケジュールの 5 時間後に開始されます。これにより、生産時間中に VDA が再起動する可能性があります。

この状況を回避するには、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットの`MaxOvertimeStartMins`パラメーターを使用できます。この値により、スケジュールされた開始時間の最大何分後に再起動スケジュールを開始できるかを指定します。

その時間（スケジュールされた時間 + `MaxOvertimeStartMins`）内にデータベース接続が復元された場合、VDA の再起動が開始されます。

その時間内にデータベース接続が復元されない場合には、VDA の再起動は開始されません。

このパラメーターを省略すると、停止時間に関係なく、スケジュールされた再起動はデータベースへの接続の復元時に開始されます。

詳しくは、コマンドレットのヘルプを参照してください。この機能は、PowerShell のみで利用可能です。再起動スケジュールを Studio で構成する場合には、この値を設定できません。

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マルチセッション 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マルチセッション 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：マルチセッション 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。

  ［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。

  Director（監視）、Studio（管理）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。

  コンソールで ［サーバー負荷指数］列（デフォルトでは非表示）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。

- 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、XenApp バージョン 6.x 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のマシンの電源管理

電源を管理できるのは、仮想シングルセッション 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 機能が有効なシングルセッション 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。マルチセッション OS マシンでは、再起動のスケジュールを作成できます。

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、仮想シングルセッション 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、仮想シングルセッション 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ます。ユーザーがログオンすると、マシンがすぐに割り当てられます。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、プール内のマシンの数がしきい値を下回ると電源がオンになる、別の未割り当てマシンの「待機」セットを指します。このしきい値は、デリバリーグループのサイズの割合で指定します。大規模なデリバリーグループの場合、しきい値を上回ると、非常に多くの数のマシンがオンになることがあります。こうした場合には、デリバリーグループのサイズを慎重に計画するか、または SDK を使用してデフォルトのバッファーサイズを調整してください。

- 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されます（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。

仮想シングルセッション **OS** マシンの電源管理

1. 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] をクリックします。
3. [電源管理] ページの [マシンの電源管理] 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] 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、ウィンドウを閉じずに行った変更を適用します。または、[**OK**] をクリックして、変更を適用して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。

セッションが切断された状態で異なる期間に移行する **VDI** マシンの電源管理

> 重要:
>
> この拡張機能は、セッションが切断された VDI マシンにのみ適用されます。セッションがログオフされている VDI マシンには適用されません。

以前のリリースでは、アクション (切断アクション = 「一時停止」 または 「シャットダウン」) が必要な期間に移行する VDI マシンの電源がオンのままになっていました。このシナリオは、アクション (切断アクション = 「何もしない」) が不要な期間 (ピーク時またはオフピーク時) にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909 以降では、指定した切断時間が経過すると、マシンは一時停止または電源をオフにされます。これは、その期間に対して構成された切断アクションによって異なります。

たとえば、VDI デリバリーグループに対して次の電源ポリシーを構成するとします:

- `PeakDisconnectAction` を 「何もしない」 に設定
- `OffPeakDisconnectAction` を 「シャットダウン」 に設定
- `OffPeakDisconnectTimeout` を 「10」 に設定

> 注:
>
> 切断アクション電源ポリシーについて詳しくは、「https://developer-docs.citrix.com/projects/

> delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy」および「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/」を参照してください。

以前のリリースでは、ピーク時にセッションが切断された VDI マシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909 以降、`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーのアクションは、期間移行時に VDI マシンに適用されます。その結果、オフピークに移行してから 10 分後にマシンの電源がオフになります。

以前の動作に戻す（つまり、セッションが切断された状態でピークからオフピークまたはオフピークからピークに移行するマシンでは何も実行しない）場合は、次のいずれかの操作を行います：

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を 1 に設定します（true、以前の動作を有効にします）。デフォルトでは、値は 0 です（false、期間の移行時に電源ポリシーの切断アクションがトリガーされます）。
  - パス：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 値の名前：LegacyPeakTransitionDisconnectedBehaviour
  - 種類：REG_DWORD
  - 値のデータ：0x00000001（1）
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用するには、マシンが次の条件を満たす必要があります：

- 切断されたセッションがある。
- 保留中の電源操作がない。
- 異なる期間に移行する VDI（シングルセッション）デリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）に切断し、電源操作が割り当てられている期間に移行するセッションがある。

カタログで電源オン状態にする **VDA** の割合の変更

1. ［デリバリーグループ］の ［電源管理］セクションで、デリバリーグループのピーク時間を調整します。
2. デスクトップグループの名前を書き留めます。
3. 管理者権限で PowerShell を起動し、次のコマンドを実行します。「Desktop Group Name」は、実行する VDA の割合を変更したデスクトップグループの名前に置き換えてください。

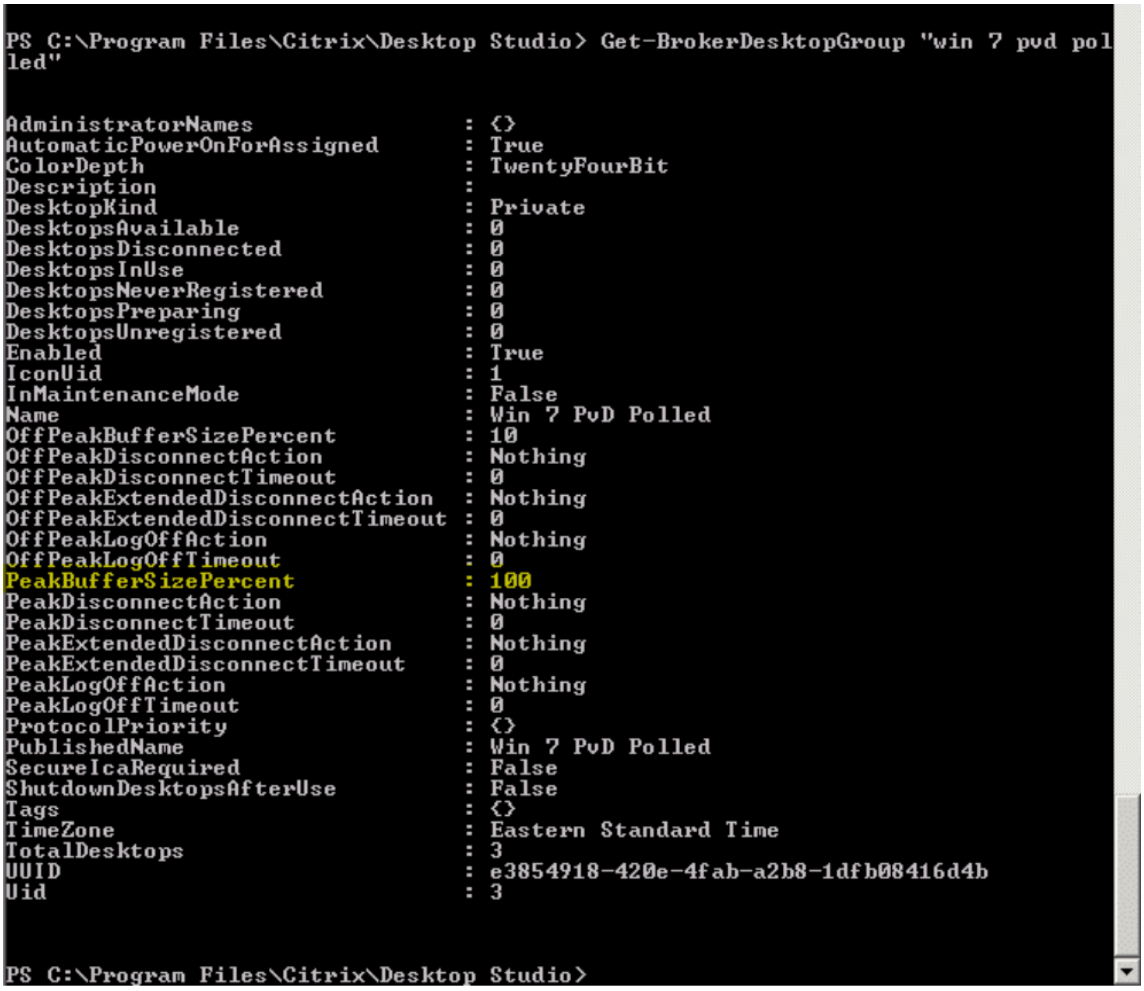
   ```
   asnp Citrix*

   ## Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
   100
   ```

   この数値の 100 により、100% の VDA が準備完了状態になるように設定されます。

4. 次のコマンドを実行して、ソリューションを確認します:

```
##Get-BrokerDesktopGroup "Desktop Group Name"
```



変更が反映されるまでには最大 1 時間かかることがあります。

ユーザーがログオフした後に VDA をシャットダウンするには、次のように入力します:

```
## Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
$True
```

ログオフ後も準備完了状態になるようにピーク時に VDA を再起動するには、次のように入力します:

```
## Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDuringPeak
 $True
```

セッション

- セッションのログオフ/切断、またはユーザーへのメッセージ送信
- セッションの事前起動およびセッション残留の構成

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。

シングルセッション 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」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、マルチセッション 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、マシンでマルチセッション OS 対応 VDA バージョン 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 Windows 向け Citrix Workspace アプリを使用している場合にのみサポートされ、Citrix Workspace アプリ側での構成も必要になります。詳しくは、使用中のバージョンの Windows 向け Citrix Workspace アプリに関する製品ドキュメントで、「セッションの事前起動」を検索してください。
- HTML5 向け Citrix Workspace アプリはサポートされません。
- 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状態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）事前起動は機能しません。ユーザーはマシン/セッションをロックできます。ただし、ユーザーが Citrix Workspace アプリ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なくなります。
- 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同時使用ライセンスを消費します。ユーザーライセンスまたはデバイスライセンスを使用する場合、ライセンスは 90 日間有効です。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 Workspace アプリ側で、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。これらのすべてを設定することができます。最初に発生したイベントによって未使用の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事前起動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。

  このタイムアウトの設定は､管理コンソールではなく SDK からのみ(`New`/`Set-BrokerSessionPreLaunch`コマンドレット）有効にできます。タイムアウトを無効にすると、コンソールや ［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。

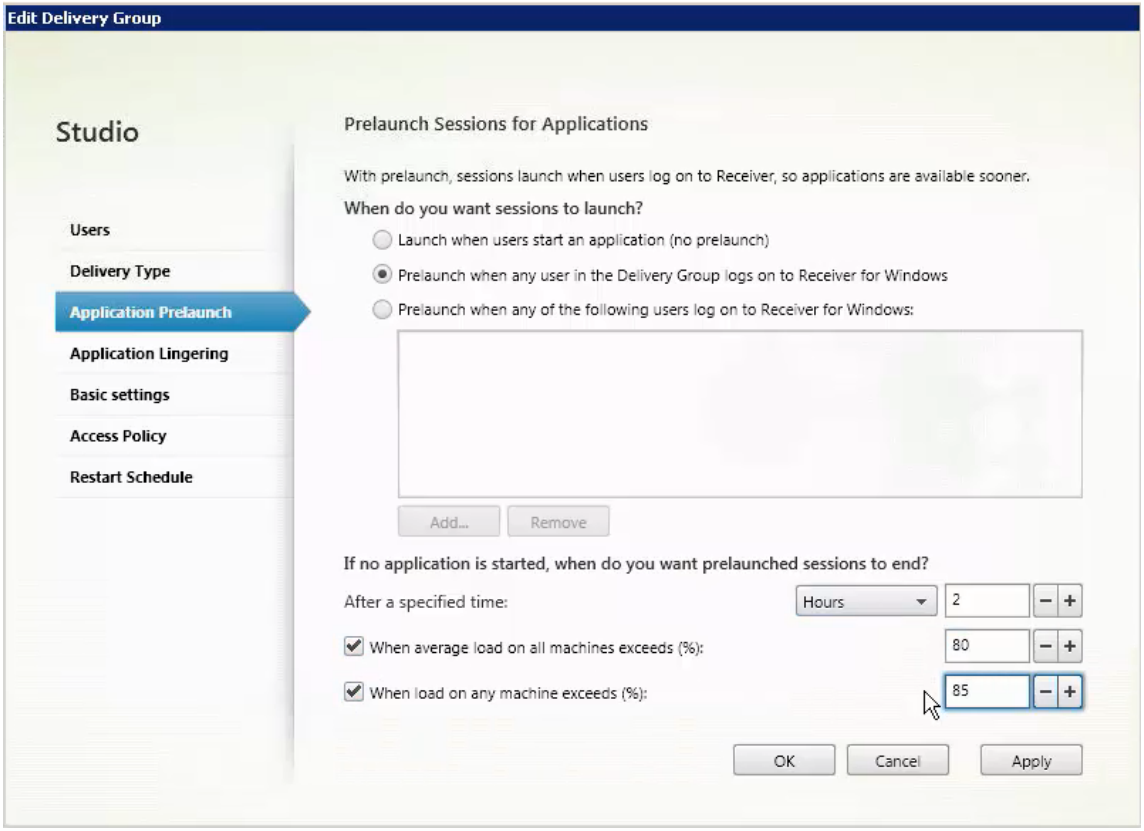
- しきい値：サーバーの負荷が高くなったときに事前起動セッションや残留セッションを自動的に終了することができます。これにより、サーバーの負荷が低い間は可能な限りセッションが保持されます。新しいユーザーセッション用のリソースが必要になったときに事前起動セッションや残留セッションが自動的に終了するため、これらのセッションが原因で接続が拒否されることはありません。

次の 2 つのしきい値を構成できます：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、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。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. 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］をクリックします。
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す。セッションの事前起動機能は無効になっています。
   - デリバリーグループ内のすべてのユーザーで、Windows 向け Citrix Workspace アプリへのログオン時に事前起動する。
   - 一覧に含まれるユーザーおよびユーザーグループでのみ、Windows 向け Citrix Workspace アプリへの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。



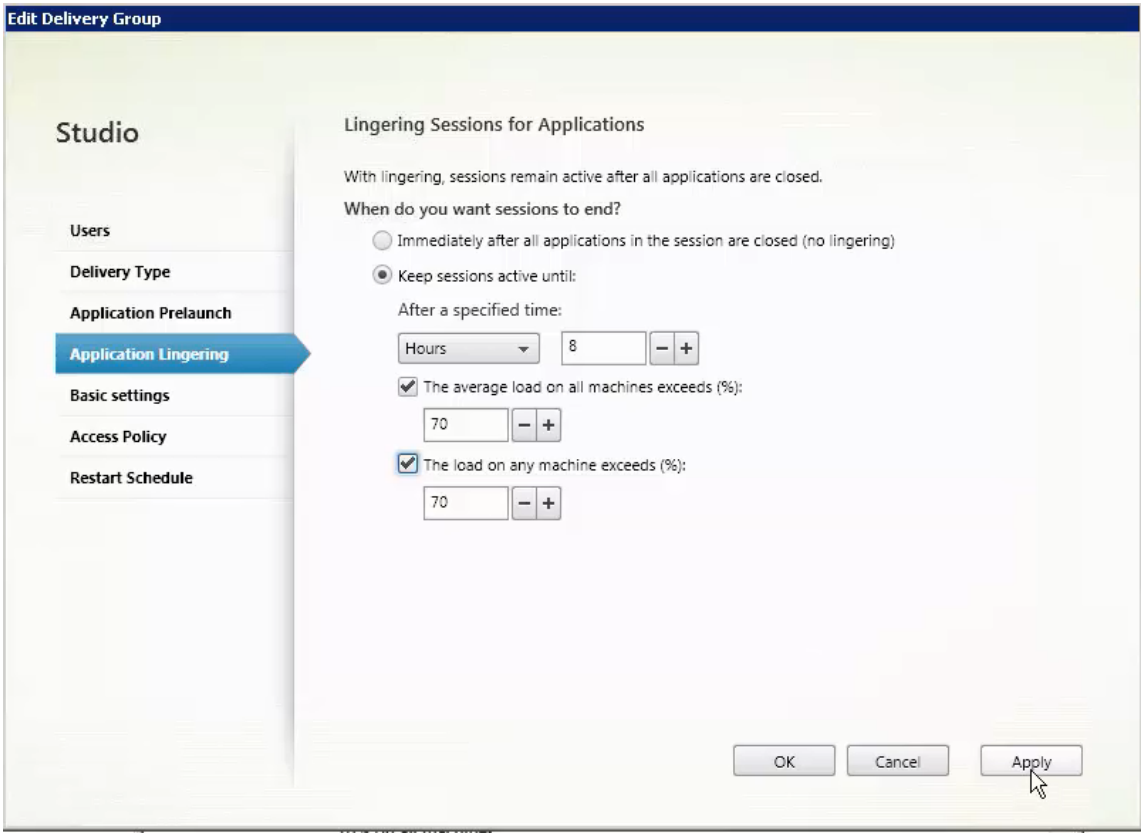
4. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。

    - 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指定します（1～99 日間、1～2,376 時間、または 1～142,560 分）。
    - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値（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指定上限値（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. 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］をクリックします。
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指定します（1～99 日間、1～2,376 時間、または 1～142,560 分）。
    - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値（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指定上限値（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

- 仲介セッションを起動する場合、Delivery Controller に登録されていない VDA は考慮されません。これにより、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。詳細画面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、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。たとえば、1 台または複数台のマシンの電源が入っておりメンテナンスモードではないのに、Controller に現在登録されていない場合があります。「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**」の場合は、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

April 26, 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。

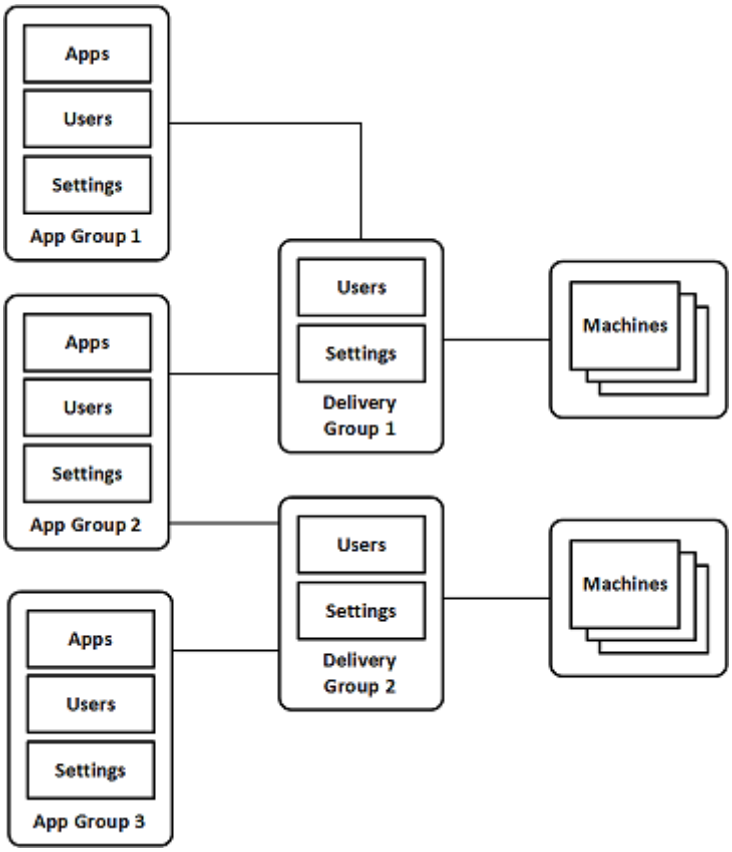
アプリケーショングループの使用は、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします。

- 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照にして、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**:

次の図に、アプリケーショングループが含まれる Citrix Virtual Apps and Desktops 環境を示します:



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。)

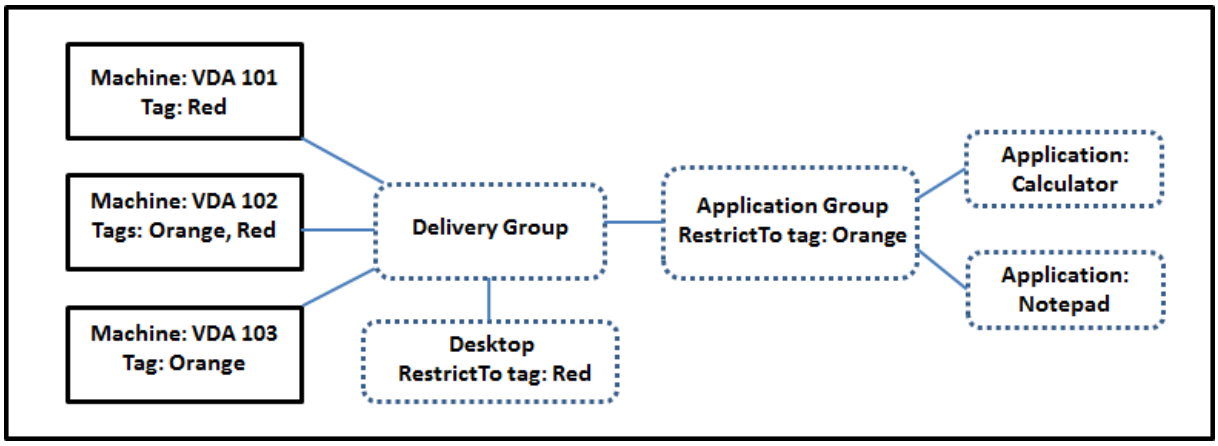
アプリケーショングループ 1 はデリバリーグループ 1 に関連付けられています。アプリケーショングループ 1 のアプリケーションには、アプリケーショングループ 1 で指定されているユーザーが、デリバリーグループ 1 のユーザー一覧にも含まれている限り、アクセスできます。これは、アプリケーショングループのユーザー一覧は関連付けられているデリバリーグループのユーザー一覧のサブセット(制限)でなければならないというガイダンスに従っています。アプリケーショングループ 1 の設定(アプリケーショングループ間で共有されるアプリケーションセッション、関連付けられているデリバリーグループなど)は、このグループ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。これには、次のことが必要です:

1. デリバリーグループで使用されているマシン上の VDA のアップグレード
2. そ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。

詳しくは、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントがバージョン 7.9 以上である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みの役割の配信管理者権限が必要です。詳しくは、委任管理を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」と表現することで、このアクションと、利用可能なソースからアプリケーションの新しいインスタンスを追加することを区別しています。同様に、デリバリーグループはアプリケーショングループに関連付けられ、アプリケーショングループはデリバリーグループに関連付けられます。追加されるのでも、お互いのコンポーネントになるのでもありません。

アプリケーショングループを使用したセッション共有

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を作成する場合、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。グループを作成す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、アプリケーショングループ作成時には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。グループを作成す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。

手順 **1.** デリバリーグループ

［デリバリーグループ］ページには、すべてのデリバリーグループが、各グループに含まれるマシンの数とともに表示されます。

- ［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）マルチセッションやシングルセッション 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。

次の両方の条件が満たされている場合は、デスクトップのみを配信する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をバージョン 7.9 より前の XenDesktop で作成し、共有マシンを含めています。
- デリバリーグループの編集権限があります。

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。

手順 **2.** 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。

展開内のユーザー一覧が指定されている場所については、「ユーザー一覧の指定場所」を参照してください。

手順 **3.** 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。それ以外の場合は、追加する前に名前を変更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。同じ名前の 2 つのアプリケーションを同じユーザーに公開する場合は、Studio の ［アプリケーション名（ユーザー用)］プロパティを変更します。これを行わないと、Citrix Workspace アプリには同じ名前が 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、次のいずれかを選択した場合は選択できません:

  - 関連するデリバリーグループのないアプリケーショングループ。
  - マシンを含まないデリバリーグループが関連付けられたアプリケーショングループ。
  - 機械を含まない配送グループ。

- 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。互換性のないソースは、一切表示されません。たとえば、アプリケーショングループにアプリケーショングループは追加できないため、このソースはアプリケーショングループ作成時には表示されません。

手順 **4.** スコープ

このページは、カスタム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、「委任管理」を参照してください。

手順 **5.** 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

April 26, 2021

> 注：
> Citrix Virtual Apps and Desktops サービスでアプリケーショングループを使用する場合、「タグによる制限」機能は現在使用できません。

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方法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、作成すると有効になります。グループを作成するときにこれを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を作成する場合、アプリケーショングループ間でのセッションの共有が有効になっています。グループを作成するときにこれを変更することはできません。詳しくは、「アプリケーショングループを使用したセッション共有」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。

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。

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、-SingleAppPerSession パラメーターを True に設定して実行します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効のアプリケーショングループを作成するには、以下を実行します:

  ```
  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
  ```


注意事項

- SingleAppPerSessionプロパティを有効にするには、SessionSharingEnabledプロパティを False に設定する必要があります。この 2 つのプロパティは、同時に有効化してはなりません。SessionSharingEnabledパラメーターは、アプリケーショングループ間のセッション共有に関するものです。
- アプリケーションセッション共有は、アプリケーショングループに割り当てられているが、デリバリーグループには割り当てられていないアプリケーションに対してのみ有効です。(デリバリーグループに直接割り当てられているアプリケーションはすべてデフォルトでセッションを共有します)。
- 1 つのアプリケーションが複数のアプリケーショングループに割り当てられている場合、グループどうしで設定が矛盾しないようにしてください。たとえば、同じオプションを一方のグループでは True に、他方のグループでは False に設定していると、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。

次の両方の条件が満たされている場合は、デスクトップのみを配信する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には共有マシンが含まれます。7.9 より前のバージョンで作成されました。
- デリバリーグループの編集権限があります。

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

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」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、元のソースからは削除されません。ただし、再度使用可能にする場合は、再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、［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

April 26, 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 バージョンの詳細については、シングルセッション OS用の VDA および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布（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。例:

  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

モニターのブランキングが機能しない

アクティブな HDX セッションがあるときに Windows PC のローカルモニターが空白になっていない場合（ローカルモニターはセッションで発生していることを表示します）、GPU ベンダーのドライバーに問題があることが原因である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display ドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先度を与えます：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前：CitrixIDD
- 種類：DWORD
- データ：3

ディスプレイアダプターの優先度とモニターの作成について詳しくは、Knowledge Center の記事「CTX237608」を参照してください。

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

April 26, 2021

App-V を Citrix Virtual Apps and Desktops で使用する

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	Citrix Virtual Apps and Desktops の Delivery Controller	Citrix Virtual Apps and Desktops の 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 Client は、アプリケーションへのオフラインアクセスをサポートしません。App-V の統合機能により、アプリケーションでの SMB 共有の使用がサポートされます。HTTP プロトコルはサポートされません。
App-V について詳しくは、Microsoft 社のドキュメントを参照してください。以下に、本書で説明する App-V コンポーネントの概要を示します。

- 管理サーバー App-V インフラストラクチャを管理したり、App-V デスクトップクライアントやリモートデスクトップサービスクライアントに仮想アプリケーションを配信したりするための中央管理コンソールです。

App-V 管理サーバーは、セキュリティ、測定、監視、および管理者によって要求されるデータ収集を認証、要求、および提供します。このサーバーは、Active Directory といくつかのツールを使用してユーザーとアプリケーションを管理します。

- 公開サーバー。App-V Client に特定ユーザー用のアプリケーションを提供し、ストリーム配信用の仮想アプリケーションパッケージをホストします。これらのパッケージは、管理サーバーから取得されます。
- クライアント。公開サーバーから仮想アプリケーションを取得したり、クライアント上のアプリケーションを公開したり、Windows デバイス上で仮想環境のランタイムを自動的にセットアップおよび管理したりします。App-V Client は VDA にインストールされ、VDA には、各ユーザープロファイルのレジストリやファイルの変更など、ユーザー固有の仮想アプリケーション設定が格納されます。

アプリケーションは、事前構成やオペレーティングシステム設定の変更を行わなくても、シームレスに使用可能になります。以下の方法で、サーバー OS およびデスクトップ OS のデリバリーグループから App-V アプリケーションを起動できます。

- Citrix Workspace アプリを使用して起動する
- App-V Client および Citrix Workspace アプリ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。動的構成ファイルに保存されたアプリケーションのカスタマイズは、アプリケーションの起動時にも適用されます。

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：アプリケーションでの検出、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。このプロセスでは、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。

  デュアル管理方式は、Studio と App-V サーバーコンソールの両方を必要とします。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。この方法では、管理サーバーが動的構成ファイルを処理します。デュアル管理方式を使用する場合、アプリケーションの起動に必要な適切な公開サーバーの登録は、Citrix App-V コンポーネントが管理します。この方式によって、公開サーバーは適切なタイミングでユーザーに対して同期されます。公開サーバーは、ログオングループや接続グループの更新など、パッケージのライフサイクルにおけるさまざまな面を維持します。

- 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と XML 展開構成ファイルを使用すると、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）。

シングル管理方式では、Studio コンソールが必要です。ネットワーク共有を検索し、1 つまたは複数の App-V パッケージを、ネットワーク共有からサイトレベルのアプリケーションライブラリ [1] に追加します。この方法では、Citrix App-V コンポーネントは、アプリケーションの起動時に展開構成ファイルを処理します（ユーザー構成ファイルはサポートされていません）。シングル管理方式を使用する場合、Citrix App-V コンポーネントはホストマシン上でパッケージのライフサイクルのあらゆる面を管理します。パッケージはブローカーの起動時、または構成の変更が検出された場合に、マシンに追加されます。パッケージは、Citrix Workspace アプリから起動要求を受信した時点で、必要に応じて個々のユーザーに最初に公開されます。

シングル管理方式では、Studio で作成された分離グループの構成の定義に従って、必要な接続グループのライフサイクルを管理します。

[1] 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。

どちらの管理方式でも、VDA がユーザーデータを破棄するように構成されている場合、次回のセッション起動時に公開（または同期）をやり直す必要があります。

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。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 サーバーまたはネットワーク共有上の App-V パッケージからアプリケーションを追加できます。

> 注:
>
> 両方の管理方式を使用しており、App-V パッケージで両方の場所に動的構成ファイルがある場合は、App-V サーバー（デュアル管理）のファイルが使用されます。

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とショートカットが一覧表示されます。

動的構成ファイル

概要

App-V パッケージは、動的構成ファイルを使用してカスタマイズできます。動的構成ファイルをパッケージに適用すると、パッケージの特性を変更するために使用できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。Citrix App-V は、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます:

- 展開構成ファイルにより、すべてのユーザーがマシン全体を構成できます。これらのファイルの名前は *<packageFileName>*_DeploymentConfig.xml となり、適用先の App-V パッケージと同じフォルダーにあります。シングルおよびデュアル管理方式によってサポートされています。
- ユーザー構成ファイルには、パッケージに対するユーザー単位のカスタマイズをサポートするユーザー固有の構成が用意されています。シングル管理では、次の形式の名前のユーザー構成ファイルを

サポートしています：\<*packageFileName*>_[UserSID \| user name \| GroupSID \| GroupName_]UserConfig.xml。これは適用先の App-V パッケージと同じフォルダーにあります。

特定のパッケージに対して複数のユーザー構成ファイルが存在する場合は、以下の優先順位で適用されます：

1. ユーザー SID
2. ユーザー名
3. AD グループ SID（最初に見つかったものが優先）
4. AD グループ名（最初に見つかったものが優先）
5. デフォルト

例

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.
    xml
MyAppVPackage_joeblogs_UserConfig.xml
MyAppVPackage_S-1-5-32-547_UserConfig.xml
MyAppVPackage_Power Users_UserConfig.xml
MyAppVPackage_UserConfig.xml
```

> 注：
>
> ファイル名のユーザー固有の部分は、オプションで末尾に指定することもできます（例：MyAppVPackage_UserConfig_**joeblogs**.xml）。

動的構成ファイルの場所

シングル管理方式では、Citrix App-V コンポーネントは App-V パッケージと同じフォルダーにある動的構成ファイルのみを処理します。パッケージ内のアプリケーションを起動すると、対応する動的構成ファイルへの変更がすべて再適用されます。動的構成ファイルがパッケージの別の場所にある場合は、マッピングファイルを使用してパッケージをデプロイメント構成ファイルにマップします。

マッピングファイルを作成するには

1. 新しいテキストファイルを開きます。
2. それぞれの動的構成ファイルに対して、「\<PackageGuid>:パス」という形式を使用して、パッケージへのパスを指定する行を追加します。

   例：

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml

3. パッケージと同じフォルダーに ctxAppVDynamicConfigurations.cfg という名前でファイルを保存します。パッケージ内のアプリケーションが起動されるたびに、このファイルに対して同じ UNC 共有が再帰的に検索されます。

> 注
>
> パッケージ内のアプリケーションが開いているユーザーセッションがある場合、動的展開構成は変更できません。現在のユーザーではなく他のユーザーがパッケージからアプリケーションを開いている場合は、動的ユーザー構成ファイルを変更できます。

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。

- App-V 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。

この構成により、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。このグループには、一連のプラグインおよびその他のアプリケーションが含まれています。これらの要素を使用して特定のユーザーのセットに制限すれば、それ以上分離グループを作成する必要はありません。

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。

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 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、シトリックスのブログの記事を参照してください。

セットアップ

次の表は、シングル管理およびデュアル管理方式を使用した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
	○	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/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利用できるパッケージと、それらに対応する動的構成ファイルを作成します。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。

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 管理サーバーおよび公開サーバーのアドレスを使用します。このタスクは、サイトの作成中または作成後に実行します。

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 Client には、各ユーザープロファイルのレジストリやファイルの変更など、ユーザー固有の仮想アプリケーション設定が格納されます。

App-V Client は、Microsoft 社から提供されます。App-V Client を、VDA がインストールされた各マシン、または仮想マシンを作成するためにマシンカタログで使用されるマスターイメージにインストールします。注：Windows 10（1607 以降）および Windows Server 2016 には、App-V Client が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 Client 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除外されます。

VDA のインストール時にこのデフォルトの挙動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ンにします。コマンドラインインターフェイスの場合は、「**/includeadditional “Citrix Personalization for App-V – VDA”**」オプションを使用します。

VDA のインストール中に Citrix App-V コンポーネントを追加せず、後で App-V アプリケーションを使用する必要が生じた場合は次の手順に従います：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］ドロップダウンリストで ［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**：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］ドロップダウンリスト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、またはアプリケーションショートカット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。

- 動的構成ファイルを使用して App-V アプリケーションのプロパティをカスタマイズすると、それらのプロパティは、それらをデリバリーグループに追加するときに行った変更を上書きします。
- App-V アプリケーションを含むデリバリーグループを後で編集しても、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。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」に変更した場合。
- 以前に公開された 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。
- 100 を超える App-V アプリケーションを単一のデリバリーグループで公開すると、アプリケーションは起動しません。適切なバインド要素で`MaxReceivedMessageSize`プロパティを使用します。このプロパティは、Delivery Controller または VDA 上の Broker Agent の構成で最大受信可能メッセージサイズを増やします。

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)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>を入力します。
- 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、http://support.microsoft.com/kb/306541を参照してください。

- App-V サーバーは Active Directory に属していますか。

  Studio のマシンと App-V サーバーが信頼関係のない異なる Active Directory ドメインに属している場合は、Studio マシン上の 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、次のメッセージが表示されます:「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)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 アプリケーションを、1 つの Web ブラウザーバージョンでしか起動できません。

- 同じ Web ブラウザーアプリを順番に複数のバージョンで公開した場合でも、VDA 上のユーザーごとに一度に 1 つのバージョンのアプリしか起動できません。同様の現象は、Citrix コンポーネントが含まれていない場合に、異なるパスのデスクトップショートカットで順番に公開されたアプリを起動しても発生します。

  ユーザーが最初に起動する Web ブラウザーのバージョンによって、後で実行される Web ブラウザーのバージョンが決まります。Firefox は、2 回目の起動を検出すると、プロセスを作成するのではなく、すでに実行中のプロセスのインスタンスを作成するよう設定されています。ほかの Web ブラウザーも同様に動作します。

  ショートカットの起動コマンドに **-no-remote** コマンドラインパラメーターを追加することで、指定した Firefox のバージョンでアプリケーションを起動できます。ほかの Web ブラウザーにも、同様の機能が備わっています。

  > 注:
  >
  > ショートカット列挙機能を利用するには、XenApp 7.17 以降を使用する必要があります。また、この双方向動作を有効にするには、両方のアプリバージョンのパッケージを変更する必要もあります。

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 Client がインストールされていますか。VDA で、「パッケージスクリプトの有効化」設定が有効ですか。
- App-V Client と VDA がインストールされているマシンで、レジストリエディター（regedit）から HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV を開きます。AppVServers キーが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 Client と VDA がインストールされたマシンまたはマスターイメージで、PowerShell ExecutionPolicy が RemoteSigned に設定されていることを確認します。Microsoft 社から提供される App-V Client は署名されてないため、この ExecutionPolicy で、PowerShell で無署名のローカルのスクリプトとコマンドレットを実行できるようにします。次の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。
- 「RegistrationManager.AttemptRegistrationWithSingleDdc: 登録できませんでした」というエラーが表示された場合は、適切なバインド要素で MaxReceivedMessageSize プロパティを使用して、Delivery Controller または VDA 上の Broker Agent の構成で最大受信可能メッセージサイズを増やします。

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。メモ帳などのテキストエディタを使用します。

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 Delivery 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

May 3, 2021

> 重要:
>
> AppDisk の機能（およびそれをサポートする Studio への AppDNA の統合）は Citrix Virtual Apps and Desktops 2003 で削除されました。代わりに、Citrix App Layeringを使用してください。

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、Citrix Virtual Apps and Desktops で 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、Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops は AppLibrary と連携し、Machine Creation Services（MCS）または Citrix Provisioning（旧称 Provisioning Services）、および Delivery Controller と通信して、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、XenApp および XenDesktop 7.8 以降のバージョンの 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 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の最も古いバージョンが、グループの機能レベルとなります。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：

- Delivery Controller 付属の MCS
- ダウンロードページでお使いの Citrix Virtual Apps and Desktops のバージョンとともに提供されるバージョンの Citrix Provisioning
- 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、Citrix Virtual Apps and Desktops で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併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。

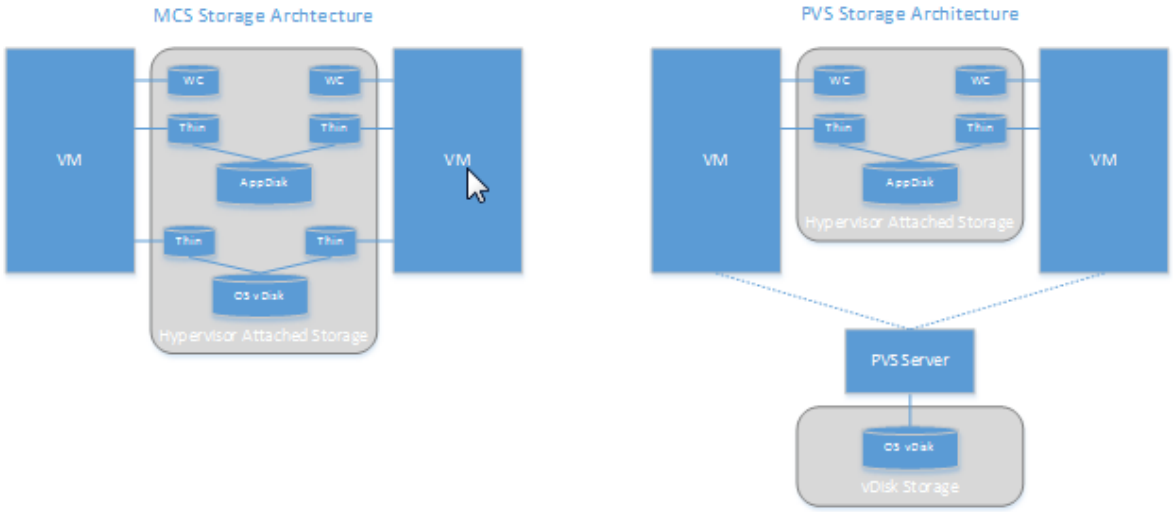
AppDNA を使用するには、以下の手順に従います:

- 「AppDNA」およびAppDisk についてよくある質問を確認してください。
- 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 Citrix Virtual Apps and Desktops のリリースで提供されるバージョンの AppDNA を使用してください。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。
- Citrix Virtual Apps and Desktops 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。次の図に、MCS および Citrix Provisioning のストレージアーキテクチャを示します。「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。

Citrix Provisioning 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。
- Citrix Provisioning では、OS vDisk と AppDisk が使用するストレージ領域は異なります。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、こうした変更に対応できるよう、Citrix Provisioning 環境のサイズを設定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: Citrix Provisioning 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、この 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 Citrix Provisioning 環境のいずれにおいても、作成した AppDisk を活用できるよう、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。Citrix Provisioning では、アプリケーションは OS vDisk には配置されないため、Citrix Provisioning 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、Citrix Provisioning 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 の作成に関する考慮事項

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。
- 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。

Citrix Provisioning 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：Citrix Provisioning を使用する場合は、「Citrix Provisioning に関する注意事項」のガイドラインに従ってください。

ウィザードが閉じると、新しい AppDisk に対する Studio の表示は「作成中」となります。AppDisk が作成されると、表示は「アプリケーションのインストールの準備完了」に変わります。

AppDisk へのアプリケーションのインストール：

ハイパーバイザー管理コンソールから、アプリケーションを AppDisk にインストールします（ヒント：仮想マシン名を忘れた場合、Studio のナビゲーションペインで［**AppDisk**］を選択し、次に［操作］ペインで［アプリケーションのインストール］を選択すると仮想マシン名が表示されます）。アプリケーションのインストールについて詳しくは、ハイパーバイザーのドキュメントを参照してください。（そのほかの注意事項：ハイパーバイザー管理コンソールからアプリケーションを AppDisk にインストールする必要があります。Studio の［操作］ペインの［アプリケーションのインストール］タスクは使用しないでください）。

アプリケーションの封印：

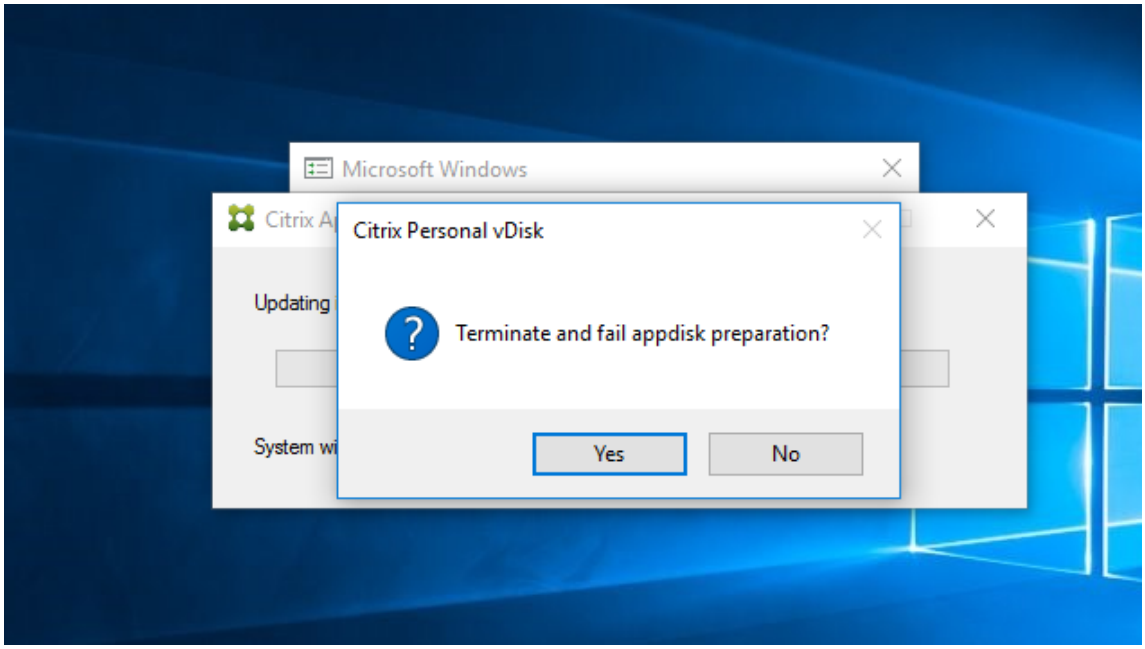
1. Studio のナビゲーションペインで［**AppDisks**］を選択します。
2. 作成した AppDisk を選択し、［操作］ペインで［**AppDisk** の封印］を選択します。

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。

［**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。

重要な **Windows Update** の考慮事項:

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。

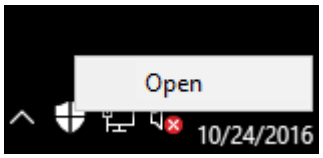
このセクションでは、次のウイルス対策アプリケーションでの例外の追加について説明します。

- 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）

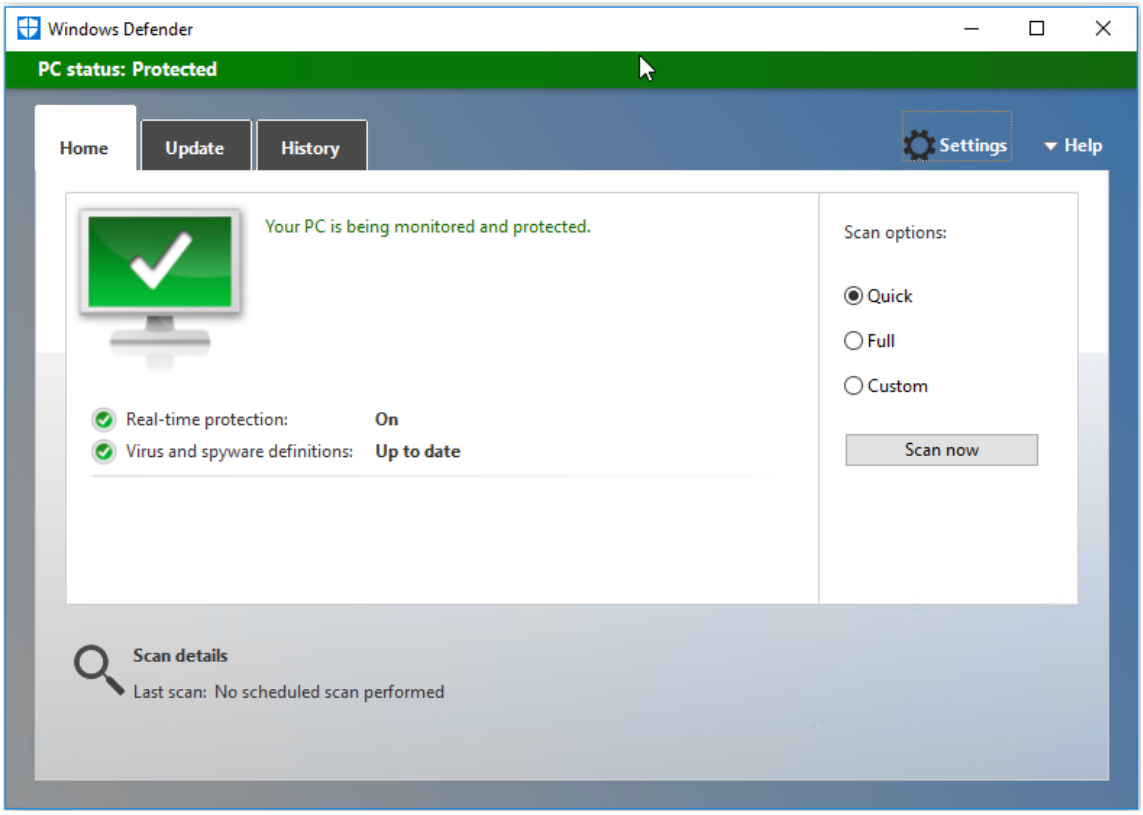
Windows Defender

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：

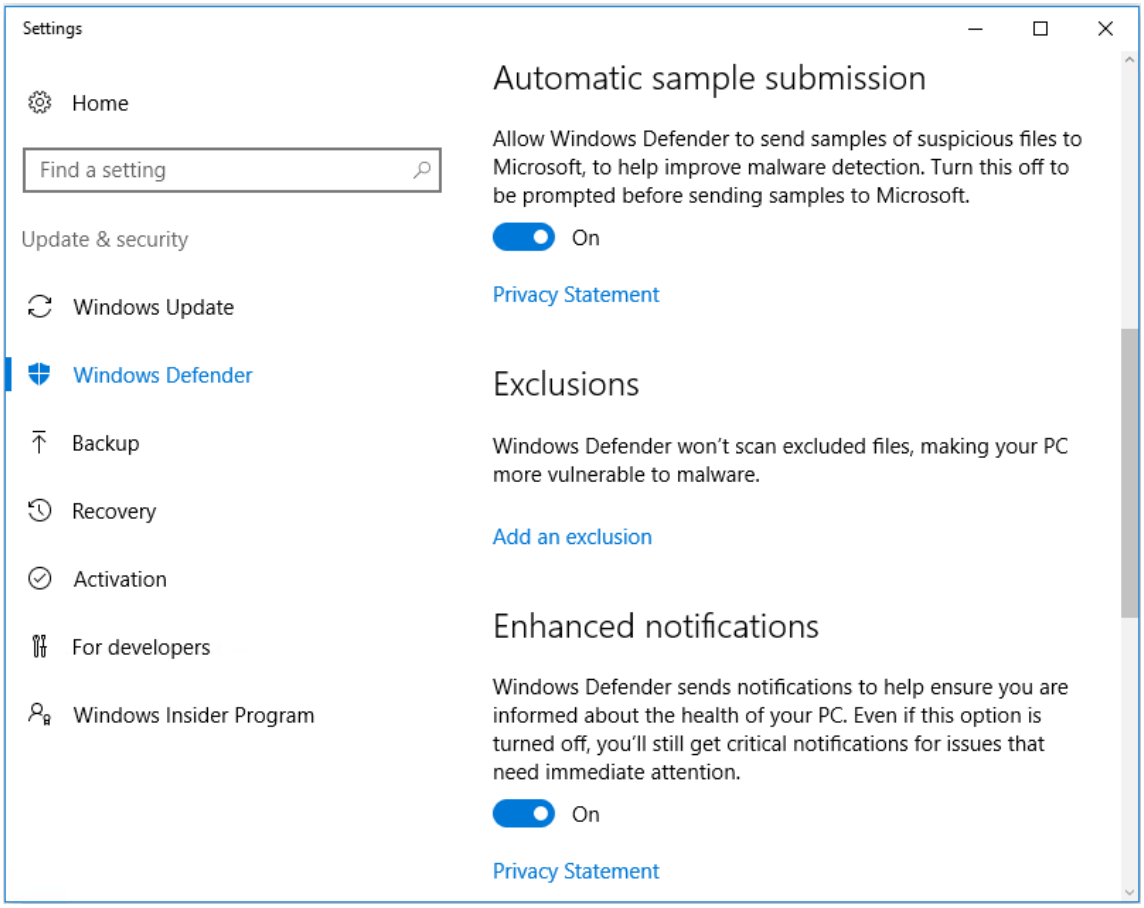
1. ローカル管理者権限でコンピューターにログオンします。
2. Windows Defender のアイコンを選択して右クリックし、［開く］ボタンを表示します：



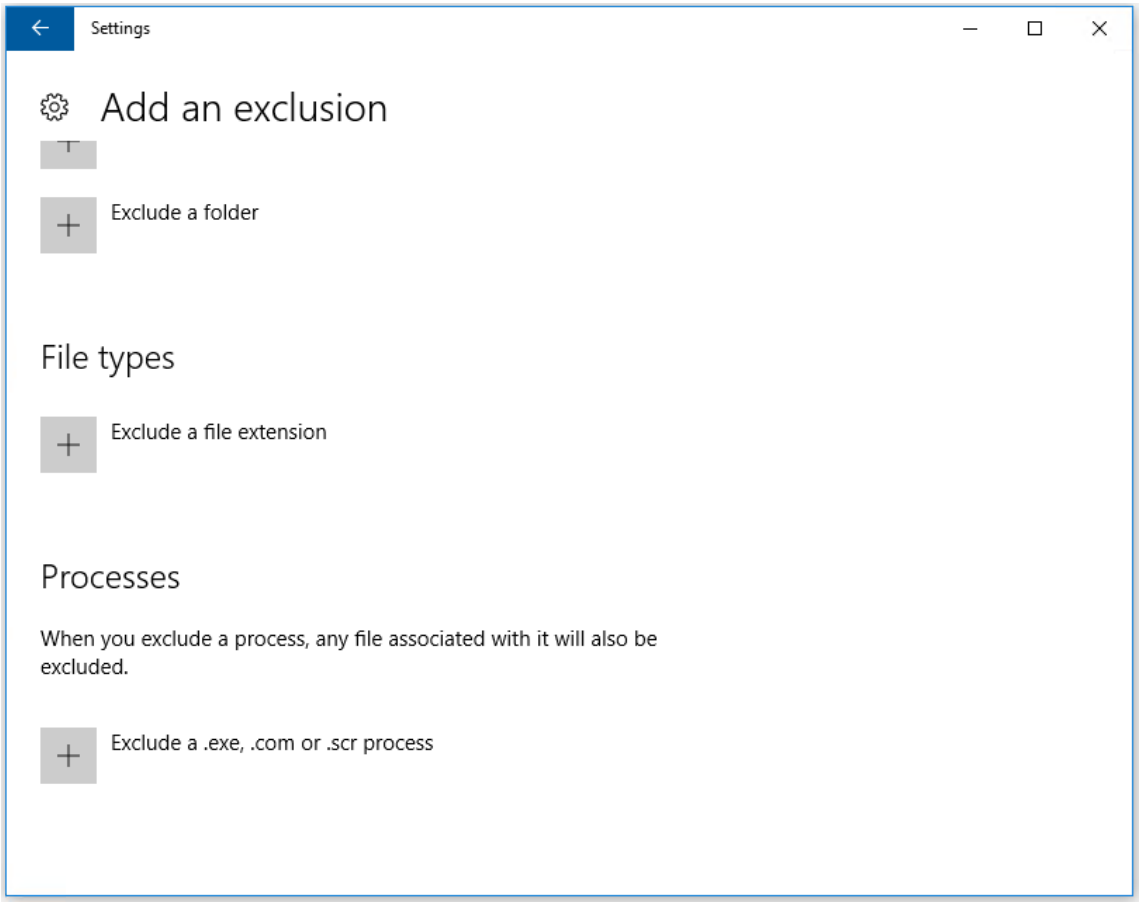
3. Windows Defender コンソールで、インターフェイスの右上部分の ［設定］を選択します：



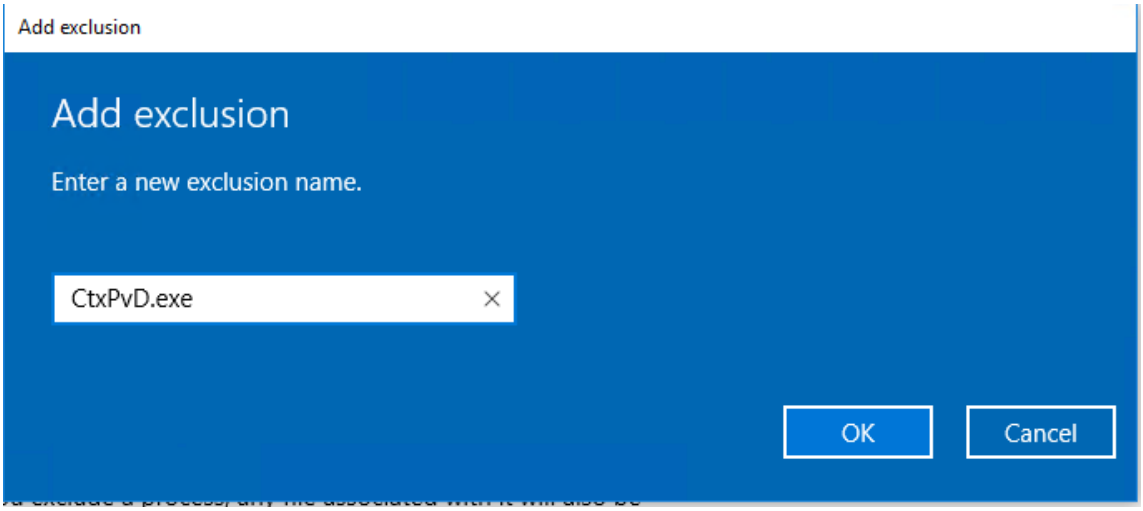
4. ［設定］画面の ［除外］部分で、［除外の追加］をクリックします：



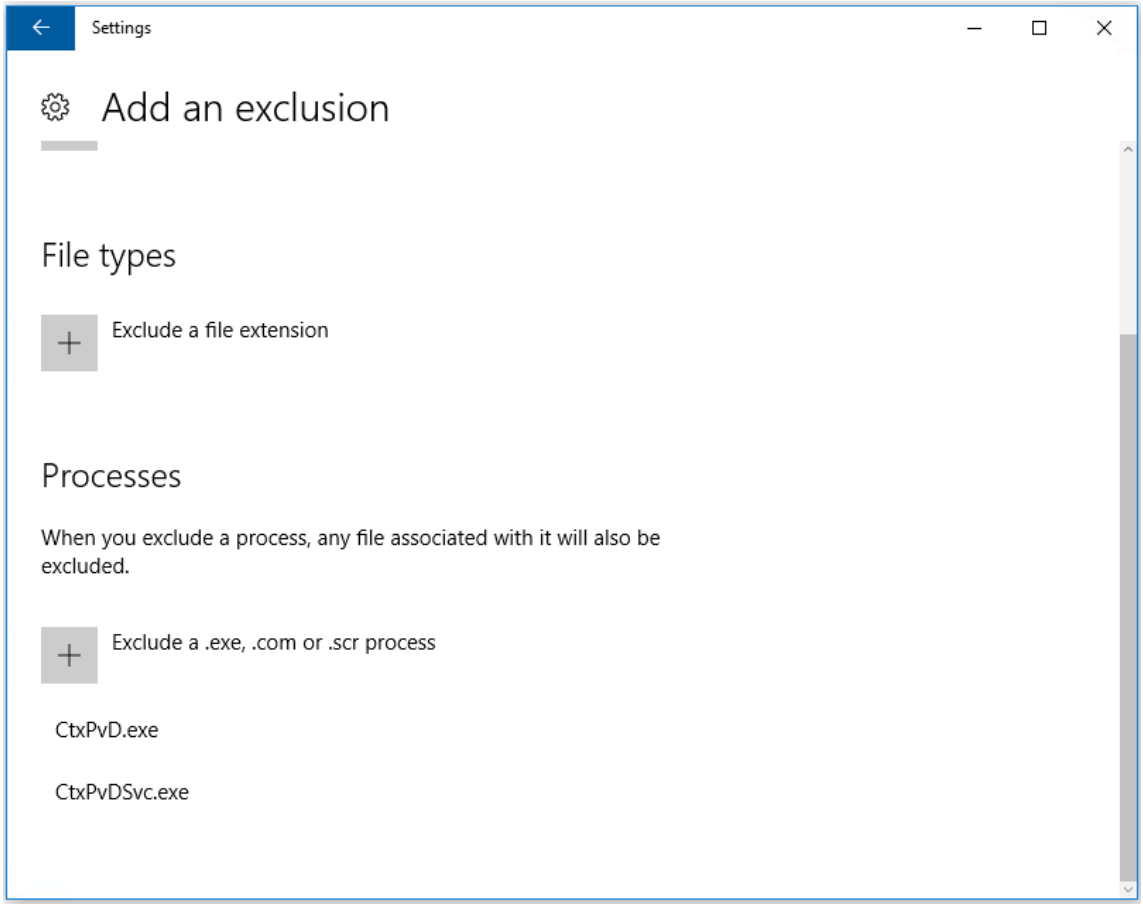
5. ［除外の追加］画面で、［**.exe**、**.com**、または**.scr** プロセスを除外します］をクリックします:



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:



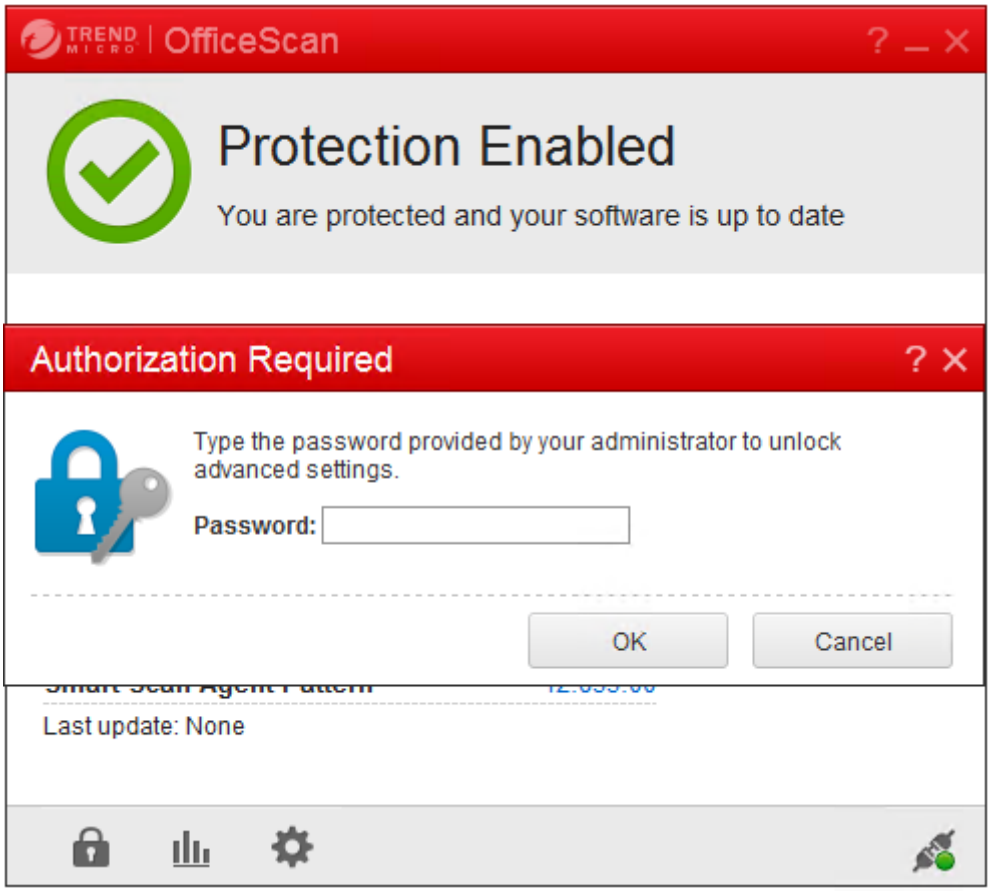
除外項目を追加すると、［設定］画面にある除外されたプロセスのリストに表示されます:



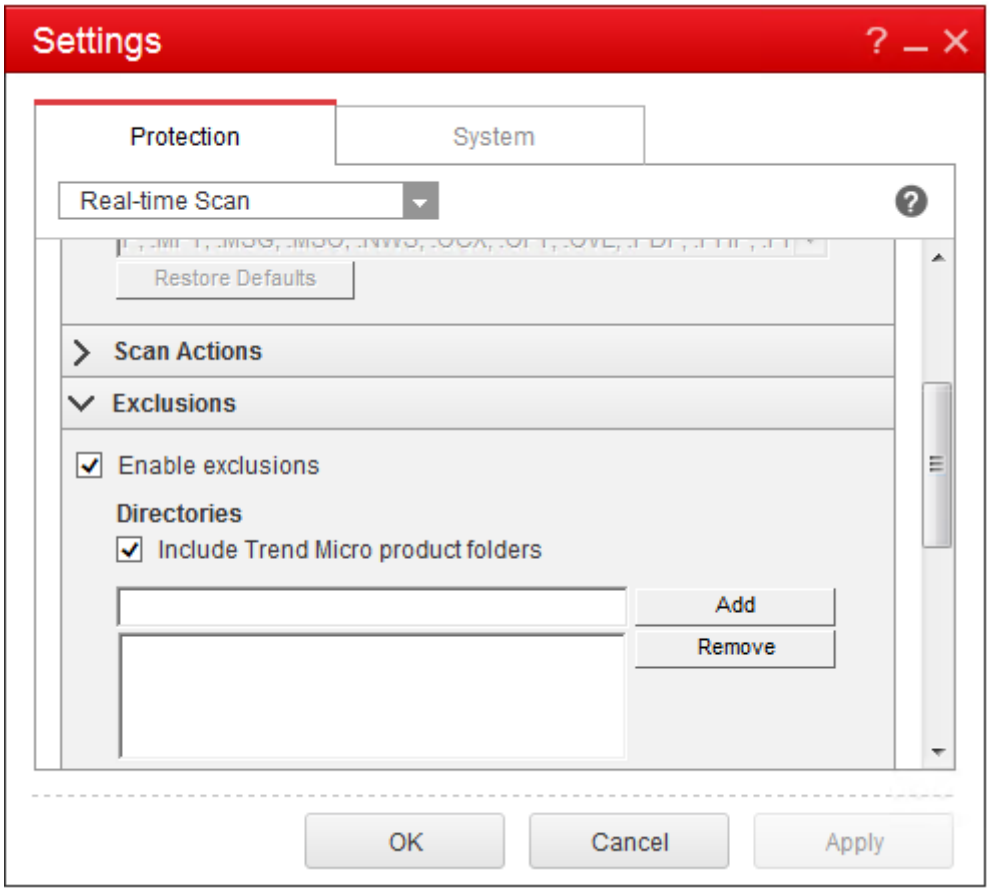
OfficeScan

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：



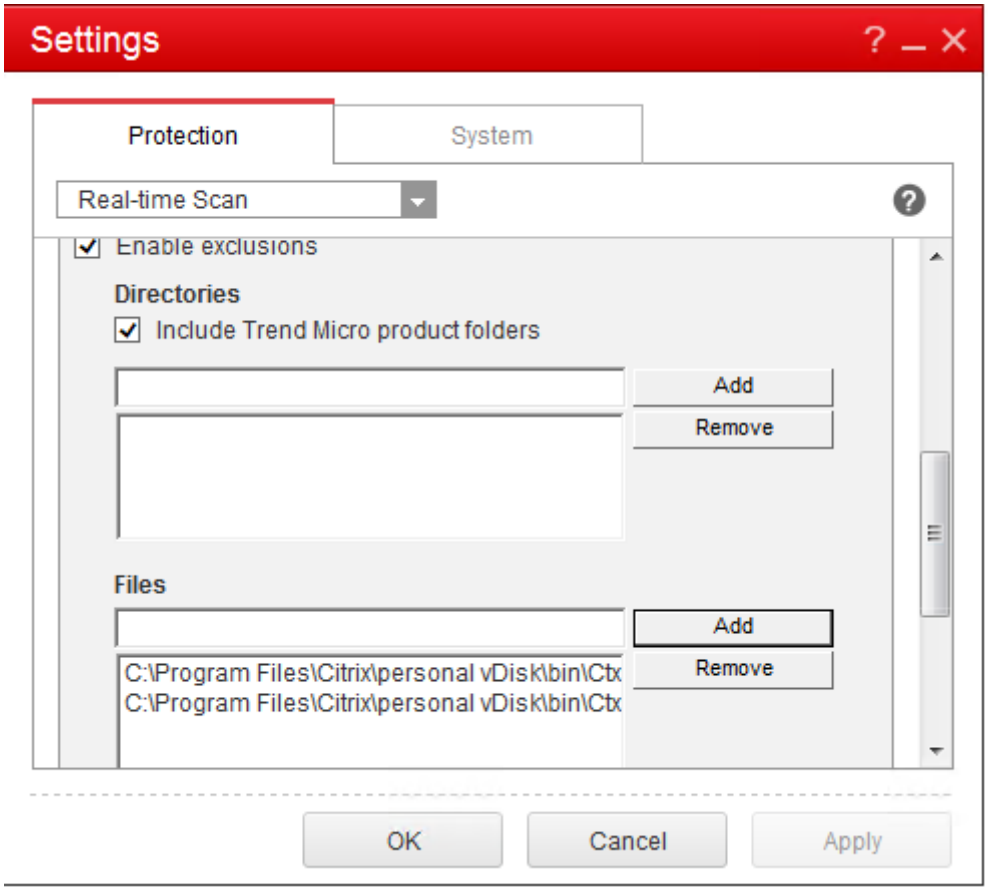
3. ［設定］アイコンをクリックして、構成オプションを表示します。
4. ［設定］画面で、［保護］タブを選択します。
5. ［保護］タブで、［除外］セクションが見つかるまでスクロールダウンします。



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
   ```

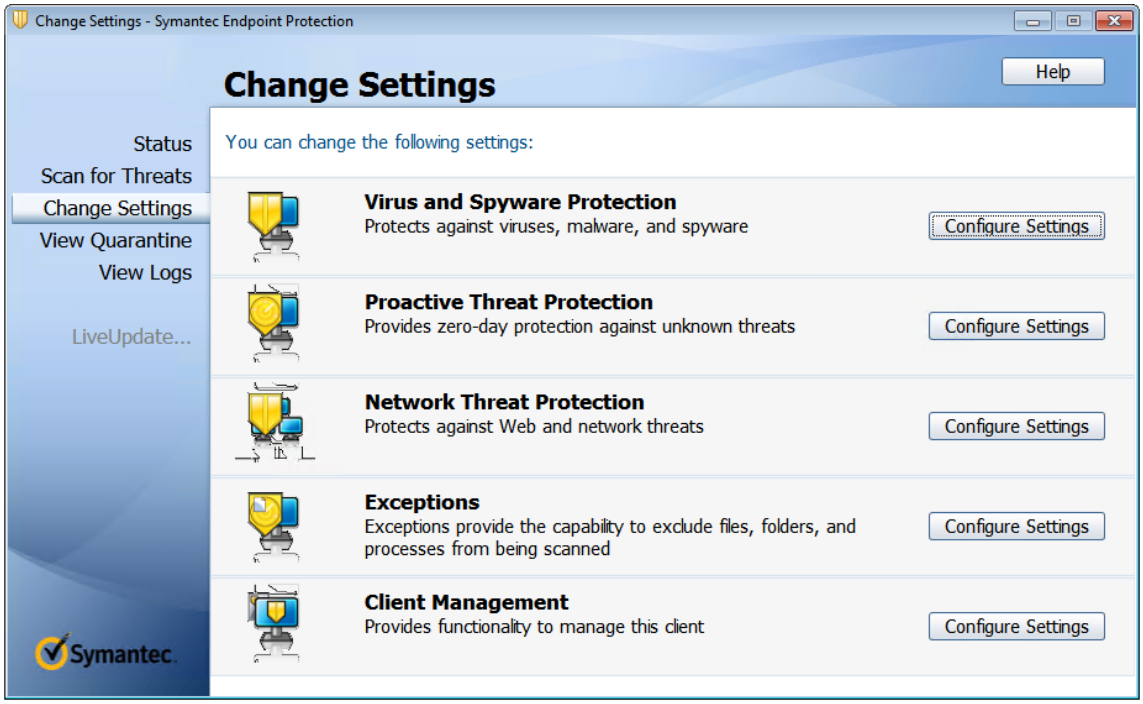



7. ［適用］をクリックし、［**OK**］をクリックして除外を追加します。

Symantec

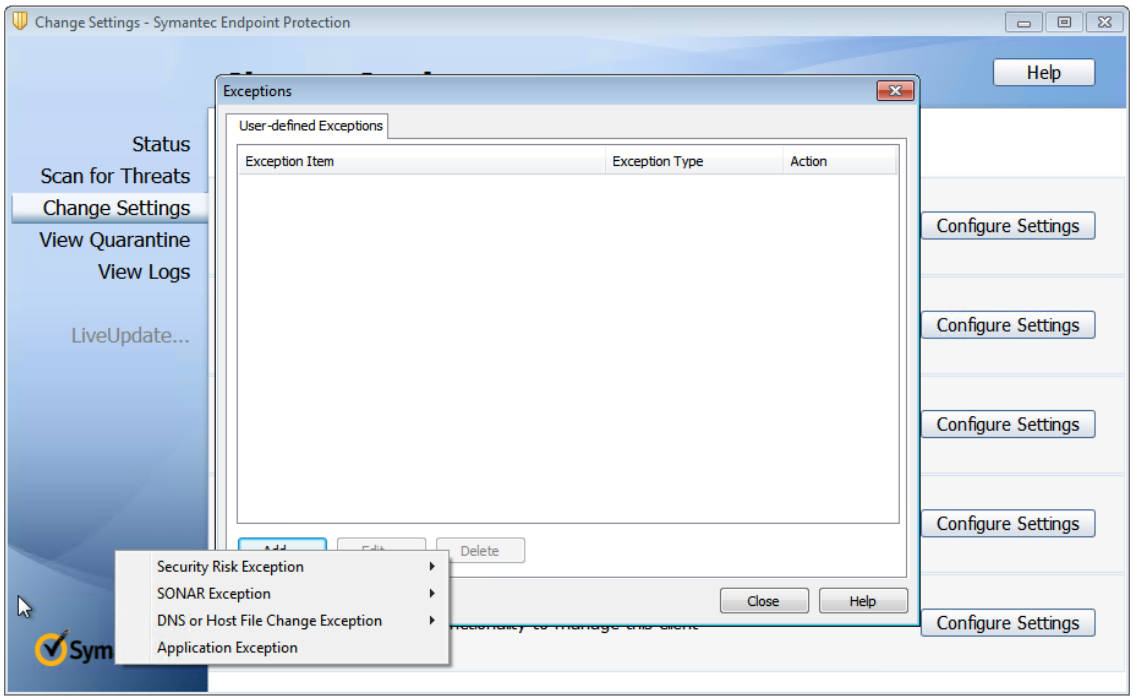
ベース仮想マシンが Symantec （バージョン 12.1.16）を使用している場合：

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:

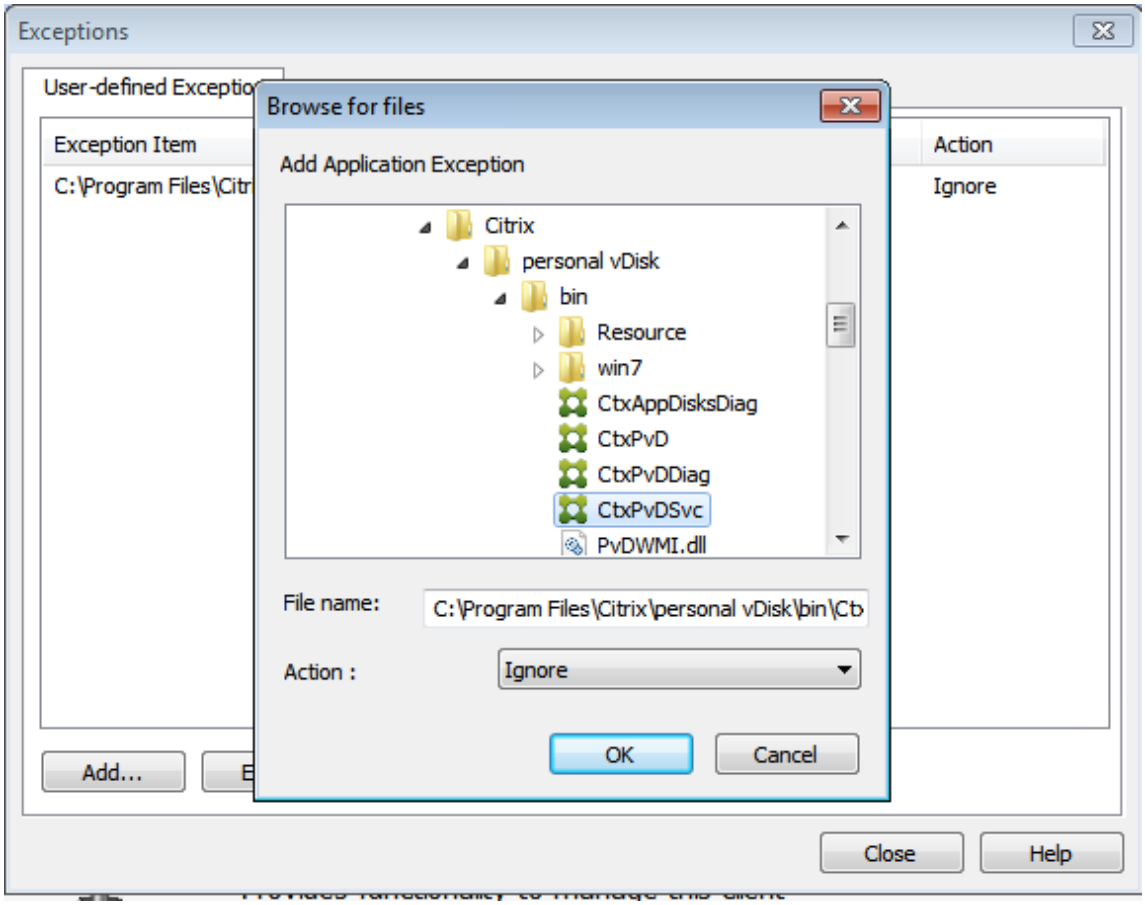


6. ［例外］画面で、次の AppDisk ファイルパスを入力し、操作を ［無視］に設定します:

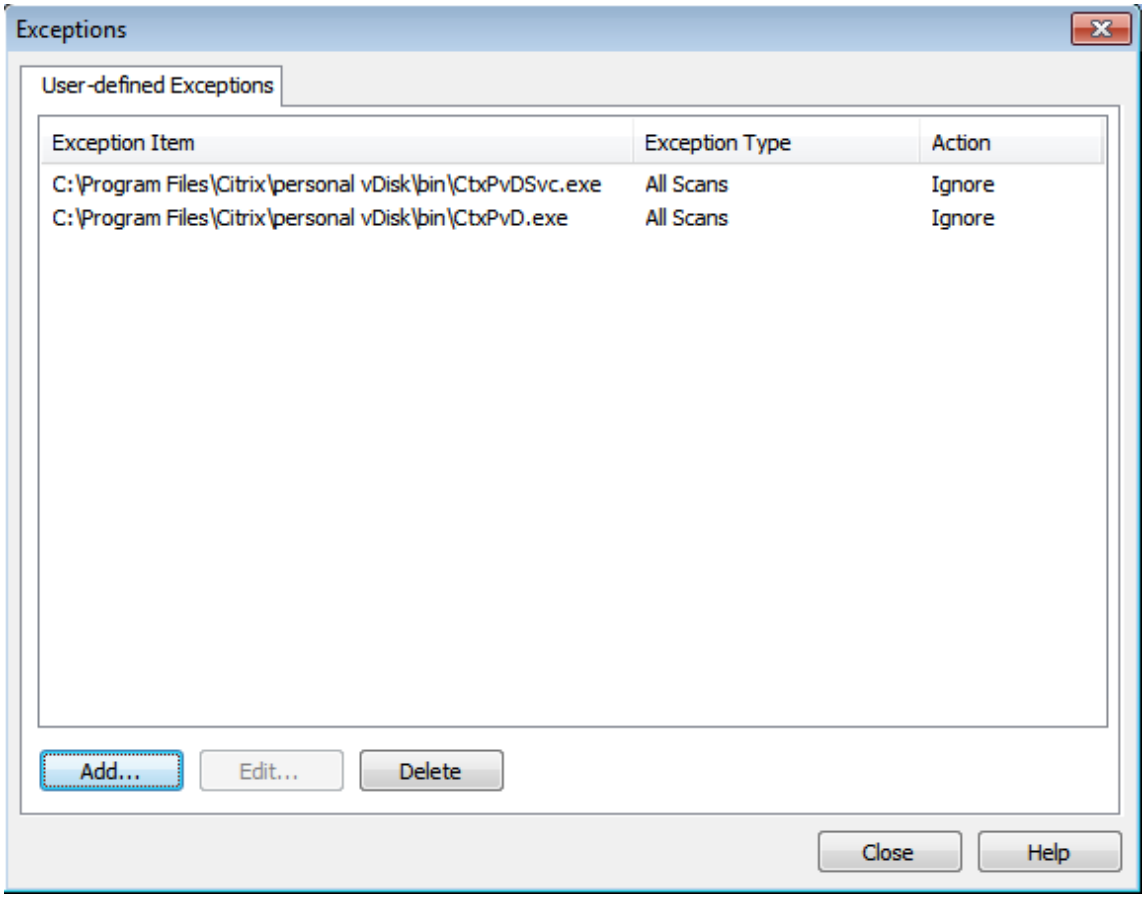
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```



```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



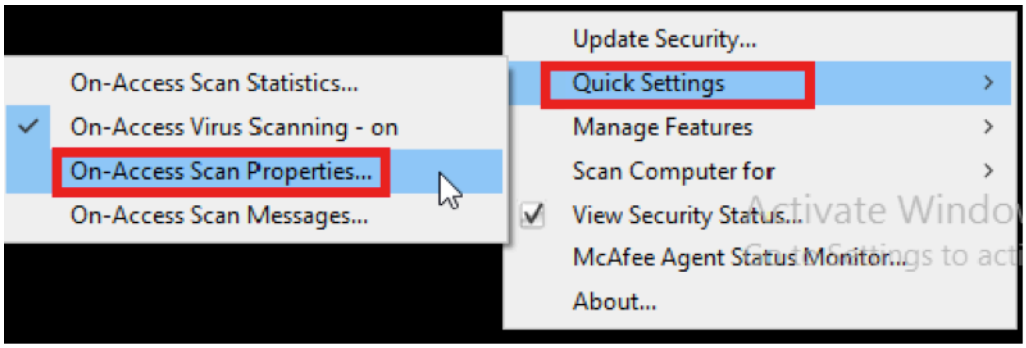
書きとめられた例外が一覧に追加されます。ウィンドウを閉じて変更を適用します。



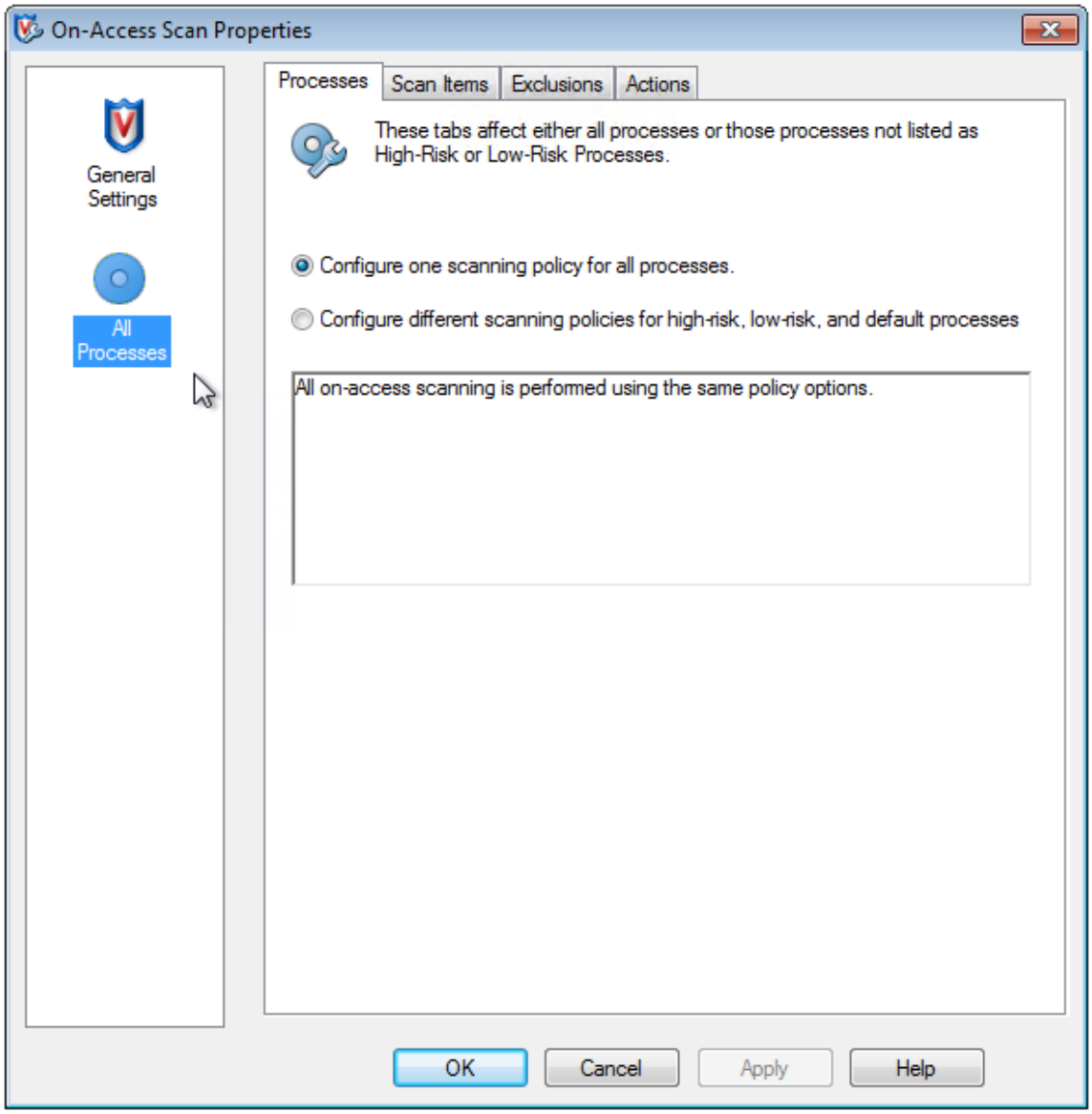
McAfee

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：

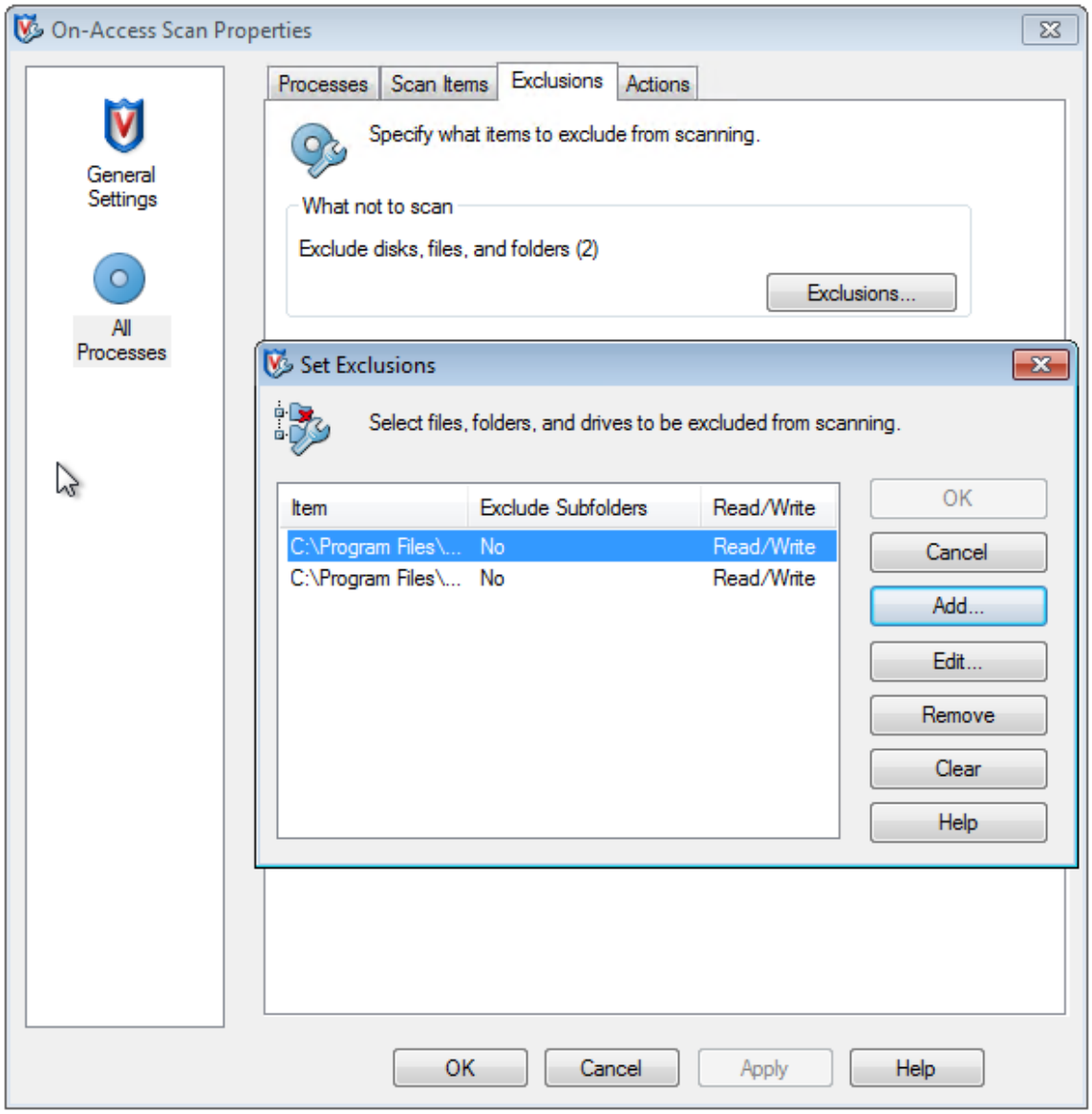
1. McAfee アイコンを右クリックし、［クイック設定］オプションを展開します。
2. 拡張メニューで、［オンアクセススキャンのプロパティ］を選択します：



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:

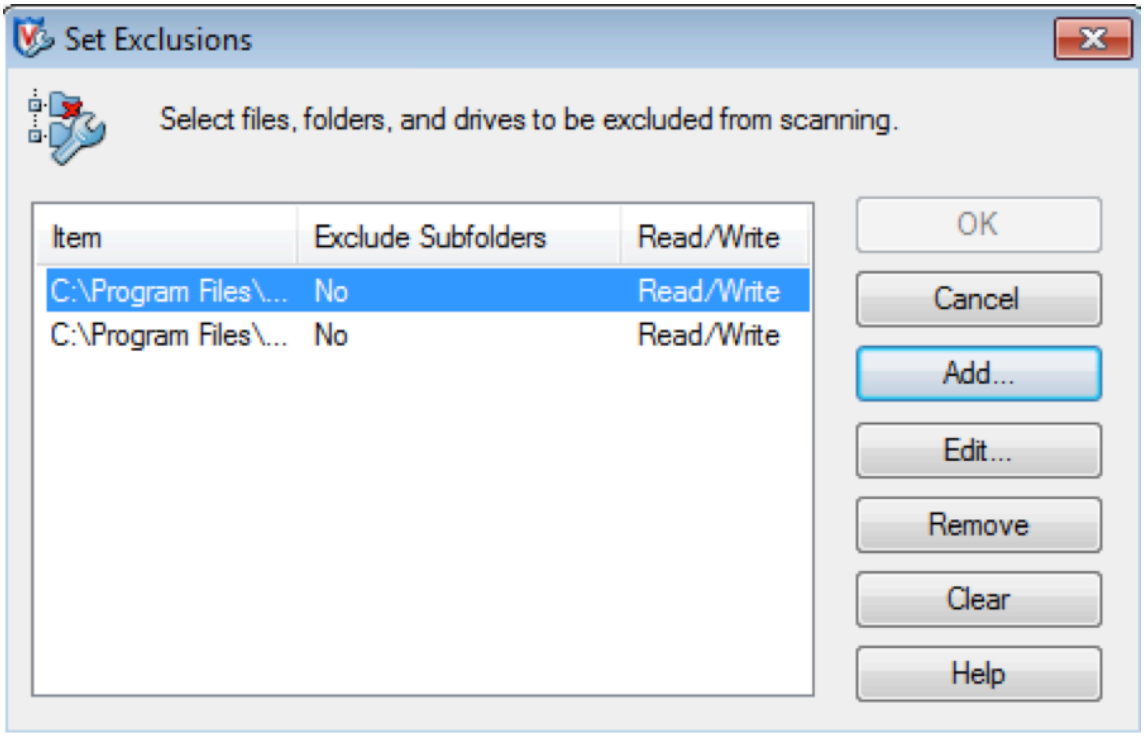


7. ［除外項目の追加］画面で、［名前/場所（ワイルドカード ***** または**?** を使用可能）］を選択します。［参照］をクリックして、除外実行ファイルを見つけます:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

8. ［**OK**］をクリックします。
9. ［除外の設定］画面に、追加された除外が表示されます。［**OK**］をクリックして変更を適用します:



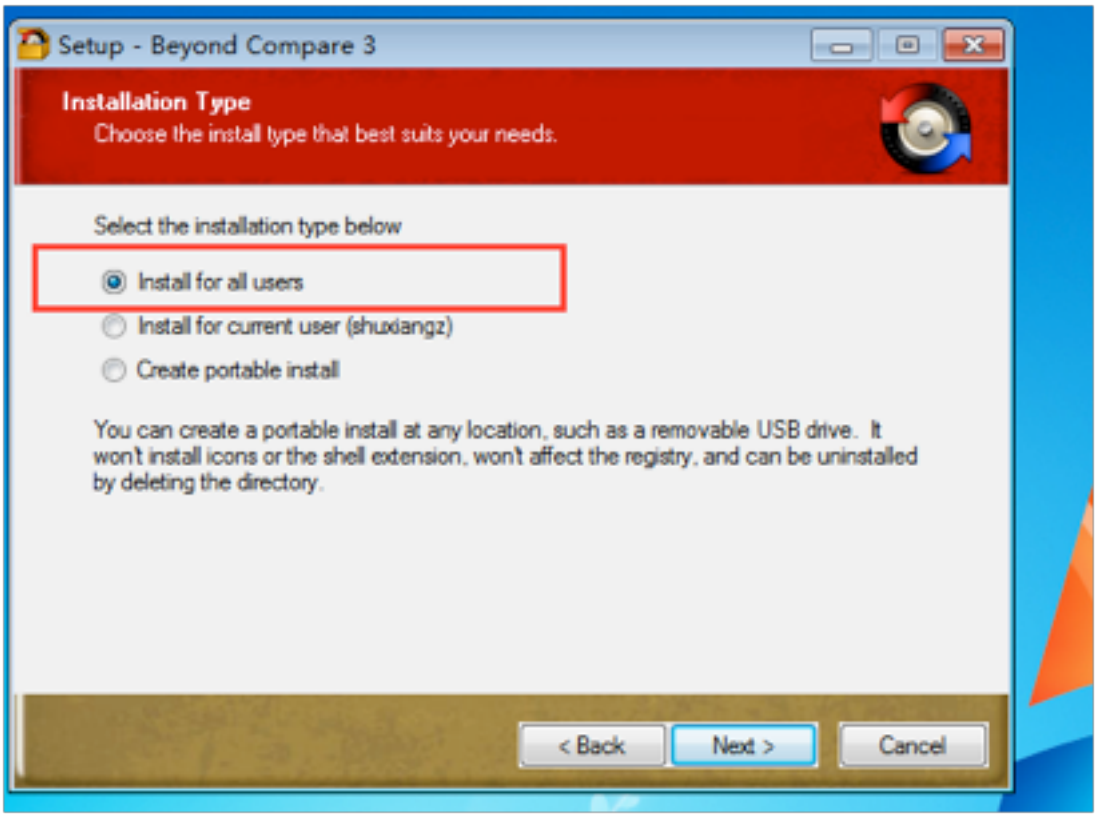
これらの除外を構成したら、AppDisk を作成します。

［スタート］メニューにアプリケーションを表示する方法

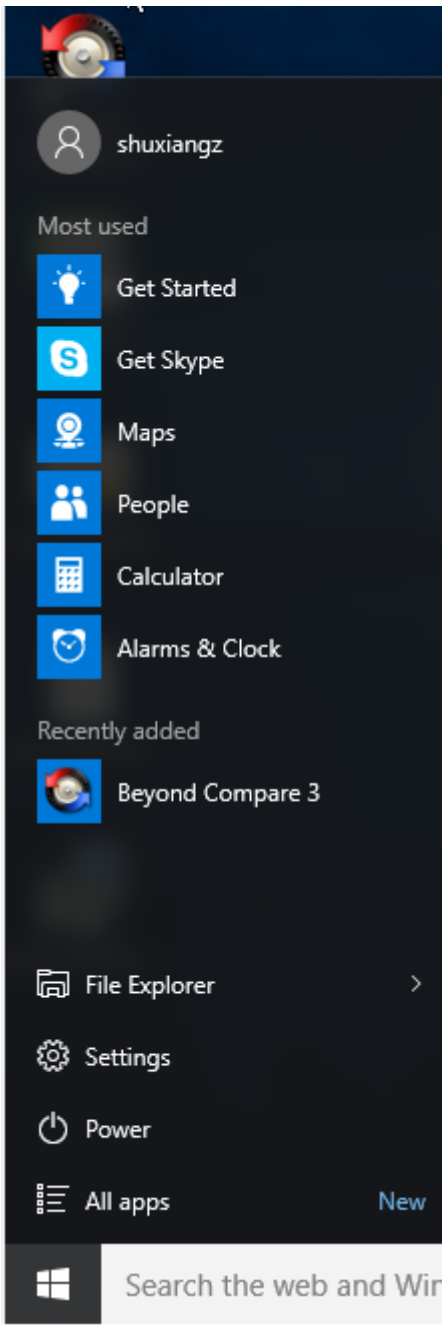
新しい AppDisk が作成され、アプリがすべてのユーザーから利用可能になると、ディスクはデスクトップにアタッチされ、アプリのショートカットが［スタート］メニューに表示されます。AppDisk が現在のユーザーに対してのみ作成およびインストールされ、ディスクがデスクトップにアタッチされた場合、アプリのショートカットは［スタート］メニューに表示されません。

たとえば、新しいアプリを作成して、それをすべてのユーザーが利用できるようにします:

1. AppDisk にアプリをインストールします（たとえば、*Beyond Compare* が選択されたアプリだとします）:

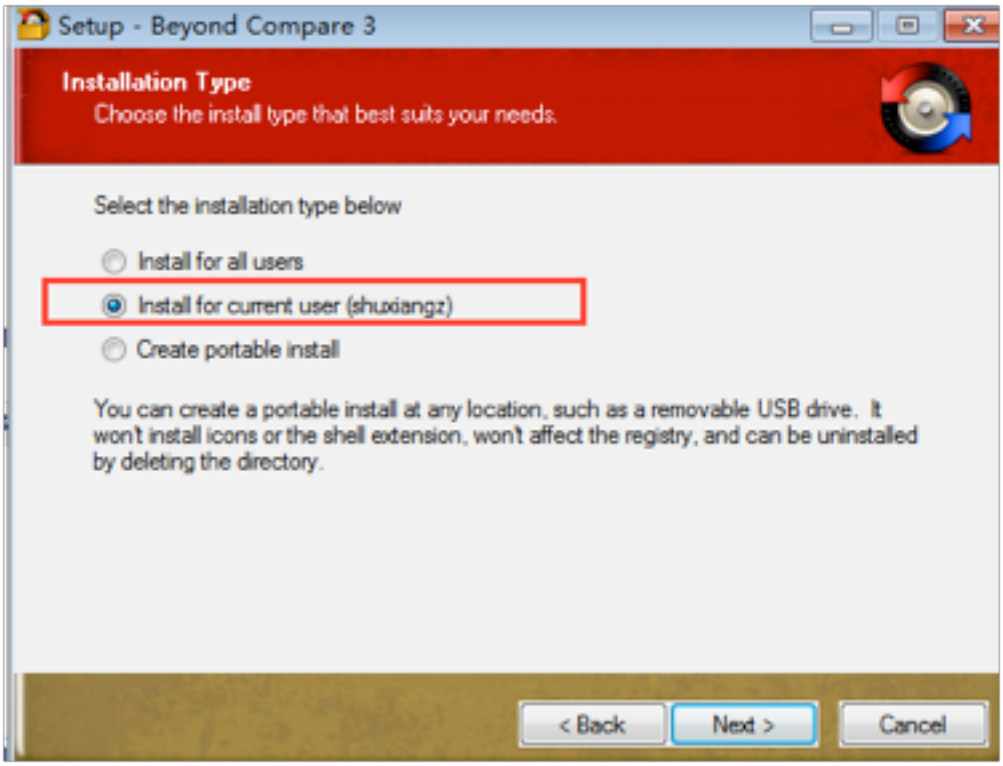


2. デスクトップにディスクをアタッチします。新しくインストールされたアプリ（*Beyond Compare*）のショートカットが、次のように［スタート］メニューに表示されます：

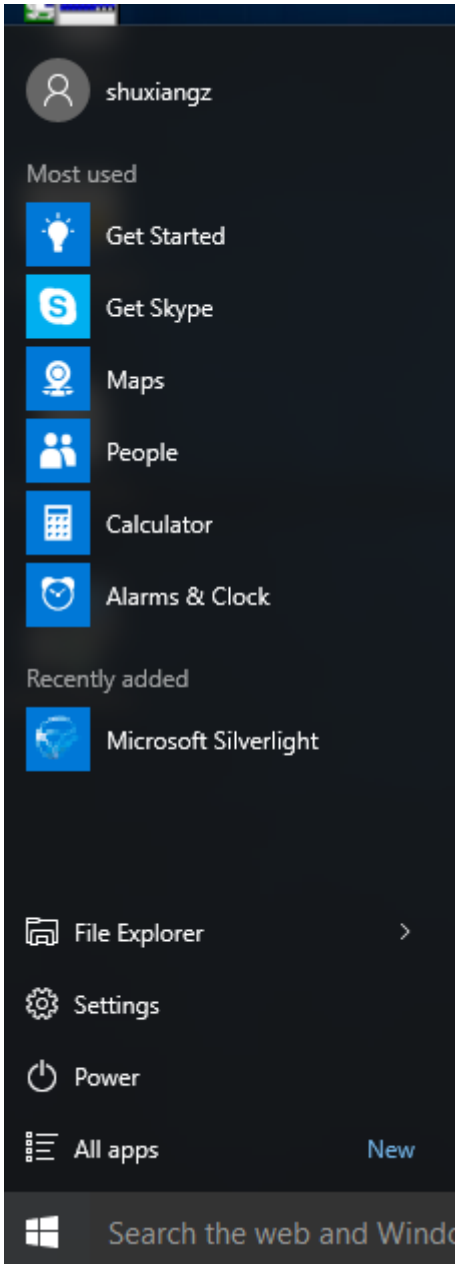


現在のユーザー用にのみアプリケーションをインストールするには:

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

AppDisk ユーザーは、診断情報を取得して、任意でCIS の Web サイトにアップロードできます。

どのように動作するのですか?

この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。シトリックスの CIS 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 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

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

このスクリプトを使って AppDisk の診断データ収集を開始し、任意で手動により CIS の Web サイトにデータをアップロードします。

```
Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: CIS にアップロードする代わりの zip ファイルのローカルパス。`-OutputFile`を省略するとアップロードが行われます。`-OutputFile`を指定すると、後で手動でアップロードできる zip ファイルが作成されます。

例:

- `Upload-AppDDiags`: 対話ユーザーが入力した資格情報を使用して、Citrix CIS Web サイトに診断データをアップロードします。
- `Upload-AppDDiags -OutputFile C:\MyDiags.zip`: 指定された zip ファイルに AppDisk 診断データを保存します。https://cis.citrix.com/にアクセスして後でアップロードできます。

Upload-PvDDiags.ps1

このスクリプトを使って PvD の診断データ収集を開始し、任意で手動により CIS の Web サイトにデータをアップロードします。

```
Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: CIS にアップロードする代わりの zip ファイルのローカルパス。`-OutputFile`を省略するとアップロードが行われます。`-OutputFile`を指定すると、後で手動でアップロードできる zip ファイルが作成されます。

例:

- `Upload-PvDDiags`: 対話ユーザーが入力した資格情報を使用して、PvD 診断データを Citrix CIS Web サイトにアップロードします。
- `Upload-PvDDiags -OutputFile C:\MyDiags.zip`: 指定された zip ファイルに PvD 診断データを保存します。https://cis.citrix.com/にアクセスして後でアップロードできます。

Virtual Apps Secure Browser

April 26, 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。

Secure Browser を使用すると、ユーザーは Web ベースのアプリケーションをシームレスに利用できるようになります。ホストされている 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。Secure Browser を使用すると、Internet Explorer と互換性のあ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。

Virtual Apps Secure Browser Edition の展開

1. シトリックスのダウンロードサイトから、Citrix Virtual Apps Secure Browser Edition ISO をダウンロードします。
2. インストール手順に従って、Citrix Virtual Apps の各種コンポーネントをインストールします。
3. インストール後、次の追加手順を実行して、Secure Browser エディションのエディションとライセンスモードを構成します:

   a) Delivery Controller で、タスクバーの青色のアイコンをクリックするか、[スタート] ボタンをクリックし、[すべてのプログラム] > [アクセサリ] > [Windows PowerShell] > [Windows PowerShell] の順に選択して、PowerShell セッションを起動します。

   64 ビットシステムでは、64 ビット版が起動します。32 ビット版と 64 ビット版の両方がサポートされます。

   b) `asnp Citrix*`と入力し、**Enter** キーを押して Citrix 固有の PowerShell モジュールをロードします（`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します: `Get-ConfigSite`を実行します。

d) ライセンスモードを Virtual Apps Secure Browser Edition に設定します：`Set-ConfigSite -ProductCode XDT -ProductEdition BAS`を実行します。

e) Virtual Apps Secure Browser Edition とライセンスモードが正しく設定されていることを確認します：`Get-BrokerSite`を実行します。

インストールの完了後、『XenApp Secure Browser 展開ガイド』で指定された構成手順を使用して、Web アプリデリバリー用の環境をさらに最適化します。

コンテンツの公開

April 26, 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。

公開したコンテンツは、ほかのアプリケーションと同様に StoreFront および Citrix Workspace アプリに表示されます。ユーザーは、アプリケーションと同じようにこれらのコンテンツにアクセスできます。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）。

```
1 New-BrokerApplication  -ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

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、公開コンテンツの場所を指定します。以下の形式を使用でき、最大文字数は 255 文字です。

- HTML Web サイトアドレス（例：http://www.citrix.com）
- Web サーバー上の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(たとえば、file://myServer/myShare or \\\\\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 Citrix Virtual Apps and Desktops サービスの場合は、Citrix Virtual Apps and Desktops のリモート 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 Citrix Virtual Apps and Desktops 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。

導入

PowerShell SDK をインストール済みのマシンで PowerShell を開きます。

次のコマンドレットにより、適切な PowerShell スナップインを追加し、返されたデリバリーグループレコードを変数に代入します。

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

Citrix Virtual Apps and Desktops サービス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-->
```

次の手順を実行して、成功したことを確認します:

- StoreFront を開き、PublishedContentApps デリバリーグループのアプリケーションにアクセスできるユーザーとしてログオンします。新しく作成したアプリケーションが、デフォルトのアイコンで表示されます。アイコンのカスタマイズ方法については、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"

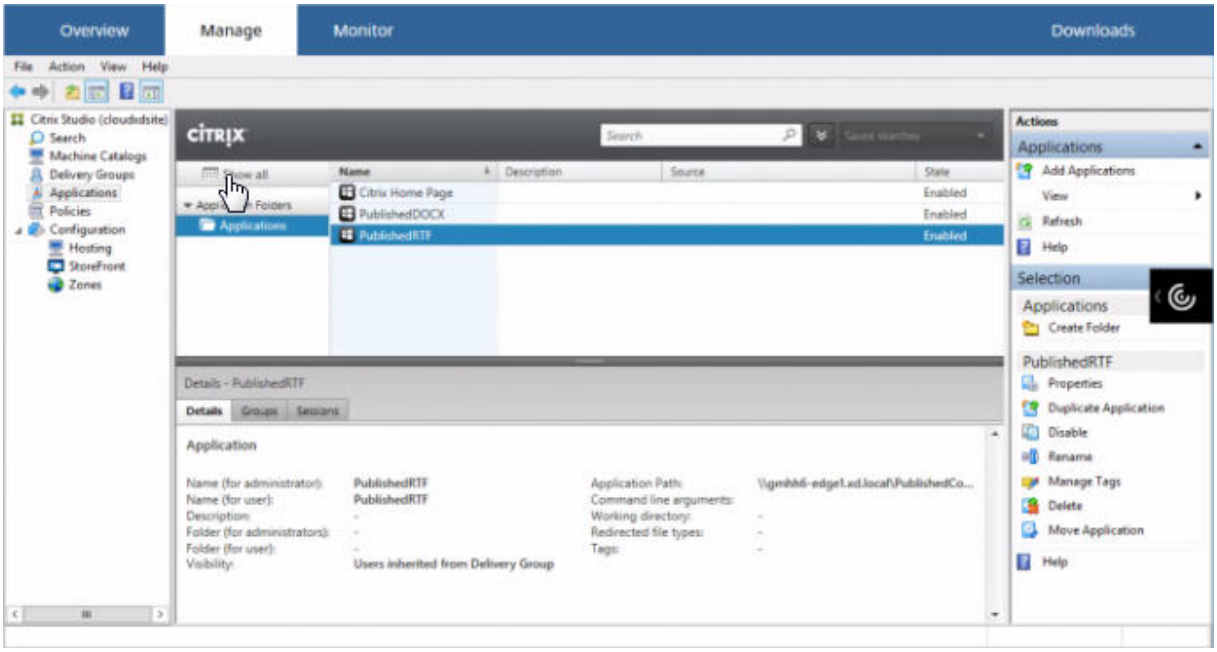
New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

次の手順を実行して、成功したことを確認します:

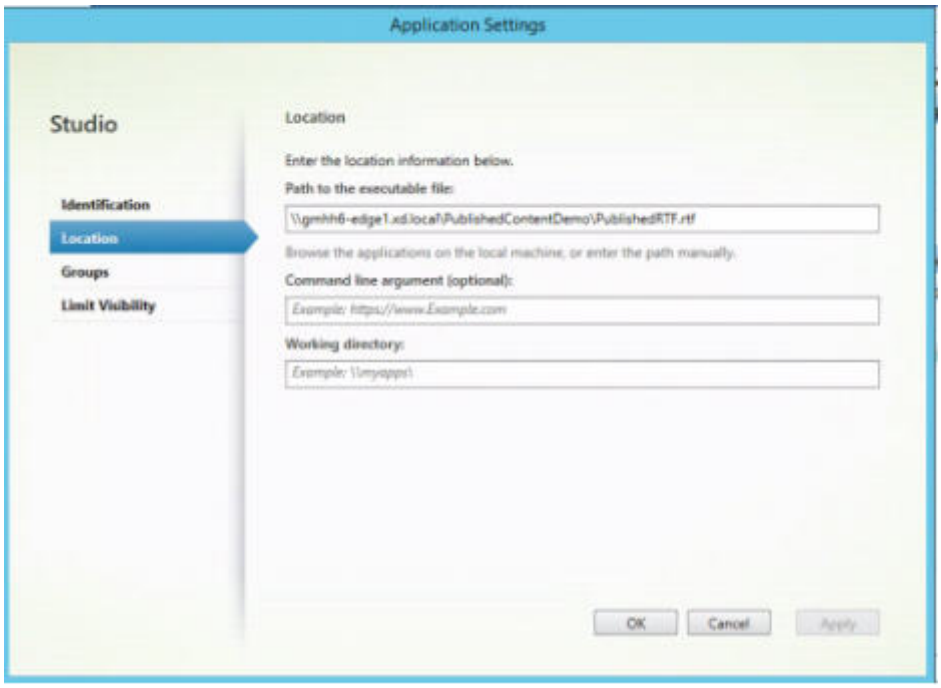
- StoreFront ウィンドウを更新して、新しく公開したドキュメントが表示されることを確認します。
- **PublishedRTF** アプリケーションおよび **PublishedDOCX** アプリケーションをクリックします。各ドキュメントが、ローカルで実行されるワードパッドで開きます。

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



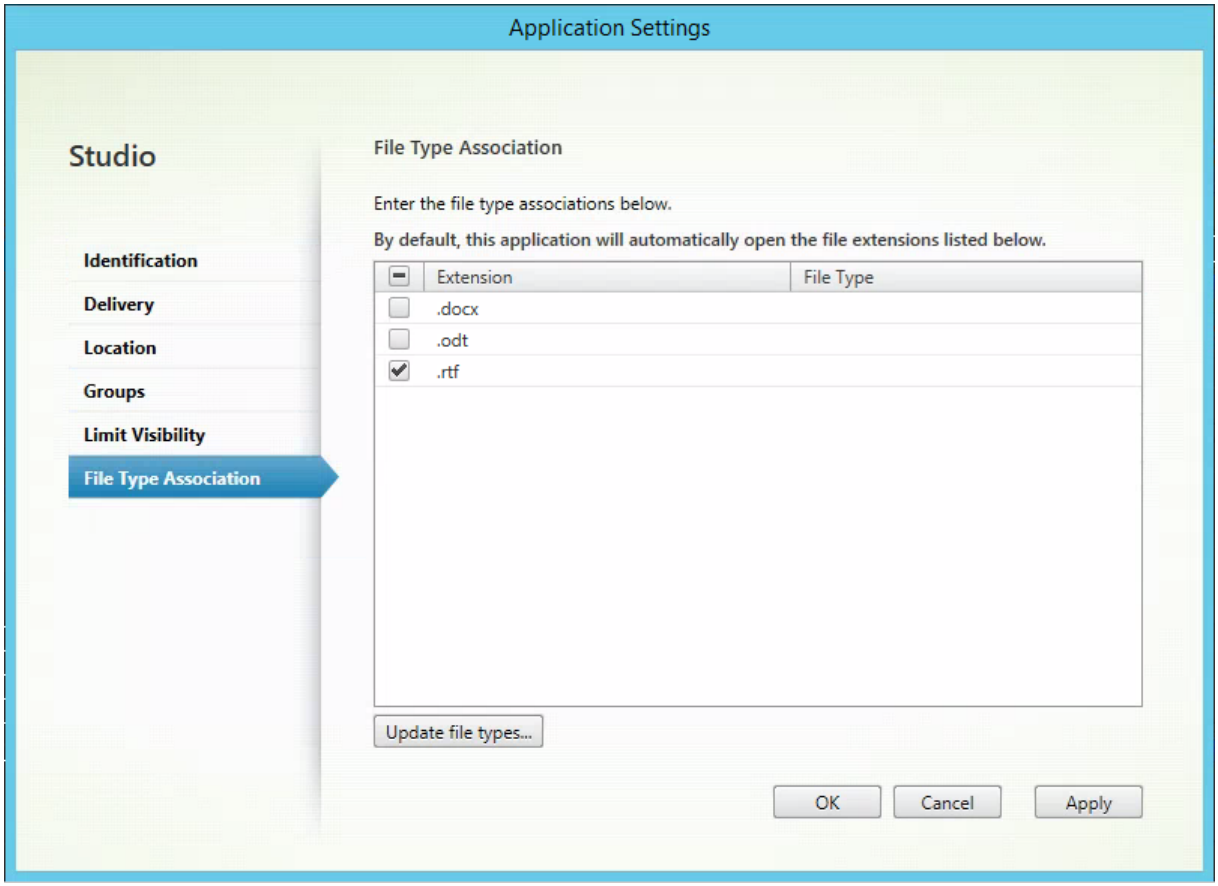
公開コンテンツには、アプリケーションのプロパティ（表示できるユーザー、グループ割り当て、ショートカットなど）が適用されます。ただし、［場所］ページでコマンドライン引数や作業ディレクトリプロパティを変更することはできません。リソースを変更するには、［場所］ページの ［実行可能ファイルのパス］を変更します。



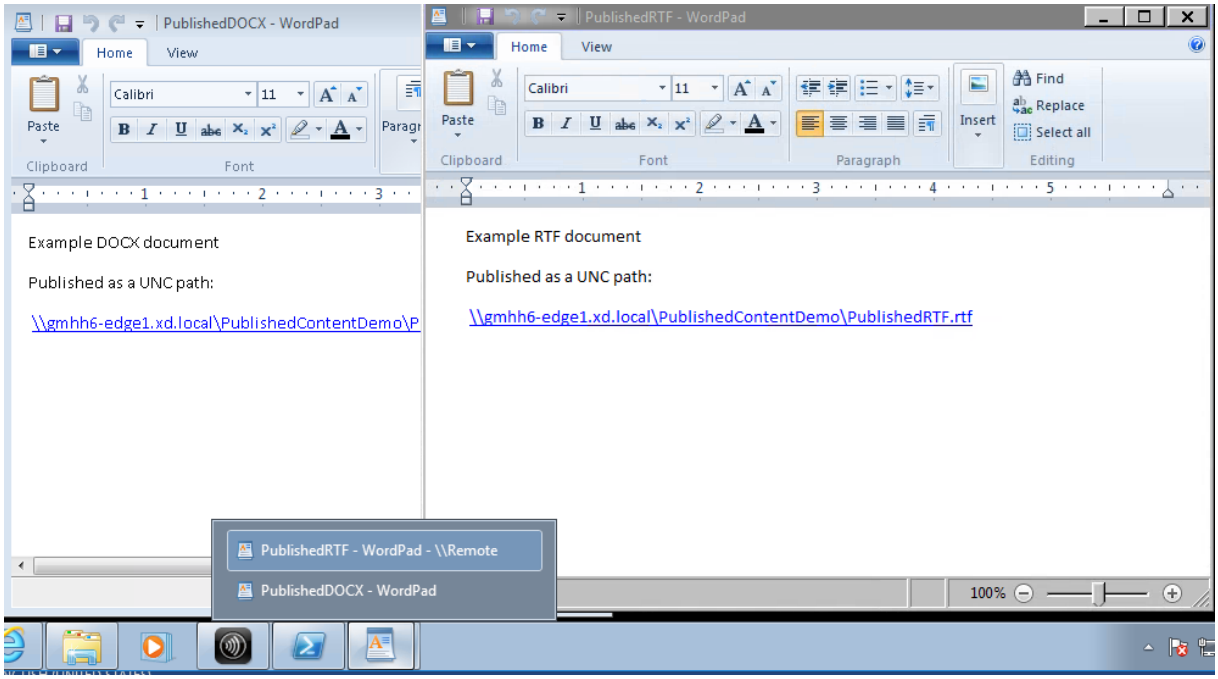
PublishedContent アプリケーションを開くのに（ローカルアプリではなく）公開アプリケーションを使用するに

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。

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

サーバー VDI

April 26, 2021

サーバー VDI（Virtual Desktop Infrastructure）機能を使用すると、サーバーオペレーティングシステムからユーザーにデスクトップを配信できます。

- エンタープライズ管理者は、エンジニアやデザイナーなどのユーザーにサーバーオペレーティングシステムを VDI デスクトップとして配信できます。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement（SPLA）に準拠します。

デスクトップエクスペリエンス拡張の Citrix ポリシー設定を使用すると、サーバーオペレーティングシステムでデスクトップオペレーティングシステムの外観を提供できます。

サーバー VDI では、次の機能を使用できません:

- Personal vDisk
- ホストされるアプリケーション

- ローカルアプリアクセス
- 直接（非仲介）デスクトップ接続
- リモート PC アクセス

サーバー VDI は現在、Windows Server 2019 および Windows Server 2016 マシン上でサポートされています。

スキャナのような TWAIN デバイスと連携するサーバー VDI には、Windows Server のデスクトップエクスペリエンス機能をインストールする必要があります。

サーバー **VDI** のインストールと構成

1. Windows サーバーでのインストールの準備
    - Windows サーバーマネージャーを使って、リモートデスクトップサービスの役割サービスがインストールされていないことを確認します。既にインストールされている場合は、それを削除します。これらの役割サービスがインストールされていると、VDA のインストールに失敗します。
    - ［1 ユーザーにつき 1 セッションに制限する］プロパティが有効であることを確認します。Windows サーバー上で、ターミナルサーバー設定のレジストリを編集します：
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer
        - DWORD fSingleSessionPerUser = 1
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスで、「quiet」および「servervdi」オプションを指定して、VDA をサポート対象のサーバーまたはサーバーマスターイメージ上にインストールします（デフォルトでインストーラーのグラフィカルユーザーインターフェイスでは、サーバーオペレーティングシステム上の Windows シングルセッション OS 対応 VDA はブロックされます。コマンドラインを使用すると、この動作が無効になります）。次のいずれかのコマンドを使用します：
    - Citrix Virtual Apps and Desktops 環境の場合：
        - `XenDesktopVdaSetup.exe /quiet /servervdi`
        - `VDAWorkstationSetup.exe /quiet /servervdi`
    - Citrix Virtual Apps and Desktops サービス環境の場合：
        - `VDAWorkstationSetup.exe /quiet /servervdi`

    その他のオプション：
    - Delivery Controller または Cloud コネクタを「controllers」オプションで指定できます。
    - ファイアウォールが手動で構成されていない限りは、`enable_hdx_ports`オプションを使ってファイアウォールのポートを開いてください。
    - イメージに VDA をインストールしており、MCS を使用してそのイメージからサーバー仮想マシンを作成する場合は、`mastermcsimage`（または`masterimage`）オプションを追加します。
    - 「baseimage」など、サーバー VDI でサポートされてない機能のオプションを指定しないでください（Personal vDisk の場合）。
    - すべてのオプションの詳細については、「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。

3. サーバー VDI のマシンカタログを作成します。カタログ作成ウィザードで次の操作を行います:

    - ［オペレーティングシステム］ページで、［シングルセッション **OS**］を選択します。
    - ［概要］ページで、管理者がサーバー VDI 用のマシンカタログを識別できるようにマシンカタログ名と説明を指定します。これは、Studio においてそのマシンカタログがサーバー VDI 用であることを示す唯一のインジケーターになります。

    VDA はサーバー上にインストールされていますが、Studio で検索すると、このサーバー VDI カタログは ［シングルセッション **OS** マシン］タブに表示されます。

4. デリバリーグループを作成し、作成したサーバー VDI カタログを選択します。

VDA のインストール中に Delivery Controller または Cloud コネクタを指定しなかった場合、必ずあとから指定します。詳しくは、「VDA 登録」を参照してください。

ユーザー個人設定レイヤー

April 26, 2021

Citrix Virtual Apps and Desktops のユーザー個人設定レイヤー機能は、非永続マシンカタログの機能を拡張します。セッション全体でユーザーのデータとローカルにインストールされたアプリケーションを保持します。Citrix App Layering を搭載した Personal vDisk（PvD）に代わる機能です。

PvD 同様、ユーザー個人設定レイヤー機能は、永続的ではないマシンカタログの Citrix Provisioning および Machine Creation Services（MCS）で動作します。機能コンポーネントは、マスター Windows 10 イメージ内の Virtual Delivery Agent と一緒にインストールされます。

ユーザーが作成するアプリケーションとデータは、イメージにマウントされた VHD ファイルにある自身のユーザーレイヤーの仮想ハードドライブに保存されます。

このドキュメントには、ユーザー個人設定レイヤー機能を展開および構成するための手順が含まれています。展開を成功させるための要件、制限、既知の問題について説明します。

ユーザー個人設定レイヤー機能を使用するには、最初にこの記事で説明されている手順を使用してレイヤーを展開する必要があります。それまでは、この機能を使用することはできません。

アプリケーションサポート

次の例外を除き、ユーザーがローカルでデスクトップにインストールするすべてのアプリケーションは、ユーザー個人設定レイヤーでサポートされます。

例外

次のアプリケーションは例外であり、ユーザー個人設定レイヤーでサポートされません:

- MS Office や Visual Studio などのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPN クライアント。
- ブートレベルのドライバーを備えたアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを備えたアプリケーション。例：プリンタードライバー。

  > 注：
  >
  > Windows GPO を使用してプリンターを使用可能にすることができます。

ユーザーがサポートされていないアプリケーションをローカルでインストールできないようにしてください。このようなアプリケーションは、マスターイメージに直接インストールします。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションを（ユーザーレイヤーに）ローカルでインストールし、アプリケーションで必要な場合にローカルユーザーやグループを追加または編集すると、そのユーザーまたはグループの変更は保持されません。

> 重要：
>
> 必要なローカルユーザーまたはグループをマスターイメージに追加します。

要件

ユーザー個人設定レイヤー機能には、次のコンポーネントが必要です：

- Citrix Virtual Apps and Desktops 7 1909 以降
- Virtual Delivery Agent（VDA）バージョン 1912
- Citrix Provisioning バージョン 1909 以降
- Windows ファイル共有（SMB）
- Windows 10 Enterprise x64 バージョン 1607 以降

> 重要：
>
> - ユーザー個人設定レイヤー機能の Preview バージョンをインストールした場合は、このリリースをインストールする前に Preview バージョンをアンインストールし、マスターイメージを再起動してください。
> - 以下の手順で説明するように、Studio でポリシーを定義し、ユーザー個人設定レイヤーが展開されるマシンカタログにバインドされた特定のデリバリーグループにポリシーを割り当てる必要があります。マスターイメージにユーザー個人設定レイヤーを構成しない場合、サービスはアイドル状態のままになり、オーサリングアクティビティに干渉することはできなくなります。マスターイメージでポリシーを設定すると、ユーザー個人設定レイヤーサービスが実行されユーザーレイヤーをマスターイメージにマウントしようとします。この環境はイメージへの変更をオーサリングするための環境であるためこれは望ましい操作ではなく、マスターイメージに予期しない動作や不安定な動作を引き起こす可能性があります。

推奨事項

ユーザー個人設定レイヤーを展開するには、このセクションの推奨事項に従ってください。

Profile Management ソリューション

ユーザーの個人設定レイヤーには、ユーザーが 1 つのマシンカタログイメージに追加したすべての変更が格納されています。移動プロファイルデータなどの拡張機能を複数のカタログイメージに追加するには、Profile Management の使用をお勧めします。詳しくは、「Profile Management のドキュメント」を参照してください。

ユーザー個人設定レイヤー機能で Profile Management を使用している場合は、ログオフ時のユーザー情報の削除をオフにします。設定の展開方法に応じて、グループポリシーオブジェクト（GPO）または Delivery Controller（DDC）のポリシーのいずれかを使用して削除をオフにできます。

利用可能な Profile Management ポリシーについて詳しくは、「Profile Management ポリシーに関する説明とデフォルト設定」を参照してください。

Microsoft System Center Configuration Manager（**SCCM**）

ユーザー個人設定レイヤー機能を SCCM とともに使用している場合は、VDI 環境でイメージを準備するための Microsoft のベストプラクティスに従ってください。詳しくは、Microsoft TechNet の記事を参照してください。

最大ユーザーレイヤーサイズ

ユーザーレイヤーサイズは最低 10GB をお勧めします。

> 注:
>
> インストール時に値がゼロ（0）の場合、デフォルトのユーザーレイヤーサイズは 10GB になります。

Windows で設定されたクォータは、最大ユーザーレイヤーサイズを上書きできます

ユーザーレイヤーファイル共有のクォータを定義することにより、Studio で設定された最大ユーザーレイヤーサイズを上書きできます。クォータが定義されている場合、ユーザーレイヤーはクォータサイズの最大値に設定されます。

ユーザーレイヤーサイズにハードクォータを設定するには、Microsoft のクォータツールのいずれかを使用します:

- ファイルサーバーリソースマネージャー（FSRM）
- クォータマネージャー

クォータは、Users という名前のユーザーレイヤーディレクトリに設定する必要があります。

> 注:
>
> クォータの増減は、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーの最大サイズは変更されません。クォータが更新されても、これらは変更されません。

ユーザー個人設定レイヤーの展開

ユーザー個人設定レイヤー機能を展開するには、次の手順をこの順序で実行します:

- 手順 1: Citrix Virtual Apps and Desktops 環境の可用性を検証します。
- 手順 2: マスターイメージを準備します。
- 手順 3: マシンカタログを作成します。
- 手順 4: デリバリーグループを作成します。
- 手順 5: デリバリーグループのカスタムポリシーを作成します。

手順 **1**: **Citrix Virtual Apps and Desktops** 環境の可用性を検証

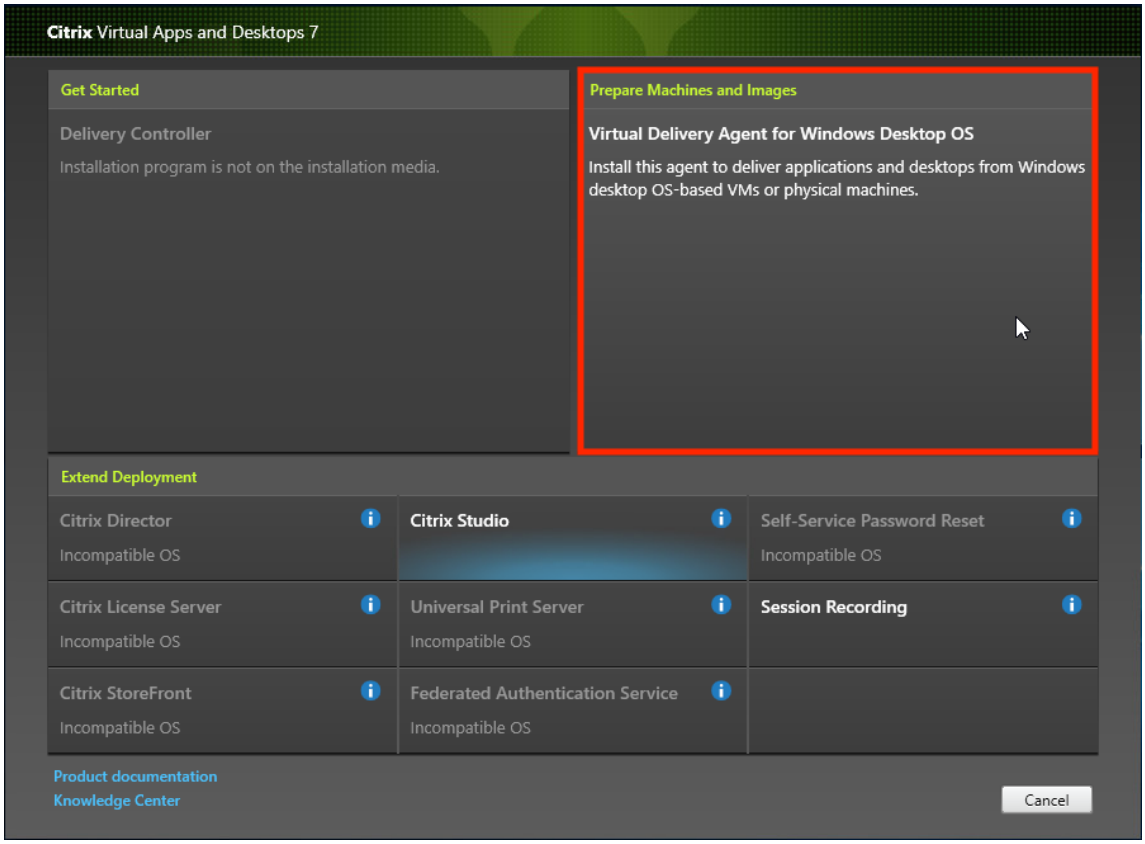
Citrix Virtual Apps and Desktops 環境でこの新機能を使用できることを確認してください。セットアップについて詳しくは、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

手順 **2**: マスターイメージの準備

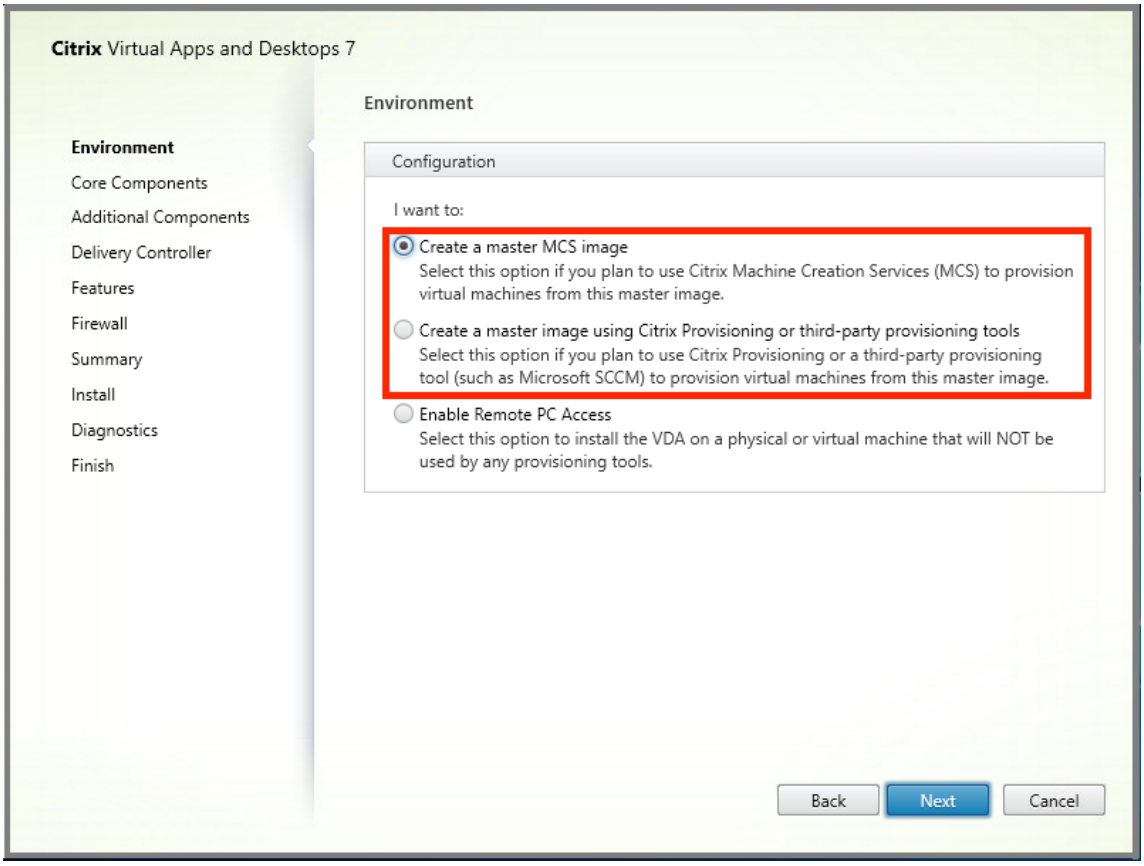
マスターイメージを準備するには:

1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、一般的にユーザーが有用だと見なすその他のアプリをインストールします。
2. Citrix Virtual Delivery Agent（VDA）1912 をインストールします。古いバージョンの VDA が既にインストールされている場合は、最初に古いバージョンをアンインストールします。新しいバージョンをインストールするときは、次のようにオプションのコンポーネントである Citrix ユーザー個人設定レイヤーを選択してインストールしてください:

    a)［**Virtual Delivery Agent for Windows Desktop OS**］のタイルをクリックします:

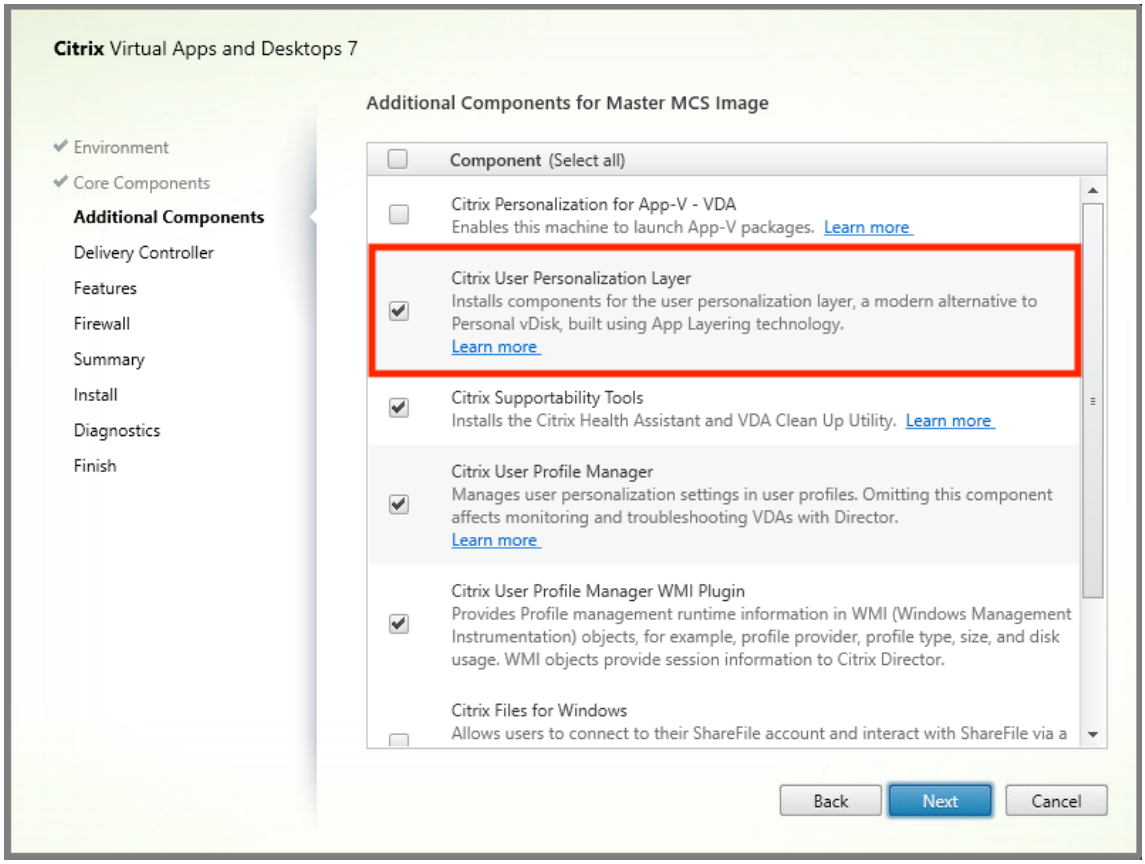


a) 環境：［マスター MCS イメージを作成する］か、［Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する］を選択します。



a) コアコンポーネント：［次へ］をクリックします。

b) 追加のコンポーネント：［**Citrix User Personalization Layer**］をオンにします。



a) 残りのインストール画面をクリックして、必要に応じて VDA を構成し、［インストール］をクリックします。イメージはインストール中に 1 回または複数回再起動します。

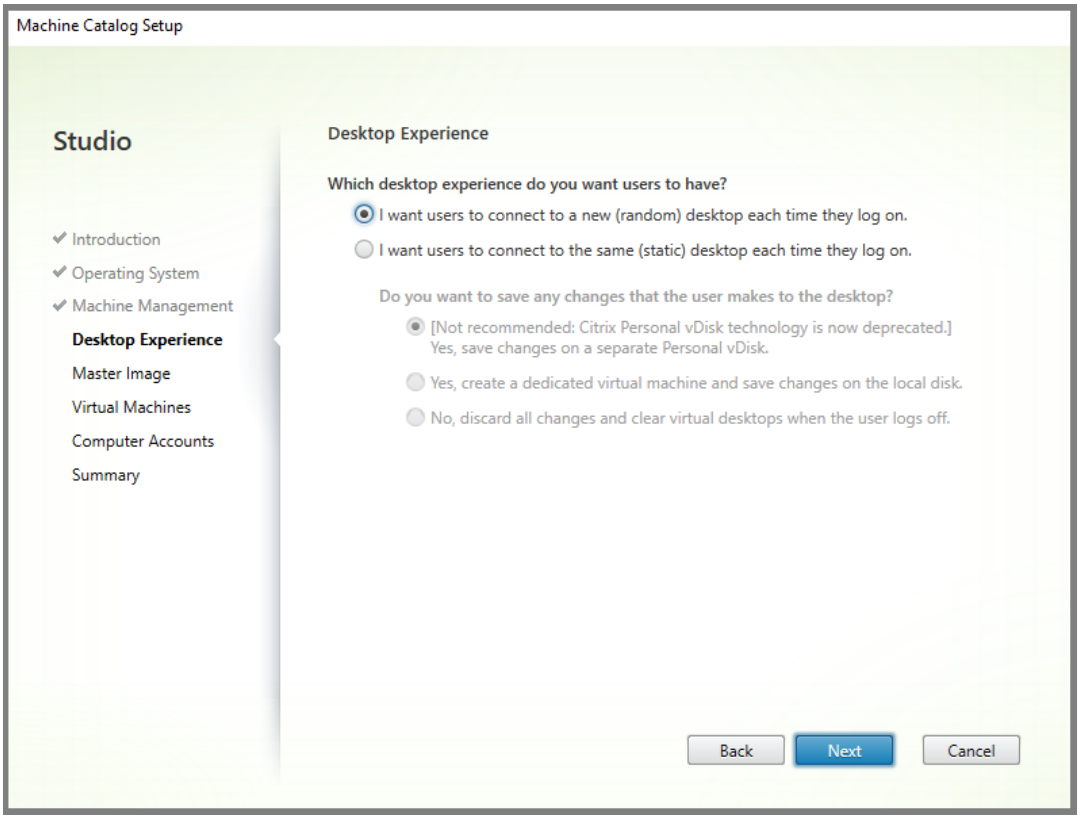
3. **Windows** の更新プログラムは無効のままにします。ユーザー個人設定レイヤーインストーラーは、イメージの Windows の更新プログラムを無効にします。更新プログラムを無効のままにします。

イメージを Studio にアップロードする準備ができました。

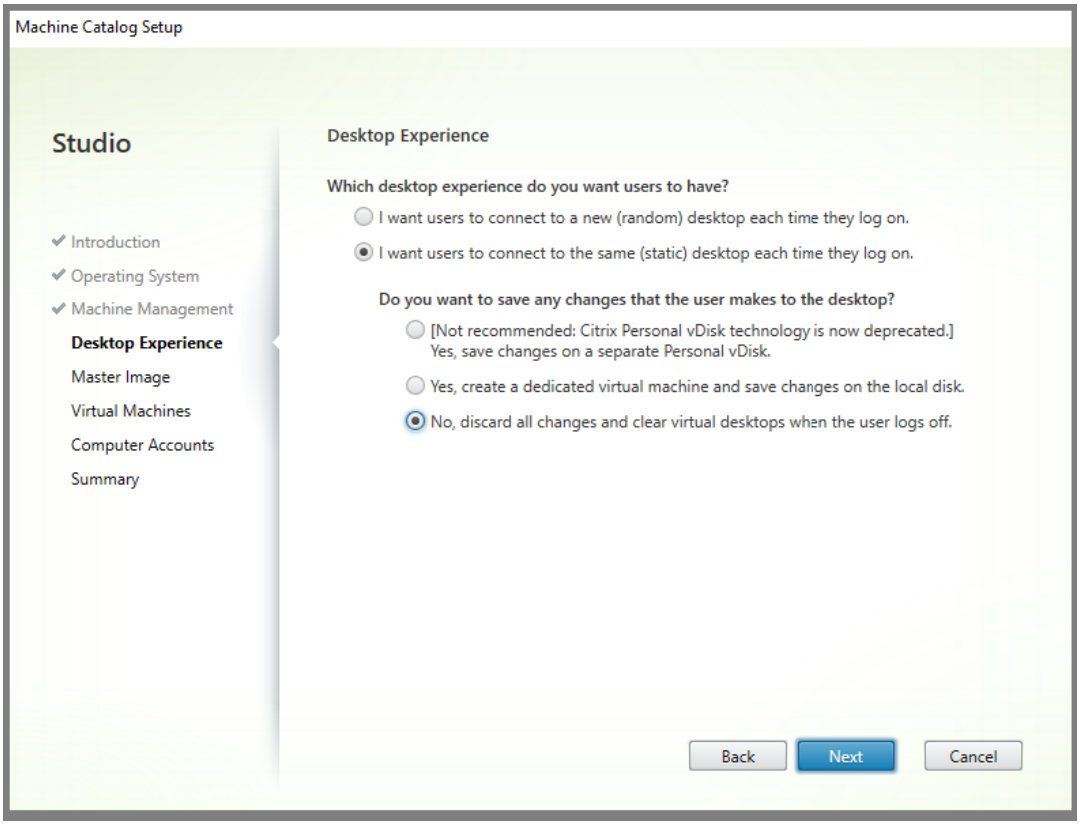
手順 **3**：マシンカタログの作成

Studio で、手順に従ってマシンカタログを作成します。カタログの作成時に次のオプションを使用します：

1. ［オペレーティングシステム］を選択して ［シングルセッション **OS**］に設定します。
2. ［マシン管理］を選択して ［電源管理されているマシン］に設定します。たとえば、仮想マシンまたはブレード PC などです。
3. ［デスクトップエクスペリエンス］を選択して、次の例のようにカタログの種類 **Pooled-random** または **Pooled-static** を選択します：
   - **Pooled-random**：



- **Pooled-static**：Pooled-static を選択する場合、デスクトップを構成して、以下のスクリーンショットのようにユーザーのログオフ時にすべての変更を破棄して仮想デスクトップを消去するようにします：



> 注:
>
> ユーザー個人設定レイヤーは、Citrix Personal vDisk を使用するように構成された、または専用仮想マシンとして割り当てられた Pooled-static カタログをサポートしていません。

4. MCS を使用している場合、マスターイメージと前述のセクションで作成されたイメージのスナップショットを選択します。
5. 環境で必要な場合、残りのカタログプロパティを構成します。

手順 **4**: デリバリーグループの作成

作成したマシンカタログのマシンも含めて、デリバリーグループを作成して構成します。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。

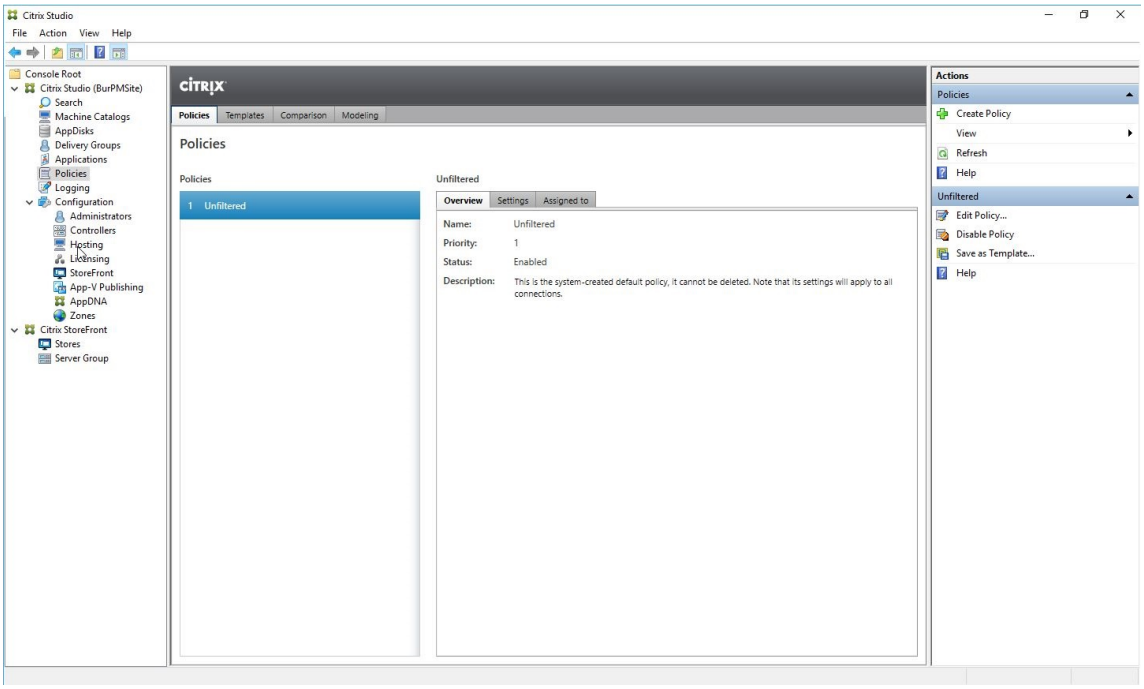
手順 **5:** デリバリーグループのカスタムポリシーの作成

Virtual Delivery Agent 内のユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します:

- ユーザーレイヤーにアクセスするネットワーク上の場所。
- ユーザーレイヤーディスクの拡大上限。

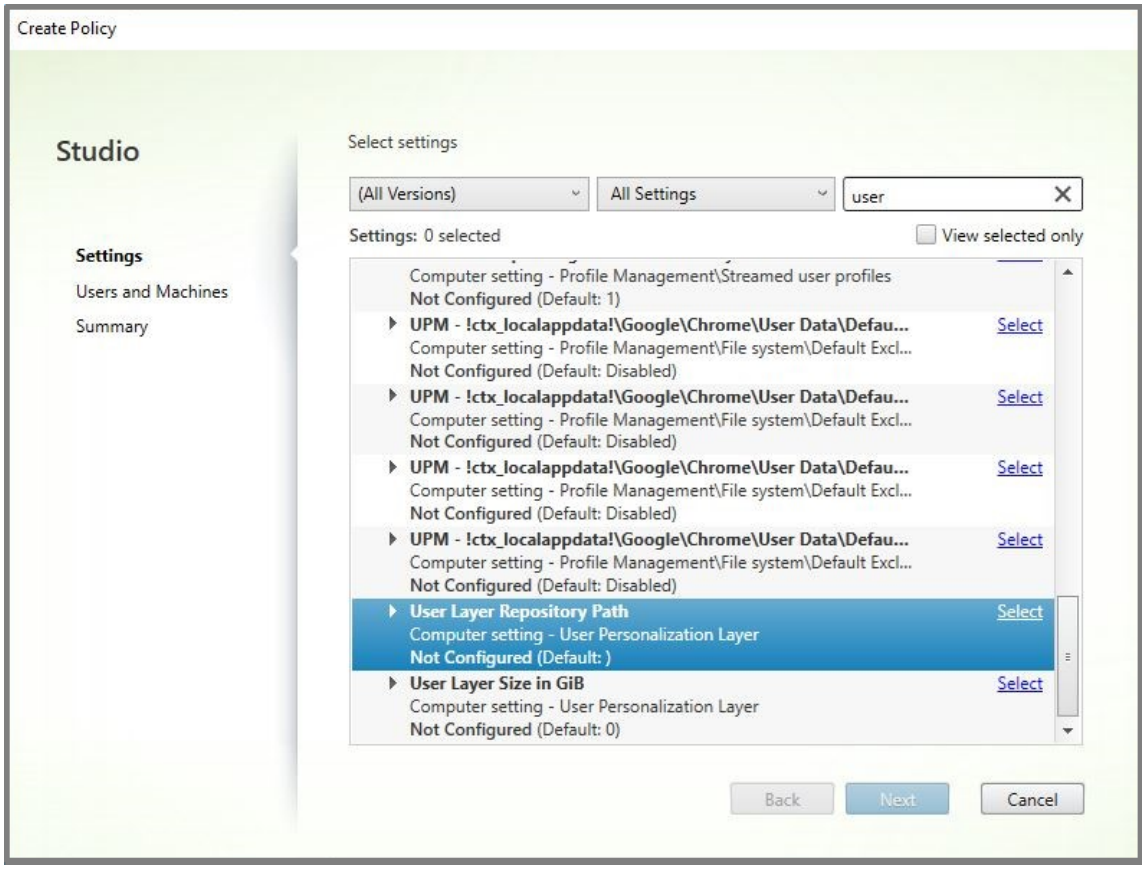
次の手順では、Studio でパラメーターをカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てる方法を説明します。

1. Studio のナビゲーションペインで［ポリシー］を選択します:

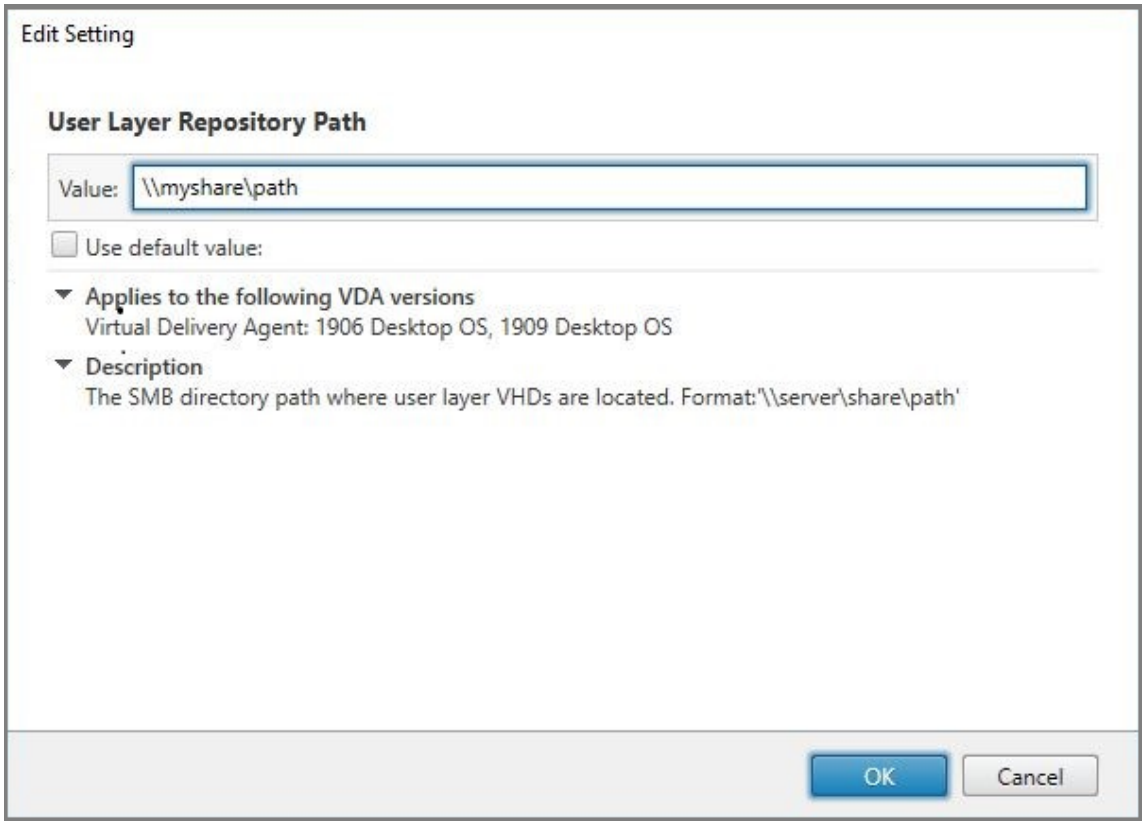


2. ［操作］ペインの［ポリシーの作成］を選択します。［ポリシーの作成］ウィンドウが開きます。
3. 検索フィールドに「ユーザーレイヤー」と入力します。次の 2 つのポリシーが利用可能なポリシーの一覧に表示されます:
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ GB

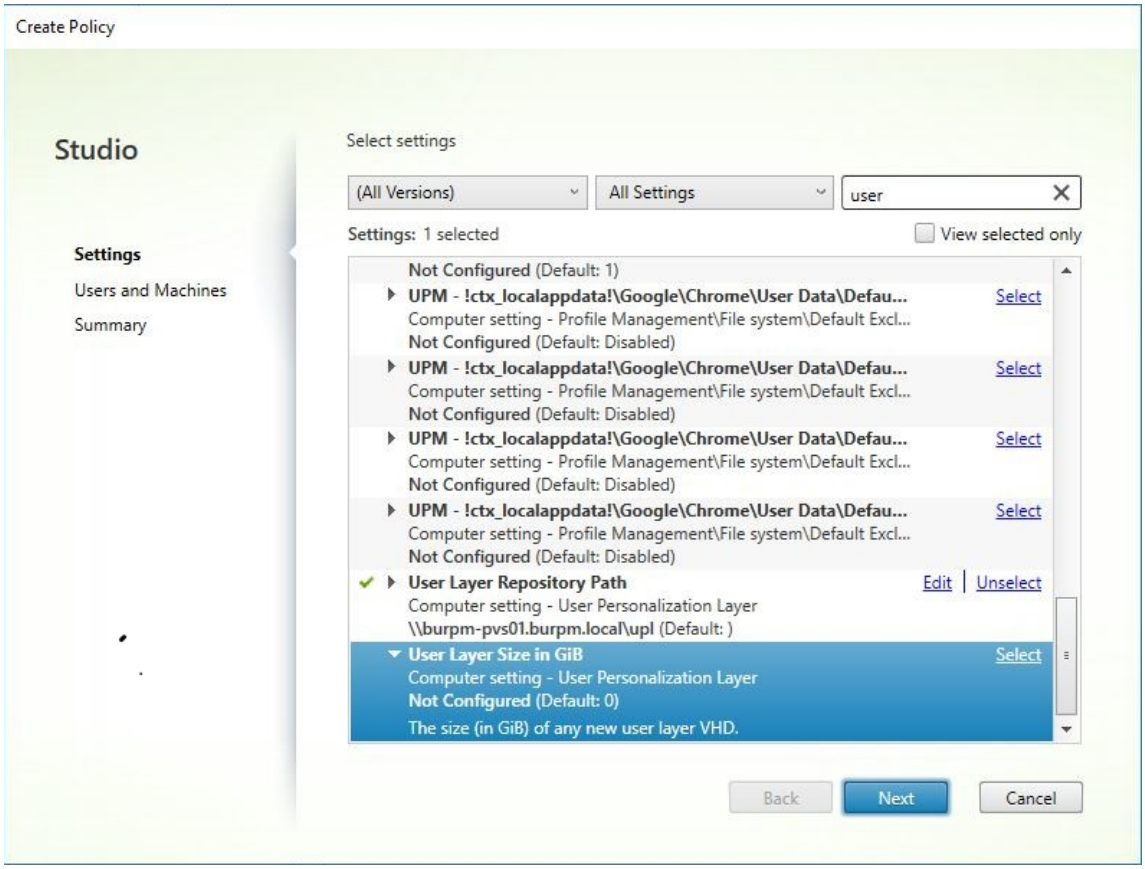
   > 注:
   >
   > ポリシーでユーザーレイヤーサイズを変更しても、既存のレイヤーのサイズは変更されません。
4. ユーザーレイヤーパスの横の ［選択］をクリックします。［設定の編集］ウィンドウが開きます。



5. 値フィールドに`\\server name or address\folder name`の形式でパスを入力し、[**OK**]をクリックします:



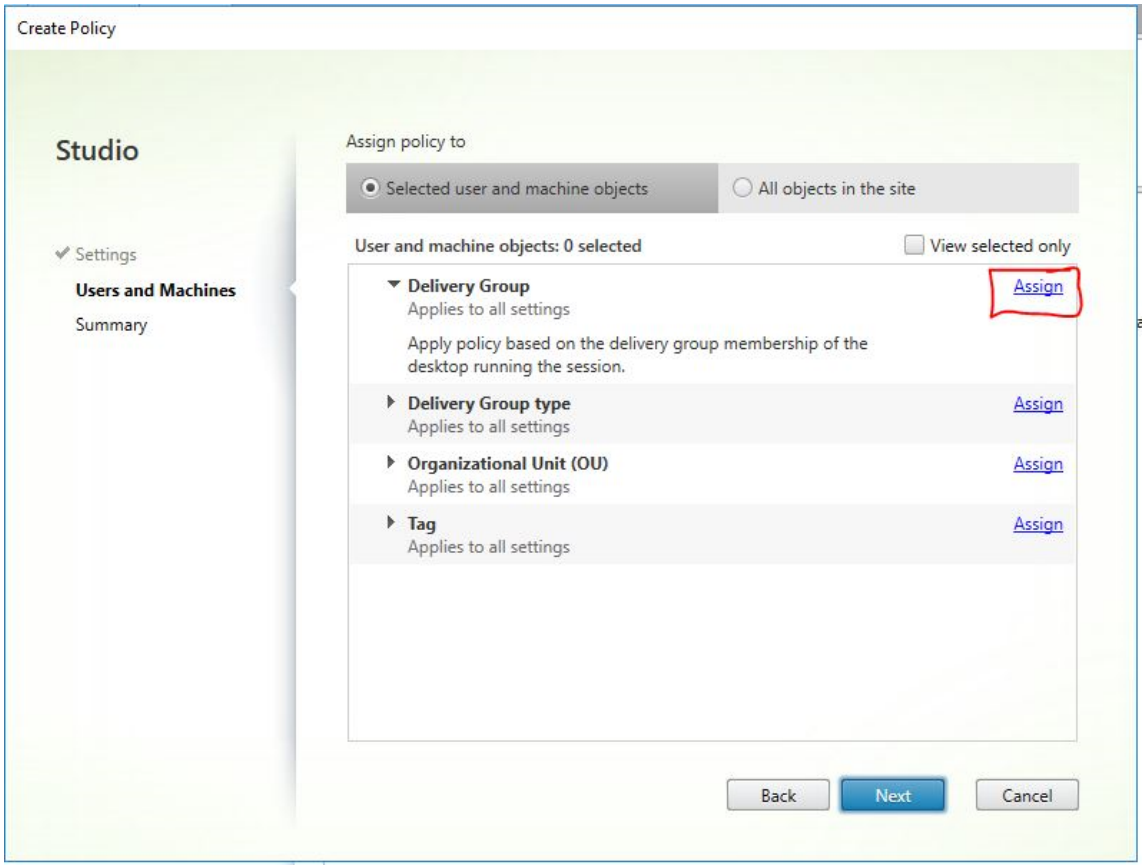
6. オプション：ユーザーレイヤーサイズ（GB）の横の ［選択］をクリックします：



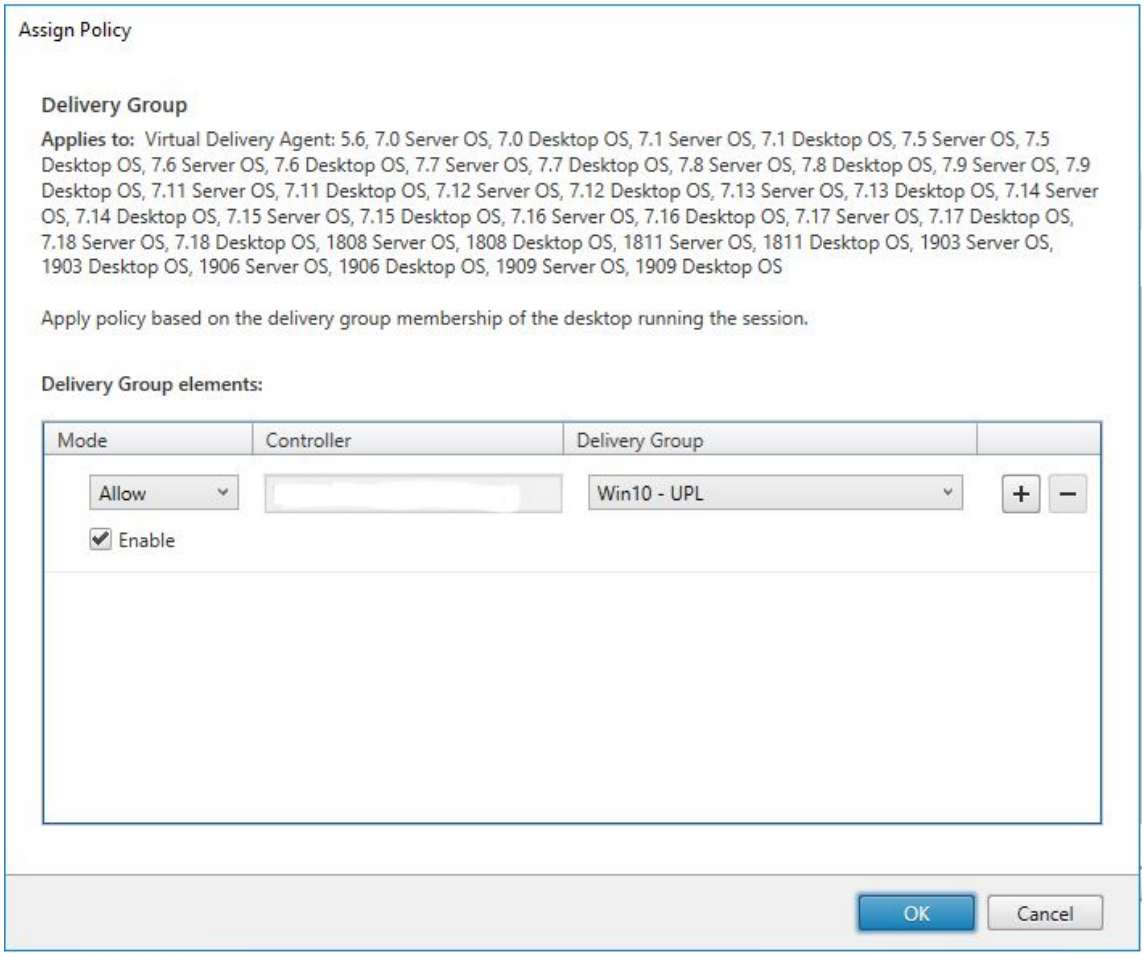
7. ［設定の編集］ウィンドウが開きます。
8. オプション：デフォルト値の 0 からユーザーレイヤーが拡大できる最大サイズ（GB）に変更します。［OK］をクリックします。

   > 注：
   >
   > デフォルト値を保持する場合、最大ユーザーレイヤーサイズは 10GB です。

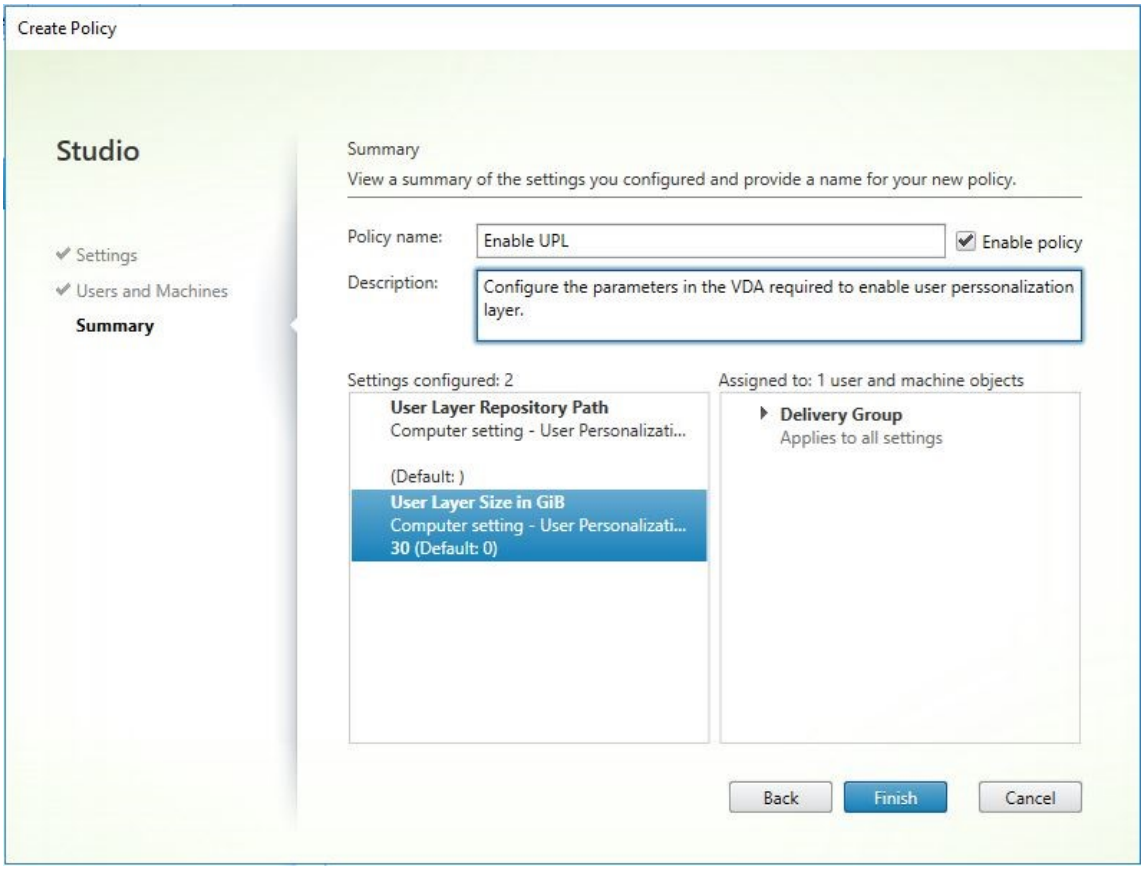
9. ［次へ］をクリックして、ユーザーとマシンを構成します。この画像で強調表示されている［デリバリーグループ割り当て］リンクをクリックします。



10. ［デリバリーグループ］メニューで、前のセクションで作成したデリバリーグループを選択します。［OK］をクリックします。



11. ポリシーの名前を入力します。チェックボックスをクリックしてポリシーを有効にし、［完了］をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定の構成

ドメイン管理者は、ユーザーレイヤーに複数のストレージの場所を指定できます。各ストレージの場所（デフォルトを含む）に対して、次の設定を使用して\Usersサブフォルダーを作成し、その場所を保護します。

設定名	値	適用先
作成所有者	変更	サブフォルダーおよびファイルのみ
所有者の権利	変更	サブフォルダーおよびファイルのみ
ユーザーまたはグループ:	フォルダーの作成/データの追加; フォルダーのスキャン/ファイルの実行; フォルダーの一覧/データの読み取り; 属性の読み取り	選択したフォルダーのみ
システム	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル

設定名	値	適用先
ドメイン管理者、および選択した管理者グループ	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、これらの通知メッセージのいずれかを受信します。

- 使用中のユーザーレイヤー

  ユーザーレイヤーは使用中のため、添付できませんでした。アプリケーションの設定やデータに加えた変更は保存されません。作業内容は必ず共有ネットワークの場所に保存してください。

- 利用できないユーザーレイヤー

  ユーザーレイヤーを添付できませんでした。アプリケーションの設定やデータに加えた変更は保存されません。作業内容は必ず共有ネットワークの場所に保存してください。

- ユーザーのサインアウト後にリセットされないシステム

  このシステムは適切にシャットダウンされませんでした。今すぐログオフしてシステム管理者に連絡してください。

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更が記録されたユーザー個人設定レイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
<!--NeedCopy-->
```

制限事項

ユーザー個人設定レイヤー機能をインストールして使用する場合、次の制限に留意してください。

- 永続マシンカタログを使用してユーザー個人設定レイヤー機能を構成しないでください。
- セッションホストは使用しないでください。
- (Windows 10 のバージョンが同じ場合であっても) 新しい OS インストールを実行しているイメージのマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用したものと同じマスターイメージ内の OS に更新を適用することです。
- 起動時ドライバー、または以前の起動用個人設定を使用しないでください。

- Personal vDisk データをユーザー個人設定レイヤーに移行しないでください。
- App Layering 完全製品から既存のユーザーレイヤーをユーザー個人設定レイヤーに移行しないでください。
- 別のマスター OS イメージを使用して作成されたユーザーレイヤーにアクセスするためにユーザーレイヤーの SMB パスを変更しないでください。
- ユーザー個人設定レイヤー仮想マシンでセキュアブートは現在サポートされていないため、有効にしないでください。
- Microsoft SCCM ソフトウェアセンターは、ユーザーレイヤーに以前にインストールされたアプリを使用不可として表示することがあります。この問題は、ユーザーがセッションからログアウトし、プール内の別のマシンのセッションに戻るときに発生します。この動作は、VDI 環境で実行される SCCM のプロパティです。ソフトウェアセンターは、ユーザーが現在のマシンにインストールしたアプリケーションのみを表示しますが、その他のアプリケーションはまだインストールされており、完全に機能しています。

  アプリケーションがインストールされていることを検証するために、ユーザーはソフトウェアセンターでアプリケーションを選択し［インストール］をクリックできます。アプリケーションがユーザーレイヤーに既にインストールされている場合、SCCM はステータスを「インストール済み」に更新し、インストールされたアプリケーションとともにアプリを一覧表示します。
- ソフトウェアセンターは、ユーザー個人設定レイヤー機能が有効になっている VDA 内で起動した直後に停止することがあります。この問題を回避するには、XenDesktop VDI 環境での SCCM の実装の Microsoft の推奨事項に従ってください。また、ソフトウェアセンターを開始する前に、ccmexec サービスが実行されていることを確認してください。
- グループポリシー（コンピューター構成）：ユーザーレイヤー設定は、マスターイメージに適用された設定を上書きします。したがって、GPO を使用して［コンピューターの設定］で行われた変更が、次のセッションログインまで保持されるとは限りません。

  この問題を回避するには、コマンドを発行するユーザーログオンスクリプトを作成します：

  ```
  gpupdate /force
  ```

  たとえば、ある顧客は各ユーザーログインで実行するように次のコマンドを設定します：

  ```
  gpudate /Target:Computer /force
  ```

  最適な結果を得るには、ユーザーのログイン後、ユーザーレイヤーで［コンピューターの設定］に直接変更を適用します。

Personal vDisk

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 2003 では、Personal vDisk 機能が削除されました。Citrix App Layering ユーザーレイヤー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。

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。

Personal vDisk 7.6.1 の新機能

このリリースには、以下の改善が含まれています。

- Personal vDisk のパフォーマンスが向上し、Personal vDisk カタログにイメージ更新を適用するときの時間が短くなりました。

このリリースでは、以下の問題が解決されています。

- 基本仮想マシン上の Microsoft Office 2010 を Microsoft Office 2013 にインプレースアップグレードすると、再構成のウィンドウが開いた後で「エラー 25004。入力したプロダクトキーは、このコンピューターでは使用できません」というエラーメッセージが表示されることがありました。これまでのリリースでは、基本仮想マシンから Office 2010 をアンインストールしてから Office 2013 をインストールすることでこのエラーを避けることができました。このリリースでは、Office 2010 をアンインストールせずにインプレースアップグレードできます（#391225）。
- ユーザーの Personal vDisk 上に新しいバージョンの Microsoft .NET が存在する場合、イメージの更新時に基本仮想マシン上の以前のバージョンで上書きされるという問題がありました。この問題により、新しいバージョンの.Net を使用する Personal vDisk 上のアプリケーション（Visual Studio など）が正しく動作しなくなることがありました（#439009）。
- Personal vDisk がインストールされ有効な Provisioning Services イメージディスクで Personal vDisk を使用しないマシンカタログを作成できないという制限事項がありました。このリリースでは、この制限事項はありません（#485189）。

Personal vDisk 7.6 について

Version 7.6 には、以下の新機能が追加されています。

- 拡張された Personal vDisk のエラー処理およびレポート。Personal vDisk が有効なマシンを Studio のマシンカタログで表示すると、［PvD］タブにイメージ更新時の監視状態や推定完了時間、および進行状況が表示されます。また、より詳細な状態情報が表示されるようになりました。
- 以前のバージョンで提供されていた Personal vDisk イメージ更新の監視ツール（Image Update Monitoring Tool）が、ISO イメージの ISO\Support\Tools\Scripts\PvdTool フォルダーに収録されています。以前のバージョンでも監視機能が提供されていましたが、このリリースではより高度なレポート機能が提供されます。

- Provisioning Services のテストモジュールを使用すると、テストカタログ内の更新済みイメージでマシンを起動できます。起動したマシンの安定性を確認した後で、テスト用の Personal vDisk を実稼働用に昇格させることができます。
- インベントリ実行時に、（Personal vDisk デスクトップ単位ではなく）2 つのインベントリの相違を計算できるようになりました。新しく追加されたコマンドを使用して、MCS カタログの既存のインベントリをエクスポートしてインポートできます。（Provisioning Services のマスター vDisk の場合は、以前のインベントリが既に含まれています。）

Version 7.1.3 で確認され Version 7.6 で解決された問題は以下のとおりです。

- Personal vDisk のアップグレードを中断すると、既存の Personal vDisk が破損することがありました。[#424878]
- Personal vDisk を長時間実行して非ページメモリリークが発生すると、仮想デスクトップが応答不能になることがありました。[#473170]

Version 7.6 で新たに確認された問題は以下のとおりです：

- アンチウイルス製品をインストールすると、インベントリや更新に時間がかかる場合があります。CtxPvD.exe および CtxPvDSvc.exe をアンチウイルス製品の除外プロセスの一覧に追加すると、パフォーマンスを向上させることができます。これらのファイルは、C:\Program Files\Citrix\personal vDisk\bin にあります。[#326735]
- マスターイメージから継承されたファイル間のハードリンクは、Personal vDisk カタログで保持されません。[#368678]
- Personal vDisk マスターイメージ上の Office 2010 を Office 2013 にアップグレードすると、仮想マシン上での Office の起動に失敗することがあります。これは、アップグレード時に Office KMS ライセンスプロダクトキーが削除されるために発生します。この問題を回避するには、マスターイメージ上で Office 2010 をアンインストールしてから Office 2013 を再インストールしてください。[#391225]
- Personal vDisk カタログは VMware Paravirtual SCSI（PVSCSI）コントローラーをサポートしません。デフォルトのコントローラーを使用してください。[#394039]
- Personal vDisk Version 5.6.0 を使用する仮想デスクトップでユーザーが作成したファイルが、Personal vDisk Version 7 へのアップグレード後に消失することがあります。この問題は、プールされた仮想マシンにログオンしたときに新しいユーザープロファイルが作成されるために発生します。現在、この問題を回避する方法はありません。[#392459]
- Windows 7 を実行する Personal vDisk で Windows システム保護機能が有効な場合、バックアップと復元機能を使用できません。システム保護を無効にするとユーザープロファイルがバックアップされますが、userdata.v2.vhd ファイルは除外されます。システム保護を無効にしてバックアップと復元機能を使ってユーザープロファイルのバックアップを作成することをお勧めします。[#360582]
- ディスクの管理ツールを使用して基本仮想マシン上で VHD ファイルを作成する場合、VHD をマウントできないことがあります。この問題を解決するには、Personal vDisk ボリュームに VHD をコピーしてください。[#355576]
- Office 2010 ソフトウェアを削除しても、そのショートカットが仮想デスクトップから削除されません。ショートカットは手作業で削除してください。[#402889]

- Microsoft Hyper-V 環境で Personal vDisk を使用するマシンカタログを作成するときに、ローカルに格納されたマシンとクラスターの共有ボリューム（CSV）に格納された vDisk を指定すると、エラーが発生して処理に失敗します。この問題を回避するには、vDisk にほかのストレージを使用してください。[#423969]
- Provisioning Services を使用するマシンカタログの仮想デスクトップに初めてログオンする場合、（ctx-pvd.exe -s reset コマンドで）Personal vDisk がリセットされていると、デスクトップの再起動を求めるメッセージが表示されます。この場合、デスクトップを再起動する必要があります。この問題は初回ログオン時にのみ発生し、それ以降のログオン時に再起動は不要です。[#340186]
- .NET 4.5 を Personal vDisk にインストールした後で、イメージの更新により.NET 4.0 をインストールまたは修正すると、.NET 4.5 に依存するアプリケーションを実行できなくなります。この問題を回避するには、基本イメージに.NET 4.5 をインストールしてイメージを更新してください。
- XenApp/XenDesktop 7.6 の「既知の問題」のトピックも参照してください。

Personal vDisk 7.1.3 について

Version 7.1.1 で確認され Version 7.1.3 で解決された問題は以下のとおりです：

- Personal vDisk 5.6.0 から Personal vDisk 7.x への直接アップグレードにより、Personal vDisk に問題が発生することがありました。[#432992]
- Personal vDisk を使用する仮想デスクトップにユーザーが断続的に接続できなくなる場合がありました。[#437203]
- Personal vDisk 5.6.5 以降から Personal vDisk 7.0 以降へのアップグレード時に Personal vDisk のイメージ更新処理が中断されると、それ以降の更新処理に失敗することがありました。[#436145]

Personal vDisk 7.1.1 について

Version 7.1 で確認され Version 7.1.1 で解決された問題は以下のとおりです：

- イメージ更新を介して Symantec Endpoint Protection 12.1.3 を更新すると、symhelp.exe によりアンチウイルス定義の破損が報告されます。[#423429]
- サービスコントロールマネージャー（services.exe）がクラッシュすると、プールされたデスクトップが Personal vDisk により再起動されることがありました。[#0365351]

Version 7.1.1 で新たに確認された問題：ありません。

Personal vDisk 7.1 について

Version 7.1 には、以下の新機能が追加されています。

- Windows 8.1 を実行するデスクトップを備えた Personal vDisk を使用できるようになりました。また、イベントログ機能も向上しています。
- コピーオンライト（CoW）はサポートされなくなりました。Personal vDisk をバージョン 7.0 から 7.1 にアップグレードすると、CoW によって管理されたデータに対するすべての変更が失われます。これは

XenDesktop 7 の評価用機能であり、デフォルトでは無効になっていました。そのため、この機能を有効にしなかった場合には、特に影響を受けません。

Version 7.0.1 で確認され Version 7.1 で解決された問題は以下のとおりです。

- Personal vDisk レジストリキーの EnableProfileRedirection の値を 1 または ON に設定し、また後からイメージの更新中に値を 0 または OFF に変更すると、Personal vDisk スペース全体がユーザーによってインストールされたアプリケーションに割り当てられ、ユーザープロファイル用の領域がなくなって vDisk 上に残ることがありました。このプロファイルのリダイレクトがカタログに対して無効で、イメージの更新中にそれを有効にする場合、ユーザーは仮想デスクトップにログオンすることができないことがあります。[#381921]
- Personal vDisk のインベントリ更新に失敗すると、デスクトップサービスによって正確なエラーがイベントビューアーに記録されませんでした。[#383331]
- Personal vDisk 7.x にアップグレードするときに、変更済の規則が保持されないという問題がありました。この問題は、Version 7.0 から Version 7.1 へのアップグレードでは発生しません。ただし、Version 5.6.5 を Version 7.1 にアップグレードする場合は、最初に規則ファイルを保存し、次にアップグレードの後で規則を再度適用する必要があります。[#388664]
- Windows 8 が動作する Personal vDisk で、Windows ストアからアプケーションをインストールできないという問題がありました。この場合、「購入処理は完了できませんでした」という内容のエラーメッセージが表示されます。Windows Update サービスを有効にしてもこの問題は解決しませんでしたが、現在はこの問題が解決されています。ただし、ユーザーがインストールしたアプリケーションは、システムの再起動後に再インストールする必要があります。[#361513]
- Personal vDisk を使用する Windows 7 のプールされたデスクトップで、一部のシンボリックリンクが欠落するという問題がありました。この問題により、C:\Users\All Users にアイコンを格納するアプリケーションでは、［スタート］メニューにアイコンが表示されませんでした。[#418710]
- インベントリの更新後にシステムに多くの変更を追加すると、更新シーケンス番号（USN）ジャーナルオーバーフローが発生し、Personal vDisk が起動しないという問題がありました。[#369846]
- 状態コード 0x20 およびエラーコード 0x20000028 により、Personal vDisk が起動しませんでした。[#393627]
- Symantec Endpoint Protection 12.1.3 により「Proactive Threat Protection は誤動作しています」というメッセージが表示され、このコンポーネントの Live Update Status を使用できませんでした。[#390204]

バージョン 7.1 の新しい既知の問題：XenDesktop 7.1 リリースの既知の問題のドキュメントを参照してください。

Personal vDisk 7.0.1 について

Version 7.0.1 の新機能：環境の変更に対して Personal vDisk がより強固になりました。イメージ更新に失敗した場合でも Personal vDisk を伴う仮想デスクトップを Delivery Controller に登録できるようになっており、また安全でないシステムシャットダウンにより vDisk が使用不可となってしまうことがなくなりました。さらに、規則ファイルを使用することで、展開時に vDisk からファイルやフォルダーを除外できるようになりました。

Version 5.6.13 で確認され Version 7.0.1 で解決された問題は以下のとおりです：

- プールされた仮想デスクトップ上でのユーザーによるグループのメンバーシップの変更内容が、イメージの更新後に失われることがありました。[#286227]
- Personal vDisk に十分な領域がある場合でも、イメージ更新がディスク容量不足によるエラーで失敗することがありました。[#325125]
- 一部のアプリケーションで仮想デスクトップの Personal vDisk へのインストールに失敗し、再起動を求めるメッセージが表示されることがありました。これは、保留中の名前変更操作によるものです。[#351520]
- マスターイメージ内で作成されたシンボリックリンクが、Personal vDisk を使用する仮想デスクトップで正しく機能しないという問題がありました。[#352585]
- Citrix Profile management と Personal vDisk を使用する環境では、プロファイルのリダイレクトが有効な場合にシステムボリューム上でユーザープロファイルを調査するアプリケーションは正常に機能しないことがありました。[#353661]
- インベントリのサイズが 2GB を超える場合に、マスターイメージ上でのインベントリの更新に失敗するという問題がありました。[#359768]
- イメージの更新がエラーコード 112 により失敗し、Personal vDisk が破損することがありました。この問題は、更新に必要な空き領域が vDisk にある場合でも発生します。[#363003]
- カタログのデスクトップ数が 250 を超える場合に、サイズ変更スクリプトの処理が失敗するという問題がありました。[#363365]
- ユーザーによる環境変数に対する変更が、イメージの更新時に失われることがありました。[#372295]
- Personal vDisk を使用する仮想デスクトップ上で作成されたローカルユーザーが、イメージ更新時に失われるという問題がありました。[#377964]
- インベントリの更新後にシステムに多くの変更を追加すると、更新シーケンス番号（USN）ジャーナルオーバーフローが発生し、Personal vDisk の起動に失敗するという問題がありました。この問題を避けるには、USN ジャーナルのサイズをマスターイメージ内で 32 MB 以上に増やして、イメージ更新を実行します。[#369846]
- Personal vDisk で AppSense Environment Manager を置き換えモードで使用する場合、レジストリハイブが正しく処理されないという問題が確認されています。これは、Personal vDisk がインストールされるときの RegRestoreKey API の動作に関連しています。Citrix と AppSense は共同でこの問題の解決にあたっています。[#0353936]

バージョンに依存しない既知の問題

- マスターイメージ上で Windows ストアとメトロアプリケーションが更新されると、vDisk がテストまたは実稼働にアップグレードされた後、PvD が有効なターゲットデバイスの競合が発生する可能性があります。さらに、アプリケーションイベントログエラーをトリガしている間に、Metro Apps の起動に失敗することがあります。PvD が有効なターゲットデバイスに対して Windows ストアと Metro アプリケーションを無効にすることをお勧めします。
- Personal vDisk 上にインストールされたアプリケーションがマスターイメージ上にインストールされた同一バージョンのアプリケーションと関連付けられている場合、イメージの更新後に Personal vDisk 上のアプリケーションが動作しなくなることがあります。この問題は、マスターイメージ上のアプリケーションをアンイ

ンストールしたりアップグレードしたりしたために、Personal vDisk 上のアプリケーションで必要なファイルがマスターイメージから削除されると発生します。この問題を回避するには、マスターイメージ上のアプリケーションを保持しておきます。

たとえば、マスターイメージ上に Office 2007 をインストールして、Personal vDisk 上に Visio 2007 をインストールします。その後で管理者がマスターイメージ上の Office 2007 を Office 2010 にアップグレードして、そのイメージを使用してマシンを更新すると、Visio 2007 が動作しなくなります。この問題を避けるには、Office 2007 をマスターイメージ上にインストールしたままにしておきます。[#320915]

- Personal vDisk を使用するデスクトップに McAfee Virus Scan Enterprise（VSE）を展開する場合は、マスターイメージ上に Version 8.8 Patch 4 以降をインストールしてください。[#303472]
- マスターイメージ内で作成されたファイルのショートカットが動作しなくなった場合（そのショートカットのリンク先の名前が Personal vDisk 内で変更された場合など）は、ショートカットを作成し直してください。[#367602]
- マスターイメージ内で絶対/ハードリンクを使用しないでください。[#368678]
- Windows 7 のバックアップと復元機能は、Personal vDisk でサポートされていません。[#360582]
- 更新したマスターイメージを適用した後で、ローカルユーザーおよびグループのコンソールがアクセス不能になったり不正なデータが表示されたりすることがあります。この問題を解決するには、仮想マシン上でユーザーアカウントをリセットします。これを行うには、セキュリティハイブのリセットが必要です。この問題は Version 7.1.2 で解決されており、Version 7.1.2 以降で作成された仮想マシンは正しく処理されます。ただし、アップグレード前に作成された仮想マシンでの問題は解決されません。[#488044]
- ESX ハイパーバイザー環境でプールされた仮想マシンを使用する場合、SCSI コントローラーの種類として［VMware Paravirtual］を選択すると再起動を確認するメッセージがユーザーに表示されます。この問題を避けるには、SCSI コントローラーの種類として LSI を使用してください。[#394039]
- Provisioning Services で作成されたデスクトップ上で Personal vDisk をリセットすると、ログオンしたユーザーに再起動を確認するメッセージが表示されることがあります。この問題が発生した場合は、デスクトップを再起動してください。[#340186]
- Windows 8.1 のデスクトップを使用するユーザーが Personal vDisk にログオンできなくなることがあります。この問題が発生すると、「システムが正しくシャットダウンされなかったため Personal vDisk が無効になっています」というメッセージが管理者に表示され、PvDActivation.log に「Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]」というメッセージが記録されます。この問題は、ユーザーの仮想マシンを正しくシャットダウンできなかった場合に発生します。この問題を解決するには、Personal vDisk をリセットしてください。[#474071]

インストールとアップグレード

April 26, 2021

Personal vDisk 7.x は、現在のバージョンの Citrix Virtual Apps and Desktops（および XenDesktop 5.6 以降）でサポートされます。各バージョンの「システム要件」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、およびサポートされるホスト（仮想化リソース）と Citrix Provisioning（旧称 Provisioning Services）のバージョンについて確認してください。Citrix Provisioning のタスクについて詳しくは、最新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、「VDA のインストール」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、Citrix Virtual Apps and Desktops のインストールメディアで提供される Personal vDisk の MSI ファイルを使用してください。

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。
- Citrix Provisioning 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 Citrix Virtual Desktops で提供されるバージョン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

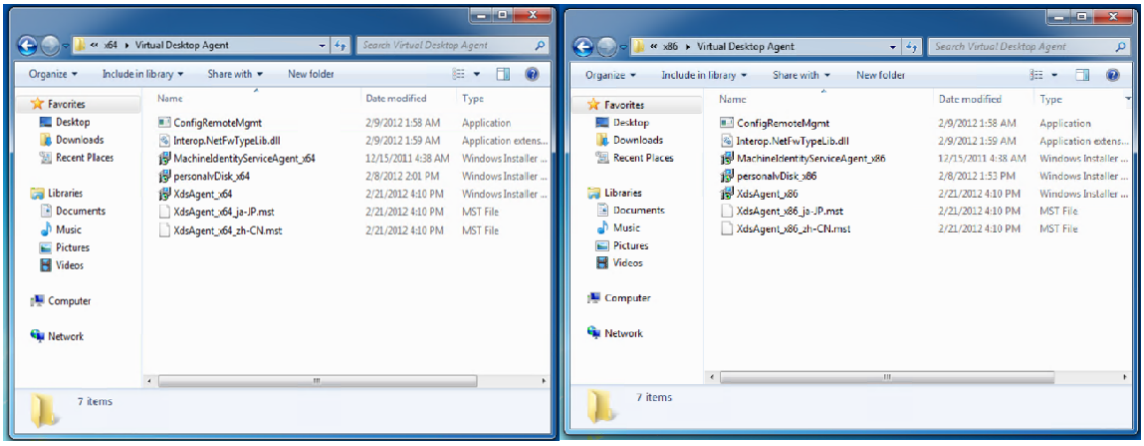
Personal vDisk ソフトウェアをアンインストールするには、以下のいずれかの方法を使用します:

- 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。

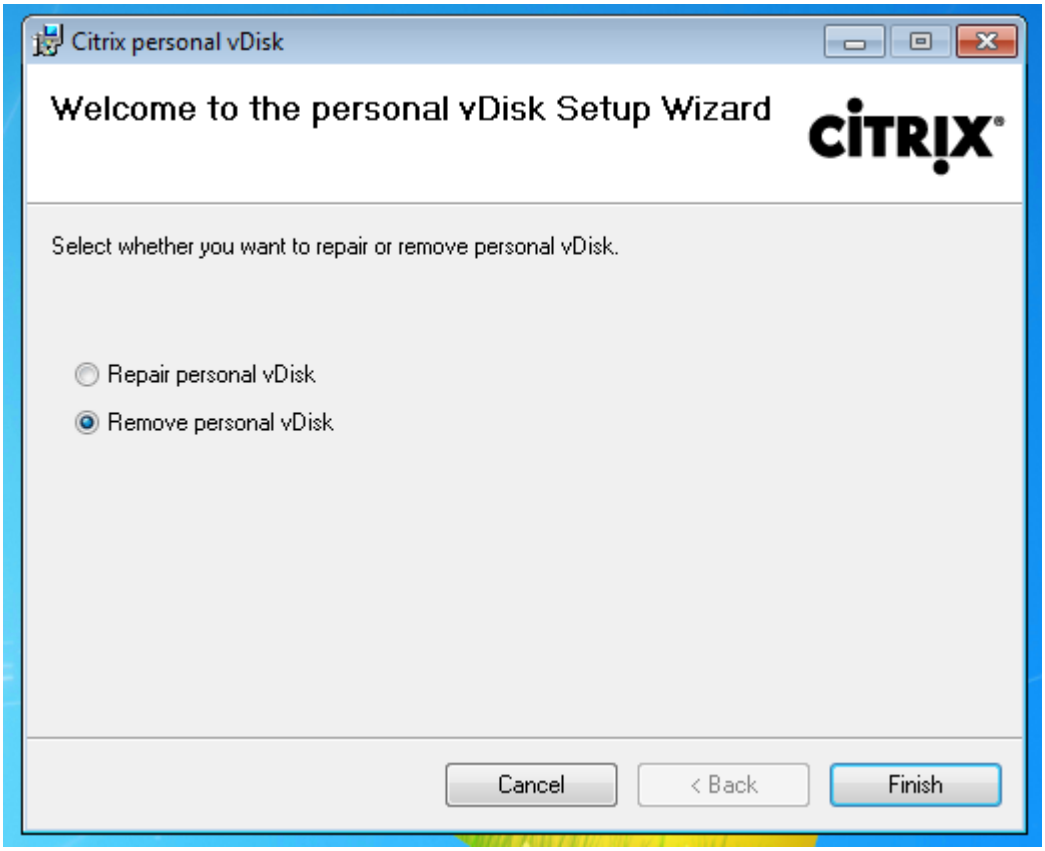
Personal vDisk をアンインストールして同じまたは新しいバージョンを再インストールする場合は、事前にレジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\personal vDisk\config をバックアップしておいてください。このレジストリキーには、変更された環境構成設定が含まれています。Personal vDisk を再インストールしたら、バックアップしたレジストリ情報を使用して、必要に応じて値を変更してください。

Personal vDisk 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。

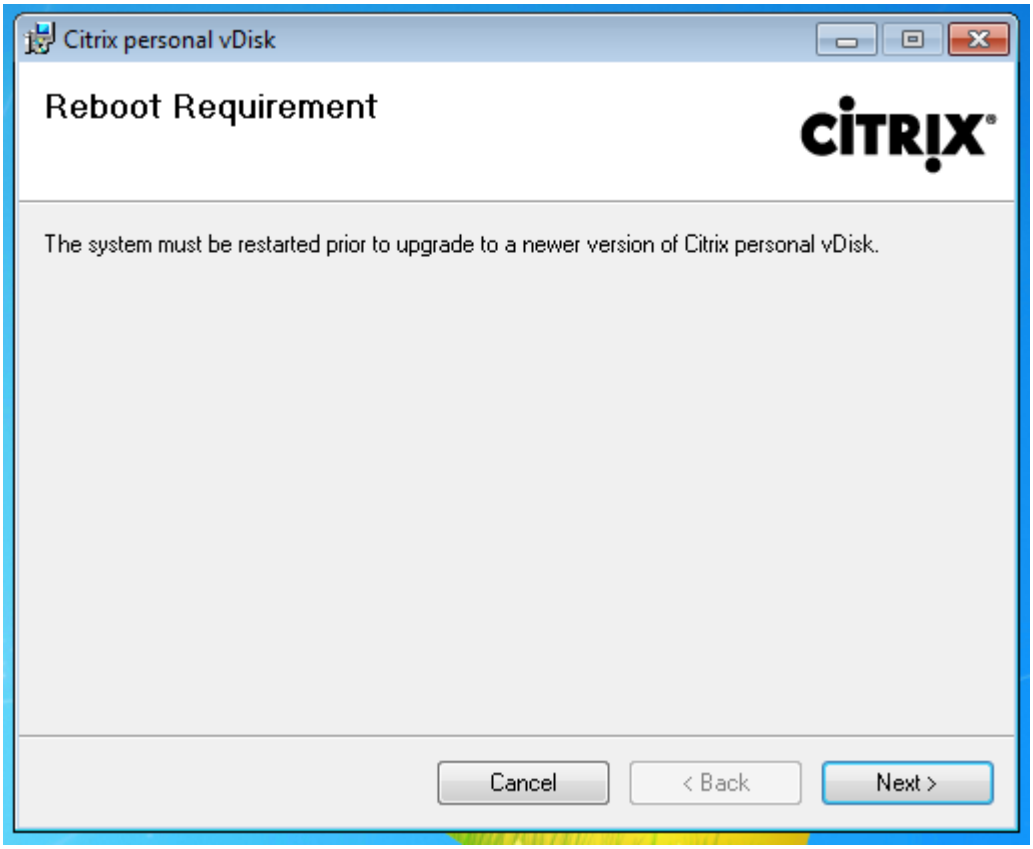
1. Citrix Virtual Apps and Desktops メディアで、vDisk インストーラーの適切なコピーを選択します。次のいずれかの場所（アップグレードされた仮想マシンが 32 ビットか 64 ビットかによる）にある最新の Personal vDisk の MSI インストーラーを見つけます:
   - 32 ビット: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
   - 64 ビット: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



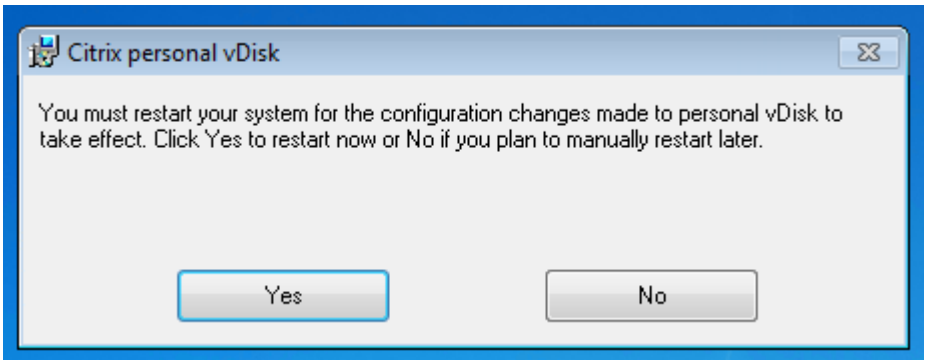
2. 既存の Personal vDisk インストールを削除します。手順 1 で見つけた Personal vDisk の MSI インストーラーパッケージを選択します。Personal vDisk のセットアップ画面が開きます。
3. [**Remove personal vDisk**] を選択します。
4. [完了] をクリックします。



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

June 7, 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、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。

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（Citrix Virtual Apps and Desktops 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では、この指定は委任管理により行われます。

そのほかの設定:

- **Windows Update** サービス: マスターイメージでは、Windows を［更新プログラムを確認しない］に構成し、Windows Update サービスを［無効］に設定します。また、Windows ストアと Metro App のアップデートと機能を無効にすることをお勧めします。
- **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 Workspace アプリなど）
- 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：Citrix Provisioning

Citrix Provisioning と Personal vDisk を併用する場合、以下の点を考慮してください：

- 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、Citrix Provisioning 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、Citrix Provisioning 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、Citrix Provisioning 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 Citrix Provisioning 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、Citrix Provisioning 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、Citrix Provisioning の書き込みキャッシュディスクのサイズが小さいと、Personal vDisk がアクティブでないとき（イメージ更新時など）にキャッシュディスクの空きが足りなくなり、マシンがクラッシュすることがあります。

Citrix Provisioning のベストプラクティスに従って Citrix Provisioning 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 Citrix Provisioning で展開する場合は、以下の点に注意してください：

- Citrix Provisioningのドキュメントの手順に従ってください。
- 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、Citrix Provisioning 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。

Citrix Provisioning 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。

- 製品ドキュメントの手順に従ってください。
- 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。
- PVD と MCS IO キャッシュの選択は、相互に排他的です。PVD をインストールすると、MCS IO キャッシュが有効になっているカタログを作成できなくなります。

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操作］の値を変更します（ほかのすべての設定値はそのまま保持します）。
   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

June 7, 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、Citrix Virtual Apps and Desktops 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。

- 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。

インポートするには:

マスターイメージ上で、管理者として次のインポートコマンドを実行します。

```
Ctxpvdsvc.exe importinventory “<path-to-exported-inventory>”
```

<path to exported inventory>には、インベントリーファイルのフルパスを指定します。通常は、<network location\ExportedPvdInventory> です。

exportinventory オプションでエクスポートされたインベントリが取得され、それがマスターイメージ上のインベントリストアにインポートされます。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

April 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、2 つのファイル：`Software.Dat.Report.txt`と`Software.Dat.delta.txt`を生成します。

`Software.Dat.Report.txt`ファイルには、HKEY_LOCAL_MACHINE\Software ハイブに対してユーザーが行った変更が記録されます。以下のセクションがあります：

- List of Applications installed on the base：レイヤー 0 にインストールされたアプリケーション
- List of user installed software：Personal vDisk のアプリケーション領域にユーザーがインストールしたアプリケーション
- List of software uninstalled by user：レイヤー 0 からユーザーが削除したアプリケーション

Software.Dat.delta.txt に記録される情報については、この表の「ハイブデルタレポート」を参照してください。

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 の UserData.V2.vhd に格納されます。正常な Personal vDisk マシンから「VER-LAST」フォルダーをインポートして、マスターイメージの最終バージョンに相当するインベントリを復元してください。

- 前のバージョンのマスターイメージに対応している **Personal vDisk** 上のインベントリは、より新しいバージョンです。

エラーコードは、4 です。前回のマスターイメージと新しいマスターイメージで Personal vDisk のバージョンが異なるとこの問題が発生します。マスターイメージに最新バージョンの Personal vDisk をインストールしてからカタログ更新を再試行してください。

- 変更ジャーナルのオーバーフローが検出されました。

  エラーコードは、5 です。インベントリ作成時にマスターイメージに加えられた変更の数が多いと、USN ジャーナルのオーバーフローが発生します。何回か再試行してもこのエラーが発生する場合は、procmon を使用して、インベントリ作成時にサードパーティソフトウェアが大量のファイルを作成したり削除したりしていないかどうかを確認してください。

- **Personal vDisk** で、ユーザーデータの格納用にシステムにアタッチされたディスクが見つかりません。

  エラーコードは、6 です。まず、ハイパーバイザーのコンソールで Personal vDisk 用のディスクが仮想マシンにアタッチ（接続）されていることを確認してください。一般的に、このエラーはデータの漏洩を防ぐソフトウェアにより Personal vDisk 用ディスクへのアクセスが阻止されると発生します。Personal vDisk 用のディスクが仮想マシンにアタッチされている場合は、データ漏洩を防ぐソフトウェアにそのディスクに対する除外規則を追加してください。

- インストール後にシステムが再起動されていません。変更内容を実装するために再起動してください。

  エラーコードは、7 です。デスクトップを再起動してから再試行してください。

- インストールが破損しています。**Personal vDisk** を再インストールしてください。

  エラーコードは、8 です。Personal vDisk を再インストールしてから再試行してください。

- **Personal vDisk** のインベントリが最新の状態ではありません。マスターイメージ内でインベントリを更新してから再試行してください。

  エラーコードは、9 です。デスクトップのシャットダウン前にマスターイメージ内で Personal vDisk インベントリが更新されていないとこのエラーが発生します。マスターイメージを再起動して、[Personal vDisk の更新] オプションを使用してデスクトップをシャットダウンし、その後で新しいスナップショットを作成してください。このスナップショットを使用してカタログを更新します。

- **Personal vDisk** の起動時に内部エラーが発生しました。詳しくは、**Personal vDisk** のログを参照してください。

  エラーコードは、10 です。このエラーは、内部エラーまたは Personal vDisk の破損により、Personal vDisk ドライバーで仮想化セッションの起動に失敗すると発生します。Controller を介してデスクトップを再起動してください。引き続き問題が発生する場合は、ログファイルを収集して Citrix のサポート担当者に問い合わせてください。

- ユーザーのパーソナル設定を格納するディスクの検索時に **Personal vDisk** でタイムアウトが発生しました。

  エラーコードは、11 です。このエラーは、再起動後 30 秒以内に Personal vDisk ドライバーで Personal vDisk 用のディスクを検出できない場合に発生します。通常、サポートされない種類の SCSI コントローラーを使用したり、ストレージで遅延が発生したりすると検出に失敗します。マシンカタログ内のすべてのデスク

トップでこのエラーが発生する場合は、テンプレート仮想マシンやマスター仮想マシンの SCSI コントローラーの種類を Personal vDisk でサポートされるものに変更してください。このエラーがマシンカタログ内の一部のデスクトップのみで発生する場合は、多くのデスクトップの同時起動などで一時的にストレージに遅延が発生していることが考えられます。ホスト接続の設定で、最大電源操作数を制限することを検討してください。

- システムが正しくシャットダウンされなかったため **Personal vDisk** が無効になっています。マシンを再起動してください。

  エラーコードは、12 です。このエラーは、Personal vDisk が有効なデスクトップで起動プロセスを完了できない場合に発生します。デスクトップを再起動してください。問題が解決しない場合は、ハイパーバイザーのコンソールでデスクトップの起動状況を監視して、デスクトップがクラッシュしているかどうかを確認します。デスクトップが起動中にクラッシュする場合は、バックアップ（バックアップがある場合）から Personal vDisk を復元するか、Personal vDisk をリセットしてください。

- **Personal vDisk** をマウントするためのドライブ文字を使用できません。

  エラーコードは、13 です。このエラーは、管理者により指定されたマウントポイントに Personal vDisk 用のディスクをマウントできない場合に発生します。指定されたドライブ文字がほかのハードウェアにより使用されていると、Personal vDisk 用ディスクのマウントに失敗します。Personal vDisk 用にほかのマウントポイントを指定してください。

- **Personal vDisk** カーネルモードドライバ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。

PvD から App Layering への移行

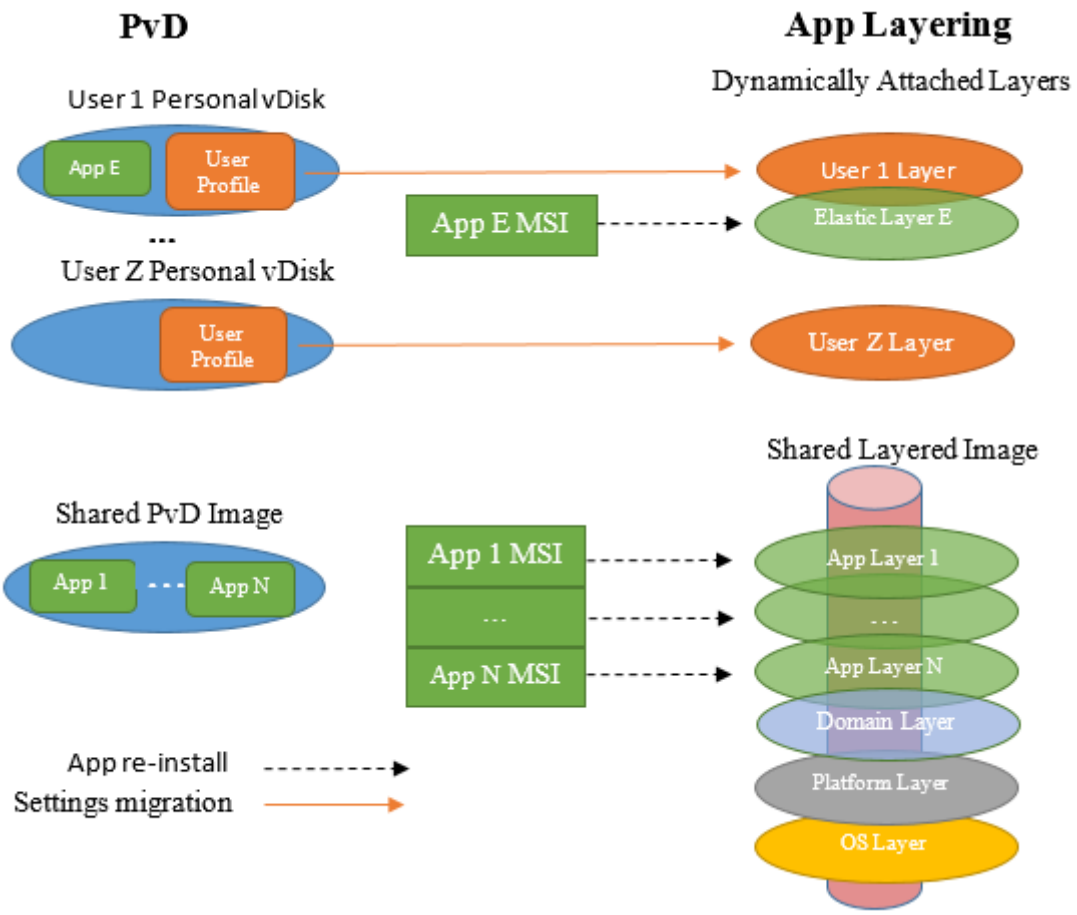
April 26, 2021

Citrix は Personal vDisk（PvD）機能を Citrix App Layering テクノロジに置き換えつつあります。PvD ベースの VM と機能的に同等な App Laying VM を作成するには、この記事の情報に従ってください。

レイヤー、およびイメージテンプレートの作成と発行のプロセスについては、Citrix App Layeringのドキュメントを参照してください。

一般的な PvD VM は、共有イメージと Personal vDisk で構成されています。共有イメージが複数のユーザーに分散され、各ユーザーにはユーザー固有の Personal vDisk が割り当てられます。一般的な App Laying VM は複数のレイヤー（OS、プラットフォーム、通常は 1 つ以上のアプリケーションレイヤーなど）で構成されています。この VM を複数のユーザーによって共有し、各ユーザーにそれぞれのユーザーレイヤーが割り当てられます。

PvD イメージ VM を共有する複数のユーザーを移行すると、機能的に同等の Application Layering 共有イメージ VM が作成されます。各ユーザーは、以下の図に示すように、Personal vDisk から新しい App Layering ユーザーレイヤーに移行された個人用のプロファイルと設定を持ちます。



この記事では、ユーザーの個人データの移行とアプリケーションの移行のそれぞれに対して異なるアプローチを取っています。個人データについては、この記事では、Personal vDisk からユーザーレイヤーにデータをコピーするツールを推奨しています。アプリケーションについては、コピーすることはお勧めしません。代わりに、アプリケーションレイヤーに個人データを再インストールすることをお勧めします。また、この記事では以下のことを前提としています:

- PvD VM で Windows 7 が実行されている。他の OS バージョンの移行は、App Layering でサポートされている OS バージョンであれば同様です。たとえば、App Laying では Windows XP はサポートされていません。
- Citrix Hypervisor がハイパーバイザーとして使用されていて、管理者は XenCenter を使用して Citrix Hypervisor を管理することに慣れている。
- マシンカタログサービス（MCS）または Citrix Provisioning（旧称 Provisioning Services）をプロビジョニングに使用している。MCS または Citrix Provisioning を使用するには、Citrix Virtual Apps and Desktops ISO が必要です。Citrix Provisioning を使用する場合は、「ProvisioningServicesxxx.iso」も必要です。

- 生成した App Laying VM を、Citrix Virtual Desktops を使用して管理している。

別のハイパーバイザーやプロビジョニングサービスを使用している場合でも、この記事に記載されている移行手順と類似しています。

この記事の例では、ユーザーが Active Directory（AD）ドメインのメンバーであることを前提としています。

PvD と **App Layering** の比較

App Layering では、ユーザー固有の情報とアプリケーションとを完全に分離するためのものです。アプリケーションはアプリケーションレイヤーに配置され（たいていはレイヤーごとに 1 つのアプリケーション）、ユーザー固有の情報はユーザーレイヤーに配置されます。ベストプラクティスとして、ユーザーは、一般的なユーティリティを持つ可能性があると考えられるアプリケーションをユーザーレイヤーにインストールしてはいけません。代わりに、そのアプリケーションを Elastic アプリケーションレイヤーにインストールします。Elastic アプリケーションレイヤーは、ログイン時にそのユーザー（および他のユーザー）の VM に動的に接続されます。

PvD では、複数のユーザーによって共有される共有イメージと、ユーザー固有の vDisk の 2 つのレイヤーしかないため、このような完全な分離はサポートされていません。共有イメージで利用できなかった場合に、ユーザーが自分の vDisk にアプリケーションをインストールすることがよくあります。

共有 PvD イメージを App Layering に移行する際に、共有 PvD イメージに含まれているすべてのアプリケーションを判別する必要があります。各アプリケーション（または関連する一連のアプリケーション）につきアプリケーションレイヤーを 1 つ作成します。以下に注意してください：

- アプリケーションに一般的なユーティリティがある場合は、アプリケーションレイヤーをイメージテンプレートに接続して、レイヤー化イメージで公開します。
- アプリケーションに少数のユーザーグループに対するユーティリティがある場合は、そのグループに割り当てます。そのグループのメンバーが VM にログインすると、そのアプリケーションが Elastic アプリケーションレイヤーとして動的に接続されます。
- アプリケーションで 1 人のユーザーに対してのみ特定の値が設定されている場合は、アプリケーションをそのユーザーのユーザーレイヤーにインストールします。

その他の **App Layering** アーティファクト

App Layering VM の作成プロセスでは、パッケージ化 VM、コネクタ、エージェント、VM テンプレートなどのいくつかのアーティファクトが作成されます。これらすべて App Laying に固有の要素であるため、以下のセクションで簡単に説明します。詳細な説明については、App Layering のドキュメントを参照してください。

パッケージ化 **VM**

App Laying でプラットフォームレイヤーとアプリケーションレイヤーの内容をカスタマイズする方法は、パッケージ化 *VM*（インストールマシンと呼ばれることもある）を作成することです。レイヤーの作成は次の 6 ステップのプロセスです。

1. Enterprise Layer Manager（ELM）で、レイヤーを作成し、レイヤー名とその他の情報を指定します。
2. ELM はパッケージ化 VM を生成し、それを（通常は）ハイパーバイザーにコピーします。
3. ハイパーバイザーで、パッケージ化 VM を起動してパッケージ化 VM をカスタマイズします。
4. カスタマイズが完了したら、パッケージ化 VM のデスクトップにある ［シャットダウンしてファイナライズ］ アイコンをクリックします。このアクションではレイヤーの整合性チェックが実行されて、再起動が保留されていないこと、および ngen が実行中でないことが確認されます。ファイナライズは、これらのタスクをすべて完了するまで終了しません。
5. ELM で、［ファイナライズ］アクションをクリックします。
6. ELM は、カスタマイズしたパッケージ化 VM に基づいてレイヤーの生成を完了し、そのパッケージ化 VM を削除します。

App Layering では、OS レイヤーの作成にはパッケージ化 VM は使用されません。代わりに、ユーザーが VM を作成し、必要に応じてそれをカスタマイズし、ELM でそれをインポートします。

コネクタとエージェント

ELM は、ハイパーバイザー、ファイル共有、プロビジョニングツールなどの他のエンティティと通信します。ELM は、それらのエンティティで VM の作成などのさまざまなタスクを実行し、VHD やファイルなどの各種データをそれらのエンティティとの間でコピーします。

コネクタは、他のエンティティと通信して一連のタスクを実行するときに ELM が使用するオブジェクトです。コネクタは、他のエンティティの名前または IP アドレス、そのエンティティにアクセスするために必要な資格情報、およびタスクを実行するために必要なその他の情報を使用して構成されます。こうした情報の例としては、データを読み取るまたは書き込むエンティティ上のファイルパスなどがあります。

次の要素によってコネクタが作成されます：

- Citrix Hypervisor コネクタ：ELM はこのコネクタを使用して、Citrix Hypervisor で VM（パッケージ化 VM など）を作成または削除します。
- ネットワークファイル共有コネクタ：このコネクタは、［ネットワークファイル共有］セクションにある［システム］タブの［設定と構成］サブタブで構成します。ELM と VM はこのプロセスを使用して、ネットワークファイル共有にファイルを作成します。
- Citrix MCS for Citrix Hypervisor コネクタ：MCS をプロビジョニングサービスとして使用している場合は、このコネクタが作成されます。ELM はこのコネクタを使用して、MCS で必要とされないドライバーを除外してから、レイヤー化イメージを Citrix Hypervisor にコピーします。
- Citrix Provisioning コネクタ：Citrix Provisioning をプロビジョニングサービスとして使用する場合は、このコネクタを作成します。ELM はこのコネクタを使用して、レイヤー化イメージ VHD を Citrix Provisioning サーバーにコピーします。さらに、Citrix Provisioning に不要なドライバーを除外してから、vDisk を作成します。

VM テンプレート

Citrix Hypervisor をハイパーバイザーとして使用している場合は、OS レイヤー VM に基づいて VM テンプレートが作成されます。このテンプレートには、OS に関する情報（ネットワークインターフェイスやプロセッサ数など）が含まれています。OS レイヤーの後に作成されるこのテンプレートは、Citrix Hypervisor コネクタの作成時に使用されます。

Citrix Provisioning サーバーへの **Unidesk** エージェントのインストール

Citrix Provisioning を使用して展開する場合は、Citrix Provisioning サーバーに Unidesk エージェントをインストールする必要があります。これにより、ELM が Citrix Provisioning サーバー上でコマンドを実行できるようになります。

App Layeringのドキュメントの「Apping Layering エージェントのインストール（Citrix Provisioning およびコネクタスクリプトで必須）」を参照してください。

共有イメージの移行

共有 PvD イメージを App Layering に移行するには、共有 PvD イメージと機能的に同等である共有レイヤー化イメージを作成します。共有レイヤー化イメージは、イメージテンプレートを公開することによって構築されます。イメージテンプレートでは、OS レイヤー、プラットフォームレイヤー、および 1 つ以上のアプリケーションレイヤーを組み合わせます。各レイヤーは管理者が作成します。以下のセクションで、その手順について説明します。

OS レイヤー

以下の手順に従って、OS レイヤーを作成します。

XenCenter で:

Citrix Hypervisor で VM を作成します。この VM が、OS レイヤーと VM テンプレートの両方の基礎になります。

VM の OS のバージョンは、移行する共有 PvD イメージの OS バージョンと一致している必要があります。この手順では、Windows 7 を実行していることを前提としています。

OS レイヤー **VM** で:

ローカル管理者アカウントを使用してログインします。

未処理の Windows アップデートをインストールします。

App Layering のドキュメントの「Windows 7 イメージの準備」で説明されている準備作業を実行します。

XenCenter で:

OS レイヤー VM のコピーを作成します。すべてのローカルストレージを削除します。VM をテンプレートに変換します。この VM テンプレートは、Citrix Hypervisor コネクタを作成するときに使用します。

ELM から:

［レイヤー］タブで、［**OS** レイヤーの作成］をクリックします。

Citrix Hypervisor を使用中で Citrix Hypervisor コネクタをまだ作成していない場合は、この段階で作成してください。「仮想マシンテンプレート」の入力を求められたら、前のセクションで作成した VM テンプレートを指定します。

［仮想マシンの選択］のプロンプトが表示されたら、上記で作成した OS レイヤー VM を選択します。

アイコンを割り当てて、その他の詳細情報を指定したら、［レイヤーを作成］をクリックします。これにより、OS レイヤー VM が ELM ストアにコピーされ、OS レイヤーが生成されます。

これで、OS レイヤーの作成が完了し、展開可能になりました。

プラットフォームレイヤー

OS レイヤーが生成されたら、共有イメージ用のプラットフォームレイヤーの作成に進むことができます。

プラットフォームレイヤーのカスタマイズでは、ユーザーの Active Directory ドメインに参加するという手順があります。ユーザーが複数の異なるドメインのメンバーである場合は、ドメインごとに個別のプラットフォームレイヤーを作成する必要があります。この記事では、すべてのユーザーが単一のドメインのメンバーであることを前提としています。

ELM から:

1. ［レイヤー］タブで、［プラットフォームレイヤーの作成］をクリックします。
2. ［OS レイヤー］パネルで、前のセクションで作成した OS レイヤーを選択します。
3. ［コネクタ］パネルで、前のセクションで作成した Citrix Hypervisor コネクタを選択します。ELM は、プラットフォームレイヤーのパッケージ化 VM を Citrix Hypervisor に書き込むときにこの情報を使用します。
4. ［プラットフォームタイプ］パネルで、［このプラットフォームを使用してレイヤー化イメージを公開する］を選択します。
5. 該当するハイパーバイザーを選択します。この記事では、［Citrix Hypervisor］を使用していることを前提としています。
6. 該当するプロビジョニングサービスを選択します。この記事では、「Citrix MCS」または「Citrix PVS」（Citrix Provisioning を使用している場合）を使用していることを前提としています。
7. Connection Broker の場合は、［Citrix XenDesktop］を選択します。

アイコンを割り当てて、その他の詳細情報を指定したら、［レイヤーを作成］をクリックします。このアクションにより、プラットフォームレイヤーのパッケージ化 VM が生成されます。完了すると、作成タスクのステータスに［アクションが必要］と表示されます。

XenCenter で:

プラットフォームレイヤーのパッケージ化 VM が生成されると、その VM が XenCenter に表示されます。以下の手順に従います。

1. その VM を起動します。

2. プラットフォームレイヤーのパッケージ化 VM で、ローカル管理者アカウントを使用してログインします。
3. プロンプトが表示されたら、再起動し、再度ログインします。
4. 普段どおりの方法でユーザーの Active Directory ドメインに参加します。つまり、［コントロールパネル］ **>** ［システム］ **>** ［設定の変更］ **>** ［変更］の順に選択します。再起動し、ローカル管理者アカウントを使用して再度ログインします。

Citrix Virtual Delivery Agent（VDA）をインストールする：

1. Citrix Virtual Apps and Desktops の ISO をマウントします。
2. AutoSelect.exe が自動的に起動されない場合は、このプログラムを実行します。
3. ［Citrix Virtual Desktops］の横にある ［開始］をクリックします。
4. ［**Virtual Delivery Agent for Windows Desktop OS**］をクリックします。

   通常は、この後に開くオプションパネルでデフォルトを選択します。ただし、

   - プロンプトが表示されたら、Delivery Controller を指定するか、または［あとで設定する（詳細）］を指定します。
   - ［Personal vDisk］が選択されていないことを確認します。

   VDA がインストールされると、プラットフォームレイヤーのパッケージ化 VM が再起動します。

再度ログインします。

Citrix Provisioning をプロビジョニングサービスとして使用している場合は、ターゲットデバイスソフトウェアもインストールする必要があります。これを行うには、次の操作を行います。

1.「ProvisionServicesxxx.iso」をマウントします。
2. 自動的に起動されない場合は「AutoSelect.exe」を実行します。
3.［ターゲットデバイスのインストール］をクリックします。
4.［ターゲットデバイスのインストール］をもう一度クリックすると、インストールウィザードが開始されます。このインストーラーでは、Citrix Diagnostic Facility（CDF）と Citrix Provisioning Service のターゲットデバイスコードをインストールします。
5. 通常は、この後に開くオプションパネルでデフォルトを選択します。
6. インストールウィザードが完了したら、［イメージ作成ウィザードを起動］をオフにして、［完了］をクリックします。
7. VM の再起動とログインを許可します。
8. Citrix Provisioning Optimizer ユーティリティを実行します。

プラットフォーム関連のソフトウェアをすべてインストールしてカスタマイズしたら、［シャットダウンしてファイナライズ］デスクトップアイコンをクリックします。

ELM から：

プラットフォームレイヤーのアイコン（そのステータスは［編集中］）を選択し、［ファイナライズ］をクリックします。

アプリケーションレイヤー

プラットフォームレイヤーが生成されたら、共有 PvD イメージからのアプリケーションレイヤーの作成に進むことができます。共有 PvD イメージにインストールされているアプリケーションを特定します。それには次のような方法があります。

- 起動可能バージョンの共有 PvD イメージがある場合は、それを起動し、［コントロールパネル］で［プログラムと機能］を選択します。
- このようなイメージがない場合は、Citrix Virtual Desktops で共有 PvD イメージを使用して、ダミーユーザー用の PvD VM を作成します。ダミーユーザーの Personal vDisk は空であるため、［プログラムと機能］に表示されるすべてのアプリケーションが共有 PvD イメージにインストールされています。

［プログラムと機能］パネルを使用して、必要なすべてのアプリケーションを確認します。

または、「移行ツール」セクションで説明する PCmover プログラムを使用することもできます。このツールは、コンピューター上のアプリケーションを特定するのに便利です。このツールは、特別にインストールされているために［プログラムと機能］に表示されていないプログラムを検出します。この目的のために使用する場合は、転送を実行せずに分析を実行できるようにします。分析が完了し、共有イメージのすべてのアプリケーションをメモしたら、PCmover を終了します。詳しくは、この記事で後述している「**PCmover** を使用して必要なアプリケーションを判別する」を参照してください。

> ヒント：
>
> 複数の PvD VM を移行する場合は、各 VM を起動してユーザーがインストールしたアプリケーションのリストを編成するのにいい機会です。共有イメージで検出されたアプリケーション以外に見つかったアプリケーションは、ユーザーがインストールしたアプリケーションです。

必要なアプリケーションの完全なリストを取得したら、1 つ以上のアプリケーションレイヤーを作成し、各アプリケーションレイヤーに 1 つまたは複数の必要なアプリケーションをインストールします。たとえば、関連するアプリケーションをすべて 1 つのアプリケーションレイヤーにインストールできます。複数のユーザーが使用するアプリケーションは、Elastic アプリケーションレイヤーにインストールできます。1 人のユーザーだけが使用するアプリケーションは、ユーザーレイヤーにインストールできます。多くのアプリケーションでは 1 つのアプリケーションレイヤーを作成するのが簡単ですが、特別な準備が必要なアプリケーションもあります。

多くのアプリケーションでは 1 つのアプリケーションレイヤーを作成するのが簡単ですが、特別な準備が必要なアプリケーションもあります Citrix のソリューションアーキテクトや App Laying コミュニティで作成された、さまざまな構成レシピを確認してください。たとえば、ユーザーレイヤーにのみインストールでき、アプリケーションレイヤーにはインストールできないアプリケーションのあることがわかります。

各アプリケーションレイヤーの **ELM** で：

1. ［レイヤー］タブで、［アプリケーションレイヤーの作成］をクリックします。
2. ［レイヤーの詳細］セクションで、［レイヤー名］と［バージョン］を指定します。
3. ［OS レイヤー］で、前のセクションで作成した OS レイヤーを選択します。
4. このアプリケーションが別のアプリケーションレイヤーにあるアプリケーションに依存している場合は、それらのアプリケーションを［前提条件レイヤー］で指定します。これにより、アプリケーションレイヤーを作成

する順序が決まります。

5. ［コネクタ］で、前のセクションで作成した Citrix Hypervisor コネクタを選択します。ELM は、このコネクタを使用してアプリケーションレイヤーのパッケージ化 VM を Citrix Hypervisor に書き込み、そこで XenCenter を使用して起動およびカスタマイズできます。
6. すべてのオプションを指定したら、［レイヤーを作成］をクリックします。これによりアプリケーションレイヤーのパッケージ化 VM が生成されます。作成が完了すると、作成タスクのステータスに［アクションが必要］と表示されます。この例では、OS レイヤーの作成時に選択したのと同じハイパーバイザーにこのアプリケーションレイヤーを展開することを前提としているため、プラットフォームレイヤーは必要ありません。

XenCenter で：

アプリケーションレイヤーのパッケージ化 VM が生成されると、その VM が XenCenter に表示されます。次のタスクを実行します。

1. その VM を起動します。
2. アプリケーションレイヤーのパッケージ化 VM で、ローカル管理者アカウントを使用してログインします。
3. 直ちに再起動が必要な場合は、再起動し、再度ログインします。
4. このアプリケーションレイヤーのアプリケーションをインストールし、必要なカスタマイズを行います。このレイヤーは複数ユーザーによって共有されるため、ユーザーごとのカスタマイズおよび設定は行わないでください。こうしたカスタマイズと設定は、この記事で後述するように、ユーザーの Personal vDisk の移行時に行います。
5. このレイヤーのアプリケーションをインストールしてカスタマイズしたら、［シャットダウンしてファイナライズ］デスクトップアイコンをクリックします。

ELM から：

1. アプリケーションレイヤーのアイコンを選択します。そのステータスは ［編集中］になっています。
2. ［ファイナライズ］をクリックします。これで、アプリケーションレイヤーの作成が完了し、展開可能になりました。
3. 必要なアプリケーションレイヤーごとにこの手順を繰り返します。

イメージテンプレート

OS レイヤー、プラットフォームレイヤー、1 つ以上のアプリケーションレイヤーを生成したら、イメージテンプレートの作成に進むことができます。どのアプリケーションレイヤーをレイヤー化イメージにバインドするか、およびどのアプリケーションレイヤーを Elastic アプリケーションレイヤーとしてユーザーに動的に割り当てるかを決定します。次の点を考慮してください。

- イメージテンプレートに含めたアプリケーションレイヤーはすべて、共有レイヤー化イメージのすべてのユーザーが利用できます。
- 特定のユーザー（または AD グループ）に割り当てたアプリケーションレイヤーは、それらのユーザー（または AD グループ）のみが利用できます。別のユーザーやグループがアプリケーションレイヤーを利用できるように、こうした割り当てはあとで柔軟に変更できます。

> 重要:
>
> これらの 2 つの選択肢は互いに排他的です。イメージテンプレートにアプリケーションレイヤーを含めて、それを個別のユーザーに割り当てることは絶対に避けてください。そうすることは不要であり、サポートされていません。

経験則として、共有 PvD イメージにインストールされているアプリケーションは、イメージテンプレートに含めることをお勧めします。また、一部のユーザーの Personal vDisk にインストールされていたアプリケーションは、Elastic アプリケーションレイヤーとして割り当て、1 人のユーザーだけが使用していて共有される可能性が低いアプリケーションは、そのユーザーのユーザーレイヤーにインストールします。

ELM から:

1. [イメージ] タブで [テンプレートの作成] をクリックします。
2. 名前とバージョンを指定します。
3. 前のセクションで作成した OS レイヤーを指定します。
4. イメージテンプレートに含めるアプリケーションレイヤーを選択します。ユーザーや AD グループに Elastic アプリケーションレイヤーとして割り当てる予定のアプリケーションレイヤーは選択しないでください。
5. [コネクタの構成] を選択します。これにより、共有イメージが公開されるときに、その共有イメージがどこに展開されるかが決まります。新しい展開ターゲットを初めて使用するときには、コネクタ構成を作成します。

Citrix Hypervisor を使用している場合は、次の 3 種類の展開が可能です:

- Citrix Hypervisor: Citrix Hypervisor コネクタを使用して、ELM は公開された共有イメージを VM として Citrix Hypervisor に展開します。そこで、XenCenter を使用して起動できます。ただし、通常は Citrix Provisioning または MCS のいずれかを選択してください。
- Citrix Provisioning: 公開した共有イメージは、Citrix Provisioning サーバー上の vDisk として展開されます。このタイプのコネクタ構成を作成する場合は、Citrix Provisioning サーバーの名前と、Citrix Provisioning の管理権限を持つユーザーのログイン資格情報を指定する必要があります。詳しくは、App Laying のオンラインドキュメントの「コネクタの構成とオプションのスクリプト（Citrix Provisioning）」を参照してください。
- Citrix MCS for Citrix Hypervisor: 公開した共有イメージは Citrix Hypervisor 上の VM として展開され、そこで Citrix Virtual Desktops を使用してマシンカタログを作成するために使用できます。

このタイプの [コネクタの構成] を作成する場合は、ELM が Citrix Hypervisor に書き込みできるように Citrix Hypervisor のアドレスと資格情報を指定し、ターゲットのストレージリポジトリを指定する必要があります。前のセクションで作成した VM テンプレートも指定します。

また、次のように指定します:

- [プラットフォームレイヤー]: 前のセクションで作成した MCS または Citrix Provisioning のいずれかのプラットフォームレイヤーを選択します。ただし、Citrix Provisioning に展開する場合はこのオプションをスキップします。
- [レイヤー化イメージディスク] パネルで: [SysPrep] オプションが表示されている場合は [一般化しない] を選択します。

- [Elastic Layering]：［アプリケーションレイヤーとユーザーレイヤー］を選択します。この設定には次の 2 つの効果があります。
  - 追加のアプリケーションレイヤーをユーザーおよび AD グループに割り当てることができます。このレイヤーは、ユーザーがログインすると動的に接続されます。
  - ユーザーの初回ログイン時に、新しいユーザーレイヤーが作成されます（App Layering バージョン 4.1 では、このオプションは明示的に有効になっている場合にのみ利用可能です。有効にするには、ELM の［システム］タブの［設定と構成］サブタブの［ラボ］セクションにある［ユーザーレイヤー］チェックボックスをオンにします。

ユーザーレイヤーでは、ユーザーのプロファイル、設定、ドキュメントなどがキャプチャされます。以下のセクションで説明していますが、ユーザーレイヤーは、移行ツールでユーザーの Personal vDisk からすべてのユーザー固有の情報を転送する際の転送先になります。

［確認と完了］パネルで、［テンプレートの作成］をクリックします。これは直ちに完了します。

共有レイヤー化イメージの公開

共有レイヤー化イメージを生成するための最後の手順は、上記で作成したイメージテンプレートを選択して、［レイヤー化イメージを公開］をクリックすることです。

これが完了すると、生成されたレイヤー化イメージが、（1）MCS の場合は Citrix Hypervisor 内の VM として、（2）Citrix Provisioning の場合は Citrix Provisioning サーバー内の vDisk として展開されます。

これで、通常の MCS または Citrix Provisioning 管理ツールを使用して、Citrix Virtual Desktops のマシンカタログおよびデリバリーグループを作成できるようになりました：

- MCS の場合は、Studio を使用してマシンカタログを作成し、共有レイヤー化イメージ VM をインポートします。
- Citrix Provisioning の場合は、Citrix Virtual Desktops インストールウィザードを使用して Studio 内にマシンカタログを作成します。

ユーザーの PvD VM を App Layering に移行するための最後の手順については、次のセクションで説明します。プロセスのプレビューとして、元の PvD VM と新しい App Layering VM を同時に実行し、そのユーザーとして App Layering VM にログインし、移行ツールを実行して、ユーザーのプロファイルと設定を PvD から App Layering ユーザーレイヤーに転送します。

移行ツール

ユーザーの Personal vDisk からそのユーザーの App Layering ユーザーレイヤーに個人情報を移行するには、PCmover または USMT という 2 つのツールのいずれかを使用することをお勧めします。

- PCmover は LapLink.com が販売しているプログラムです。ユーザーの PvD VM と App Laying VM を実行し、PCmover を使用してそのユーザーの設定を PvD VM から App Laying VM に転送できます。ネットワークを介して情報を転送して 2 つの VM を同時に実行することも、情報をファイルで転送して 2 つの VM を連続的に実行することもできます。

PCmover には使いやすい GUI があり、転送される情報を細かく調整できます。移行する PvD VM が複数ある場合は、PCmover の Policy Manager を使用してポリシーファイルを作成することを検討してください。ポリシーファイルを使用すると、最小限の操作で移行を実行できます。

詳しくは、PCmover ユーザーガイドを参照してください。

- USMT は、Microsoft が Windows 自動インストールキット（AIK）の一部として提供している一連のプログラムです。転送ファイルを書き込む際には、scanstate プログラムが PvD VM 上で実行されます。この転送ファイルを読み取り適用する場合には、loadstate プログラムが App Laying VM 上で実行されます。どの情報が転送されるかは、いくつかの XML ファイルによって決まります。これらの XML ファイルは、デフォルト値がニーズに合わない場合は編集できます。

この記事では、PCmover を実行することを前提としています。

ユーザー情報の移行

この時点で、元の共有 PvD イメージを取得済みであり、機能的に同等な App Laying の共有レイヤー化イメージを作成済みである必要があります。1 つまたは複数のユーザー PvD VM があり、それぞれの VM に、App Layering ユーザーレイヤーに移行するユーザープロファイルおよびその他の情報が含まれている Personal vDisk があります。

各ユーザーについて、ユーザーの PvD VM を起動し、共有レイヤー化イメージを起動し、両方の VM でユーザーのドメイン資格情報を使用してログインし、PCmover を実行します。

ユーザー情報を移行するには、以下の手順に従います：

1. PvD VM と共有レイヤー化イメージの両方からアクセス可能な共有に、PCmover をインストールします。
2. スタジオで、そのユーザーの PvD VM を起動します。そのユーザーとしてログインします。ファイアウォールを無効にします。
3. ELM で、そのユーザーに必要なすべての Elastic アプリケーションレイヤーをユーザーに割り当てます。
4. ユーザーが自分のユーザーレイヤーが存在するディレクトリに対し、書き込みアクセス権を持っていることを確認します。オンラインドキュメントの「ユーザーレイヤーフォルダーのセキュリティを構成する」を参照してください。
5. Studio で、共有レイヤー化イメージ VM を起動します。そのユーザーとしてログインします。ユーザーの初回ログイン時に、この VM によりネットワークファイル共有内にユーザーレイヤーが作成されます。ファイアウォール、ウイルス対策アプリケーション、スパイウェア対策アプリケーションを無効にします。
6. PvD VM 上で PCmover を実行します。
   a) ［PC to PC Transfer］を選択し、［Next］をクリックします。
   b) ［Old］を選択し、［Next］をクリックします。
   c) ［Wifi or Wired Network］を選択し、［Next］をクリックします。
   d) PCmover が PvD VM をスキャンするのに数分かかります。スキャンが終わったら、［Next］をクリックします。
   e) 転送が完了したときに電子メール通知を受信しないことを前提として、［Next］をクリックします。
   f) パスワードを入力するか、または空欄のままにします。パスワードを指定することによって、ユーザー情報が PvD VM から共有レイヤー化イメージ VM のみに送信され、他の VM には送信されないようにで

きます。次に、［Next］をクリックします。

7. App Laying VM で PCmover を実行します。
   a) ［PC to PC Transfer］を選択し、［Next］をクリックします。
   b) ［New］を選択し、［Next］をクリックします。
   c) 必要なシリアル番号検証値を入力します。
   d) ［Network Name］に PvD VM の名前を指定し、［Next］をクリックします。
   e) ［Application Selections］パネルに移動します。アプリケーションをすべて選択解除することをお勧めします。必要なすべてのアプリケーション用のアプリケーションレイヤーが作成されている必要があります。
   f) ［User Account Selections］パネルに移動します。Personal vDisk の所有者以外のすべてのユーザーを編集して［Do not transfer this user］をオンにすることをお勧めします。
   g) ［Custom Settings］パネルに移動します。［Files and Settings Only］を選択することをお勧めします。
   h) ［Drive Selections］パネルに移動します。「C:」以外のすべてのドライブを編集して［Do not transfer this drive］をオンにすることをお勧めします。
   i) すべてのパネルで指定し終わったら、［Next］をクリックします。
   j) 転送が完了したときに電子メール通知を受信しないことを前提として、［Next］をクリックします。

この時点で、PCmover が、ファイルと設定を PvD VM からそのユーザーの App Layering ユーザーレイヤーに転送し始めます。

PCmover を使用して必要なアプリケーションを判別する

PCmover を使用して PvD VM を分析し、インストールされているアプリケーションを判別できます。この方法は、［コントロールパネル］の［プログラムと機能］の代わりに使用できます。

1. PvD VM 上で PCmover を実行します。
2. ［PC to PC Transfer］を選択し、［Next］をクリックします。
3. ［Old］を選択し、［Next］をクリックします。
4. ［File Storage Device］を選択し、［Next］をクリックします。
5. ［Application Selections］パネルに移動し、インストールされているアプリケーションをメモします。
6. PCmover をキャンセルします。

コンポーネントの削除

April 26, 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。たとえば、Delivery 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。

以下に記載されていない機能の削除については、機能のドキュメントを参照してください。

準備

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。詳しくは、「Controller の削除」を参照してください。

Studio と Director を終了してから削除してください。

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 Virtual Apps *version*］** または ［**Citrix Virtual Desktops *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ます。アンインストールするコンポーネントを選択します。

  StoreFront は、［**Citrix StoreFront**］を右クリックしてから ［アンインストール］を選択して削除することもできます。

- VDA をアンインストールするには、［**Citrix Virtual Delivery Agent *version***］を選択し、右クリックしてから ［アンインストール］を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。アンインストール後にデフォルトでマシンが自動的に再起動します。

- 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`オプションを指定します。
- 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`オプションを指定します。

コマンドとパラメータの詳細については、「コマンドラインを使ったインストール」を参照してください。

たとえば、Studio をアンインストールするには次のコマンドを実行します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

コマンドラインを使って **VDA** をアンインストールする

インストールメディアの\x64\XenDesktop Setup ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、/remove および/components オプションを使用します。
- すべてのコンポーネントをアンインストールするには、/removeall オプションを使用します。

コマンドとパラメータの詳細については、「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。

アンインストール後にデフォルトでマシンが自動的に再起動します。

たとえば、VDA および Citrix Workspace アプリ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、「スクリプトを使用した VDA のインストールと削除」を参照してください。

アップグレードと移行

April 26, 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しなくても、既存の環境をアップグレードすることで Citrix Virtual Apps and Desktops 7 の最新リリース（CR）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。

アップグレード後は、ライセンス対象の最新機能やテクノロジを利用できるようになります。さらに、以前のバージョンからの修正や機能拡張も使用することができます。

アップグレードの概要

1. アップグレードを開始する前に、「環境のアップグレード」の記事を確認してください。これは、アップグレードの準備と実装方法を学ぶための主要な情報源です。
2. 準備ガイダンスを完了します。

3. インストーラを実行して、コアコンポーネントをアップグレードします。
4. データベースとサイトをアップグレードします。
5. マスターイメージ上で（またはマシン上で直接）VDA をアップグレードします。
6. 他のコンポーネントをアップグレードします。

各準備とアップグレードの手順については、「環境のアップグレード」を参照してください。

アップグレードできるバージョン

Citrix アップグレードガイドには、アップグレードできる Citrix Virtual Apps and Desktops（および XenApp と XenDesktops）のバージョンが表示されています。

よく寄せられる質問

このセクションでは、Citrix Virtual Apps and Desktops のアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops** 環境をアップグレードするための正しい順序はありますか

  VDA はいつでも任意の順序でアップグレードできます。サイトをアップグレードする前に、コントローラーの半数をアップグレードしてください。サイトのアップグレード後、残りのコントローラーをアップグレードします。詳しくは、「アップグレードの順序」および「アップグレード手順」を参照してください。

- サイトには、いくつかの **Delivery Controller** が（異なるゾーンに）あります。一部のみをアップグレードするとどうなりますか? 同じメンテナンスウィンドウ中にサイト内のすべての **Controller** をアップグレードする必要がありますか?

  各 Controller のさまざまなサービスが相互に通信するため、ベストプラクティスは、同じメンテナンスウィンドウ中にすべての Delivery Controller をアップグレードすることです。異なるバージョンを保持すると、問題が発生する場合があります。メンテナンスウィンドウ中に、半分の Controller をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。（詳しくは、「アップグレード手順」を参照してください。）

- 最新バージョンに直接アップグレードできますか。それとも増分アップグレードが必要ですか。

  アップグレードするバージョンのドキュメントの「新機能」に別途明記されていない限り、常に中間リリースを省略して最新バージョンにアップグレードすることができます。「アップグレードガイド」を参照してください。

- お客様は長期サービスリリース（**LTSR**）環境から最新リリースにアップグレードできますか

  はい。お客様が長期間にわたって長期サービスリリースを継続して使用する必要はありません。ビジネス上の要件および機能に基づいて、LTSR 環境を最新リリースに移行できます。

- コンポーネントのバージョンを混在させることはできますか

Citrix では各サイト内ですべてのコンポーネントを同じバージョンに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。詳しくは、「混在環境に関する考慮事項」を参照してください。

- どのくらいの頻度で最新リリースをアップグレードする必要がありますか。

  最新リリースは、リリース日の 6 か月後にメンテナンス終了（EOM）になります。Citrix では、常に最近の最新リリースを採用することをお勧めします。最新リリースは、リリース日の 18 か月後に製品終了（EOL）になります。詳しくは、「最新リリースのライフサイクル」を参照してください。

- **LTSR** または **CR** のどちらにアップグレードすべきしょうか。

  最新リリース（CR）は、最新の画期的なアプリ、デスクトップ、サーバー仮想化機能を提供します。CR を導入することによって、最新テクノロジを活用し、競合に差をつけることができます。

  長期サービスリリース（LTSR）は、長期間にわたって同じ基本バージョンを維持する必要がある大企業の実稼働環境に最適です。

  詳しくは、「サービスオプション」を参照してください。

- 使用しているライセンスはアップグレードが必要でしょうか。

  現在のライセンス日が期限切れになっていないこと、およびアップグレード対象のリリースに対して有効であることを確認してください。CTX111618を参照してください。更新については、「カスタマーサクセスサービスの更新ライセンス」を参照してください。

- アップグレードにはどれくらい時間がかかりますか。

  展開のアップグレードに必要な時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間は不明です。

- ベストプラクティスについて教えてください。

  準備ガイドを理解し、記載手順に従ってください。

- どのオペレーティングシステムがサポートされていますか。

  アップグレードするバージョンに関する「システム要件」の記事に、サポート対象の OS が記載されています。

  現在の展開で、サポートされていないオペレーティングシステムを使用している場合は、「以前のオペレーティングシステム」を参照してください。

- どのバージョンの **VMware vSphere**（**vCenter + ESXi**）がサポートされていますか。

  CTX131239に、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- 使用中のバージョンの **EOL** スケジュールを教えてください。

  製品マトリクスで確認してください。

- 最新のリリースにはどのような既知の問題がありますか。

  - Citrix Virtual Apps and Desktops

- StoreFront
- Citrix Provisioning
- Citrix ライセンスサーバー
- Windows 向け Citrix Workspace アプリ

詳細情報

長期サービスリリース（LTSR）展開の更新には、累積更新プログラム（CU）を使用します。CU は LTSR のベースラインコンポーネントを更新します。各 CU には、独自の Metainstaller が含まれます。

また、それぞれに専用のドキュメントがあります。たとえば 7.15 LTSR の場合、LTSR の「新機能」ページで最新 CU のリンクを確認してください。各 CU ページには、サポートされているバージョンの情報、手順、CU のダウンロードパッケージへのリンクが含まれています。

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。移行処理により、より新しいコンポーネントのインストール、新しいサイトの作成、既存のファームからのデータのエクスポート、および新しいサイトへのデータのインポートが行われます。

XenApp および XenDesktop のバージョンの移行、または以前の Citrix Virtual Apps and Desktops のバージョンの移行用に、サポートされているツールやスクリプトはありません。アップグレードは、「Citrix アップグレードガイド」に記載されている Citrix Virtual Apps and Desktops バージョンでサポートされており、この製品ドキュメントで説明しています。

以前の XenApp 6.x の移行コンテンツについては、以下を参照してください。スクリプトや記事は用意しておらず、保持もされていません。

- XenApp 6.x バージョンのオープンソース移行スクリプトは、https://github.com/citrix/xa65migrationtoolから入手できます。Citrix ではこれらの移行スクリプトに対応しておらず、保持もしていません。
- 7.x での変更点
- XenApp 6.5 ワーカーから新しい VDA へのアップグレード
- XenApp 6.x からの移行

環境のアップグレード

May 3, 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。これはインプレースアップグレードと呼ばれます。アップグレードできる Citrix Virtual Apps and Desktops のバージョンについては、「Citrix アップグレードガイド」を参照してください。

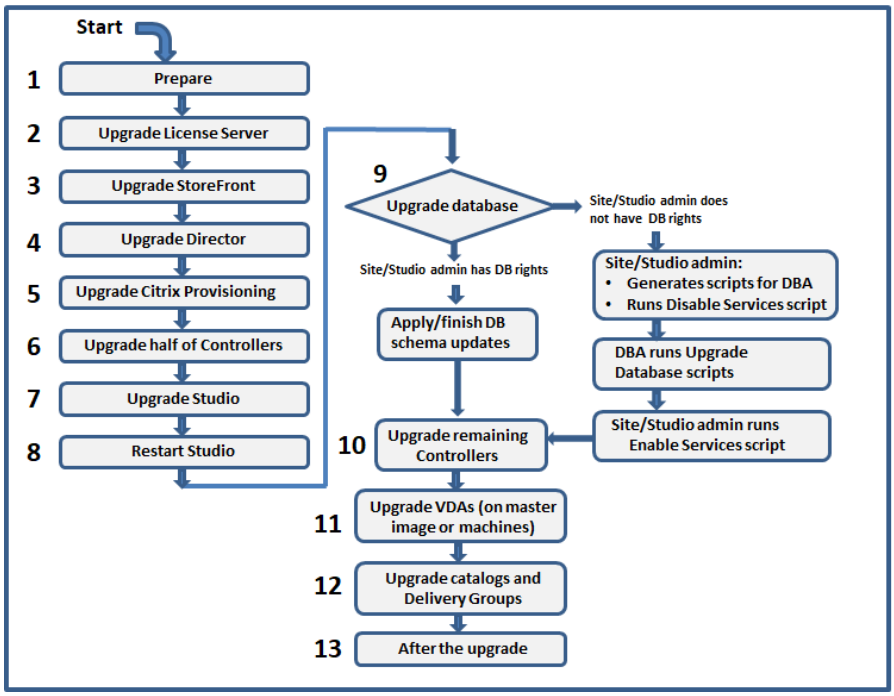
アップグレードを開始するには、新しいバージョンでインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、およびその他の特定のコンポーネントをアップグレードします。その後に、データベースとサイトをアップグレードします。

全製品インストーラー（およびスタンドアロン VDA インストーラー）でインストールできるコンポーネントの新しいバージョンが提供されている場合は、その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でインストールされていない他のコンポーネント（Citrix Provisioning や Profile Management など）については、そのコンポーネントのマニュアルを参照してください。ホストのアップグレードについては、該当するドキュメントを参照してください。

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を示します。アップグレード手順には、図の各手順の詳細が記載されています。



アップグレード手順

主な製品コンポーネントのほとんどは、そのコンポーネントを含むマシンで製品インストーラーを実行するとアップグレードできます。

1 つのマシンに複数のコンポーネント（Studio や License Server など）が含まれている場合、製品メディアに新しいバージョンのソフトウェアが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには、次の手順に従います:

- 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実行するには、マシンにログオンし、メディアを挿入するか、新しいリリース用の ISO ドライブをマウントします。**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には、該当するコマンドを発行します。「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**: 準備

アップグレードを開始する前に、準備ができていることを確認します。次のセクションにある必要なタスクを読み、完了します:

- VDA を 1912 以降にアップグレードする
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- 事前サイトテスト
- SQL Server のバージョンチェック

手順 **2**: ライセンスサーバーのアップグレード

新しいバージョンの Citrix License Server ソフトウェアがインストールされている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードします。

まだ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かどうかの確認を行っていない場合、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。

手順 **3**: **StoreFront** のアップグレード

インストールメディアに新しいバージョンの StoreFront ソフトウェアが含まれている場合は、StoreFront サーバーが存在するマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、[拡張展開] セクションから [**Citrix StoreFront**] を選択します。
- コマンドラインから`CitrixStoreFront-x64.exe`を実行します。これは Citrix Virtual Apps and Desktops のインストールメディアの`x64`フォルダーにあります。

手順 **4**: **Director** のアップグレード

インストールメディアに新しいバージョンの Director ソフトウェアが含まれている場合は、Director が含まれているマシンでインストーラーを実行します。

手順 **5**: **Citrix Provisioning** のアップグレード

Citrix Provisioning のインストールメディアは、Citrix Virtual Apps and Desktops のインストールメディアとは別に入手します。Citrix Provisioning サーバーおよびターゲットデバイスのソフトウェアをインストールおよびアップグレードする方法については、「Citrix Provisioning 製品ドキュメント」を参照してください。

手順 **6**: **Delivery Controller** の半分のアップグレード

たとえば、サイトに 4 つの Controller がある場合、そのうちの 2 つでインストーラーを実行します。

半数の Controller をアクティブなままにしておくことによって、ユーザーがそのサイトにアクセスできます。VDA はこれらの残りの Controller に登録されます。使用可能な 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。アップグレード済みの Controller では、サイト全体がアップグレードされるまで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。

実際のアップグレードが開始される前に、最初の Controller で事前サイトテストが実行されます。詳しくは、「事前サイトテスト」を参照してください。

手順 **7**: **Studio** のアップグレード

Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシン上にあったため）、Studio を含むマシンでインストーラーを実行します。

手順 **8**: **Studio** の再起動

アップグレードした Studio を再起動します。アップグレードプロセスが自動的に再開されます。

手順 **9**: データベースとサイトのアップグレード

SQL Server データベースのスキーマを更新するために必要な権限について、「準備」で確認します。

- SQL Server データベーススキーマを更新するために十分な権限がある場合は、データベースの自動アップグレードを開始できます。「データベースとサイトの自動アップグレード」に進みます。
- 十分なデータベース権限がない場合は、スクリプトを使用する手動アップグレードを開始し、（必要な権限を持つ）データベース管理者の支援によって続行できます。手動アップグレードの場合、Studio ユーザーはスクリプトを生成し、サービスを有効または無効にするスクリプトを実行します。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 モードで使用して、データベーススキーマを更新するその他のスクリプトを実行します。「データベースとサイトの手動アップグレード」に進みます。

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。

データベースとサイトの自動アップグレード

1. 新しくアップグレードした Studio を起動します。
2. サイトのアップグレードを自動的に開始するよう指定して、準備ができていることを確認します。

データベースとサイトのアップグレードが続行されます。

データベースとサイトの手動アップグレード

1. 新しくアップグレードした Studio を起動します。
2. サイトを手動でアップグレードするよう指定します。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。
3. データベースがバックアップされたことを確認します。

   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、表示されます。製品バージョンのアップグレード後にデータベースのスキーマが変更されていない場合、該当するスクリプトは生成されません。たとえば、App Orchestration ログデータベーススキーマが変更されていない場合、`UpgradeLoggingDatabase.sql`スクリプトは生成されません。
4. 以下のスクリプトを順番に実行します。

   - `DisableServices.ps1`: Studio ユーザーはこの PowerShell スクリプトを Controller で実行して、製品サービスを無効にします。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、モニターデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。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`: Studio ユーザーは、この PowerShell スクリプトを Controller で実行して、製品サービスを有効にします。

   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 で自動的に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。
5. 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。

手順 **10**: 残りの **Delivery Controller** のアップグレード

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] タブで、[残りの **Delivery Controller** のアップグレード] を選択します。

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。Controller のサービスをサイトに登録するため、またはゾーン ID が存在しない場合に作成するために、追加のサイトアップグレードを要求するメッセージが Studio によって表示されることがあります。

手順 **11**: **VDA** のアップグレード

> 重要:
>
> VDA をバージョン 1912 以降にアップグレードする場合には、「VDA を 1912 以降にアップグレードする」を参照してください。

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。

Machine Creation Services とマスターイメージを使用してマシンを作成した場合は、ホストに移動し、マスターイメージの VDA をアップグレードします。使用可能な任意の VDA インストーラーを使用できます。

- グラフィカルインターフェイスのガイダンスについては、「VDA のインストール」を参照してください。
- コマンドラインのガイダンスについては、「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。

Citrix Provisioning を使用してマシンを作成した場合、アップグレードに関するガイダンスについては、Citrix Provisioning 製品ドキュメントを参照してください。

手順 **12**: マシンカタログとデリバリーグループの更新

- VDA がアップグレードされたマシンを使用するカタログの更新。
- VDA がアップグレードされたマシンを使用するカタログのアップグレード。
- VDA がアップグレードされたマシンを使用するデリバリーグループのアップグレード。

手順 **13**: アップグレード後

アップグレードが完了したら、新しくアップグレードしたサイトをテストできます。Studio の [ナビゲーション] ペインで、[**Citrix Studio**（サイト名）] を選択します。[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。

サイトデータベースにローカルの Microsoft SQL Server Express を使用している場合に、SQL Server Browser サービスが開始されてないと、Windows Server 2016 上の Controller に対するテストが失敗する可能性があります。これを回避するには、以下の操作を行います:

- （必要に応じて）SQL Server Browser サービスを有効にして開始します。
- SQL Server（SQLEXPRESS）サービスを再開始します。

展開の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

Microsoft SQL Server Express LocalDB ソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDB の置き換え」を参照してください。

VDA を 1912 以降にアップグレードする

Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、その VDA をバージョン 1912 以降にアップグレードすることはできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから新しくインストールする必要があります。

この手順は、PvD を使用したことがない場合でも適用されます。

影響を受けているかを判断する

以前のバージョンで使用された PvD のインストール方法:

- VDA インストーラーのグラフィカルインターフェイスでは、PvD は ［追加コンポーネント］ページのオプションです。7.15 LTSR およびそれ以前の 7.x リリースでは、デフォルトでこのオプションが有効になっています。そのため、デフォルトを変更しない場合（または任意のリリースでこのオプションを有効にすることを選択した場合）、PvD がインストールされました。
- コマンドラインでは、`/baseimage`オプションによって PvD がインストールされます。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合、PvD がインストールされました。

VDA に PvD がインストールされているかどうかわからない場合は、マシンまたはイメージで新しい VDA（1912 LTSR 以降）のインストーラーを実行します。

- PvD がインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されるページで ［キャンセル］をクリックして、インストーラーを閉じます。
  - CLI では、コマンドが失敗してメッセージが表示されます。
- PvD がインストールされていない場合、アップグレードが続行されます。

必要なアクション

VDA に PvD がインストールされていない場合は、通常のアップグレード手順に従ってください。

VDA に PvD がインストールされている場合:

1. 現在の VDA をアンインストールします。詳しくは、「コンポーネントの削除」を参照してください。
2. 新しい VDA をインストールします。

Windows 7 または Windows 10（1607 以前、更新なし）マシンで PvD を引き続き使用する場合、使用できる最新バージョンは VDA 7.15 LTSR です。

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。

- **Preview**、**Early Release**、または **Technology Preview** バージョン： Early Release、Technology Preview、プレビューバージョンからアップグレードすることはできません。

- 以前のオペレーティングシステム上のコンポーネント： Microsoft または Citrix でサポートされなくなったオペレーティングシステムに、現行の VDA をインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。

- 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、「混在環境に関する考慮事項」を参照してください。

- 製品選択：以前のバージョンからアップグレードする場合、インストール時に設定されていた製品（Citrix Virtual Apps または Citrix Virtual Apps and Desktops）を選択または指定しないでください。

混在環境に関する考慮事項

アップグレードするときには、Citrix ではすべての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。そうすることにより、そのエディションおよびバージョンで追加および強化された機能をすべて使用できるようになります。

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。

環境によっては、すべての VDA を最新バージョンにアップグレードできない場合がります。マシンカタログを作成する際に、マシンにインストールされている VDA バージョンを指定できます（これは機能レベルと呼ばれます）。デフォルトでは、VDA の推奨最小バージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトより以前の VDA が含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。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。

デフォルトの最小 VDA バージョンの設定を使用してカタログが作成されていて、デフォルトバージョンより以前の VDA を格納するマシンが複数ある場合は、それらのマシンは Controller に登録できず、動作しません。

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。

バージョンが異なる複数のサイト

環境内に製品バージョンが異なるサイトがある（たとえば、XenDesktop 7.18 のサイトと Citrix Virtual Apps and Desktops 1909 のサイト）場合は、StoreFront を使用して、異なる製品バージョンからアプリケーションとデスクトップを集約することをお勧めします。詳しくは、「StoreFront」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。

以前のオペレーティングシステム

コンポーネントの以前のバージョンを、サポートされているオペレーティングシステム（OS）バージョンを実行していたマシンにインストールしたとします。新しいコンポーネントバージョンを使用したい場合でも、現行バージョンのコンポーネントでその OS がサポートされなくなっています。

たとえば、Windows Server 2008 R2 マシンにサーバー VDA をインストールしたとします。VDA を現在のリリースにアップグレードしたいものの、アップグレード後の現在のリリースでは Windows Server 2008 R2 はサポートされていません。

許容されなくなったオペレーティングシステム上にコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません。」などのエラーメッセージが表示されます。

以上の考慮事項を、最新リリースおよび長期サービスリリースのバージョンのアップグレードで検討します（LTSR バージョンへの CU の適用には影響しません）。

サポートされている OS については、リンク先を参照してください：

- Citrix Virtual Apps and Desktops（最新リリース）：
  - Delivery Controller、Studio、Director、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront 、セルフサービスパスワードリセット、Session Recordingについては、最新リリースのシステム要件を参照してください。
- LTSR については、LTSR バージョンおよび CU のコンポーネントリストを参照してください（Citrix Virtual Apps and Desktopsの製品ドキュメントのメインページで、お使いの LTSR バージョンを選択します）。

無効なオペレーティングシステム

次の表に、現行リリースのコンポーネントのインストールまたはアップグレードに対して有効でない、以前のオペレーティングシステムの一覧を示しています。記載されている各 OS でサポートされている最新の有効なコンポーネントのバージョンと、インストールおよびアップグレードが無効になったときのコンポーネントのバージョンを示しています。

表のオペレーティングシステムには、サービスパックと更新プログラムが含まれています。

オペレーティングシステム	コンポーネント/機能	最新の有効バージョン	インストール/アップグレードが不可能になるバージョン
Windows 7 および Windows 8	VDA	7.15 LTSR	7.16
Windows 7 および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
1607 より前の Windows 10 バージョン	VDA	7.15 LTSR	7.16
Windows 10 x86 のバージョン	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	その他のインストーラーコンポーネント	7.17	7.18
Windows Server 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
Windows Server 2012 R2	サーバー VDI	7.15 LTSR	7.16

Windows XP および Windows Vista は、7.x のコンポーネントまたはテクノロジでは無効です。

* Delivery Controller、Studio、Director、VDA などがあります。

対応の手順

選択肢があります。次の操作を実行できます:

- 現在の OS を引き続き使用する
- マシンを再イメージ化またはアップグレードする
- 新しいマシンを追加してから古いマシンを削除する

現在の **OS** を引き続き使用する

この方法は、VDA では実現可能です。以前の OS のマシンを引き続き使用する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを使用し続ける
- 最新の有効なコンポーネントバージョンをダウンロードし、コンポーネントをそのバージョンにアップグレードする（最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています）

たとえば、Windows 7 SP1 マシンで 7.14 VDA を使用しているとします。Windows 7 OS マシン上で最新の有効な VDA バージョンは、XenApp および XenDesktop 7.15 LTSR です。7.14 を使用し続けるか、または 7.15 LTSR VDA をダウンロードして VDA をそのバージョンにアップグレードします。以前のバージョンの VDA は、新しいバージョンの Delivery Controller がある展開で動作します。たとえば、7.15 LTSR VDA は、Citrix Virtual Apps and Desktops 7 1808 の Controller に接続できます。

マシンを再イメージ化またはアップグレードする

これらの方法は、VDA、およびコアコンポーネント（Delivery Controller など）がインストールされていない他のマシンで実現可能です。次のいずれかのオプションを選択します：

- メンテナンスモードをオンにしてすべてのセッションを終了できるようにして、マシンのサービスを停止した後に、サポートされている Windows OS バージョンにマシンを再イメージ化してから、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずに OS をアップグレードするには、OS をアップグレードする前に Citrix ソフトウェアをアンインストールします。そうしないと、Citrix ソフトウェアがサポートされていない状態になります。次に、新しいコンポーネントをインストールします。

新しいマシンを追加してから古いマシンを削除する

この方法は、Delivery Controller などのコアコンポーネントがあるマシンで OS をアップグレードする必要がある場合に適しています。

Citrix ではサイト内のすべての Controller が同じ OS であ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。たとえば、2 台の Windows Server 2016 マシンに 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. 現行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。たとえば、2 台の Windows Server 2008 R2 マシン上の 2 台の Controller を取り外します。「Delivery Controller」に記載されている、Controller を取り外すための推奨事項に従います。

準備

アップグレードを開始する前に、次の情報を確認し、必要な作業を完了してください。

インストーラーとインターフェイスを選択する

製品 ISO から全製品インストーラーを使用して、コンポーネントをアップグレードします。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。

インストールの詳細：インストーラーを開始するために必要な準備の完了後は、インストールに関する記事で表示される画面（グラフィカルユーザーインターフェイスを使用している場合）や入力画面（コマンドラインインターフェイスを使用している場合）を確認できます。

- グラフィカルインターフェイスを使用したコアコンポーネントのインストールまたはアップグレード
- コマンドラインを使用したコアコンポーネントのインストールまたはアップグレード
- グラフィカルインターフェイスを使用した VDA のインストールまたはアップグレード
- コマンドラインを使用した VDA のインストールまたはアップグレード

シングルセッション 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 Citrix では推奨しています。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。

VDA を現行リリースにアップグレードする場合、アップグレード処理中にマシンの再起動が発生します（この要件は 7.17 リリースから導入されました）。この再起動は回避できません。再起動後に、アップグレードが再開されます（コマンドラインで`/noresume`を指定していない場合）。

データベースのアクション

サイト、監視、および Configuration Logging データベースをバックアップします。CTX135207の手順に従ってください。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。

サポートされなくなったバージョンの SQL Server のアップグレードについて詳しくは、「SQL Server のバージョンチェック」を参照してください。（これは、サイト、モニター、および構成ログデータベースに使用される SQL Server に言及しています）。

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、自動で Microsoft SQL Server Express LocalDB がインストールされます以前のバージョンを置き換えたい場合、新しいバージョンは SQL Server Express 2017 LocalDB CU16 以降であることが必要です。コンポーネントとサイトのアップグレード後に、SQL Server Express LocalDB を新しいバージョンに置き換える方法については、「SQL Server Express LocalDB の置き換え」を参照してください。

Citrix ライセンスが最新であることを確認する

Citrix ライセンスの管理に関する総合的な情報は、「Citrix ライセンスのアクティブ化、アップグレード、管理」を参照してください。

全製品インストーラーを使用して、ライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。「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前に、Customer Success Services / Software Maintenance / Subscription Advantage 日が新しい製品バージョンに対して有効であることを確認してください。製品の Version 7.x からのアップグレードでは、この日付が 2020.0215 以降である必要があります。

Citrix ライセンスサーバーに互換性があることを確認してください

Citrix ライセンスサーバーに新しいバージョンとの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 Citrix コンポーネントをアップグレードする前に、Delivery Controller があるマシンで ISO ファイルに収録されている`XenDesktopServerSetup.exe`インストーラーを実行します。互換性に問題がある場合は、問題を解決するための推奨手順がインストーラーから提示されます。
- インストールメディアの`XenDesktop Setup`ディレクトリで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示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードします。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールや PowerShell セッションなど、ファイルのロックの原因になりうるすべてのプログラムを終了してください。

マシンを再起動すると、ロックされているファイルや保留中の Windows 更新プログラムがない状態になります。

アップグレードの開始前に、サードパーティの監視エージェントサービスを停止し、無効にしてください。

適切な権限があることを確認する

製品コンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。

サイトデータベースおよびサイトは、自動または手動で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を開始するとスクリプトが生成されます。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、SQL Server Management Studio などのツールを使用して、その他のスクリプトを実行します。

その他の準備作業

- 必要に応じて、テンプレートをバックアップし、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。

事前サイトテスト

Delivery Controllers およびサイトを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。このテストでは、次のことが確認されます：

- サイトデータベースにアクセスでき、バックアップされている
- 基本的な Citrix サービスへの接続が正しく機能している
- Citrix ライセンスサーバーのアドレスが使用可能である
- 構成ログデータベースにアクセスできる

テストの実行後に、その結果のレポートを表示できます。検出された問題を修正し、テストを再実行できます。事前サイトテストを実行して問題を解決できない場合、サイトの仕組みに影響を与える可能性があります。

テスト結果が含まれているレポートは、インストールログと同じディレクトリにある HTML ファイル（PreliminarySiteTestResult.html）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストの実行

- 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アップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページがあります。テストの実行後、レポートを表示して見つかった問題が解決されたら、テストを再実行できます。テストが正常に完了したら、［次へ］をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを表示して問題を解決したら、コマンドを再実行します。

Citrix では Controller およびサイトのアップグレードを続行する前に、事前サイトテストを実行して問題を解決しておくことをお勧めします。テストを実行する時間に比べて十分な利点があります。ただし、この推奨アクションは無効にできます。

- グラフィカルインターフェイスを使用してアップグレードする場合、テストをスキップしてアップグレードを続行できます。
- コマンドラインでアップグレードする場合、テストはスキップできません。デフォルトでは、サイトテストが失敗すると、インストーラーが失敗し、アップグレードは実行されません。通常は、/ignore_site_test_failureオプションが含まれているとサイトテストの失敗は無視され、アップグレードが進行します（例外については、「SQL Server のバージョンチェック」を参照してください）。

複数の **Controller** をアップグレードする場合

1 つの Controller でアップグレードを開始した後、（最初のアップグレードが完了する前に）同じサイトの別の Controller のアップグレードを開始した場合：

- 最初の Controller で事前サイトテストが完了した場合、他の Controller のウィザードに事前サイトテストページは表示されません。
- 他の Controller でアップグレードを開始したときに、最初の Controller でテストが進行中の場合、他の Controller のウィザードにサイトテストページが表示されます。ただし、最初の Controller のテストが終了すると、最初の Controller のテスト結果のみが保持されます。

サイトの正常性に関係しないテストの失敗

- メモリ不足のために事前サイトテストが失敗した場合は、使用可能なメモリを増やしてからテストを再実行してください。
- ユーザーにアップグレードの権限があり、サイトテストを実行していない場合は、事前サイトテストが失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行します。

SQL Server のバージョンチェック

正常な Citrix Virtual Apps and Desktops 展開では、Microsoft SQL Server のバージョンがサイト、モニター、構成ログデータベースでサポートされている必要があります。サポート対象外のバージョンの SQL Server で Citrix 展開環境をアップグレードすると、機能的な問題が発生する可能性があり、サイトがサポートされなくなります。

アップグレードする Citrix リリースで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」で対象リリースについて参照してください。

Controller をアップグレードする場合、サイト、モニター、構成ログデータベースで使用する現在インストールされている SQL Server のバージョンを Citrix インストーラーがチェックします。

- 現在インストールされている SQL Server のバージョンがアップグレードする Citrix リリースでサポートされたバージョンではないと判断した場合:
  - グラフィカルインターフェイス: メッセージが表示されアップグレードが停止します。[**I understand**]、[**Cancel**] を順にクリックして Citrix インストーラーを閉じます（アップグレードを続行することはできません）。
  - コマンドラインインターフェイス:（コマンドに/ignore_db_check_failureオプションが含まれていても）コマンドは失敗します。

  SQL Server のバージョンをアップグレードした後、再度 Citrix アップグレードを開始します。
- インストールされている SQL Server のバージョンがチェックで判断できなかった場合、アップグレードするバージョンでインストールされているバージョンがサポートされているかを確認してください（システム要件）。
  - グラフィカルインターフェイス: メッセージが表示されアップグレードが停止します。
    * 現在インストールされている SQL Server のバージョンがサポートされている場合、[**I understand**] をクリックしてメッセージを閉じ、[**Next**] をクリックして Citrix アップグレードを続行します。
    * 現在インストールされている SQL Server のバージョンがサポートされていない場合、[**I understand**] をクリックしてメッセージを閉じ、[**Cancel**] をクリックして Citrix アップグレードを終了します。SQL Server のバージョンをサポート対象のバージョンにアップグレードした後、再度 Citrix アップグレードを開始します。
  - コマンドラインインターフェイス: メッセージが表示され、コマンドは失敗します。メッセージを閉じた後:
    * 現在インストールされている SQL Server のバージョンがサポートされている場合は、/ignore_db_check_failureオプションで再度コマンドを実行します。
    * 現在インストールされている SQL Server のバージョンがサポートされていない場合、サポートされているバージョンにアップグレードしてください。再度コマンドを実行して Citrix アップグレードを開始します。

SQL Server のアップグレード

新しい SQL Server を起動してサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、SQL Server Express（サイト作成時に Citrix 製品が自動的にインストール）を使用している場合:

1. 最新の SQL Server Express バージョンをインストールします。
2. データベースを接続解除します。
3. 新しい SQL Server Express にデータベースを接続します。
4. 接続文字列を移行します。

詳しくは、「接続文字列の構成」および Microsoft SQL Server の製品ドキュメントを参照してください。

SQL Server Express LocalDB の置き換え

バージョン 1912 より前の Delivery Controller をインストールしている場合、Microsoft SQL Server Express LocalDB 2014 が自動的にインストールされています。このソフトウェアは、ローカルホストキャッシュ機能で使用されます。

Citrix Virtual Apps and Desktops バージョン 1912 以降では、Delivery Controller をインストールすると、新しいバージョンの SQL Server Express LocalDB がインストールされます。

ただし、展開をバージョン 1912 以降にアップグレードすると、SQL Server Express LocalDB のバージョンは自動的にアップグレードされません。このセクションのガイダンスを使用して、ソフトウェアを新しいバージョンに置き換えます。

必要な準備:

- （アップグレードするバージョンの）Citrix Virtual Apps and Desktops インストールメディア。メディアには Microsoft SQL Server Express LocalDB 2017 のコピーが含まれています。
- Windows Sysinternals ツールを Microsoft サイトからダウンロード。

手順:

1. Citrix Virtual Apps and Desktops コンポーネント、データベース、サイトのアップグレードを完了します（これらのアップグレードによって、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が影響を受けます。SQL Server Express LocalDB を使用するローカルホストキャッシュデータベースは影響を受けません）。
2. Microsoft サイトから Delivery Controller にPsExecをダウンロードします。Microsoft ドキュメントPsExec v2.2を参照してください。
3. Citrix High Availability Service を停止します。
4. コマンドプロンプトでPsExecを実行し、Network Service アカウントに切り替えます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORK SERVICE"cmd
   ```

   必要な場合、whoamiを使用してコマンドプロンプトが Network Service アカウントとして動作しているかを確認できます。

   ```
   whoami
   ```

   ```
   nt authority\network service
   ```

5. SqlLocalDB が含まれるフォルダーに移動します。

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

6. CitrixHA（LocalDB）を停止して削除します。

   ```
   1 SqlLocalDB stop CitrixHA
   2 SqlLocalDB delete CitrixHA
   3 <!--NeedCopy-->
   ```


7. C:\Windows\ServiceProfiles\NetworkServiceで関連ファイルを削除します。

```
HADatabaseName.*
HADatabaseName_log.*
HAImportDatabaseName.*
HAImportDatabaseName_log.*
<!--NeedCopy-->
```

   ヒント: 展開にHAImportDatabaseName.*およびHAImportDatabaseName_log.*が含まれていないことがあります。

8. Windows のプログラムを削除する機能でサーバーから SQL Server Express LocalDB 2014 をアンインストールします。
9. SQL Server Express LocalDB 2017 をインストールします。Citrix Virtual Apps and Desktops インストールメディアのSupport > SQLLocalDBフォルダーでsqllocaldb.msiをダブルクリックします。
10. Citrix High Availability Service を起動します。
11. CitrixHAは、次回の構成の同期で再度作成されます。数分後にSqlLocalDBユーティリティを使用してCitrixHAが再度作成されていることを確認します。

    ```
    SqlLocalDB i

    CitrixHA

    MSSQLLocalDB
    ```

    手順 6 の完了後、SqlLocalDB iを実行した場合、CitrixHAは削除されているため出力には含まれません。手順 10 の完了後は、SqlLocalDB iからの出力にCitrixHAが含まれます。

セキュリティ

April 24, 2021

Citrix Virtual Apps and Desktops 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。Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps または Citrix Virtual Desktops 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、Citrix Virtual Apps and Desktops 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。多要素認証を使用して、Citrix Virtual Apps and Desktops 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

Citrix Virtual Desktops は、ID 管理からウイルス対策ソフトウェアまで、さまざまなサードパーティセキュリティソリューションを統合できます。サポートされている製品の一覧については、http://www.citrix.com/readyを参照してください。

Citrix Virtual Apps and Desktops 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

April 26, 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、「http://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。

プラットフォーム特定のアンチマルウェアソフトウェアの使用を検討します。

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、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/about）に正規登録されています。

すべてのネットワーク通信が正しく保護され、セキュリティポリシーに従って暗号化されている必要があります。IPSec を使用して、Microsoft Windows コンピューターの間でのすべての通信を保護できます。その方法について

詳しくは、使用するオペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、デフォルトで 128 ビット暗号化を行う Citrix SecureICA で保護できます。SecureICA は、デリバリーグループの作成または更新時に設定できます。

Windows ベストプラクティスをアカウント管理に適用します。Machine Creation Services または Provisioning Services によって複製される前に、アカウントをテンプレートやイメージに作成しないでください。保存された、権限が付与されているドメインアカウントを使用して、タスクをスケジュールしないでください。共有 Active Directory マシンアカウントを手動で作成しないでください。こうすることにより、ローカルの永続アカウントのパスワードがマシンへの攻撃によって取得され、他者所有の MCS/PVS 共有イメージへのログオンに使用されるのを阻止することができます。

ユーザー権限の管理

ユーザーには、必要な権限だけを付与します。デスクトップのユーザーには、Microsoft Windows での権限（グループポリシーの［ユーザー権利の割り当て］およびグループメンバーシップ）がそのまま適用されます。このリリースの利点の 1 つは、仮想デスクトップが格納されているコンピューターに対する物理的な制御を許可せずに、デスクトップに対するユーザーの管理権限を付与できることです。

デスクトップ権限を計画するときは、以下の点に注意してください。

- デフォルトでは、権限を持たないユーザーがデスクトップに接続すると、ユーザーデバイスのタイムゾーンではなく、そのデスクトップを実行しているシステムのタイムゾーンが表示されます。デスクトップの使用時にローカルの時刻が表示されるようにする方法については、「デリバリーグループの管理」を参照してください。
- デスクトップの管理者権限を持つユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールデスクトップの場合、管理者権限を持つユーザーはそのデスクトップのすべてのユーザー（将来のユーザーを含む）に信頼されている必要があります。このため、プールデスクトップのすべてのユーザーは、この状況によってデータのセキュリティに永続的な危険性が存在することを認識する必要があります。これは、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。

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。

- マルチセッション OS 対応 Virtual Delivery Agent（VDA）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。
- シングルセッション OS 対応 VDA を含む Citrix Virtual Apps and Desktops 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）：Citrix Virtual Apps または Citrix Virtual Desktops 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）：Citrix Virtual Apps または Citrix Virtual Desktops のメトリックスを収集し、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 Config Synchronizer 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反映させせす。
- 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、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。

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。

```
1 HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer
2 値の名前: AllowMultipleRemotePCAssignments
3 種類: REG_DWORD
```



```
4  値のデータ：0（複数ユーザーの割り当て無効）、1（デフォルト。複数ユーザーの割り当て有効）
```

既存のユーザー割り当てを削除するには、SDK コマンドを使用します。これにより、VDA に単一ユーザーが割り当てられるようになります。

- 割り当てられているすべてのユーザーを VDA から削除するには以下のコマンドを実行します。`$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループから VDA を削除するには、次のコマンドを実行します：`$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

社内の物理 PC を再起動します。

XML 信頼

XML 信頼設定は、以下を使用する展開に適用されます：

- オンプレミス StoreFront。
- パスワードを必要としない利用者（ユーザー）認証テクノロジ。このようなテクノロジの例がドメインパススルー、スマートカード、SAML、Veridium ソリューションです。

XML 信頼設定を有効にすると、ユーザーはアプリケーションを正常に認証して起動できます。Delivery Controller は、StoreFront から送信された資格情報を信頼します。Delivery Controller と StoreFront 間の通信を保護している場合にのみこの設定を有効にします（ファイアウォール、IPsec、またはその他のセキュリティ推奨事項を使用）。

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。

Citrix Virtual Apps and Desktops PowerShell SDK を使用して、XML 信頼設定を確認、有効化、または無効化します。

- XML 信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行して`TrustRequestsSentToTheXMLServiceP`の値を調べます。
- XML 信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`を実行します。
- XML 信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`を実行します。

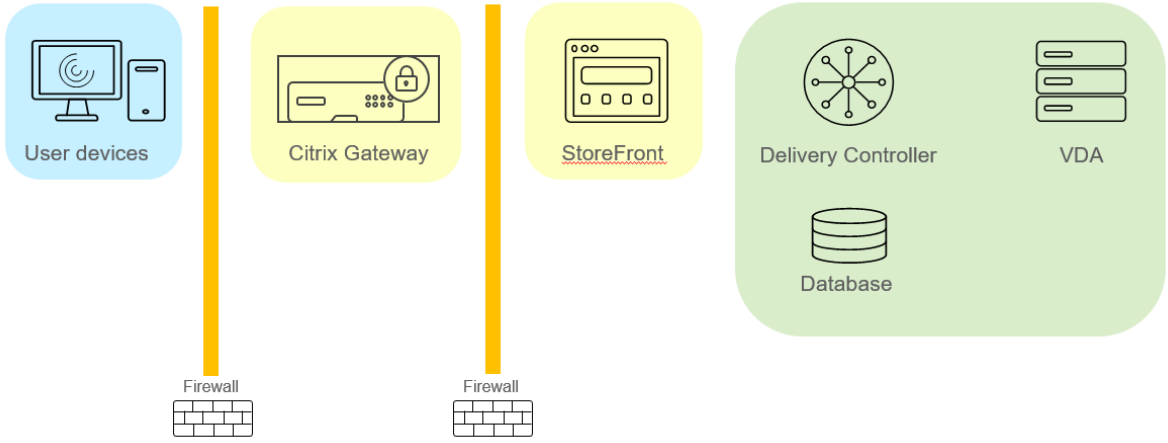
Citrix Virtual Apps and Desktops と Citrix Gateway の統合

April 26, 2021

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、Citrix Gateway を StoreFront の前に追加することをお勧めします。

> 注:
>
> Citrix Virtual Apps and Desktops を Citrix 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。

次の図に、Citrix Gateway を含む簡略化された Citrix の展開例を示します。Citrix Gateway は StoreFront と通信して、Citrix Virtual Apps and Desktops 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 Workspace アプリ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、Citrix Gateway を使用してログオンおよび認証を行います。Citrix 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

April 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	全体的な情報に加えて、指定されたスコープのすべてのオブジェクトを表示できますが、変更はできません。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。監視対象のデリバリーグループについて、マシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンのセッションや電源を管理できます。
マシンカタログ管理者	マシンカタログを作成および管理したり、マシンカタログにマシンをプロビジョニングしたりできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンを使用してマシンカタログを作成できます。この役割では、基本イメージを管理したりソフトウェアをインストールしたりできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信したり、それらのセッションを管理したりできます。ポリシーや電源管理設定など、アプリケーションおよびデスクトップの構成を管理することもできます。
ホスト管理者	ホスト接続およびその関連リソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

この製品の一部のエディションでは、必要に応じてカスタムの役割を作成して、より詳細な権限を委任することができます。カスタムの役割では、コンソールにおける操作またはタスク単位で権限を割り当てることができます。

- スコープ：接続、マシンカタログ、デリバリーグループなど、その管理者が管理できるオブジェクトをグループ化したものです。スコープでは、組織の要件に基づいてオブジェクトをグループ化します（営業チームで使用されるデリバリーグループのセットなど）。オブジェクトを複数のスコープに含めることができます。つまり、1 つまたは複数のスコープでオブジェクトをラベル付けすることができます。組み込みのスコープである「すべて」には、すべてのオブジェクトが含まれています。［すべての管理権限を実行できる管理者］の役割は、常にこのスコープとペアになります。

例

XYZ 社は自社の部署（経理、営業、倉庫）およびそのデスクトップオペレーティングシステム（Windows 7 または Windows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は 5 つのスコープを作成し、各デリバリーグループに 2 つのスコープ（部署を表すスコープと使用するオペレーティングシステムを表すスコープ）を割り当てました。

次の管理者を作成しました。

管理者	役割	スコープ
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。しかし、管理者はこれを考え直しました。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ます。委任管理はありません。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。

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。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。役割やスコープは削除されませ

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：［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：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：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：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。

上ペインに、作成した管理者が表示されます。管理者を選択すると、その詳細が下ペインに表示されます。［警告］列に、管理者に割り当てられた役割とスコープのペアに、使用できない役割またはスコープが含まれているかどうかが示されます。割り当てられた役割とスコープのペアに使用できない役割またはスコープが含まれている場合、次の警告メッセージが表示されます：

- 割り当てられている役割またはスコープが使用できません
  - 管理者からスコープ/役割ペアを削除します。

> 重要：
>
> 警告メッセージは、割り当てられた役割とスコープのペアに使用できない役割またはスコープ（もしくはその両方）が含まれている場合にのみ表示されます。

管理者から役割とスコープのペアを削除するには、次のいずれかの手順を実行します：

- 役割とスコープのペアを削除する。
  1. ［アクション］ペインで、［管理者の編集］をクリックします。
  2. ［管理者の編集］ウィンドウで、役割とスコープのペアを選択し、［削除］をクリックします。
  3. ［**OK**］をクリックして終了します。
- 管理者を削除する。
  1. ［アクション］ペインで、［管理者の削除］をクリックします。
  2. ［**Studio**］ウィンドウで、［削除］をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自身が持っている権限のみを有効にできます。これにより、管理者は現在よりも多くの権限を持つ役割を作成して自身に割り当てる（または既に割り当てられた役割を編集する）ことができなくなります。

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するエディションのみで、［操作］ペインに関連エントリが表示されます。

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：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。
- カスタム役割を作成する：［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：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。
- カスタム役割を編集する：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。
- カスタム役割を削除する：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、Unicode 文字で 64 文字以下の名前を付けることができます。スコープ名には、次の文字は使用できません：バックスラッシュ、スラッシュ、セミコロン、コロン、番号記号、コンマ、アスタリスク、疑問符、等号、

小なり記号、大なり記号、パイプ、角かっこ、丸かっこ、二重引用符、アポストロフィ。説明には、256 文字までの Unicode 文字を入力できます。

スコープをコピーまたは編集するときにオブジェクトをスコープから削除すると、管理者がそのオブジェクトにアクセスできなくなる可能性があることに注意してください。編集するスコープにいくつかの役割が関連付けられている場合は、編集により役割/スコープ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：［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）。
- スコープのコピー：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。
- スコープの編集：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。
- スコープの削除：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\ にあります。

  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、-Showにより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、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

April 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。Citrix Virtual Apps または Citrix Virtual Desktops でスマートカードを使用するには:

- 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。Citrix Virtual Apps または Citrix Virtual Desktops 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、ドキュメントや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。Citrix Virtual Apps and Desktops は、こうした用途に対応しています。

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。Citrix Virtual Apps または Citrix Virtual Desktops 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 Workspace アプリ（Citrix Receiver 4.3 以降）を使用して、Windows 8 および Windows 10 でサポートされます。

- Citrix Virtual Apps and Desktops（旧称 XenApp および XenDesktop）の XenApp および XenDesktop 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、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。

Citrix Virtual Apps and Desktops 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動作確認が行われています。ただし、そのほかのスマートカードおよびミドルウェアも使用できます。Citrix 互換のスマートカードとミドルウェアについて詳しくは、http://www.citrix.com/readyを参照してください。

ミドルウェア	スマートカード
GemAlto Mini Driver for .NET カード	Gemalto .NET v2+

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 Workspace アプリ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にのみ、スマートカードがサポートされます。

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+

高速スマートカード

高速スマートカードは、既存の HDX PC/SC ベースのスマートカードリダイレクトの改良版です。遅延が大きい WAN 環境でスマートカードを使用する場合のパフォーマンスが向上しています。

高速スマートカードは、現在サポートされている Windows 用の VDA がインストールされたホストマシン上ではデフォルトで有効になっています。高速スマートカードを、たとえば診断する目的でホスト側で無効にするには、「暗号化リダイレクトを無効にする」レジストリを任意のゼロ以外の値に設定します:

```
1 HKLM\SOFTWARE\Citrix\SmartCard
2 CryptographicRedirectionDisable (DWORD)
3 <!--NeedCopy-->
```

クライアント側では、高速スマートカードを有効にするには、関連する StoreFront サイトの *default.ica* ファイルに SmartCardCryptographicRedirection ICA パラメーターを含めます:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
```

制限事項:

- 高速スマートカードをサポートしているのは Citrix Receiver for Windows のみです。default.ica ファイルで高速スマートカードを設定している場合、Windows 用以外の Citrix Receiver は、既存の PC/SC リダイレクトでも動作します。
- 高速スマートカードがサポートされているダブルホップシナリオは、両方のホップで高速スマートカードが有効になっている ICA > ICA のみです。高速スマートカードでは ICA > RDP のダブルホップシナリオはサポートされていないため、これらのシナリオでは動作しません。
- 高速スマートカードでは Cryptography Next Generation はサポートされていません。したがって、高速スマートカードでは楕円曲線暗号（ECC）スマートカードはサポートされていません。
- 高速スマートカードでは、読み取り専用キーコンテナ操作のみがサポートされています。たとえば、スマートカードを高速スマートカードに登録することはできません。
- 高速スマートカードでは、スマートカード PIN の変更はサポートされていません。

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 Workspace アプリ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 Workspace アプリ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、Citrix Virtual Apps and Desktops 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。

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:
>
> Citrix Virtual Apps または Citrix Virtual Desktops 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、Citrix Virtual Apps and Desktops と互換性がある必要があります。詳しくは、ベンダーのドキュメントを参照してください。ミニドライバーモデルのスマートカードを使用する仮想デスクトップでは、スマートカードミニドライバーが自動的にダウンロードされます。また、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。さらに、PKCS#11 ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要：Citrix ソフトウェアをインストールする前に、物理的なコンピューターにドライバーと CSP ソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10 で実行する Internet Explorer でスマートカードを実行するユーザーの信頼済みサイトの一覧に Citrix Receiver 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 Workspace アプリや 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 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.** Citrix 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 Workspace アプリ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。
- Windows 向け Citrix Workspace アプリ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 Workspace アプリ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

April 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	Citrix Gateway 経由で接続
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	Citrix Gateway 経由で接続

種類	StoreFront への接続
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。

Citrix 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、Citrix 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 Citrix Gateway にログオンできます。これにより、Citrix 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、Citrix 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 Citrix 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。

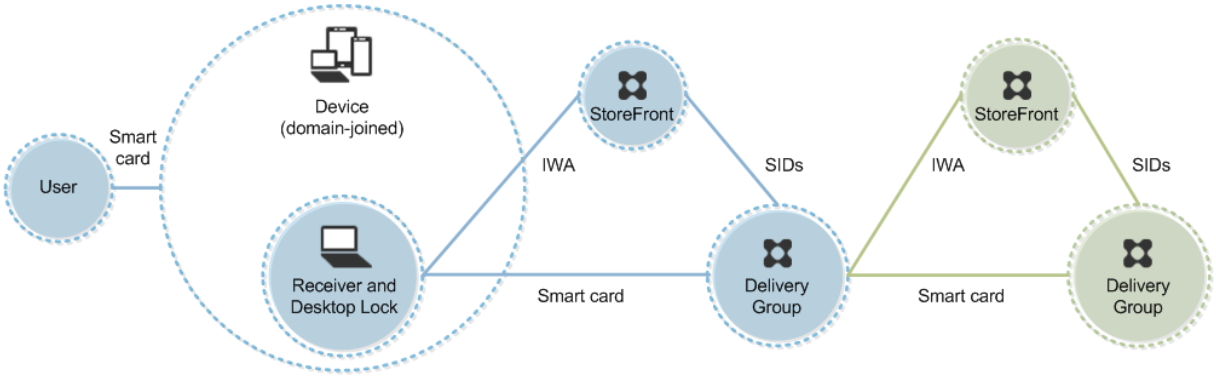
ポリシー設定	デスクトップの動作
何もしない	何もしない。
ワークステーションをロック	デスクトップセッションは切断され、仮想デスクトップはロックされます。
ログオフを強制する	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効な場合、セッションはログオフされてユーザーのデータは消失します。
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

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。

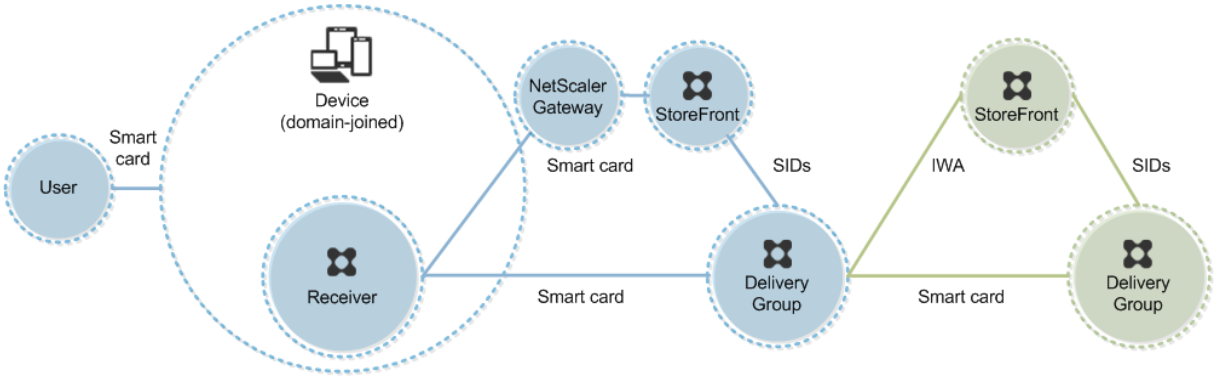


ユーザーは、スマートカードと PIN を使ってデバイスにログオンします。Receiver は、StoreFront サーバーにアクセスするユーザーを統合 Windows 認証（IWA）で認証します。StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。Receiver でシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要はありません。

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、Citrix 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。



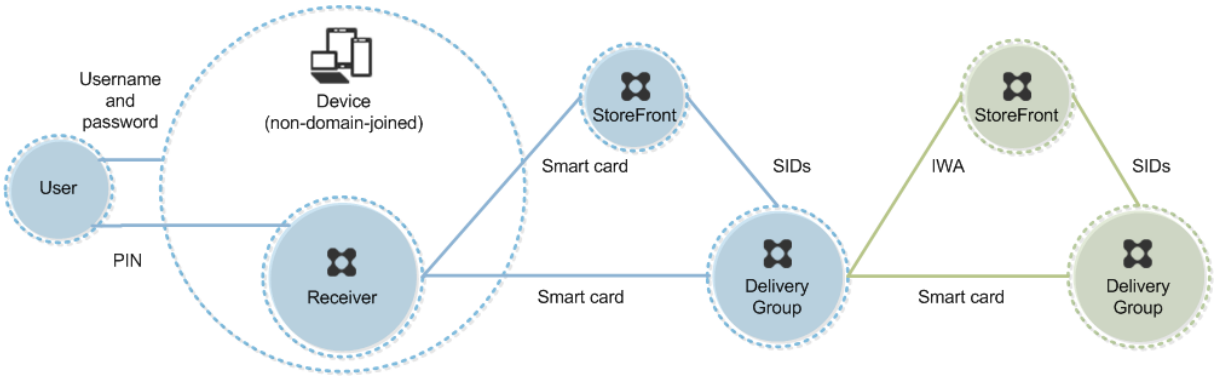
ユーザーはスマートカードと PIN を使ってデバイスにログオンし、次に Citrix Gateway/Access Gateway にもう一度ログオンします。この展開では Receiver で 2 モード認証を使用できるため、この 2 つ目のログオンではスマートカードと PIN を使用したりユーザー名とパスワードを入力したりできます。

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 Citrix Virtual Apps または Citrix Virtual Desktops 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。



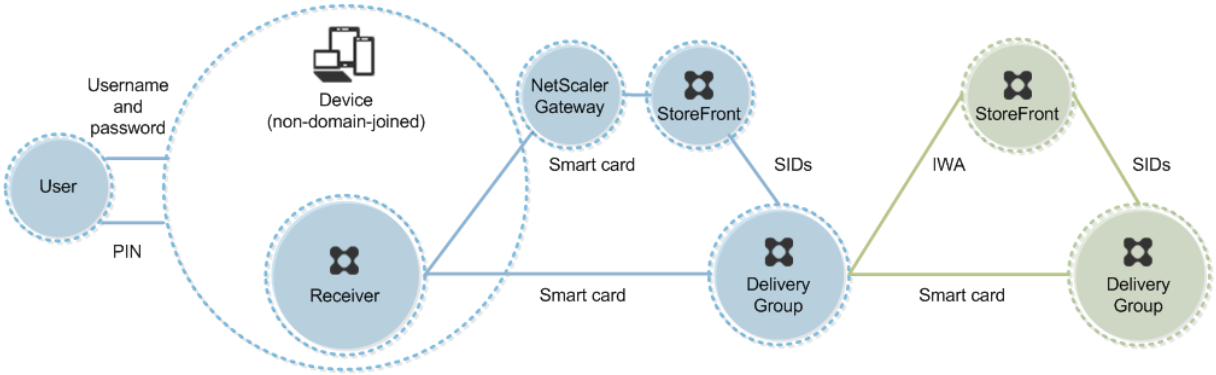
ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。この展開では 2 モード認証を使用できるため、Receiver ではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。その後、Receiver が Storefront への認証を実行します。

StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops 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。

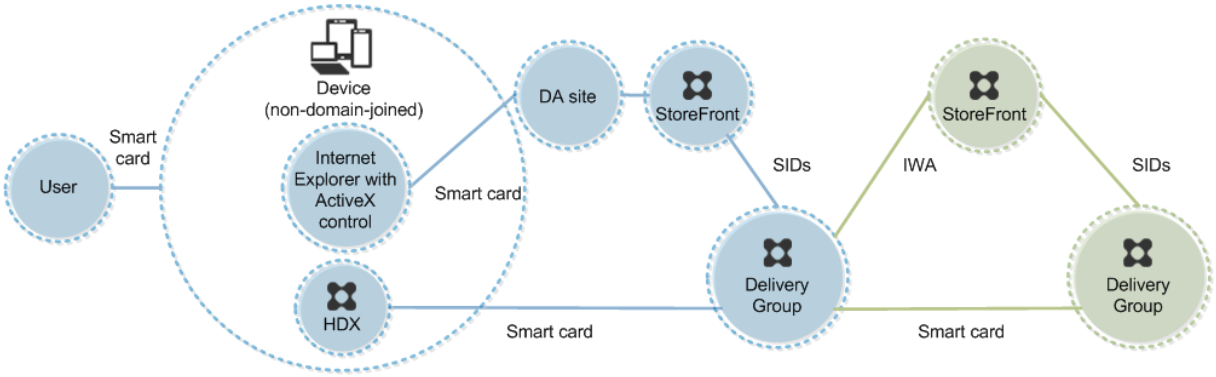
StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要があります。

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、Citrix Virtual Apps、Citrix Virtual Desktops、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。



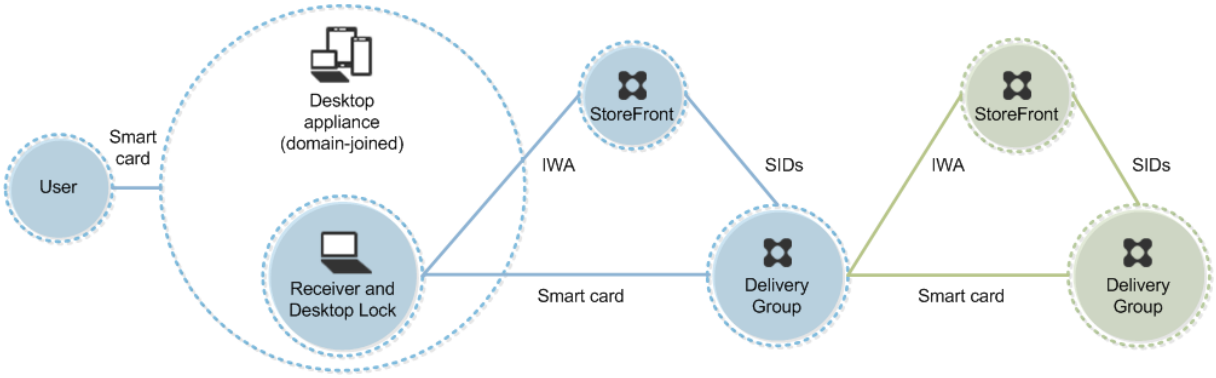
ユーザーは、スマートカードを使ってデバイスにログオンします。Desktop Lock を実行するデバイスは、キオスクモードで動作する Internet Explorer を介してデスクトップアプライアンスサイトを起動するように構成されます。サイトの ActiveX コントロールにより PIN の入力が求められ、それが StoreFront に送信されます。StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。割り当てられたデスクトップグループ一覧で使用可能な（アルファベット順で）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、Citrix Virtual Apps、Citrix Virtual Desktops、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 Citrix Virtual Apps または Citrix Virtual Desktops 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

April 26, 2021

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Citrix Gatewayのドキュメントを参照してください。

シングルサインオン機能を使用できるかどうかは、以下を含むさまざまな要因により決定されます。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアの PIN キャッシュポリシー。

> 注:
>
> スマートカードリーダーが接続されたマシン上の Virtual Delivery Agent（VDA）にユーザーがログオンすると、前回使用された認証方法（スマートカードまたはパスワードなど）の画面が開く場合があります。この結果、シングルサインオンが有効な場合はシングルサインオン用の画面が開きます。この画面ではログオンできないため、ユーザーは［ユーザーの切り替え］をクリックしてほかの画面を開く必要があります。

アプリ保護

April 26, 2021

アプリ保護は、Citrix Workspace アプリのアドオン機能で、Citrix Virtual Apps and Desktops 公開リソースの使用時にセキュリティを強化する機能です。

2 つのポリシーは Citrix HDX セッションでキーロガー対策および画面キャプチャ対策機能を提供します。Windows 向け Citrix Workspace アプリ 1912 以降または Mac 向け Citrix Workspace アプリ 2001 以降のこれらのポリシーは、キーロガーやスクリーンスクレーパーからデータを保護するのに役立ちます。

キーロガー対策が有効な場合:

- キーロガーには暗号化されたキーストロークが表示されます。
- この機能は、保護ウィンドウにフォーカスがある場合にのみアクティブになります。

画面キャプチャ対策が有効な場合:

- キャプチャする画面は、Windows OS では空白の画面になります。macOS では、保護されたウィンドウのコンテンツのみが空白になります。
- 保護されたウィンドウが表示されている（最小化されていない）場合、この機能がアクティブになります。

これらのポリシーは PowerShell のみで構成します。GUI の管理機能はありません。この設定が必要となるのは、特定のデリバリーグループの機能を有効または無効にする場合だけです。

この機能の購入後、アプリ保護ライセンスとアプリ保護ポリシーを有効にして、`FeatureTable.OnPrem.AppProtection.xml`機能テーブルをインポートしてください。

> 免責:
>
> アプリ保護ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングすることで有効になります（画面のキャプチャまたはキーボードの操作が必要な特定の API 呼び出し）。つまり、このアプリ保護ポリシーは、カスタムの目的別に構築されたハッカーツールに対しても保護を提供できます。ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てきます。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。

制限事項

これらの制限は設計段階で存在します:

- HDX または RDP セッションでは、キーロガー対策はサポートされていません。エンドポイント保護は引き続きアクティブです。この制限は、ダブルホップシナリオにのみ適用されます。
- Citrix Workspace アプリまたは Citrix Receiver のサポートされていないバージョンを使用する場合、この機能はサポートされません。この場合、リソースは非表示になります。
- Citrix Cloud サービスの機能サポートはありません。アプリ保護は、オンプレミスの Citrix Virtual Apps and Desktops 環境でのみサポートされます。
- StoreFront Web ストアの機能サポートはありません。

正常な動作

正常な動作は、保護されたリソースが含まれる StoreFront ストアにアクセスする方法によって異なります。リソースには、サポートされるネイティブの Citrix Workspace アプリクライアントを使用してアクセスできます。

- **StoreWeb** での動作 - アプリ保護ポリシーが有効なアプリケーションは StoreFront Web ストアで列挙されません。
- サポートされていない **Citrix Receiver** または **Citrix Workspace** アプリでの動作 - アプリ保護ポリシーが有効なアプリケーションは列挙されません。
- サポートされているバージョンの **Citrix Workspace** アプリでの動作 - 保護されたリソースが列挙され正常に起動します。

以下の条件下で保護が適用されます:

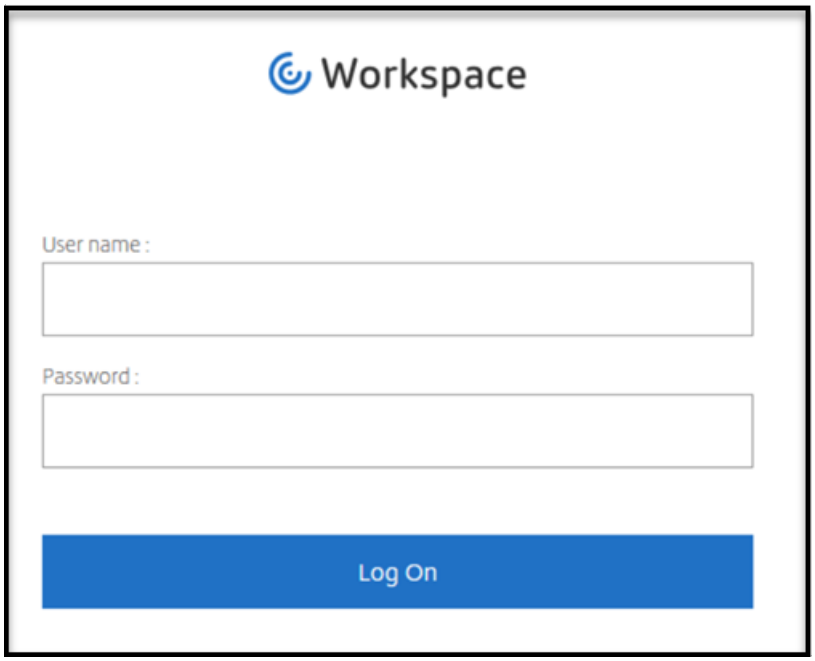
- スクリーンキャプチャ対策 - 保護されたウィンドウが画面に表示されている場合に有効になります。保護を無効にする場合は、すべての保護ウィンドウを最小化します。
- キーロガー対策 - 保護されたウィンドウにフォーカスがある場合に有効になります。保護を無効にする場合は、フォーカスを別のウィンドウに移動します。

アプリ保護によって保護される内容

Citrix Workspace アプリ以外のウィンドウのスクリーンショットをキャプチャするには、最初に保護されたウィンドウを最小化する必要があります。

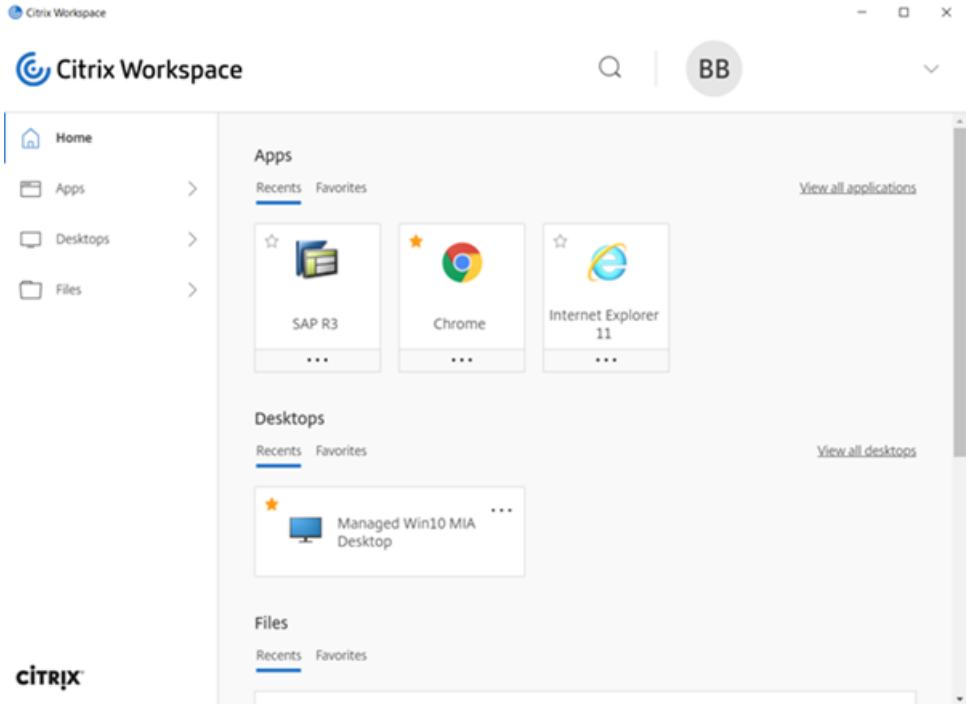
デフォルトでは、アプリ保護は次の Citrix のウィンドウを保護します:

- **Citrix** ログオンウィンドウ - Citrix Workspace の認証ダイアログボックスは、Windows オペレーティングシステムでのみ保護されます。



- **Citrix Workspace** アプリの **HDX** セッションウィンドウ（管理されたデスクトップの例）

- セルフサービスストアウィンドウ



アプリ保護によって保護されていない内容

ナビゲーションバーの Citrix Workspace アプリアイコンの項目:

- コネクションセンター
- 高度な設定のすべてのリンク
- 個人設定

- 更新プログラムのチェック
- サインアウト

システム要件

Citrix コンポーネントの最小バージョン:

- Windows 向け Citrix Workspace アプリ 1912 長期サービスリリースのリリース
- Windows 向け Citrix Workspace アプリ 2002
- Mac 向け Citrix Workspace アプリ 2001
- StoreFront 1912
- Delivery Controller 1912
- 有効な Citrix ライセンス
  - アプリ保護のアドオンライセンス
  - Citrix Virtual Apps and Desktops 1912

オペレーティングシステムプラットフォーム:

エンドポイントでサポートされるオペレーティングシステムです。VDA は、すべてのオペレーティングシステムをサポートしています。

- Windows 10
- Windows 8.1
- Windows 7
- macOS High Sierra（10.13）以降

構成

アプリ保護を購入後、完全に構成して機能を有効にするには、次の手順を実行します:

1. アプリ保護ライセンスをインポートします。
2. Workspace アプリを構成します。
3. `FeatureTable.OnPrem.AppProtection.xml`機能テーブルをインポートします。
4. Delivery Controller でアプリ保護ポリシーを有効にします。

1. ライセンス

アプリ保護を利用するには、Citrix ライセンスサーバーにアドオンライセンスをインストールする必要があります。Citrix Virtual Desktops 1912 以降のバージョンのライセンスが必要です。アプリ保護アドオンライセンスを購入する場合は、シトリックスの営業担当者にお問い合わせください。

1. ライセンスファイルをダウンロードして、既存の Citrix Virtual Desktops ライセンスとともに Citrix ライセンスサーバーにインポートします。

2. Citrix Licensing Manager を使用してライセンスファイルをインポートするか（優先される方法）、またはライセンスサーバーのライセンスファイルを`C:\Program Files (x86)\Citrix\Licensing\MyFiles`にコピーして、Citrix Licensing サービスを再起動します。詳しくは、「ライセンスのインストール」を参照してください。

2. Citrix Workspace アプリ

Citrix Workspace アプリでアプリ保護を構成します。

Windows 向け **Citrix Workspace** アプリ：

以下の方法で、Citrix Workspace アプリにアプリ保護コンポーネントを追加できます：

- Citrix Workspace アプリのインストール時。
- Citrix Workspace アプリインストール後にコマンドラインインターフェイスを使用。

Citrix Workspace アプリのインストール時に/`includeappprotection`スイッチを有効にしたことを確認します。

詳しくは、「アプリ保護」を参照してください。

Mac 向け **Citrix Workspace** アプリ：

Mac 向け Citrix Workspace アプリでは、別途アプリ保護を構成する必要はありません。

3. 機能テーブルファイル

この機能の購入後、アプリ保護ライセンスとアプリ保護ポリシーを有効にして、`FeatureTable.OnPrem.AppProtection.xml`機能テーブルをインポートしてください。

Citrix Virtual Apps and Desktops 1912 以降のダウンロードページの **Components** セクションには必要な XML ファイルが含まれています。ファイルをダウンロードするには Citrix アカウントが必要です。

デフォルトでは、アプリ保護は無効になっています。この機能を有効にするには、`Import-ConfigFeatureTable`コマンドレットを使用してアプリ保護が有効になっている`FeatureTable.OnPrem.AppProtection.xml`機能テーブルをインポートします。このコマンドレットをサイト全体で一度実行します。詳しくは、「Import-Configfeaturetable」を参照してください。

```
Import-ConfigFeatureTable -Path .\FeatureTable.OnPrem.AppProtection.xml
```

インストール済みの任意の Delivery Controller マシンで、または FMA PowerShell スナップインとともにスタンドアロンの Studio がインストールされたマシンでこのコマンドレットを実行できます。

アプリ保護が有効になっていることを確認するには、`Get-ConfigEnabledFeature | Select-String -Pattern 'AppProtection'`を実行します。

4. デリバリーグループ

インストール済みの任意の Delivery Controller マシンで、または FMA PowerShell スナップインとともにスタンドアロンの Studio がインストールされたマシンで PowerShell SDK を使用して、アプリ保護デリバリーグループの次のプロパティを有効にします。

- AppProtectionKeyLoggingRequired：True
- AppProtectionScreenCaptureRequired：True

いずれかのポリシーを各デリバリーグループで個別に有効にできます。たとえば、DG1 でのみキーロガーからの保護を構成でき、DG2 でのみ画面キャプチャからの保護を構成できます。DG3 で両方のポリシーを有効にできます。

例：

DG3 という名前のデリバリーグループで両方のポリシーを有効にするには、サイトの Delivery Controller で次のコマンドを実行します：

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

この設定を検証するには、次のコマンドレットを実行します：

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired,
AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

さらに、XML 信頼を有効にします：

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

StoreFront と Broker の間のネットワークを確実に保護してください。詳しくは、Knowledge Center のCTX236929およびXenApp および XenDesktop XML Service の保護を参照してください。

推奨

アプリ保護ポリシーは、主にエンドポイントのセキュリティと保護を強化することに重点を置いています。環境に関するその他のセキュリティ推奨事項とポリシーをすべて確認します。セキュリティと制御のポリシーテンプレートは、許容率が低い環境での推奨構成に使用できます。詳しくは、「ポリシーテンプレート」を参照してください。

トラブルシューティング

アプリケーションが列挙されていないか起動していません：

- 影響を受けるユーザーが Citrix Workspace アプリのサポートされているバージョンを使用していることを確認します。
- StoreFront サーバーでこの機能が有効になっていることを確認します。
- デリバリーグループの適切な機能が有効になっていることを確認します。

アプリ保護ポリシーが適切に適用されていません：

- StoreFront で機能が有効になっていることを確認します。
- デリバリーグループの適切な機能が有効になっていることを確認します。
- この機能がエンドポイントにインストールされていることを確認します。
- 影響を受けるユーザーが Citrix Workspace アプリのサポートされているバージョンを使用していることを確認します。
- Citrix Workspace アプリのインストール時に/includeappprotection スイッチを有効にしたことを確認します。

Citrix ウィンドウ以外でスクリーンショットが機能していません:

- 保護されている Citrix ウィンドウを最小化するか閉じます。

Transport Layer Security（TLS）

April 26, 2021

Citrix Virtual Apps and Desktops は、コンポーネント間の TCP ベースの接続で TLS（Transport Layer Security）プロトコルをサポートしています。Citrix Virtual Apps and Desktops は、アダプティブトランスポートを使用して、UDP ベースの ICA/HDX 接続用の DTLS（Datagram Transport Layer Security）プロトコルもサポートしています。

TLS と DTLS は似ており、同じデジタル証明書をサポートします。TLS を使用するように Citrix Virtual Apps サイトまたは Citrix Virtual Desktops サイトを設定すると、DTLS も使用するように設定されます。次の手順を使用します。これらの手順は、TLS と DTLS の両方に共通していますが、以下の点が異なります。

- 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。

- Citrix Workspace アプリと Virtual Delivery Agent（VDA）間の TLS 接続を有効にします。これを行うには、以下のタスクを実行する必要があります:
  - 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）。概要については、「VDA 上の TLS 設定」を参照してください。TLS/DTLS を設定するには、Citrix 提供の PowerShell スクリプトを使用することを強くお勧めします。詳しくは、「VDA 上の TLS 構成：PowerShell スクリプトの使用」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「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。
* Machine Creation Services または Provisioning Services によってプロビジョニングされたプールされた VDA では、VDA マシンイメージは再起動時にリセットされ、以前の TLS 設定は失われます。VDA を再起動するたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

> 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の TLS を有効にする方法については、CTX137556を参照してください。

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。サーバー証明書を入手して Controller 上にインストールおよび登録し、TLS 証明書のポート構成を行うには、以下のタスクが必要です。

Controller に IIS がインストールされている場合は、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771438(v=ws.10)の手順に従ってください。

Controller に IIS がインストールされていない場合は、以下の方法で証明書を構成します。

1. http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspxの手順に従って、TLS サーバー証明書を入手し Controller にインストールします。certreq ツールについて詳しくは、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736326(v=ws.10)を参照してください。
2. ポートで証明書を構成します。https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificateを参照してください。

Controller を Windows Server 2016 にインストールし、StoreFront を Windows Server 2012 にインストールする場合は、TLS の暗号の組み合わせ順を変更するために、Controller で構成を変更する必要があります。

> 注:
>
> 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。また、これらの暗号の組み合わせを TLS_DHE_ の暗号の組み合わせより前に配置する必要があります。

> 注:
>
> 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。

> 注:
>
> ポートが変更されると、ライセンスの互換性およびアップグレードに関するメッセージが Studio に表示されます。この問題を解決するには、以下の PowerShell コマンドレットを順に実行してサービスインスタンスを再登録してください:

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
      XML_HTTPS |
```



```
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
<!--NeedCopy-->
```

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 構成を完了しておいてください。

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。サポートされる SSL プロトコルを指定するときは、許可する最低バージョンを指定します。

  たとえば、最低バージョンとして TLS 1.1 を指定すると、TLS 1.1 および TLS 1.2 のプロトコルを使用した接続が許可されます。最低バージョンとして SSL 3.0 を指定すると、サポートされる SSL プロトコルのすべてのバージョンが許可されます。最低バージョンとして TLS 1.2 を指定すると、TLS 1.2 の接続のみが許可されます。

  DTLS 1.0 は TLS 1.1 に対応し、DTLS 1.2 は TLS 1.2 に対応します。

- どの **TLS** 暗号の組み合わせが許可されるのか。

  暗号の組み合わせにより、この接続において使用する暗号化が選択されます。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 Workspace アプリまたは 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 は、GOV（ernment）、COM（mercial）、および ALL の 3 つの暗号の組み合わせ（コンプライアンスモードとも呼ばれます）をサポートします。確立できる暗号スイートは、Windows の FIPS モードによっても異なります。Windows の FIPS モードについては、http://support.microsoft.com/kb/811833を参照してください。次の表は、各セットの暗号の組み合わせを示しています:

TLS/DTLS 暗号の組み合わせ	**ALL**	**COM**	**GOV**	**ALL**	**COM**	**GOV**
FIPS モード	無効	無効	無効	有効	有効	有効
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*	○		○	○		○
TLS_ECDHE_	○		○	○		○
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA				○	○	

* Windows Server 2012 R2 ではサポートされていません。

> 注:
>
> VDA では、DHE 暗号スイート（例:TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CB TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）はサポートされません。これらの暗号スイートが Windows で選択されても、Citrix Receiver では使用できません。
>
> Citrix Gateway を使用している場合、バックエンド通信に対する暗号の組み合わせのサポートについては、Citrix ADC のドキュメントを参照してください。TLS がサポートする暗号の組み合わせについては、「Citrix ADC アプライアンスで利用可能な暗号」を参照してください。DTLS がサポートする暗号の組み合わせについては、「DTLS 暗号サポート」を参照してください。

VDA 上の **TLS** 構成：**PowerShell** スクリプトの使用

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にある TLS 証明書をインストールします。その場所に複数の証明書が存在する場合は、証明書の拇印を PowerShell スクリプトに指定します。

> 注:
>
> PowerShell スクリプトは、XenApp および XenDesktop 7.16 LTSR から、VDA の完全修飾ドメイン名に基づいて正しい証明書を検索します。VDA の完全修飾ドメイン名に 1 つの証明書のみが存在する場合は、拇印を指定する必要はありません。

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。

TLS を有効にすると、DHE の暗号の組み合わせは無効になります。ECDHE の暗号の組み合わせは影響を受けません。

TLS を有効にすると、スクリプトは指定された TCP ポートの既存の Windows ファイアウォール規則をすべて無効にします。その後、ICA サービスが TLS TCP および UDP ポートでのみ着信接続を受け入れることを許可する新しい規則を追加します。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）

ユーザーは TLS または DTLS を使用した場合にのみ接続できるようになります。TLS または DTLS 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。

> 注:
>
> DTLS は、ICA/HDX の UDP でのオーディオリアルタイムトランスポート、または ICA/HDX Framehawk ではサポートされていません。

「ネットワークポート」を参照してください。

このスクリプト内には、以下の構文および使用例が記載されています。Notepad++ などのツールを使用してこれらを参照できます。

> 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>"]
```


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。デフォルトは以下のとおりです。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。有効な値:「TLS_1.0」（デフォルト）、「TLS_1.1」、「TLS_1.2」。
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 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 443 '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（Windows シングルセッション OS 対応 VDA の場合）または NT SERVICE\TermService（Windows マルチセッション OS 対応 VDA の場合）に付与します。VDA がインストールされたマシン上で、以下の手順を行います：

手順 **1**：Microsoft 管理コンソール（MMC）を起動します：［スタート］>［ファイル名を指定して実行］> mmc.exe。

手順 **2**：MMC に証明書スナップインを追加します。

1. ［ファイル］>［スナップインの追加と削除］の順に選択します。
2. ［証明書］を選択して［追加］をクリックします。
3. ［このスナップインで管理する証明書］で［コンピューターアカウント］をクリックし、［次へ］をクリックします。
4. ［このスナップインで管理するコンピューター］で［ローカルコンピューター］をクリックし、［完了］をクリックします。

手順 **3**：コンソールツリーの［証明書（ローカルコンピューター）］>［個人］>［証明書］で証明書を右クリックして、［すべてのタスク］>［秘密キーの管理］の順に選択します。

手順 **4**：アクセス制御リストエディターで［(FriendlyName）プライベートキーのアクセス許可］ダイアログボックスが開きます。ここで（FriendlyName）は、TLS 証明書の名前です。以下のいずれかのサービスを追加して、［読み取り］アクセスを許可します。

- Windows シングルセッション OS 対応 VDA では「PORTICASERVICE」
- Windows マルチセッション OS 対応 VDA では「TERMSERVICE」

手順 **5**：インストールした TLS 証明書をダブルクリックします。［証明書］ダイアログボックスの［詳細］タブをクリックして、一番下までスクロールします。［拇印］をクリックします。

手順 **6**：regedit を実行して、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd を開きます。

1. SSL Thumbprint キーを編集して、TLS 証明書の拇印の値をバイナリ値にコピーします。［バイナリ値の編集］ダイアログボックスでは、不明な項目（「0000」や特殊文字など）は無視して構いません。
2. SSLEnabled キーを編集して、DWORD 値を 1 に変更します（この DWORD 値を 0 にすると SSL が無効になります）。
3. このレジストリパスでは、必要に応じて以下のデフォルト値を変更できます。

   SSLPort の DWORD 値 – SSL ポート番号。デフォルト：443。

SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.2、3 = TLS 1.1、4 = TLS 1.2。デフォルト：2（TLS 1.2）。

SSLCipherSuite の DWORD 値 – 1 = GOV、2 = COM、3 = ALL。デフォルト：3（ALL）。

手順 **7**：デフォルトの 443 以外の TLS TCP ポートおよび UDP ポートを使用する場合は、そのポートが Windows ファイアウォールで開放されていることを確認します（Windows ファイアウォールで受信規則を作成するときは、［接続を許可する］および［有効］が選択されていることを確認してください）。

手順 **8**：ほかのアプリケーションやサービスなど（IIS など）がその TLS TCP ポートを使用していないことを確認します。

手順 **9**：Windows マルチセッション OS 対応 VDA の場合は、変更を適用するためのマシンを再起動します（Windows シングルセッション OS 対応 VDA のマシンを再起動する必要はありません）。

> 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）、HTML5 向け Citrix Workspace アプリ、および Chrome 向け Citrix Workspace アプリからの接続に影響します。これには、Citrix Gateway を使用した接続も含まれます。
>
> この手順は、Citrix 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 Citrix 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 2012 R2、Windows Server 2016、または Windows 10 Anniversary Edition 以降）上で、［コンピューターの構成］>［ポリシー］>［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_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> 注：
>
> 最初の 6 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、暗号の組み合わせは、クライアント（Citrix Workspace アプリまたは 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。

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。

Windows 向け Citrix Workspace アプリで TLS 関連の接続エラーが発生した場合は、Desktop Viewer を無効にしてから接続を再試行してください。接続エラーは解決されないままでも、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。

HDX アダプティブトランスポートを使用するほとんどの構成は、DTLS で正常に機能します（最新バージョンの Citrix Workspace アプリ、Citrix Gateway、および VDA を使用する DTLS など）。Citrix Workspace アプリと Citrix Gateway との間で DTLS を使用する構成、および Citrix Gateway と VDA との間で DTLS を使用する構成には、追加で操作が必要な場合があります。

次の場合は、追加で操作が必要になります。

- HDX アダプティブトランスポートおよび DTLS をサポートする Citrix Receiver バージョン：Receiver for Windows（4.7、4.8、4.9）、Receiver for Mac（12.5、12.6、12.7）、Receiver for iOS（7.2、7.3.x）、または Receiver for Linux（13.7）

および、次のいずれかにも該当する場合:

- Citrix Gateway バージョンで VDA への DTLS がサポートされていますが、VDA バージョンで DTLS（バージョン 7.15 以前）がサポートされていません。
- VDA バージョンで DTLS（バージョン 7.16 以降）がサポートされていますが、Citrix Gateway バージョンで VDA への DTLS がサポートされていません。

Citrix Receiver からの接続が失敗しないようにするには、次のいずれかを実行します。

- Citrix Receiver を、Receiver for Windows Version 4.10 以降、Receiver for Mac 12.8 以降、または Receiver for iOS Version 7.5 以降に更新します。または、
- Citrix Gateway を、VDA への DTLS をサポートしているバージョンに更新します。または、
- VDA をバージョン 7.16 以降に更新します。または、
- VDA で DTLS を無効にします。または、
- HDX アダプティブトランスポートを無効にします。

> 注:
>
> Receiver for Linux 用の適切な更新プログラムは、まだ利用できません。Receiver for Android（バージョン 3.12.3）は、HDX アダプティブトランスポート、および Citrix Gateway を介した DTLS をサポートしていないため、影響を受けません。
>
> VDA で DTLS を無効にするには、VDA ファイアウォール構成を変更して UDP ポート 443 を無効にします。「ネットワークポート」を参照してください。

Controller と **VDA** の間の通信

Windows Communication Framework（WCF）のメッセージレベルの保護によって、Controller と VDA との間の通信がセキュリティで保護されます。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、およびブラウザーコンテンツリダイレクト

HTML5 ビデオリダイレクションおよびブラウザーコンテンツリダイレクトを使用して、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。

Web ブラウザーコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクションについて詳しくは、「マルチメディアのポリシー設定」を参照してください。

ユニバーサルプリントサーバーの **Transport Layer Security**（**TLS**）

April 24, 2021

Transport Layer Security（TLS）プロトコルは、Virtual Delivery Agent（VDA）とユニバーサルプリントサーバーとの間の TCP ベースの接続でサポートされています。

> 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。

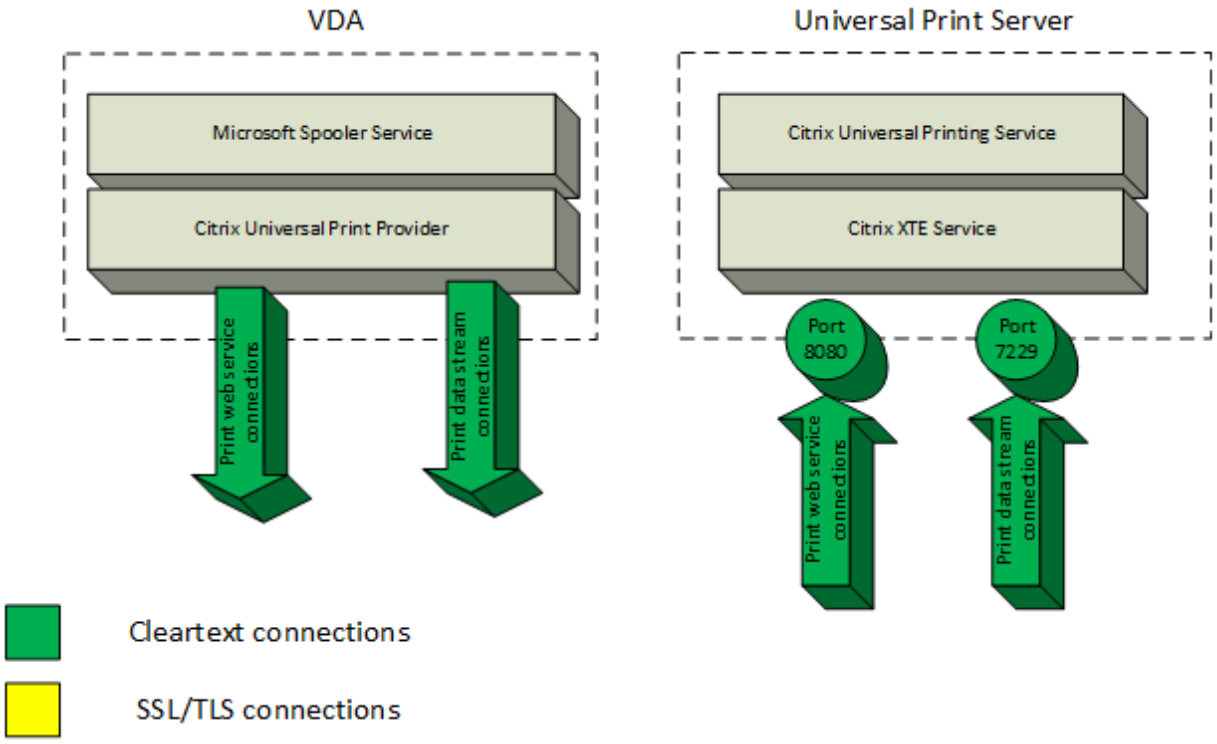
VDA とユニバーサルプリントサーバー間の印刷接続の種類

クリアテキスト接続

印刷に関連する次の接続は VDA から開始され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、［**SSL** が有効］ポリシー設定が **Disabled**（デフォルト）に設定されている場合のみ確立されます。

- クリアテキスト印刷 Web サービス接続（TCP ポート：8080）
- クリアテキスト印刷データストリーム（CGP）接続（TCP ポート：7229）

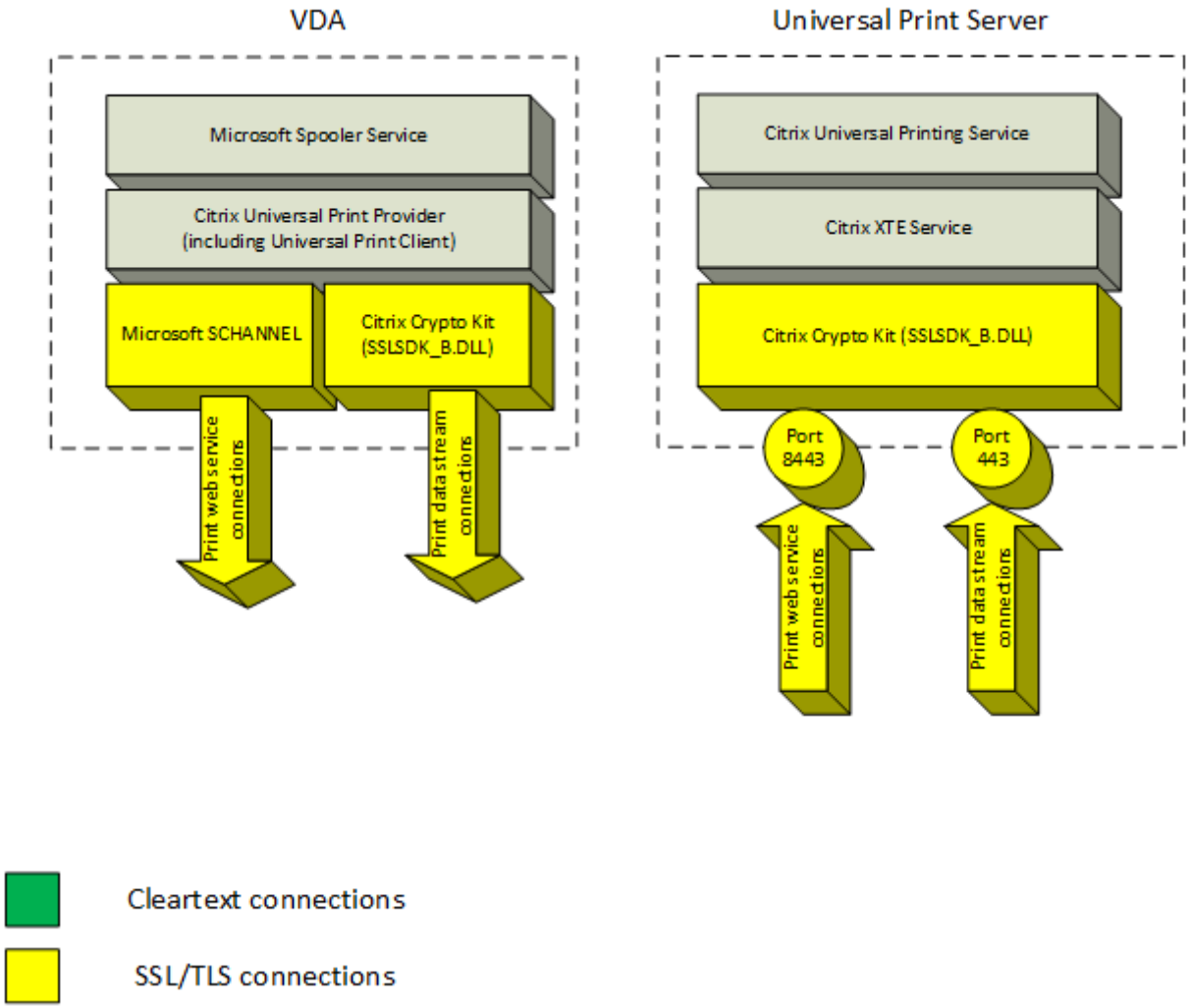
Microsoft Windows 印刷スプーラーサービスで使用されるポートについては、Microsoft 社のサポート文書「Windows のサービス概要およびネットワークポート要件」を参照してください。このドキュメントの SSL/TLS 設定は、NETBIOS および Windows 印刷スプーラーサービスで確立された RPC 接続には適用されません。［ユニバーサルプリントサーバーの有効化］ポリシー設定が ［有効。**Windows** のリモート印刷機能にフォールバックする］に設定されている場合、VDA は Windows ネットワーク印刷プロバイダー（win32spl.dll）をフォールバックとして使用します。



暗号化された接続

印刷に関連する SSL/TLS 接続は、VDA から開始されユニバーサルプリントサーバーのポートに接続します。これらの接続は、［**SSL** が有効］ポリシー設定が **Enable** に設定されている場合のみ確立されます。

- 暗号化印刷 Web サービス接続（TCP ポート：8443）
- 暗号化印刷データストリーム（CGP）接続（TCP ポート：443）



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft のグループポリシーとレジストリを使用して、暗号化印刷 Web サービス接続（TCP ポート：8443）で Microsoft SCHANNEL SSP を構成します。Microsoft SCHANNEL SSP のレジストリ設定については、Microsoft 社のサポート文書「TLS Registry Settings」を参照してください。

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）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_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> 注:
>
> このグループポリシー設定が構成されている場合、暗号化印刷 Web サービス接続（デフォルトポート：8443）が両方の SSL 暗号の組み合わせ一覧に表示されているときのみ、VDA は暗号の組み合わせを選択します:
>
> - グループポリシーの SSL 暗号の組み合わせ順一覧
> - 選択した SSL 暗号の組み合わせポリシー設定（COM、GOV、または ALL）に関連した一覧
>
> 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の組み合わせを必要とする場合、このグループポリシーの暗号の組み合わせ順一覧に追加することが必要な場合があります。
>
> 重要:
>
> 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。
>
> Citrix ポリシーを使用して暗号化印刷データストリーム（CGP）接続（TCP ポート：443）の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

ユニバーサルプリントサーバーは、SSL/TLS サーバーとして機能します。

`Enable-UpsSsl.ps1` PowerShell スクリプトを使用して SSL/TLS 設定を構成します。

ユニバーサルプリントサーバーに **TLS** サーバー証明書をインストールする

HTTPS 接続を使用する場合、ユニバーサルプリントサーバー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。クライアント証明書はサポートしません。Microsoft Active Directory 証明書サービスまたは他の証明機関を使用して、ユニバーサルプリントサーバーの証明書を要求します。

証明書サービスを使用して証明書を登録/要求する場合、次の点に注意してください:

1. 証明書をローカルコンピューターの個人証明書ストアに配置します。
2. 証明書のサブジェクト識別名（Subject DN）のコモンネーム属性をユニバーサルプリントサーバーの完全修飾ドメイン名（FQDN）に設定します。証明書テンプレートでこれを指定します。
3. 証明書要求や秘密キーの生成に使用される暗号化サービスプロバイダー（CSP）を **Microsoft Enhanced RSA** および **AES Cryptographic Provider**（暗号）に設定します。証明書テンプレートでこれを指定します。
4. キーサイズを 2048 ビット以上に設定します。証明書テンプレートでこれを指定します。

ユニバーサルプリントサーバーで **SSL** を構成する

ユニバーサルプリントサーバー上の XTE サービスは、受信接続を待機します。SSL が有効な場合は、SSL サーバーとして機能します。受信接続には、印刷コマンドを含む印刷 Web サービス接続と、印刷ジョブを含む印刷データストリーム接続の 2 種類があります。これらの接続で SSL を有効にできます。SSL はこれらの接続の機密性と完全性を保護します。デフォルトでは、SSL は無効になっています。

SSL の構成に使用される PowerShell スクリプトはインストールメディアにあり、次のファイル名です: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

ユニバーサルプリントサーバーでリスニングポート番号を構成する

以下は XTE サービス用のデフォルトのポートです:

- クリアテキスト印刷 Web サービス（HTTP）TCP ポート: 8080
- クリアテキスト印刷データストリーム（CGP）TCP ポート: 7229
- 暗号化印刷 Web サービス（HTTPS）TCP ポート: 8443
- 暗号化印刷データストリーム（CGP）TCP ポート: 443

ユニバーサルプリントサーバー上の XTE サービスで使用されるポートを変更するには、管理者として次の PowerShell コマンドを実行します（Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意事項については後述を参照してください）:

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` ま た は `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサルプリントサーバーの **TLS** 設定

負荷分散構成で複数のユニバーサルプリントサーバーがある場合、すべてのユニバーサルプリントサーバー上で一貫した TLS 設定を構成するようにしてください。

ユニバーサルプリントサーバー上に 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ユニバーサルプリントサーバーに付与されます。ユニバーサルプリントサーバーには、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。
- TLS 接続でどの TCP ポートが使用されるのか。

Windows ファイアウォールを使用する環境では、これらの TCP ポートでの受信接続が許可されている必要があります。Enable-UpsSsl.ps1 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。

ユニバーサルプリントサーバーは TLS プロトコルバージョン 1.2、1.1、1.0 をサポートしています。許可する最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

- どの TLS 暗号の組み合わせが許可されるのか。

暗号の組み合わせにより、接続において使用する暗号化アルゴリズムが選択されます。VDA とユニバーサルプリントサーバーは、暗号の組み合わせのさまざまなセットをサポートできます。VDA が接続を開始して、サポートする TLS 暗号の組み合わせの一覧を送信すると、ユニバーサルプリントサーバー側では、構成済みの暗号の組み合わせの一覧内に VDA のいずれかの暗号の組み合わせと一致するものがあるかどうかがチェックされます。一致した場合、接続が確立されます。一致する暗号の組み合わせがない場合、ユニバーサルプリントサーバーは接続を拒否します。

ユニバーサルプリントサーバーは、OPEN、FIPS、および SP800-52 ネイティブ暗号キットモードに対し、GOV（政府）、COM（商業）、ALL という以下の暗号の組み合わせをサポートします。使用できる暗号の組み合わせは、**SSL FIPS** モードポリシー設定や Windows の FIPS モードによっても異なります。Windows FIPS モードについて詳しくは、Microsoft 社のサポート文書を参照してください。

暗号の組み合わせ（優先度の高い順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECI AES256_	○		○	○		○	○		○
TLS_ECDHE_RSA_ AES256_CBC_SHA384			○	○		○	○		○
TLS_ECI AES256_	○	○		○	○		○	○	

PowerShell スクリプトを使用したユニバーサルプリントサーバー上の **TLS** 構成

証明書ストアの［ローカルコンピューター］**>**［個人］**>**［証明書］領域にある TLS 証明書をインストールします。その場所に複数の証明書が存在する場合は、証明書の拇印を`Enable-UpsSsl.ps1` PowerShell スクリプトに指定します。

> 注:
>
> PowerShell スクリプトは、ユニバーサルプリントサーバーの完全修飾ドメイン名を基にして正しい証明書を見つけます。ユニバーサルプリントサーバーの完全修飾ドメイン名に 1 つの証明書のみが存在する場合は、証明書の拇印を指定する必要はありません。

Enable-UpsSsl.ps1スクリプトは VDA からユニバーサルプリントサーバーへの TLS 接続を有効または無効にします。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。

TLS を有効にすると、スクリプトはユニバーサルプリントサーバーの TCP ポートで既存の Windows ファイアウォール規則をすべて無効にします。その後、XTE サービスが TLS TCP および UDP ポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。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:

- クリアテキスト印刷 Web サービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDA は TLS を使用している場合にのみこれらの接続を確立できます。

> 注:
>
> TLS を有効にしても、VDA からユニバーサルプリントサーバーへの Windows 印刷スプーラーの RPC/SMB 接続には影響しません。
>
> 重要:
>
> 最初のパラメーターとして、**Enable** か **Disable** のどちらかを指定します。CertificateThumbprint パラメーターは、ローカルコンピューターの個人証明書ストアの 1 つの証明書のみがユニバーサルプリントサーバーの完全修飾ドメイン名を持つ場合、オプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

パラメーター	説明
有効化	XTE サーバーで SSL/TLS を有効にします。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	XTE サーバー上で SSL/TLS 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。

パラメーター	説明
CertificateThumbprint "<thumbprint>"	ローカルコンピューターの個人証明書ストア内にある 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。
HTTPPort <port>	クリアテキスト印刷 Web サービス（HTTP/SOAP）ポート。デフォルト：8080
CGPPort <port>	クリアテキスト印刷データストリーム（CGP）ポート。デフォルト：7229
HTTPSPort <port>	暗号化印刷 Web サービス（HTTPS/SOAP）ポート。デフォルト：8443
CGPSSLPort <port>	暗号化印刷データストリーム（CGP）ポート。デフォルトは以下のとおりです。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。有効な値：“TLS_1.0”、“TLS_1.1”、“TLS_1.2”。デフォルト：TLS_1.2。
SSLCipherSuite “<name>”	TLS 暗号の組み合わせパッケージの名前。二重引用符で囲みます。有効な値：“GOV”、“COM”、“ALL”（デフォルト）。
FIPSMode <Boolean>	XTE サーバーで FIPS 140 モードを有効または無効にします。有効な値：$true で FIPS 140 モードを有効にし、$falseFIPS 140 モードを無効にします。

例

次のスクリプトは TLS を有効にします。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-UpsSsl.ps1 -Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトは TLS を無効にします。

```
Enable-UpsSsl.ps1 -Disable
```

FIPS モードの構成

米国の Federal Information Processing Standards（FIPS）モードを有効にすると、FIPS 140 準拠の暗号化のみがユニバーサルプリントサーバーの暗号化接続に使用されるようにできます。

クライアントで FIPS モードを構成する前に、サーバーで FIPS モードを構成してください。

Windows FIPS モードを有効/無効にする方法については、Microsoft のドキュメントサイトを参照してください。

クライアントで **FIPS** モードを有効にする

Delivery Controller で Citrix Studio を実行して、Citrix ポリシー設定 ［**SSL FIPS** モード］を **Enabled** に設定します。Citrix ポリシーを有効にします。

各 VDA でこの操作を繰り返します:

1. Windows の FIPS モードを有効にします。
2. Linux VDA を再起動します。

サーバーで **FIPS** モードを有効にする

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. Windows の FIPS モードを有効にします。
2. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1`スクリプトを`-Enable -FIPSMode $true`パラメーターで実行します。
4. ユニバーサルプリントサーバーを再起動します。

クライアントで **FIPS** モードを無効にする

Delivery Controller で Citrix Studio を実行して、Citrix ポリシー設定 ［**SSL FIPS** モード］を **Disabled** に設定します。Citrix ポリシーを有効にします。Citrix ポリシー ［**SSL FIPS** モード］設定を削除することもできます。

各 VDA でこの操作を繰り返します:

1. Windows の FIPS モードを無効にします。
2. Linux VDA を再起動します。

サーバーで **FIPS** モードを無効にする

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. Windows の FIPS モードを無効にします。
2. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1`スクリプトを`-Enable -FIPSMode $false`パラメーターで実行します。
4. ユニバーサルプリントサーバーを再起動します。

SSL/TLS プロトコルバージョンを構成する

デフォルトの SSL/TLS プロトコルバージョンは TLS 1.2 です。TLS 1.2 は、実稼働環境で推奨される唯一の SSL/TLS プロトコルです。トラブルシューティングのためには、実稼働環境以外で一時的に SSL/TLS プロトコルバージョンの変更が必要な場合があります。

SSL 2.0 と SSL 3.0 は、ユニバーサルプリントサーバーではサポートされていません。

サーバーで SSL/TLS プロトコルバージョンを設定する

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1`スクリプトを`-Enable -SSLMinVersion`バージョンパラメーターで実行します。テストの終了後は、TLS 1.2 に戻すことを忘れないようにしてください。
3. ユニバーサルプリントサーバーを再起動します。

クライアントで SSL/TLS プロトコルバージョンを設定する

各 VDA でこの操作を繰り返します:

1. Delivery Controller でポリシー設定 ［**SSL** プロトコルバージョン］を必要なプロトコルバージョンに設定して、ポリシーを有効にします。

2. Microsoft SCHANNEL SSP のレジストリ設定については、Microsoft 社のサポート文書「TLS Registry Settings」を参照してください。レジストリ設定を使用して、クライアント側の **TLS 1.0**、**TLS 1.1** または **TLS 1.2** を有効にします。

> 重要:
>
> テストの終了後は、レジストリ設定を元の値に戻すのを忘れないでください。

3. Linux VDA を再起動します。

トラブルシューティング

接続エラーが発生した場合は、C:\Program Files (x86)\Citrix\XTE\logs\error.log のユニバーサルプリントサーバーのログファイルをチェックしてください。

SSL/TLS ハンドシェイクが失敗した場合は、このログファイルに「**SSL handshake from client failed**」というメッセージが表示されます。このような失敗は、VDA とユニバーサルプリントサーバーの SSL/TLS プロトコルバージョンが一致しない場合に発生することがあります。

ユニバーサルプリントサーバーのホスト名を含む次のポリシー設定でユニバーサルプリントサーバーの完全修飾ドメイン名を使用します:

- セッションプリンター

- プリンター割り当て
- 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と VDA のシステムクロック（日付、時刻、およびタイムゾーン）が正しいことを確認してください。

デバイス

April 26, 2021

HDX は、どんな場所にあるどんなデバイスでも高品位なユーザーエクスペリエンスを提供します。「デバイス」セクションの記事では、以下のデバイスについて説明します。

- 一般的な USB デバイス
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- TWAIN デバイス
- Web カメラ

最適化された **USB** デバイスと一般的な **USB** デバイス

最適化された USB デバイスとは、Citrix Workspace アプリが特定のサポートを提供しているデバイスです。たとえば、HDX マルチメディア仮想チャネルを使用して Web カメラをリダイレクトする機能などのサポートです。一般的なデバイスとは、Citrix Workspace アプリで特定のサポートがない USB デバイスのことです。

一般的な USB のリダイレクト機能では、一般モードに設定されていなければ、最適化された仮想チャネルをサポートする USB デバイスをデフォルトではリダイレクトできません。

一般的に、USB デバイスは一般モードよりも最適化モードで優れたパフォーマンスを発揮します。ただし、USB デバイスが最適化モードでの機能を完全に備えていない場合があります。そのデバイスの機能を完全に利用するには、一般モードに切り替える必要がある場合もあります。

USB 大容量記憶装置デバイスでは、Citrix ポリシーによって制御されるクライアントドライブマッピングまたは一般的な USB のリダイレクト機能のどちらか、またはその両方を使用できます。主な違いは次のとおりです。

一般的な USB のリダイレクト機能とクライアントドライブ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挿入された大容量記憶装置デバイスがクライアント側ドライブのマッピングによりリダイレクトされます。

これらの条件が満たされると、大容量記憶装置は一般的な USB のリダイレクト機能を使用してリダイレクトされます。

- 一般的な USB のリダイレクト機能とクライアントドライブマッピングのポリシーの両方が有効になっています。
- デバイスが自動リダイレクトに構成されています。
- 大容量記憶装置がセッションの開始前または後に挿入されます。

詳しくは、「http://support.citrix.com/article/CTX123015」を参照してください。

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（仮想セッションで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）。	Citrix Virtual Desktops のみ

複数のモニターによる **DPI** の混在

Citrix Virtual Apps and Desktops 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、Knowledge Center の記事CTX201696を参照してください。

一般的 **USB** デバイス

April 26, 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。これらのデバイスには、以下のものが含まれます:

- モニター
- マウス
- キーボード
- ボイスオーバー IP 電話
- ヘッドセット
- Web カメラ
- スキャナー
- カメラ

- プリンター
- ドライブ
- スマートカードリーダー
- 描画用タブレット
- 署名パッド

最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN 経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDX テクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なときに汎用 **USB** リダイレクトを提供します。汎用 USB リダイレクトの構成について詳しくは、「汎用 USB リダイレクト」を参照してください。

USB デバイスおよび Windows 向け Citrix Workspace アプリについて詳しくは、「複合 USB デバイスリダイレクトの構成」および「[USB サポートの構成]」を参照してください。(/ja-jp/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

モバイルおよびタッチスクリーンデバイス

April 26, 2021

Windows Continuum を使用したタッチスクリーンデバイス用タブレットモード

Continuum は、クライアントデバイスの使用方法に対応する Windows 10 の機能です。このバージョンの Continuum サポートは、モードの動的変更を含めて、VDA バージョン 7.16 および Citrix Receiver for Windows バージョン 4.10 から利用できます。

Windows 10 VDA は、タッチ対応クライアントのキーボードまたはマウスの存在を検出し、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、Windows 10 VDA はクライアントをタブレット/モバイルモードにします。この検出は接続時と再接続時に行われます。また、キーボードやマウスの動的な取り付けや取り外し時にも行われます。

この機能はデフォルトで有効にされています。このバージョンの機能を無効にするには、ICA ポリシー設定の記事にあるタブレットモードの切り替えのポリシー設定を編集します。

XenApp 7.14 と 7.15 LTSR および XenDesktop 7.14 と 7.15 LTSR に含まれる機能バージョンの場合は、レジストリ設定を使用してこの機能を無効にします。詳しくは、「タッチスクリーンデバイス用タブレットモード」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

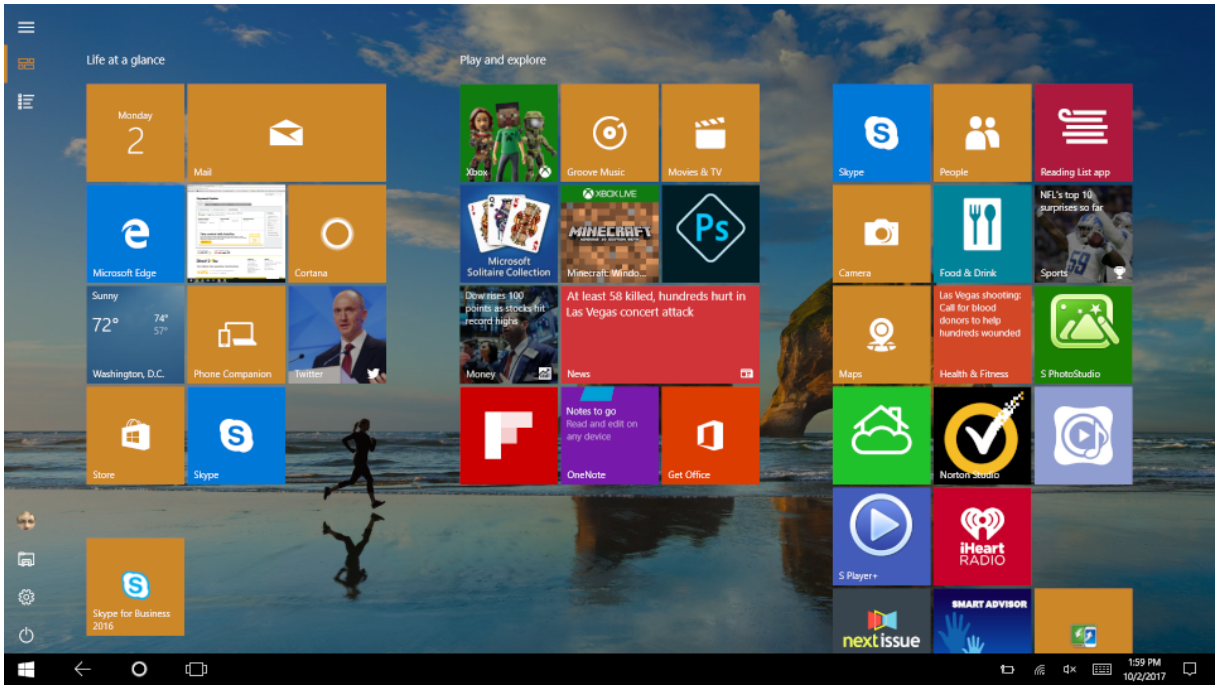
- スタート画面や開始したアプリケーションを全画面で開く
- タスクバーに［戻る］ボタンを表示
- タスクバーからアイコンを削除

File Explorer にアクセスできます。

デスクトップモードでは、PC とキーボードとマウスを使用するのと同じ方法で対話する従来のユーザーインターフェイスが提供されます。

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 Citrix Virtual Desktops 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「XenServer 7.2 リリースノート」を参照してください。

HTML5 向け Citrix Workspace アプリ（Light バージョン）は、Windows Continuum 機能をサポートしていません。



ラップトップ/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します：
xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

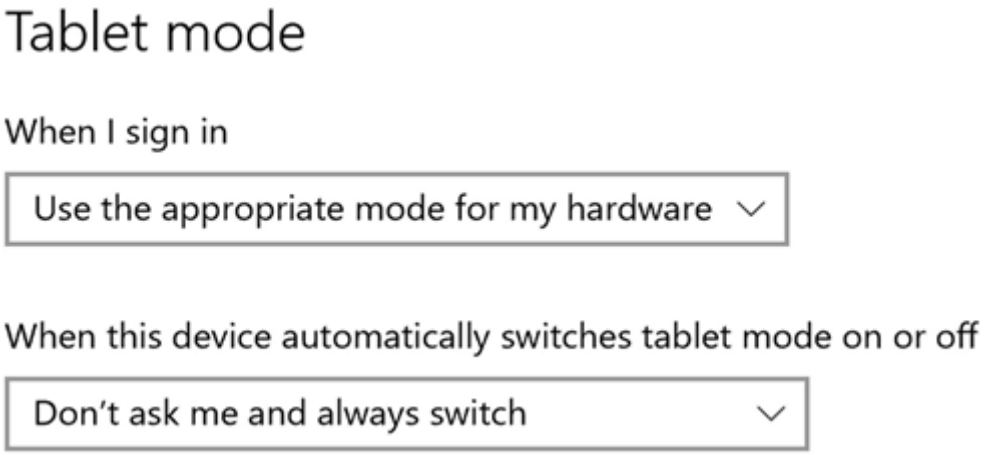
> 重要：
> メタデータ設定を変更した後で既存のマシンカタログの基本イメージを更新しても、以前にプロビジョニングされた VM には影響しません。XenServer VM の基本イメージを変更した後、カタログを作成し、基本イメージを選択し、新しい MCS（Machine Creation Services）マシンをプロビジョニングします。

セッション開始前：

セッション開始前に VDA で［設定］**>**［システム］**>**［タブレットモード］に移動して、ドロップダウンメニューから以下のオプションを設定することをお勧めします:

- ハードウェアに適切なモードを使用する
- 確認なしで常に切り替える

セッション開始前にこれらのオプションを設定しない場合には、セッション開始後に設定し、VDA を再起動してください。



Microsoft Surface Pro および **Surface Book** のペン

Windows Ink を使用するアプリケーションで標準のペン機能をサポートします。この機能には、Windows 10 バージョン 1809 以降で実行されている Virtual Delivery Agent (VDA) と Windows 向け Citrix Workspace アプリバージョン 1902 以降を使用するクライアントデバイスが必要です。サポートされるペン機能には、ポインティング、消去、筆圧、Bluetooth 信号、オペレーティングシステムのファームウェアやペンモデルによって異なるその他の機能が含まれます。たとえば、筆圧は最大 4096 レベルまで可能です。この機能はデフォルトで有効になっています。

Windows Ink とペン機能のデモを見るには、以下の画像をクリックしてください:

システム要件

- Citrix Virtual Apps and Desktops バージョン 1903 以降
- Windows 向け Citrix Workspace アプリバージョン 1902 以降
- Microsoft Windows 10 バージョン 1809 以降

無効化および有効化

この機能を無効または有効にするには、レジストリを以下のように設定します:

HKEY_LOCAL_MACHINE\Software\ Citrix\Citrix Virtual Desktop Agent\PenApi

値の名前：DisablePen

種類：DWORD

値のデータ:

1 - 無効

0 - 有効

シリアルポート

April 26, 2021

ほとんどの新しい PC には、シリアル（COM）ポートは内蔵されていません。シリアルポートは USB コンバーターを使用して簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、旧式

のチェックリーダー、パッドなどがあります。一部の USB 仮想 COM ポートデバイスでは、Windows 提供のドライバー（usbser.sys）の代わりにベンダー固有のドライバーが使用されます。これらのドライバーを使用すると、USB デバイスの仮想 COM ポートを別の USB ソケットに接続しても変更されないように強制することができます。これは、［デバイスマネージャー］**>**［ポート（**COM** & **LPT**）］**>**［プロパティ］から、またはデバイスを制御するアプリケーションから設定できます。

クライアント側 COM ポートのマッピングを使用すると、ユーザーのエンドポイント上の COM ポートに接続されているデバイスを仮想セッション中に使用できるようになります。これらのマッピングは他のネットワークマッピングと同様に使用できます。

各 COM ポートには、オペレーティングシステムのドライバーによって COM1 や COM2 などのシンボリックリンク名が割り当てられます。アプリケーションはそのリンクを使用してポートにアクセスします。

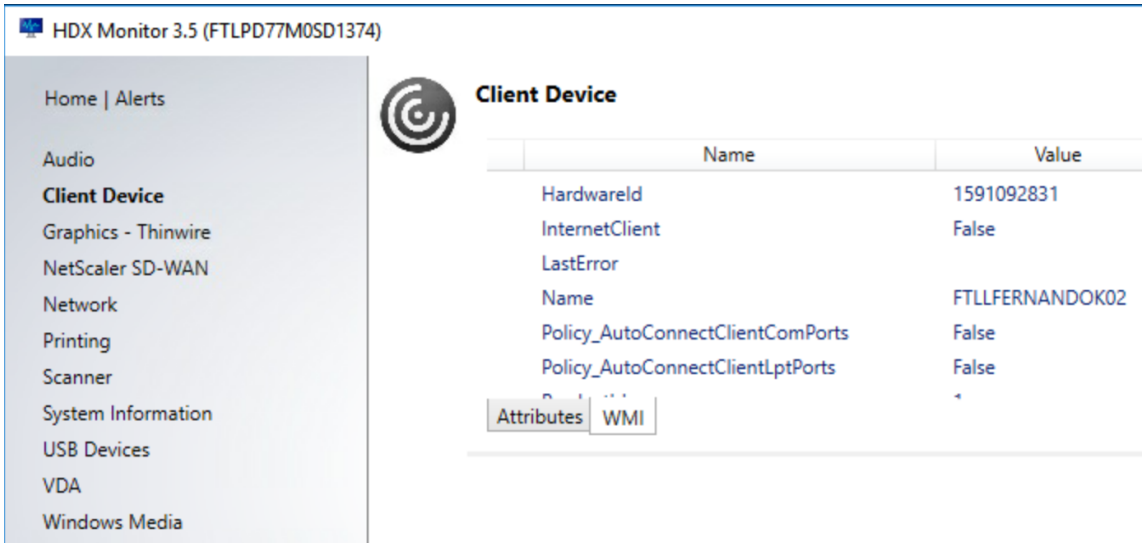
> 重要:
> デバイスは USB を直接使用してエンドポイントに接続できるため、汎用 USB リダイレクトを使用してデバイスをリダイレクトすることはできません。一部の USB デバイスは仮想 COM ポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でそのポートにアクセスできます。オペレーティングシステムは、COM ポートを抽象化して、ファイル共有のように扱うことができます。仮想 COM でよく使用されるプロトコルは CDC ACM と MCT の 2 つです。RS-485 ポート経由で接続すると、アプリケーションがまったく機能しないことがあります。RS-485 を COM ポートとして使用するには、RS-485-to-RS232 コンバーターを入手してください。
> 重要:
> 一部のアプリケーションは、デバイス（たとえば、署名パッド）がクライアントワークステーションの COM1 または COM2 に接続されている場合に限り、そのデバイスを一貫して認識します。

クライアント **COM** ポートをサーバーの **COM** ポートにマップする

クライアントの COM ポートを Citrix セッションにマップするには、次の 3 つの方法があります。

- Studio ポリシー。ポリシーについて詳しくは、「ポートリダイレクトのポリシー設定」を参照してください。
- VDA コマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. ［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］の Studio ポリシーを有効にします。適用すると、一部の情報が HDX Monitor で利用可能になります。



2. ［クライアント **COM** ポートを自動接続する］でポートのマッピングに失敗した場合は、そのポートを手動でマップするか、またはログオンスクリプトを使用します。VDA にログオンし、コマンドプロンプトウィンドウで次のように入力します:

   NET USE COMX: \\CLIENT\COMZ:

   または

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   < X > は VDA 上の COM ポートの番号です（マッピングに使用できるのはポート 1～9 です）。**< Z >** は、マップするクライアント COM ポートの番号です。

   その操作が成功したことを確認するには、VDA コマンドプロンプトで **NET USE** と入力します。マップされているドライブ、LPT ポート、およびマップされている COM ポートの一覧が表示されます。

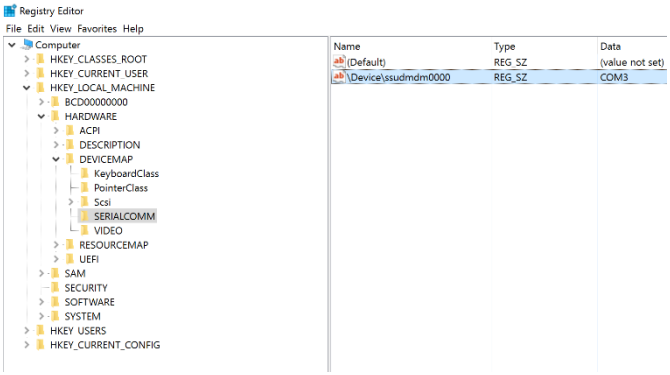
3. その COM ポートを仮想デスクトップやアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされている COM ポート名を指すようにします。たとえば、クライアントの COM1 をサーバーの COM3 にマップしている場合は、COM ポートデバイスアプリケーションを VDA にインストールし、セッション中に COM3 を指すようにします。この方法でマップした COM ポートは、ユーザーデバイスの COM ポートと同じように使用できます。

> 重要:
> COM ポートのマッピング機能は、TAPI をサポートしません。Windows テレフォニーアプリケーションプロ

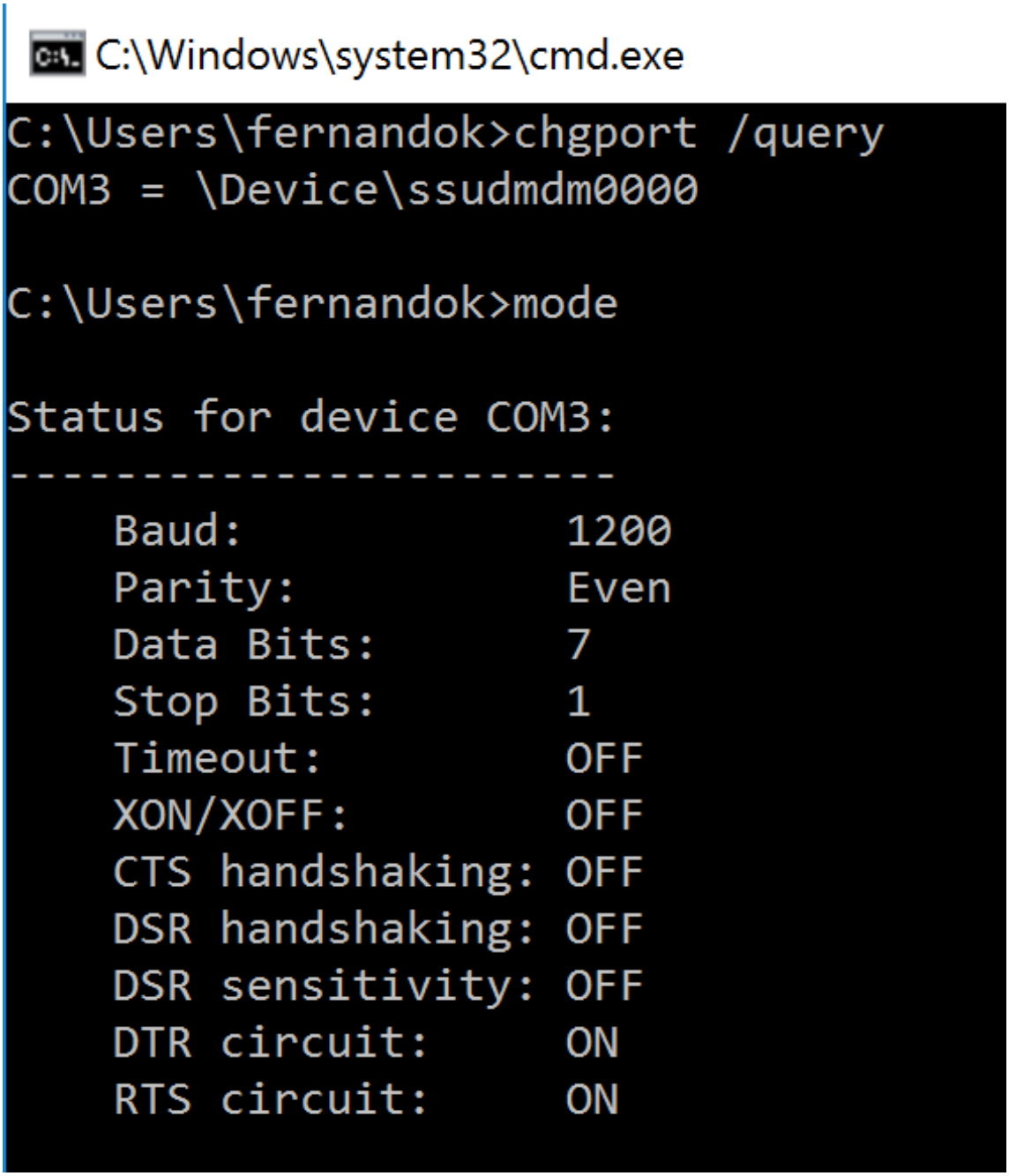
> グラミングインターフェイス（TAPI）デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、ファックス、および音声通話のテレフォニー機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加的サービスも管理します。

トラブルシューティング

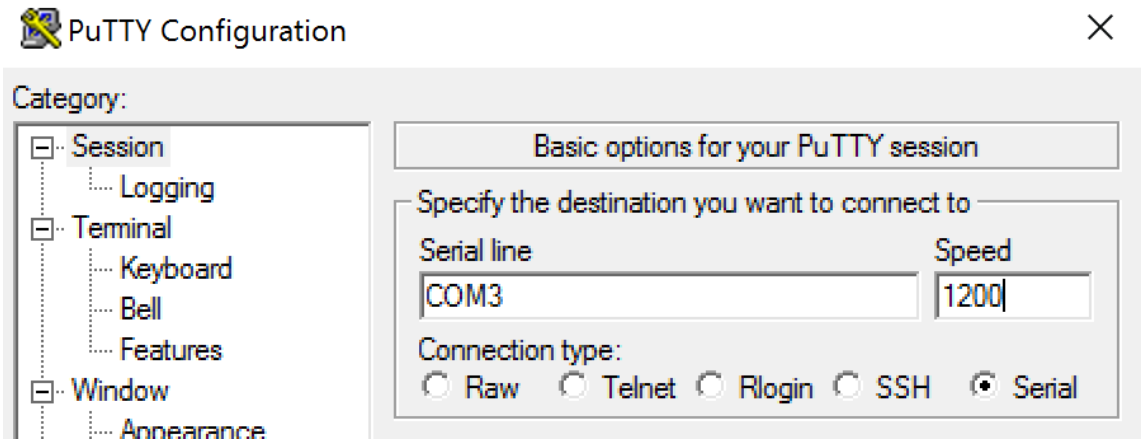
1. Citrix をバイパスしてエンドポイントからデバイスに直接アクセスできることを確認します。ポートが VDA にマップされていない間は、Citrix セッションに接続していません。デバイスに付属しているトラブルシューティングの指示に従って、まずデバイスがローカルに動作することを確認します。
   デバイスがシリアル COM ポートに接続されている場合は、次のハイブにレジストリキーが作成されています:



   この情報は、コマンドプロンプトで **chgport /query** を実行して確認することもできます。



デバイスのトラブルシューティングの手順を利用できない場合は、PuTTY セッションを開いてみます。［セッション］を選択し、［シリアル回線］で COM ポートを指定します。



ローカルのコマンドウィンドウで **MODE** コマンドを実行すると、その出力に、使用中の COM ポート、および PuTTY セッションで必要なボーレート/パリティ/データビット/ストップビットの情報が表示されます。PuTTY 接続に成功した場合は、**Enter** キーを押すとデバイスからのフィードバックが表示されます。入力した文字が画面上で繰り返されるか、または応答が返されます。この手順が正常に行われない場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカル COM ポートを VDA にマップし（ポリシーまたは **NET USE COM< X >: \\CLIENT\COM< Z >** を使用）、今回は VDA PuTTY から、前と同じ PuTTY 手順を繰り返します。PuTTY が「**Unable to open connection to COM1. Unable to open serial port**」というエラーで失敗する場合は、別のデバイスが COM1 を使用している可能性があります。

3. **chgport /query** を実行します。VDA 上の Windows の組み込みシリアルドライバーによって、VDA の COM1 ポートに\Device\Serial0 が自動的に割り当てられている場合は、次のようにします：
   A. VDA でコマンドウィンドウを開いて、次のコマンドを入力します：**NET USE**

   B. VDA の既存のマッピング（たとえば、COM1）を削除します。

   NET USE COM1 /DELETE

   C. そのデバイスを VDA にマップします。

   NET USE COM1: \\CLIENT\COM3:

   D. VDA 上のアプリケーションが COM3 を指すようにします。

   最後に、ローカル COM ポート（COM3 など）を VDA の別の COM ポート（COM1 以外の COM3 など）にマップしてみます。アプリケーションがそのポートを指すようにします：
   NET USE COM3: \\CLIENT\COM3

4. この時点でポートがマップされていることを確認できた場合、PuTTY は動作していますがデータは渡されていないため、競合状態である可能性があります。ポートがマップされる前にアプリケーションがそのポートに接続して開き、ロックしているためにマップできない可能性があります。次のいずれかを試してみます。

   - 同じサーバーで公開されている別のアプリケーションを開きます。ポートがマップされるまで数秒待ってから、そのポートを使用しようとする実際のアプリケーションを開きます。

- Studio ではなく Active Directory のグループポリシーエディターから、COM ポートリダイレクトポリシーを有効にします。有効にするポリシーは、［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］です。この方法で適用されるポリシーは、Studio ポリシーより前に処理され、COM ポートがマップされることが保証される可能性があります。Citrix ポリシーは VDA にプッシュされ、次の場所に格納されています。
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- このログオンスクリプトをユーザーに対して使用するか、またはアプリケーションを公開する代わりに使用して、VDA の任意のマッピングを削除した後に仮想 COM ポートを再マッピングしてから、そのアプリケーションを起動する.bat スクリプトを公開します。

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (or whatever value needed)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed)
START C:\Program Files\<Your Software Path>\
```

5. 最後の手段としては、Sysinternals の Process Monitor があります。VDA でこのツールを実行するときは、COM3、picaser.sys、CdmRedirector など（特に、<your_app>.exe）のオブジェクトを検索してフィルタリングします。「アクセスが拒否されました」などのエラーが表示されることがあります。

特殊キーボード

April 26, 2021

Bloomberg キーボード

> 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 Virtual Apps and Desktops では、Bloomberg モデル 4 Starboard キーボード（およびそれ以前のモデル 3）がサポートされています。このキーボードを使用すると、金融分野の顧客は、キーボードの特殊機能を使用して金融市場データにアクセスし、取引を迅速に実行できます。

このキーボードは KVM スイッチボックスと互換性があり、次の 2 つのモードで動作します。

- PC（USB ケーブル 1 本、KVM なし）
- KVM モード（USB ケーブル 2 本、1 本は KVM 経由）

> 重要:
> Bloomberg キーボードは 1 つのセッションのみで使用することをお勧めします。複数の同時セッション（1 つのクライアントからのマルチセッション）でこのキーボードを使用することはお勧めしません。

Bloomberg キーボードモデル 4 は、1 つの物理シェル内に次の 4 つの USB デバイスを備える、USB 複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を増減するためのキーおよびスピーカーとマイクをミュートするためのキーが付いているオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが備わっています。
- これらのすべてのデバイスをシステムに接続するための USB ハブ。

要件:

- Windows 向け Citrix Workspace アプリが接続するセッションで、USB デバイスがサポートされている必要があります。
- Bloomberg キーボードモデル 3 および 4 は、Windows 向け Citrix Workspace アプリ 1808 以降および Citrix Receiver for Windows 4.8 以降でサポートされています。
- モデル 4 の KVM モード（USB ケーブル 2 本、1 本は KVM 経由）を使用するには、Windows 向け Citrix Workspace アプリ 1808 以降または Citrix Receiver for Windows 4.12 以降が必要です。

Windows 向け Citrix Workspace アプリでの Bloomberg キーボードの構成について詳しくは、「Bloomberg キーボードの構成」を参照してください。

Bloomberg キーボードのサポートを有効にする:

デフォルトでは、Bloomberg キーボードの拡張サポートは無効になっています。接続する前にクライアントマシンで次のレジストリエントリを編集して、このサポートを有効にします。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

値の名前:**EnableBloombergHID**（dword）

値:0 = 無効、1 = 有効

サポートを確認する:

Bloomberg キーボードのサポートが Citrix Workspace アプリで有効になっているかどうかを確認するには、Desktop Viewer で Bloomberg キーボードのデバイスが正しく報告されているかどうかを確認します。

デスクトップの場合:

Desktop Viewer を開きます。Bloomberg キーボードのサポートが有効になっている場合は、Desktop Viewer で USB アイコンの下に次の 3 つのデバイスが表示されています。

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

シームレスアプリケーションのみの場合:

Citrix Workspace アプリの通知領域アイコンから［コネクションセンター］メニューを開きます。Bloomberg キーボードのサポートが有効になっている場合は、［デバイス］メニューに 3 つのデバイスが表示されています。

各デバイスに付いているチェックマークは、そのデバイスがそのセッションでリモートであることを示しています。

TWAIN デバイス

April 26, 2021

要件

- スキャナーは TWAIN 準拠である必要があります。
- ローカルデバイスに TWAIN ドライバーをインストールします。サーバー上には TWAIN ドライバーは必要ありません。
- スキャナーをローカルに接続します（USB 経由など）。
- スキャナーが Windows Image Acquisition サービスではなくローカルの TWAIN ドライバーを使用していることを確認します。
- テストに使用するユーザーアカウントに、ICA セッション内の帯域幅を制限しているポリシー（たとえば、クライアント USB デバイスリダイレクトの最大帯域幅）が適用されていないことを確認します。

ポリシー設定について詳しくは、「TWAIN デバイスのポリシー設定」を参照してください。

Web カメラ

April 26, 2021

高品位 Web カメラストリーミング

サーバーのアプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。アプリケーションから Web カメラを選択します。Web カメラとアプリケーションがどちらも高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。1920x1080 までの Web カメラ解像度がサポートされています。

この機能を使用するには、Citrix Receiver for Windows の最小バージョン 4.10 が必要です。HDX Web カメラリダイレクトをサポートする Citrix Workspace アプリプラットフォームの一覧については、「Citrix Workspace アプリの機能マトリックス」を参照してください。

高品位 Web カメラストリーミングについて詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

> 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。

レジストリキーを使用してこの機能を無効または有効にすることができます。次の設定では 352x288 のデフォルトの解像度が使用されます。

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

値の名前：Enable_HighDefWebcam

種類：REG_DWORD

データ：

0 = 高品位 Web カメラストリーミングを無効化

1 = 高品位 Web カメラストリーミングを有効化

クライアントのレジストリキーを使用して、特定の解像度を設定することができます。カメラが指定された解像度をサポートしていることを確認してください。

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

値の名前：DefaultWidth

種類：REG_DWORD

データ（10 進数）：必要な幅（1280 など）

値の名前：DefaultHeight

種類：REG_DWORD

データ（10 進数）：必要な高さ（720 など）

グラフィック

April 26, 2021

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、Citrix Virtual Apps and Desktops 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。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、Citrix Virtual Apps and Desktops 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

Citrix Virtual Apps and Desktops 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 シングルセッション 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シングルセッション 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 マルチセッション OS のための GPU アクセラレーション

HDX 3D Pro 機能により、Windows マルチセッション 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

> 重要:
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。その代わりにThinwireでアダプティブトランスポートを有効にします。

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ます。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

関連情報

- HDX 3D Pro
- Windows シングルセッション OS のための GPU アクセラレーション
- Windows マルチセッション OS のための GPU アクセラレーション
- Framehawk
- Thinwire
- テキストベースのセッションウォーターマーク

HDX 3D Pro

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで VDA をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）

> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

Citrix Virtual Apps and Desktops の HDX 3D Pro 機能を使用すると、グラフィック処理装置（GPU）によるハードウェアアクセラレーションで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。

HDX 3D Pro のポリシー設定については、「3D 画像ワークロードの最適化」を参照してください。

サポート対象の Citrix Workspace アプリすべてで、3D グラフィックを使用できます。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、Windows 向け Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリを最新バージョンにすることをお勧めします。サポート対象の Citrix Workspace アプリについて詳しくは、「Citrix Workspace アプリのライフサイクルマイルストーン」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 シングルセッション OS マシンと Windows マルチセッション 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 シングルセッション OS のための GPU アクセラレーション」および「Windows マルチセッション 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、AMD および Intel GVT-d による GPU パススルー
  - NVIDIA GRID、AMD 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
- Microsoft Azure NV シリーズ
- Amazon Web Services（AWS）EC2 G3 インスタンス

サポートされる XenServer のバージョンについては、「Citrix XenServer ハードウェア互換性リスト（英語）」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 マルチセッション OS のための GPU アクセラレーション

April 26, 2021

HDX 3D Pro 機能により、Windows マルチセッション 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、GPU 仮想化（vGPU）を行わなくても、Citrix Virtual Apps がアクセスする GPU を複数のユーザーで共有できます。

このトピックの説明にはレジストリの編集が含まれています。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、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 Passthrough 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、http://www.techpowerup.com/gpuz/で提供されています。

- 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。

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 マルチセッション 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:000000
- [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:0000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:00000001

Windows シングルセッション **OS** のための **GPU** アクセラレーション

April 26, 2021

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シングルセッション 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 Pro 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 プロセッサーファミリの詳細については、「第 5 世代インテル Core プロセッサー」および「第 6 世代インテル 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のページ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 ベースまたは H.265 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。H.264 によるハードウェアエンコーディングは、NVENC をサポートする NVIDIA、Intel、AMD カードで使用されます。H.265 による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（システムトレイアイコン）がユーザーの通知領域に表示されます。このアイコンは、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。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator で新しいレジストリ設定を構成します。
  - 値の名前：HKEY_LOCAL_MACHINE_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。
  - 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。シングルセッション OS マシンの場合、HDX 3D Pro 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。このサポートについて詳しくは、「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のページを参照）。NVIDIA GRID vGPU を使用すると、複数の仮想マシンで単一の物理 GPU に同時に直接アクセスできます。このとき、仮想化されていないオペレーティングシステムで動作するものと同じ NVIDIA グラフィックドライバーが使用されます。

- Virtual Direct Graphics Acceleration（vDGA）を使った VMware vSphere および VMware ESX のサポート - RDS および VDI の両方のワークロードで、vDGA 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、「http://www.citrix.com/intel」お

よび「http://www.intel.com/content/www/us/en/servers/data-center-graphics.html」を参照してください。

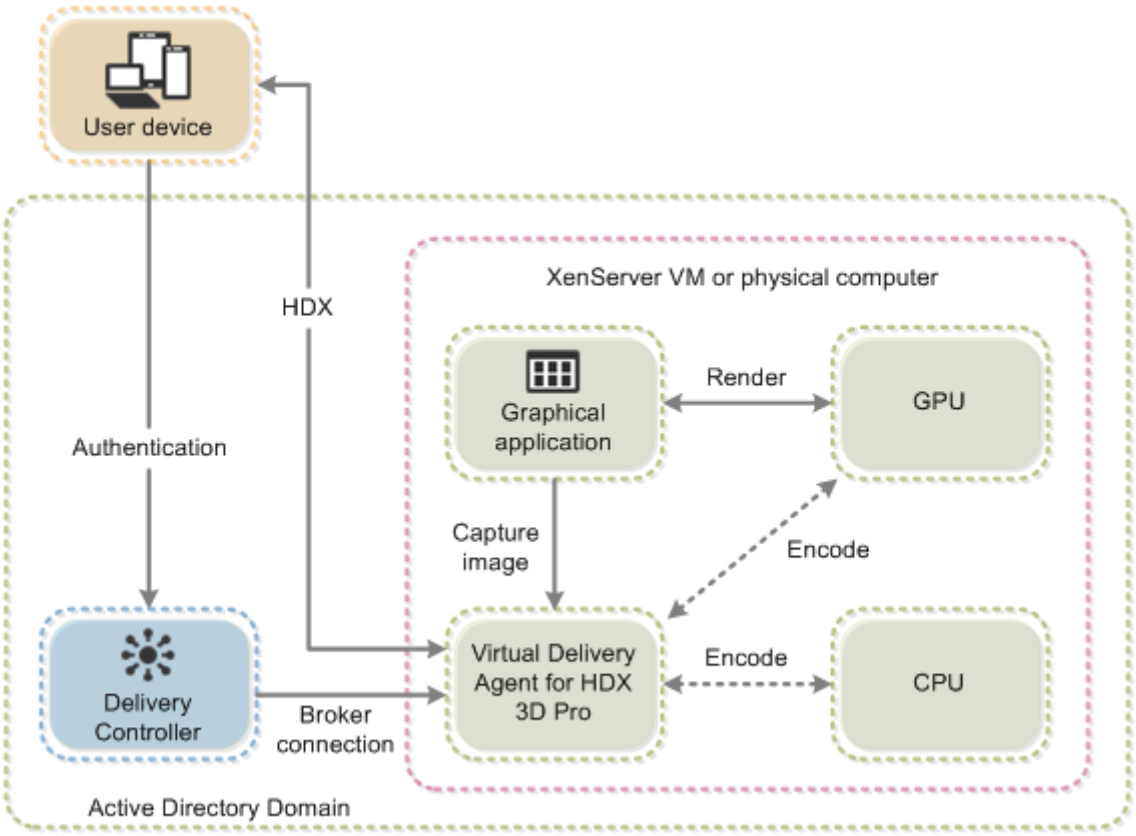
- AMD FirePro S シリーズのサーバーカードでの AMD RapidFire のサポート。HDX 3D Pro では、マルチモニター（最大 6 つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。注：HDX 3D Pro による AMD MxGPU（GPU 仮想化）のサポートで対応しているのは、VMware vSphere の vGPU のみです。GPU パススルーに対応しているのは、XenServer と Hyper-V です。詳しくは、「AMD 仮想化ソリューション」を参照してください。
- NVIDIA GPU の高パフォーマンスビデオエンコーダー、AMD GPU、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）によって制御されます。この機能により 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 Workspace アプリ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 でユーザーが認証されます。Controller は VDA for HDX 3D Pro にアクセスし、グラフィカル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、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。この転送は、Citrix Workspace アプリと VDA for HDX 3D Pro の間の直接 HDX 接続を介して行われます。



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 Workspace アプリ - Desktop Viewer 基本設定］ダイアログボックスで Desktop Viewer ウィンドウの解像度を変更できます。

支店など、帯域幅が制限された接続を複数のユーザーで共有している場合、ポリシーの ［セッション全体の最大帯域幅］設定を使用して、各ユーザーが使用できる帯域幅を制限することをお勧めします。この設定により、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、Knowledge Center のCTX128190を参照してください。

Thinwire

April 26, 2021

はじめに

Thinwire は Citrix HDX テクノロジの一部で、Citrix Virtual Apps and Desktops 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。

このようなバランスの良さから、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、Citrix Virtual Apps and Desktops 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。

HDX 3D Pro

デフォルト設定では、Thinwire は 3D または高度にインタラクティブなグラフィックを提供し、グラフィック処理装置（GPU）を使用できます（存在する場合）。ただし、GPU を使用するシナリオでは、Citrix ポリシーの ［**3D** グラフィックの負荷の最適化］または ［表示品質］**>**［操作時は低品質］ポリシーを使用して、HDX 3D Pro モードを有効にすることをお勧めします。これらのポリシーは、GPU が存在する場合、ハードウェアアクセラレーションを使用して、Thinwire がビデオコーデック（H.264 または H.265）で画面全体をエンコードできるよう構成します。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、「H.264 の［操作時は低品質］」、「HDX 3D Pro」または「Windows シングルセッション 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

Thinwire は、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、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。組み込みの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。

> 注:
>
> このリリースでは、従来のグラフィックモードはサポートされていません。これは、Windows 7 および Windows 2008 R2 で XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、および以前の VDA リリースを使用している場合の後方互換性のためにのみ含まれています。

- 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、Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.6 FP3 以降の VDA バージョンで利用できます。Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.9 以降の VDA バージョンでは、［選択された場合ビデオコーデックを使用する］オプションがデフォルト設定になっています。
- Thinwire はすべての Citrix Workspace アプリでサポートされています。ただし、8 ビットまたは 16 ビットグラフィックで帯域幅の使用量が少なくなるなど、Thinwire の機能は Citrix Workspace アプリによってサポートの有無が異なることがあります。こうした機能のサポートは、Citrix Workspace アプリ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にして対話操作性を改善することを検討できます。表示品質は、特に 8 ビットの色数で影響を受けることがあります。

エンコーディング方法

Thinwire は、ポリシーとクライアントの機能に応じて、2 つの異なるエンコーディングモードで動作できます。

- 全画面 H.264 または H.265 による Thinwire
- 選択的な H.264 または H.265 による Thinwire

従来の GDI リモート処理では、Thinwire ビットマップエンコーダーではなく XPDM リモート処理ドライバーが使用されます。

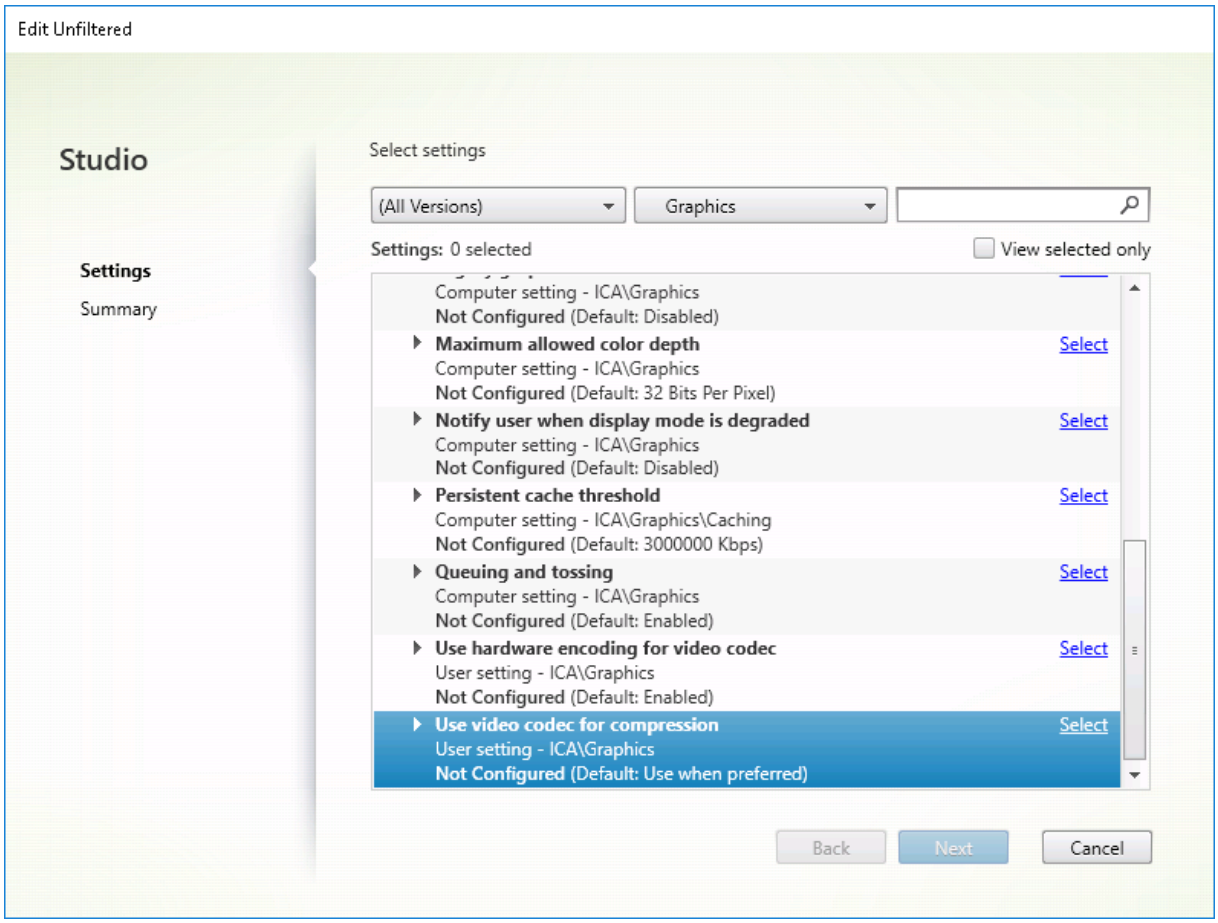
構成

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。これは、機能的に ［領域をアクティブに変更］と同等です。

- 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他のテクノロジと組み合わせて Thinwire を使用し続けます。例:
  - ［領域をアクティブに変更］。Thinwire の状況に応じたディスプレイテクノロジは、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 または H.265 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 または H.265 を使用して配信し、ユーザーエクスペリエンスと帯域幅を最適化します。H.264 4:2:0（［視覚的無損失］ポリシーが無効）の場合、最終イメージは完全に無損失ではなく、特定のシナリオには適さないことがあります。この場合、H.264 の［操作時は低品質］の使用を検討してください。



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す。Thinwire はこれらすべてをサポートします。

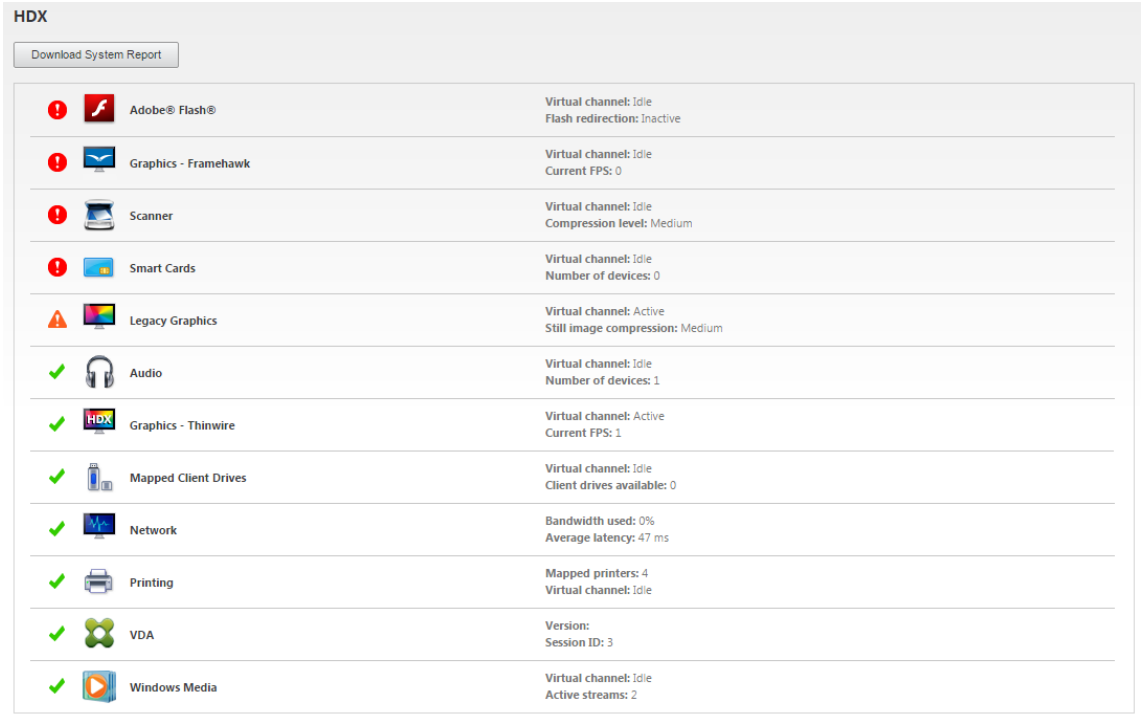
- 単純なグラフィックスの優先色深度
- ターゲットフレーム数
- 表示品質

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。

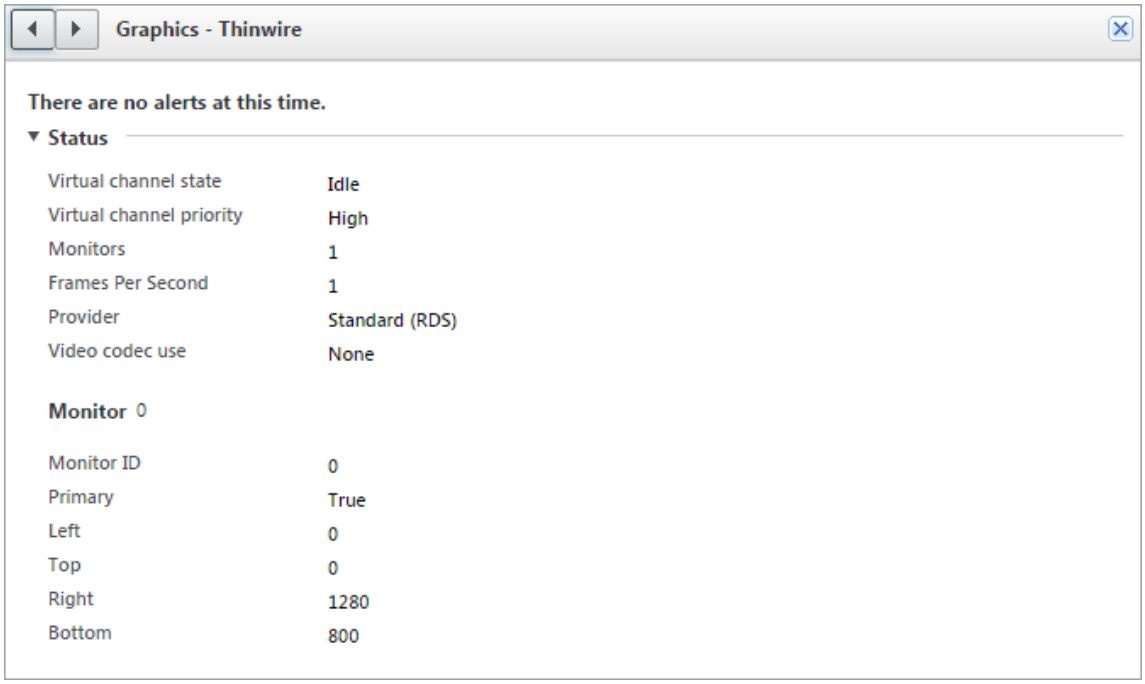
Thinwire のモニター

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。



3. ［グラフィック **- Thinwire**］を選択します。



無損失圧縮コーデック（**MDRLE**）

通常のデスクトップセッションでは、画面の大半が単純なグラフィックまたはテキスト領域です。Thinwire はこれらの領域の範囲を決定し、2DRLE コーデックを使用して無損失エンコーディングの領域を選択します。Citrix Workspace アプリのクライアント側では、これらの要素は、セッション表示時に Citrix Workspace アプリ側の 2DRLE デコーダーを使用してデコードされます。

XenApp および XenDesktop 7.17 では、より高い圧縮率の MDRLE コーデックが追加されており、通常のデスクトップセッションでは 2DRLE コーデックよりも少ない帯域幅しか消費しません。この新しいコーデックは、サーバーの拡張性には影響を与えることはありません。

消費帯域幅が抑えられるため、通常、（特に共有リンクまたは制約付きリンクで）セッションのインタラクティブ性が向上するとともに、コストを削減できます。たとえば、MDRLE コーデック使用時の予想される帯域幅消費量は、Office などの一般的なワークロードの場合、XenApp および XenDesktop 7.15 LTSR と比較して約 10～15%少なくなります。

MDRLE コーデックには構成は不要です。Citrix Workspace アプリで MDRLE デコードがサポートされている場合、VDA では、VDA の MDRLE エンコードと Citrix Workspace アプリの MDRLE デコードが使用されます。Citrix Workspace アプリで MDRLE デコードがサポートされていない場合、VDA では、自動的に 2DRLE エンコードにフォールバックされます。

MDRLE の要件:

- Citrix Virtual Apps and Desktops: VDA バージョン 7 1808 以降
- XenApp および XenDesktop: VDA バージョン 7.17 以降
- Windows 向け Citrix Workspace アプリ: バージョン 1808 以降

- Citrix Receiver for Windows バージョン 4.11 以降

プログレッシブモード

Citrix Virtual Apps and Desktops 1808 では、プログレッシブモードが導入され、デフォルトで有効になっています。制約のあるネットワーク環境（デフォルト：帯域幅 <2Mbps、または遅延 >200 ミリ秒）では、Thinwire が圧縮するテキストや静止画の量が増えて、画面アクティビティの対話操作性が改善されます。画面アクティビティが停止すると、大幅に圧縮されたテキストや画像は、その後徐々に、ランダムなブロック単位でシャープになります。このような方法で圧縮およびシャープ化して総合的な対話操作性を改善しながら、キャッシュ使用を低減し帯域幅の使用を増やしていきます。

Citrix Virtual Apps and Desktops 1906 の場合、プログレッシブモードはデフォルトで無効になっています。現在は、別のアプローチを使用しています。静止画の画質は、現在、ネットワーク状況に基づいて ［表示品質］設定ごとに事前定義された最小値および最大値の間で変化します。明示的なシャープ化の手順が存在しないため、Thinwire は、プログレッシブモードの利点をほぼすべて提供しながら画像配信を最適化し、キャッシュ効率を維持します。

プログレッシブモードの動作を変更する

> 重要：
>
> 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。

プログレッシブモードの状態は、次のレジストリキーを使用して変更できます。

`HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\`

種類：REG_DWORD

値の名前：ProgressiveDisplay

値のデータ：

0 = 常時オフ（プログレッシブモードが無効。この値がデフォルト）

1 = 自動（ネットワーク状態に基づいてオンとオフを切り替える）

2 = 常時オン

H.264 の ［操作時は低品質］

［操作時は低品質］は、対話操作性のために画像配信や最終イメージの品質を最適化する Thinwire の特別な構成です。［表示品質］ポリシーを ［操作時は低品質］に設定することで有効にできます。

［操作時は低品質］の設定は画面のアクティビティ中に H.264（または H.265）を使用して画面を圧縮し、アクティビティが停止すると完全な無損失へシャープ化します。可能な限り最高のフレーム数を維持するために、使用可能なリ

ソースの H.264（または H.265）画質に適応します。シャープ化の手順は、手順の開始後にユーザーが画面のアクティビティを開始した場合でも対応できるように、徐々に行われます。たとえば、モデルを選択してから、それを回転させる場合などです。

H.264 の ［操作時は低品質］では、ハードウェアアクセラレーションのような全画面 H.264 または H.265 のすべての利点を利用できますが、最終的な、無損失画面は保証されていません。これは、完全に無損失な最終イメージが必要な 3D タイプのワークロードにとって重要なポイントです。たとえば、医療画像を操作する場合です。また、H.264 の ［操作時は低品質］は全画面 H.264 4:4:4 よりも少ないリソースを使用します。その結果、［操作時は低品質］を使用すると通常、視覚的無損失 H.264 4:4:4 よりもフレーム数が多くなります。

> 注:
>
> ［表示品質］ポリシーに加えて ［圧縮にビデオコーデックを使用する］ポリシーを ［可能であれば使用］（デフォルト）または ［領域をアクティブに変更］に設定します。［圧縮にビデオコーデックを使用する］ポリシーを ［ビデオコーデックを使用しない］に設定して H.264 以外の［操作時は低品質］に戻すことができます。これによって動画は H.264（または H.265）の代わりに JPEG でエンコードされます。

テキストベースのセッションウォーターマーク

April 26, 2021

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

> 重要
>
> テキストベースのセッションウォーターマーキングは、セキュリティ機能ではありません。このソリューションは、データ盗難を完全に防止するものではありませんが、ある程度の抑止力とトレーサビリティを提供します。この機能の使用時の完全な情報トレーサビリティが保証されるわけではありませんが、この機能を他のセキュリティソリューションと適切に組み合わせることをお勧めします。

セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークによって、データ盗難を追跡するための情報が伝えられます。最も重要なデータは、画面イメージが撮影された現在のセッションのログオンユーザーの ID です。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などのその他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークのポリシー設定を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

Virtual Delivery Agent:

マルチセッション OS 7.17
シングルセッション OS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリケーションアクセス、Windows Media リダイレクト、MediaStream、Web ブラウザーコンテンツリダイレクト、および HTML5 ビデオリダイレクトが使用されるセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- 全画面ハードウェアアクセラレーションモード（全画面 H.264 または H.265 エンコーディング）でセッションが実行されている場合は、セッションウォーターマークはサポートされておらず、表示されません。
- これらの HDX ポリシーを設定すると、ウォーターマーク設定が有効にならず、ウォーターマークがセッション画面に表示されません。

［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］を ［有効］
［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

- これらの HDX ポリシーを設定すると、動作が不確定となり、ウォーターマークが表示されないことがあります。

  ［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］を ［有効］
  ［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

  ウォーターマークが表示されるようにするには、［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］を ［無効］に設定するか、または ［圧縮にビデオコーデックを使用する］を ［領域をアクティブに変更］か ［ビデオコーデックを使用しない］に設定します。
- セッションウォーターマークでは、Thinwire のみがサポートされており、Framehawk またはデスクトップコンポジションリダイレクト（DCR）グラフィックモードはサポートされていません。
- ［Session Recording］を使用する場合、録画されたセッションにウォーターマークは含まれません。
- Windows リモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが **Print Screen** キーを押して画面をキャプチャした場合、VDA 側でキャプチャされる画面にウォーターマークは含まれません。キャプチャされたイメージがコピーされるのを防ぐために対策を講じることをお勧めします。

マルチメディア

April 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。

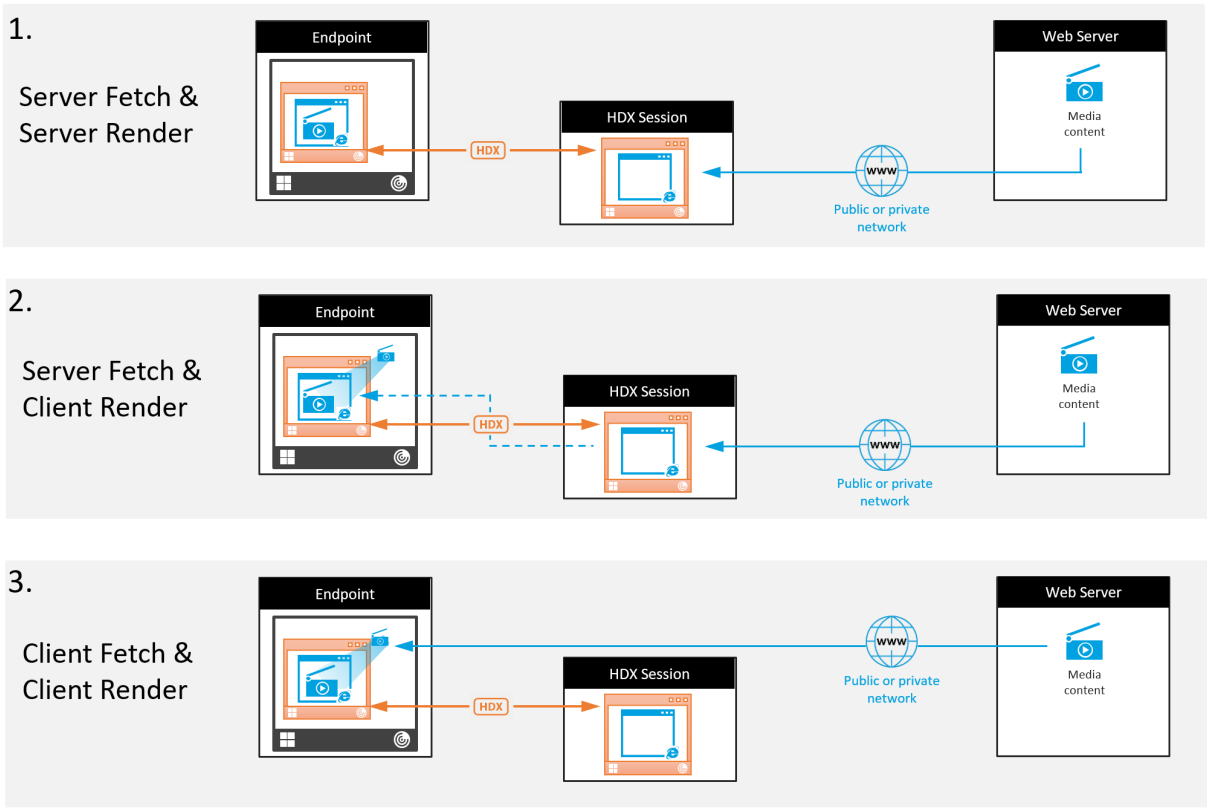
サーバー側でレンダリングするマルチメディア配信で、オーディオとビデオコンテンツは、アプリケーションによって Citrix Virtual Apps and Desktops サーバー上でデコードおよびレンダリングされます。コンテンツは圧縮され、ICA プロトコルでユーザーデバイス上の Citrix Workspace アプリに配信されます。この方法は、さまざまなアプリケーションとメディア形式に対して、最大レートの互換性を提供します。ビデオ処理は数値計算であるため、サーバー側でレンダリングされたマルチメディア配信はオンボードのハードウェアアクセラレーションの利点を大幅に活かすことがきます。たとえば、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、AMD RapidFire、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。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するようにすれば、高サーバースケーラビリティを維持できます。

- 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。
- HTML5 ビデオが一般的になり、Citrix ではこの種類のコンテンツに対するリダイレクト機能が導入されています。HTML5、HLS、DASH、または WebRTC を使用している Web サイトについては、Web ブラウザーコンテンツのリダイレクトをお勧めします。
- 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応用できます。

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、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**:**

シングルセッション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い開発を可能にする、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

オーディオリダイレクト	いいえ
Web ブラウザーコンテンツのリダイレクト	いいえ
HDX Web カメラリダイレクト	はい
HTML5 ビデオリダイレクト	はい
Windows Media リダイレクト	はい

オーディオ機能

April 26, 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ことをお勧めしますが、DTLS を使った UDP オーディオ暗号化は Citrix Gateway と Citrix Workspace アプリ間でのみ有効です。このため、TCP トランスポートの方が望ましい場合もあります。TCP では、Virtual Delivery Agent（VDA）と Citrix Workspace アプリ間の、エンドツーエンドの TLS 暗号化がサポートされます。

音質

一般的に、音質を高くするほど、オーディオデータの転送に必要な帯域幅が大きくなり、サーバーの CPU にも負担がかかります。オーディオデータを圧縮すると、セッションのパフォーマンスと音質とのバランスを考慮しながら、ユーザーの操作感を最適化できます。これを行うには、サウンドファイルに適用する圧縮レベルを制御するには、Citrix ポリシーを使用します。

デフォルトでは、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］に設定されています。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）では、この音質を使用しないでください。リアルタイム通信に適していないオーディオパスに遅延が発生する可能性があるためです。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は「スピーチに最適化」ポリシー設定をお勧めします。

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、帯域幅の消費を最小限に抑えることができます。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。

設定の詳細については、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

オーディオの再生と録音の帯域幅ガイドライン:

- 高品質（デフォルト）
  - ビットレート：再生では約 100kbps（最小 75、最大 175 kbps）、マイクキャプチャでは約 70kbps
  - チャンネル数：再生用 2（ステレオ）、マイクキャプチャ用 1（モノラル）
  - 周波数：44100Hz
  - ビット深度：16 ビット
- 中品質（VoIP 用に推奨）
  - ビットレート：再生では約 16kbps（最小 20、最大 40kbps）、マイクキャプチャでは約 16kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：16000Hz（ワイドバンド）
  - ビット深度：16 ビット

- 低品質
  - ビットレート：再生では最大 11kbps（最小 10、最大 25kbps）、マイクキャプチャでは最大 11kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：8000Hz（狭帯域）
  - ビット深度：16 ビット

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 ［許可］のままにしておきます。これがデフォルトの設定です。

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。

設定の詳細については、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

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。

セキュリティ上の理由から、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がマイクを使用しようとすると、警告メッセージが表示されます。ユーザーは、マイクを使用する前にアクセスを許可するか拒否するかを選択できます。この警告は、ユーザーが Citrix Workspace アプリ側で無効にできます。

設定の詳細については、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

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］の機能を使用すると、ユーザーのセッションが開始されるまでプラグを差し込んだ状態にしなくても、オーディオデバイスを認識できます。

この設定項目は、Windows マルチセッション OS マシンのみに適用されます。

設定の詳細については、「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。

設定の詳細については、「帯域幅のポリシー設定」を参照してください。ユーザーデバイス側の［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。

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が生じる場合、最適なユーザーエクスペリエンスを提供するために、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
>
> Citrix 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。Citrix Gateway が Citrix Virtual Apps and Desktops 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 Citrix 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、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］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 UDP ポートの範囲について詳しくは、「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。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

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 Components**］**>** ［**Citrix Workspace**］**>** ［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。
- 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. Citrix 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。Citrix Gateway で DTLS を構成します。詳しくは、「こちらの記事」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、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。たとえば、自分のデバイスや家庭のコンピューターを持ち込む場合などです。

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\\App_Data\default.ica を開きます。ストア名 >
2. [アプリケーション] セクションで以下の項目を入力します。

   ; リアルタイム転送を有効にします

   EnableRtpAudio=true

   ; ゲートウェイを介したリアルタイム転送を有効にします

   EnableUDPThroughGateway=true

   ;Audio quality を「Medium」に設定します

   AudioBandwidthLimit=1

   ;UDP ポートの範囲を表します

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

ユーザーデータグラムプロトコル（UDP）オーディオは、default.ica の編集で有効になっている場合、そのストアを使用するすべてのユーザーに対して有効化されます。

マルチメディア会議でのエコーの解消

オーディオまたはビデオ会議にユーザーが参加したときに、音声にエコーがかかって聞こえることがあります。通常、この問題はスピーカーとマイクが近すぎる場合に発生します。このため、オーディオまたはビデオ会議ではヘッドセットを使用することをお勧めします。

HDX には、会議中のエコーを最小限に抑えるためのエコーキャンセル機能が用意されており、デフォルトで有効になっています。エコーキャンセル機能の効果は、スピーカーとマイクとの距離により異なります。デバイスが互いに近すぎたり遠すぎたりしないように注意してください。

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。

Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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（推奨）。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 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 Teams の HDX 最適化
  - HDX RealTime Optimization Pack、Microsoft Skype for Business の配信を最適化
  - Cisco Jabber Softphone for VDI（以前は VXME と呼ばれていました）
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox（以前はVDI Communicatorと呼ばれていました）
  - Zoom VDI Plugin
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic ディクテーションデバイス
- ローカルアプリケーションアクセス。Citrix Virtual Apps and Desktops の機能により、ソフトフォンなどのアプリケーションは、Windows ユーザーの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。ICA を介したボイスオーバー IP。

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 Workspace アプリ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。

Citrix Virtual Apps and Desktops 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。
- 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。

Citrix Virtual Apps and Desktops 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 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP にも対応しています。Windows 向け Citrix Workspace アプリ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 Workspace アプリ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 Workspace アプリ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 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP に対応しています。また、Dell Wyse は ThinOS（WTOS）のボイスオーバー IP 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、Citrix Virtual Desktops 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、データセンターとリモートオフィス間には NetScaler SD-WAN を使用することをお勧めします。これにより、高いサービス品質が維持されます。NetScaler SD-WAN は、UDP を含むマルチストリーム ICA をサポートします。また、単一の TCP ストリームの場合は、さまざまな ICA 仮想チャネルの優先度を識別し、優先度の高いリアルタイムの音声データを優先的に扱うことができます。

HDX 構成を検証するには、Director またはHDX Monitorを使用してください。

リモートユーザーの接続：Citrix Gateway 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きます。

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 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。例:

- G711 の音質は高いものの、通話で 1 秒あたり 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、通話で 1 秒あたり 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されます。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 Citrix Virtual Apps and Desktops サーバーへの LAN または LAN のような接続上にある場合は、ボタンまたはディスプレイ（またはその両方）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をサポートします。

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ます。その後、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 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。このアプローチ

は LAN 接続のユーザーに制限されます。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です。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、優れた音声品質と低遅延を実現します。ただし、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、ボタンが付いたオーディオデバイスを使う場合です。たとえば、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。デバイス上でローカルに動作するボタンでは問題ありません。

制限事項

> 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。

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDS セッションを開始します。オーディオファイルが再生されず、エラーメッセージが表示されることがあります。

回避策として、このレジストリキーを RDS マシンに追加し、マシンを再起動します:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

値の名前: EnableSvchostMitigationPolicy

種類: REG_DWORD

データ: 0

Web ブラウザーコンテンツのリダイレクト

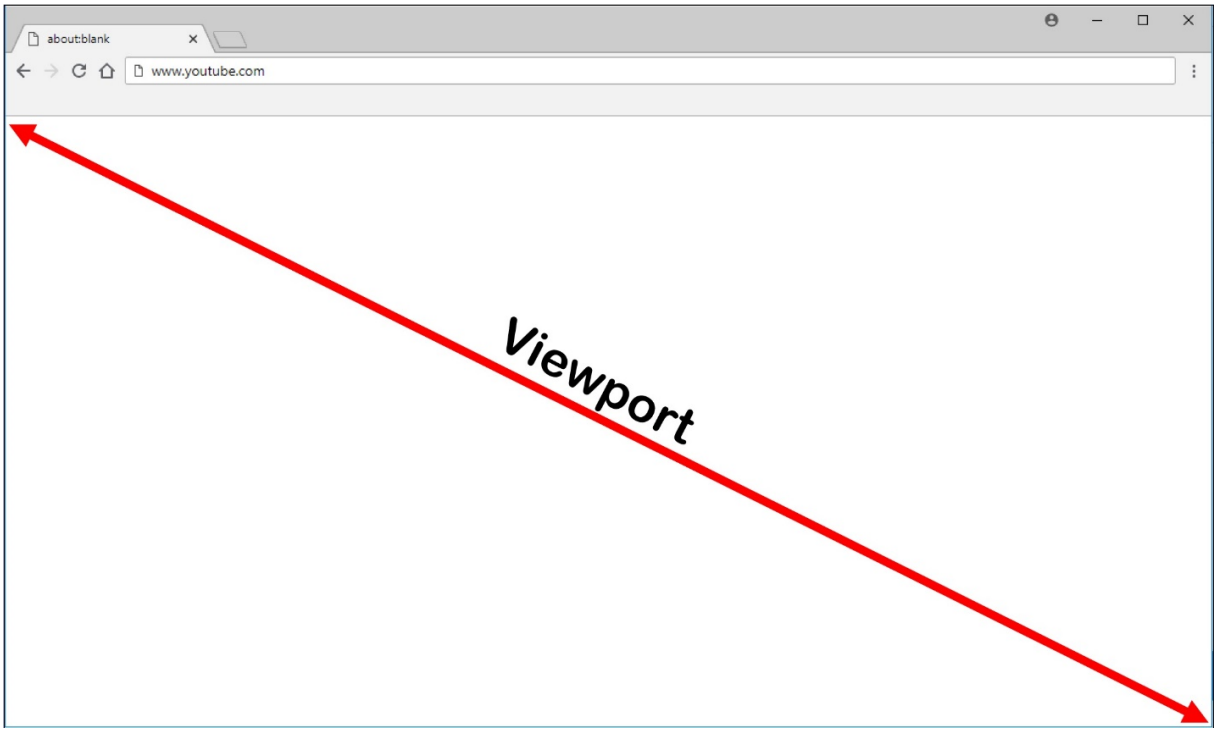
April 24, 2021

Web ブラウザーのコンテンツリダイレクトのために、VDA 側のホワイトリストに登録された Web ページのレンダリングができません。この機能は、Citrix Workspace アプリを使用してクライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

> 注:
>
> ブラックリストを使用することで、Web ページを VDA 側にリダイレクトする（クライアント側ではリダイレクトされない）ように指定できます。

このオーバーレイ Web レイアウトエンジンは、VDA 上ではなくエンドポイントデバイス上で実行され、エンドポイントの CPU、GPU、RAM、およびネットワークを使用します。

Web ブラウザーのビューポートだけがリダイレクトされます。ビューポートは、コンテンツが表示される Web ブラウザー内の長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイス内にあり、リダイレクト時も VDA の Web ブラウザーで実行されます。



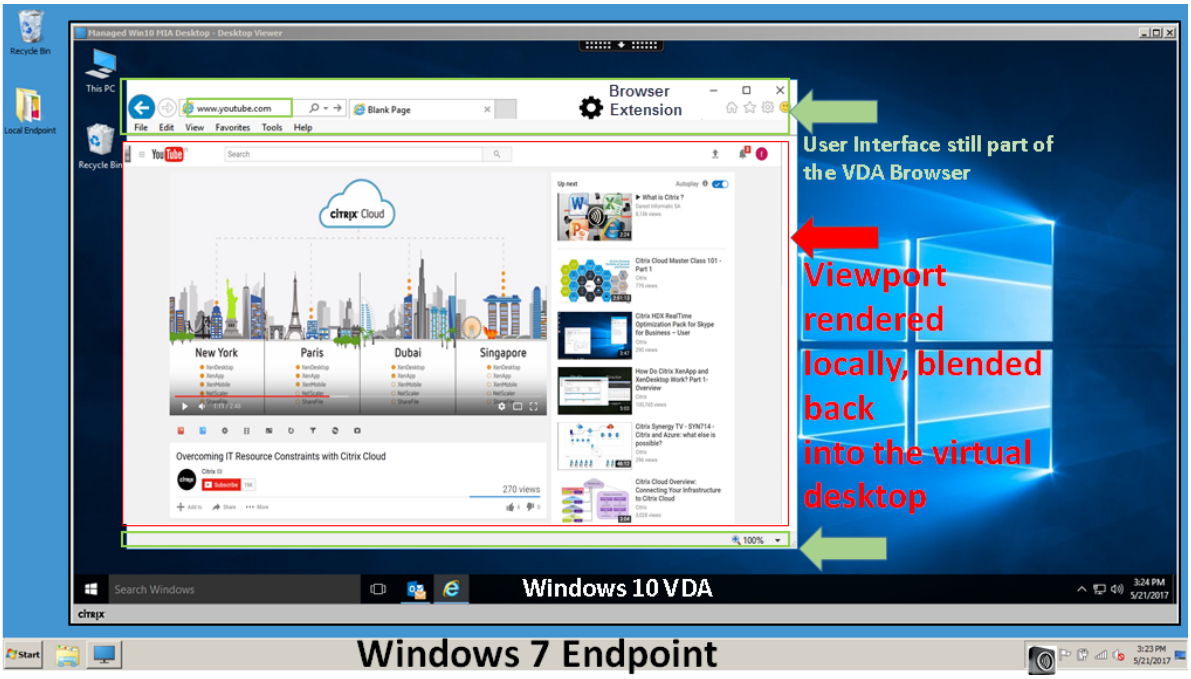
1. リダイレクト用にホワイトリストに登録された URL、または特定の URL パスのリダイレクトを無効にするブラックリストを含む、アクセス制御リストを指定する Studio ポリシーを設定します。ユーザーがナビゲートしている URL がホワイトリストと一致することやブラックリストと一致しないことを、VDA 上の Web ブラウザーで検出するために、Web ブラウザーの拡張機能によって比較が実行されます。Internet Explorer 11 向けの Web ブラウザー拡張機能はインストールメディアに含まれており、自動的にインストールされます。Chrome 向けの Web ブラウザー拡張機能は Chrome ウェブストアで提供されており、グループポリシーと ADMX ファイルを使用して展開できます。Chrome の拡張機能は、ユーザーごとにインストールします。拡張機能を追加または削除する場合に、ゴールデンイメージを更新する必要はありません。
2. ホワイトリスト内に一致するものがあり（例：`https://www.mycompany.com/`）、ブラックリスト内の URL と一致するもの（例：`https://www.mycompany.com/engineering`）がない場合、仮想チャネル（CTXCSB）は、リダイレクトが必要であることを Citrix Workspace アプリに指示し、URL をリレーします。Citrix Workspace アプリは、ローカルレンダリングエンジンをインスタンス化し、Web サイトを表示します。
3. Citrix Workspace アプリは、Web サイトを仮想デスクトップブラウザーのコンテンツ領域にシームレスにブレンドします。

ロゴの色は、Chrome 拡張機能のステータスを指定します。それは、以下の 3 つの色のいずれかです：

- 緑：アクティブで接続されています。

- グレー：現在のタブではアクティブではないかアイドル状態です。
- 赤：壊れているか動作していません。

拡張メニューの ［オプション］を使用して、ログをデバッグできます。



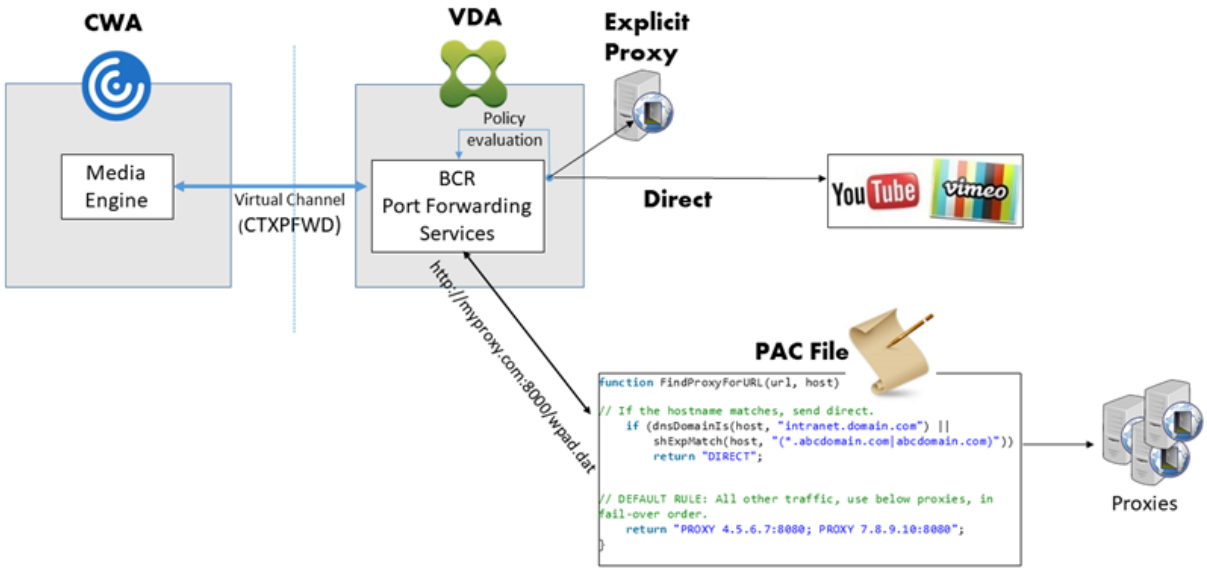
Citrix Workspace アプリがコンテンツをどのようにフェッチするかのシナリオを次に示します：

- サーバーフェッチとサーバーレンダリング：サイトをホワイトリストに登録していないか、リダイレクトに失敗したため、リダイレクトはありません。VDA 上での Web ページのレンダリングに戻り、Thinwire を使用してグラフィックスを遠隔操作します。ポリシーを使用してフォールバックの動作を制御します。VDA での CPU、RAM、および帯域幅の消費量が多い
- サーバーフェッチとクライアントレンダリング：Citrix Workspace アプリは仮想チャネル（CTXPFWD）を使用して、Web サーバーから VDA を通じてコンテンツに接続し、フェッチします。このオプションは、クライアントにインターネットアクセスがない場合（シンクライアントなど）に便利です。VDA では CPU と RAM の消費量は少なくなりますが、ICA 仮想チャネルでは帯域幅が消費されます。

  このシナリオには 3 つの動作モードがあります。プロキシという用語は、VDA がインターネットアクセスのためにアクセスするプロキシデバイスを意味します。

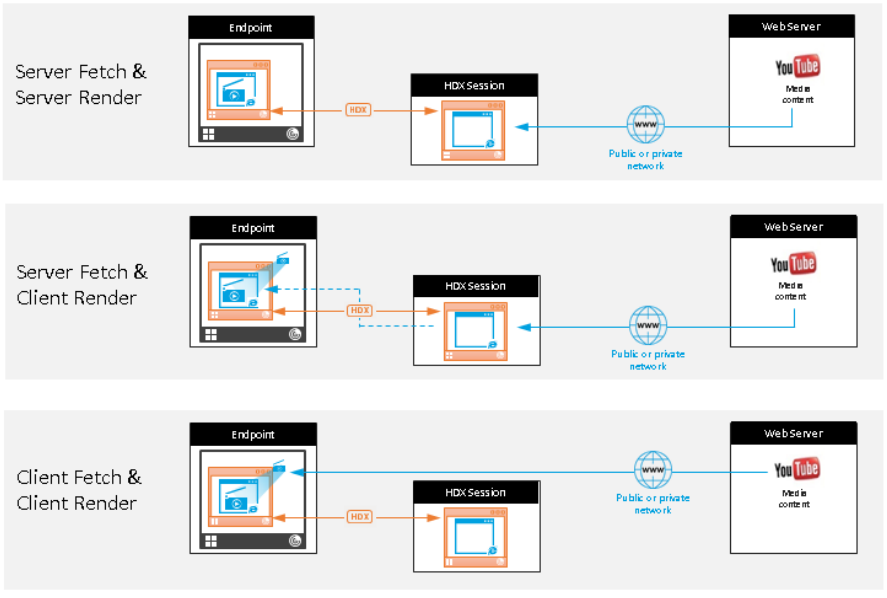
  選択可能なポリシーオプション：

  - Explicit Proxy - データセンターに単一の明示的なプロキシがある場合。
  - Direct or Transparent - プロキシがない場合、または透過プロキシを使用している場合。
  - PAC files - PAC ファイルに依存して、指定された URL のフェッチに VDA のブラウザーが適切なプロキシサーバーを自動で選択できる場合。



- クライアントフェッチとクライアントレンダリング：Citrix Workspace アプリは Web サーバーに直接接続するため、インターネットにアクセスする必要があります。このシナリオでは、XenApp および XenDesktop サイトからネットワーク、CPU、および RAM の使用量をすべてオフロードします。

Redirection scenarios



Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

フォールバックのメカニズム：

クライアントのリダイレクトが失敗することがあります。たとえば、クライアントマシンでインターネットに直接アクセスできない場合、エラー応答が VDA に返される可能性があります。このような場合、VDA 上の Web ブラウザーは、サーバー上のページをリロードしてレンダリングできます。

既存の［**Windows** メディアフォールバック防止ポリシー］を使用することで、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを、［クライアントにあるすべてのコンテンツのみを再生］または［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］に設定します。これらの設定は、クライアントのリダイレクトが失敗した場合に、サーバー上でのビデオ要素の再生を禁止します。このポリシーは、Web ブラウザーコンテンツリダイレクトが有効になっており、［アクセス制御リスト］ポリシーにフォールバックする URL がある場合にのみ有効です。この URL は、ブラックリストポリシーに含めることはできません。

システム要件:

Windows エンドポイント:

- Windows 7、8.x、10
- Windows 向け Citrix Workspace アプリ 1808 以降
- Citrix Receiver for Windows 4.10 以降

> 注:
>
> Windows 向け Citrix Workspace アプリ 1912 LTSR およびそのすべての累積更新プログラムは、Web ブラウザーコンテンツのリダイレクトをサポートしていません。

Linux エンドポイント:

- Linux 向け Citrix Workspace アプリ 1808 以降
- Citrix Receiver for Linux 13.9 以降
- シンクライアント端末には WebKitGTK+ が必要です。

Citrix Virtual Apps and Desktops 7 1808、XenApp および XenDesktop 7.15 CU5、7.18、7.17、7.16:

- VDA オペレーティングシステム: Windows 10（バージョン 1607 以降）、Windows Server 2012 R2、Windows Server 2016
- VDA 上の Web ブラウザー:
  - Google Chrome v66 以降（ユーザーエンドポイント上の Windows 向け Citrix Workspace アプリ 1809、Citrix Virtual Apps and Desktops 7 1808 VDA、Web ブラウザーコンテンツリダイレクト拡張機能が必要）
  - 次のオプションを構成した Internet Explorer 11:
    - ［インターネットオプション］ > ［詳細設定］**>** ［セキュリティ］の下にある ［拡張保護モードを有効にする］をオフにします。
    - ［インターネットオプション］**>** ［詳細設定］**>** ［ブラウズ］の下にある ［サードパーティ製のブラウザー拡張を有効にする］をオンにします。

トラブルシューティング

トラブルシューティングについて詳しくは、Knowledge Center のhttps://support.citrix.com/article/CTX230052を参照してください。

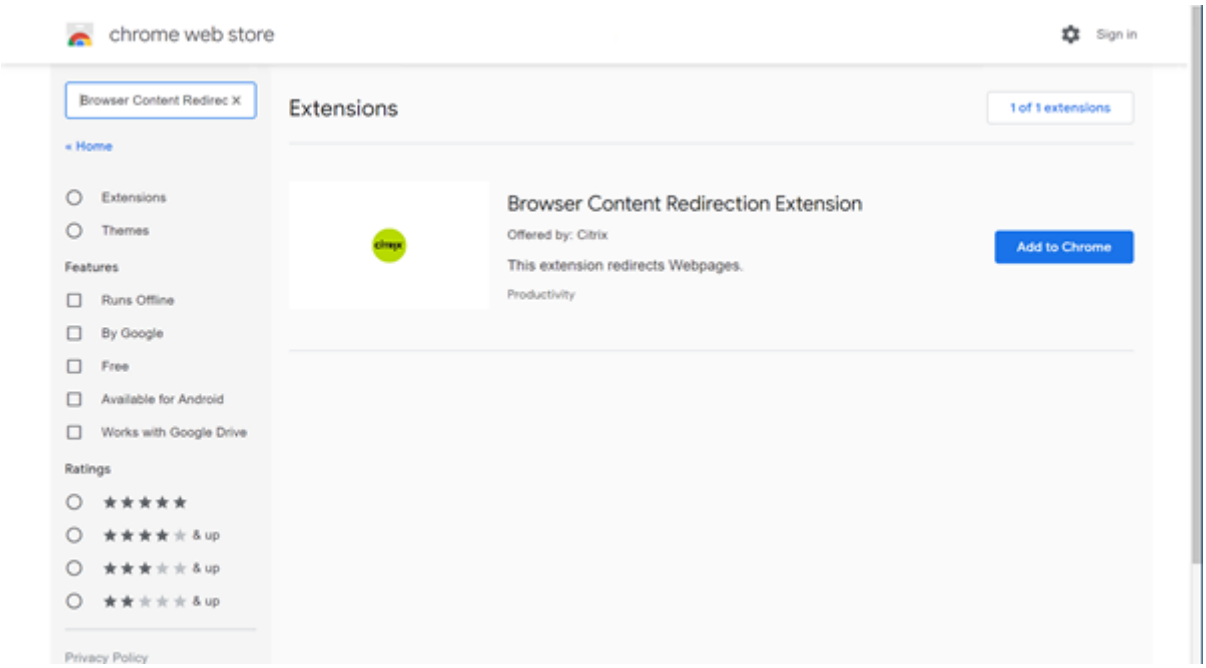
Chrome 向けの **Web** ブラウザーコンテンツリダイレクト拡張機能

Chrome で Web ブラウザーコンテンツリダイレクトを使用するには、Chrome ウェブストアから Browser Content Redirection Extension を追加します。Citrix Virtual Apps and Desktops 環境で、[**Chrome** に追加] をクリックします。

> 重要:
>
> この拡張機能は VDA にのみ必要であり、ユーザーのクライアントマシンには不要です。

システム要件

- Chrome v66 以上
- Browser Content Redirection Extension
- Citrix Virtual Apps and Desktops 7 1808 以降
- Windows 向け Citrix Workspace アプリ 1809 以降

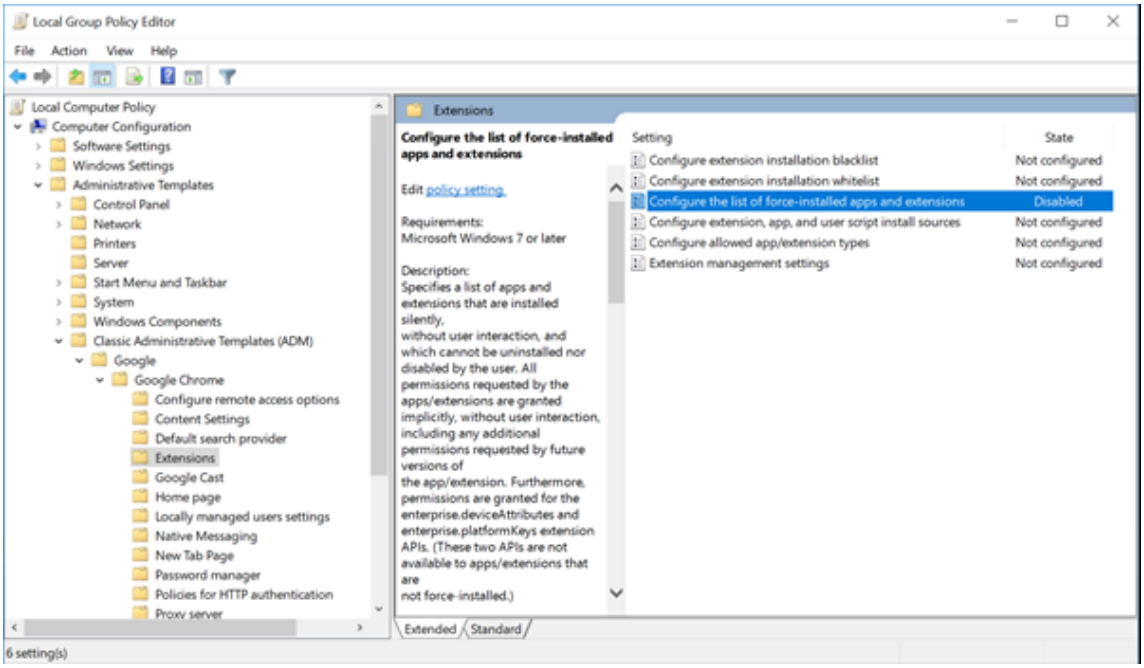


この方法は、ユーザーごとに行います。組織内の大規模なユーザーグループにこの拡張機能を展開するには、グループポリシーを使用して展開します。

グループポリシーを使用して拡張機能を展開する

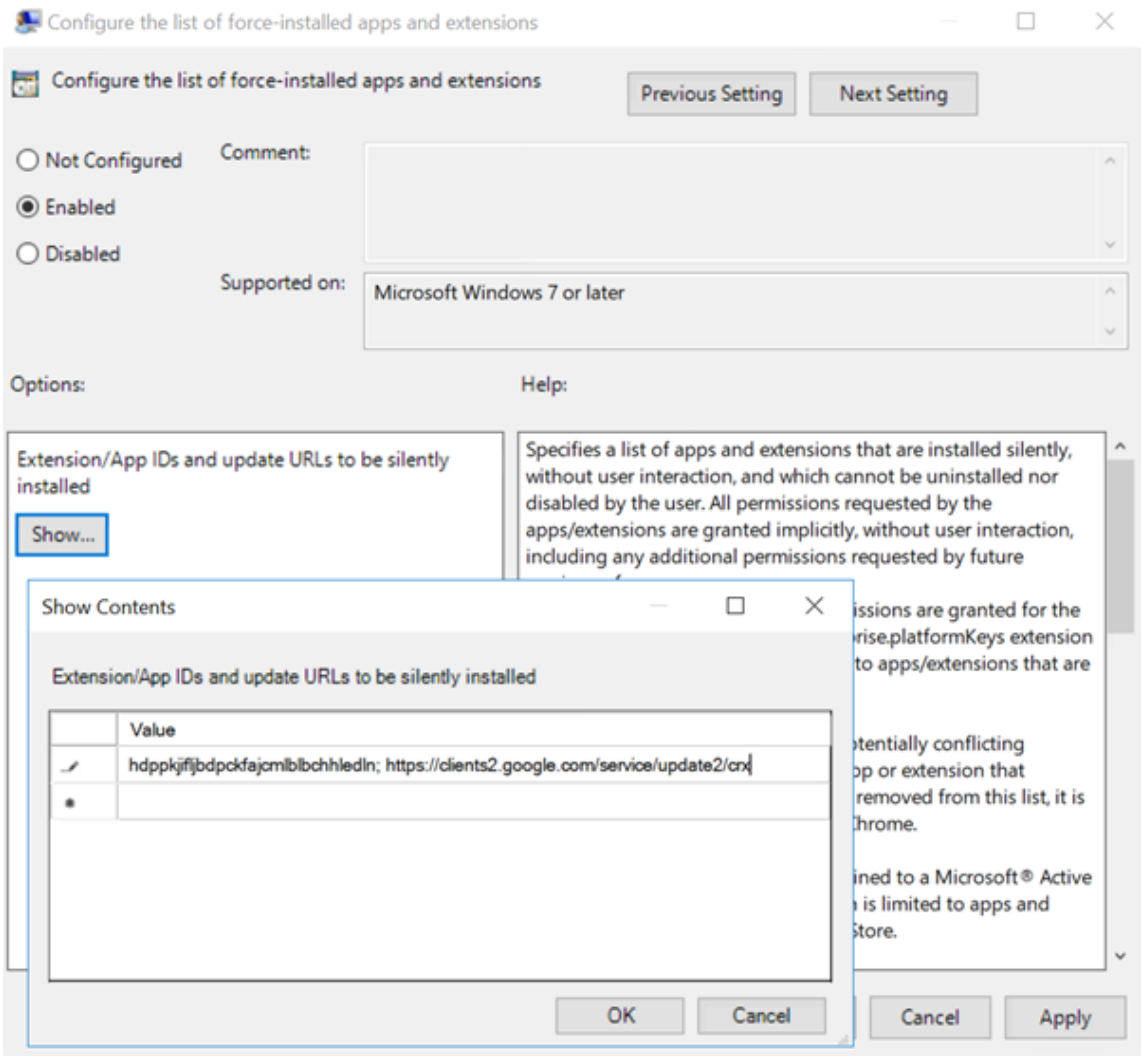
1. 現在の環境に Google Chrome ADMX ファイルをインポートします。ポリシーテンプレートをダウンロードしてグループポリシーエディターにインストールし、構成を行う方法については、https://support.google.com/chrome/a/answer/187202?hl=enを参照してください。

2. グループポリシー管理コンソールを開き、［ユーザーの構成］**>**［管理用テンプレート］**>**［従来の管理用テンプレート（**ADM**）］**>**［**Google**］**>**［**Google Chrome**］**>**［拡張機能］の順に選択します。［強制インストールするアプリと拡張機能のリストを設定します］設定を有効にします。



3. ［表示］をクリックして、拡張機能 ID に対応する文字列と、Browser Content Redirection Extension の更新用 URL を次のように指定します。

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```

4. 設定を適用し、`gpupdate`が更新されると、ユーザーへこの拡張機能が自動で配信されます。ユーザーのセッションで Chrome ブラウザーを起動すると、この拡張機能が既に適用されています。ユーザーがこの機能を削除することはできません。

   拡張機能の更新は、設定で指定した更新用 URL を通じて、ユーザーのマシンに自動でインストールされます。

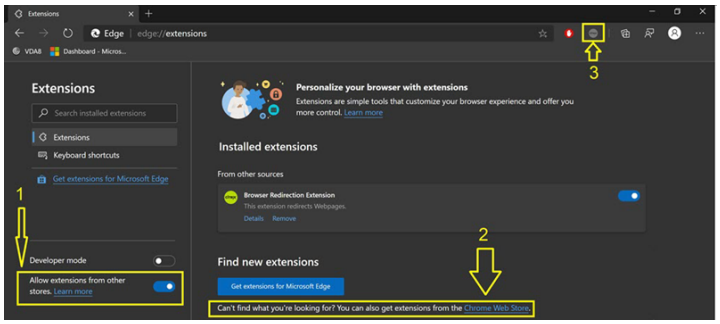
   [強制インストールするアプリと拡張機能のリストを設定します］設定を ［無効］に設定すると、この拡張機能はすべてのユーザーの Chrome から削除されます。

Chromium 版 **Edge** 向けの **Web** ブラウザーコンテンツリダイレクト拡張機能

Edge で Web ブラウザーコンテンツのリダイレクト拡張機能をインストールするには、インストール済みの Edge ブラウザーがバージョン **83.0.478.37** 以降であることを確認します。

1. メニューで［拡張機能］オプションをクリックし、［他のストアからの拡張機能を許可します。］をオンにします。

2. **Chrome** ウェブストアリンクをクリックすると、拡張機能が右上のバーに表示されます。
   Microsoft Edge の拡張機能について詳しくは、拡張機能を参照してください。



Web ブラウザーコンテンツのリダイレクトおよび DPI

> 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。

ユーザーのマシン上で Web ブラウザーコンテンツのリダイレクトの DPI（スケール）を 100% を超えて設定して使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するには、Web ブラウザーコンテンツのリダイレクトを使用するときに DPI を設定しないでください。この問題を回避するもう 1 つの方法は、ユーザーのマシン上で次のレジストリキーを作成して、Chrome で Web ブラウザーコンテンツのリダイレクトの GPU アクセラレーションを無効にすることです。

\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream

値の名前：GPU

種類：DWORD

データ：0

HDX ビデオ会議と Web カメラビデオ圧縮

April 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

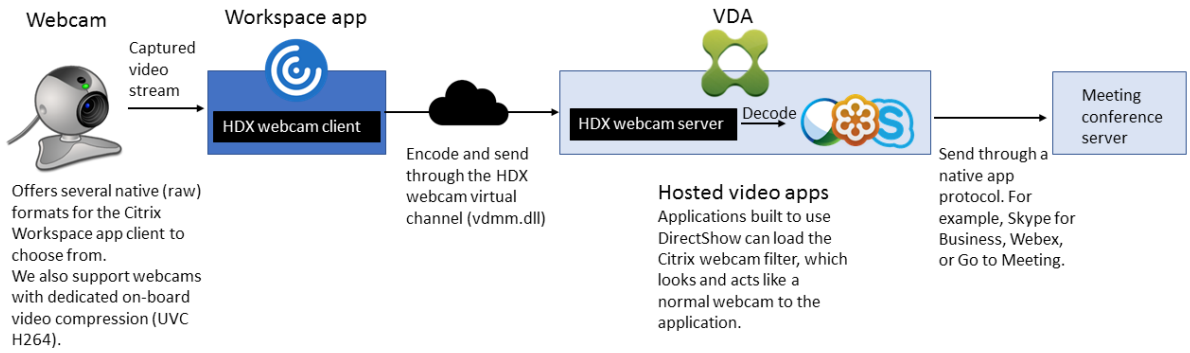
> ジストリファイルのバックアップを作成してから、レジストリを編集してください。

Web カメラは、HDX Web カメラビデオ圧縮または HDX プラグアンドプレイ汎用 USB リダイレクトにより、仮想セッション内で実行されるアプリケーションで使用できます。各モードの切り替えは、[**Citrix Workspace** アプリ] **>** [基本設定] **>** [デバイス] で行えます。
可能であれば常に、HDX Web カメラビデオ圧縮を使用することをお勧めします。
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って USB デバイスのリダイレクトを無効にします。このデフォルト設定は、Citrix Workspace アプリユーザーが **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] を選択すると無効になります。

HDX Web カメラビデオ圧縮

HDX Web カメラビデオ圧縮は、最適化 Web カメラモードとも呼ばれます。この Web カメラビデオ圧縮では、クライアントオペレーティングシステムに含まれるマルチメディアフレームワークテクノロジにより、キャプチャデバイスのビデオをインターセプトし、トランスコードおよび圧縮します。各キャプチャデバイスの製造元から、OS カーネルのストリーミングアーキテクチャに組み込まれるドライバーが提供されています。

クライアントは、Web カメラとの通信を処理します。その後、サーバーで適切に表示できるビデオのみを、サーバーに送信します。サーバーが Web カメラと直接やり取りをするわけではありませんが、統合によりデスクトップでも同様のエクスペリエンスが得られます。Citrix Workspace アプリがビデオを圧縮するため、帯域幅が節約され、WAN シナリオでの回復性の向上します。



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）。

- マルチメディア会議
- Windows Media リダイレクト

Web カメラで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。ソフトウェア圧縮が使用されるようにするには、レジストリキーに次の DWORD キー値を追加します：

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

DeepCompress_ForceSWEncode=1

HDX Web カメラビデオ圧縮の要件

サポートされるクライアント: Citrix Workspace アプリ for Windows、Citrix Workspace アプリ for Mac、Citrix Workspace アプリ for Chrome、Citrix Workspace アプリ for Linux。

> 注:
>
> Windows 用の Citrix Workspace アプリと Chrome 用の Citrix Workspace アプリのみが、64 ビットのアプリのための Web カメラのリダイレクトをサポートしています。

サポートされるビデオ会議アプリケーション（32 ビットおよび 64 ビット）は以下のとおりです:

- Adobe Connect
- Cisco Webex および Webex for Teams
- GoToMeeting
- Google Hangouts および Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015
- Microsoft Lync 2010 および 2013
- Microsoft Skype 7 以上
- Windows 8.x 以降および Windows Server 2012 R2 以降で動作するメディアファンデーション形式のビデオアプリケーション

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

  データ：240

  値の名前：DefaultWidth、種類：REG_DWORD

  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

  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。
- HDX Web カメラを使用する場合、可能であれば、Web カメラの製造元から入手した Web カメラドライバーをクライアントにインストールしてください。

高品位 **Web** カメラストリーミング

サーバーのアプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。アプリケーションから Web カメラを選択します。Web カメラとアプリケーションが高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。1920x1080 までの Web カメラ解像度がサポートされています。

この機能を使用するには、Windows 向け Citrix Workspace アプリバージョン 1808 以降、または Citrix Receiver for Windows バージョン 4.10 以降が必要です。

レジストリキーを使用してこの機能を無効または有効にすることができます。次の設定では 352x288 のデフォルトの解像度が使用されます。

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

値の名前：Enable_HighDefWebcam

種類：REG_DWORD

データ：

0 = 高品位 Web カメラストリーミングを無効化

1 = 高品位 Web カメラストリーミングを有効化

クライアントのレジストリキーを使用して、特定の解像度を設定することができます。カメラが指定された解像度をサポートしていることを確認してください。

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

値の名前：DefaultWidth

種類：REG_DWORD

データ（10 進数）：必要な幅（1280 など）

値の名前：DefaultHeight

種類：REG_DWORD

データ（10 進数）：必要な高さ（720 など）

HDX プラグアンドプレイ汎用 **USB** リダイレクト

HDX プラグアンドプレイ汎用 USB リダイレクト（アイソクロナス）は、汎用 Web カメラモードとも呼ばれます。HDX プラグアンドプレイ汎用 USB リダイレクトの利点は、シンクライアントやエンドポイントにドライバーをイン

ストールする必要がないことです。USB スタックは仮想化されており、ローカルクライアントに接続した周辺機器はすべてリモート VM へ送信されます。リモートデスクトップは、ネイティブ接続の場合と同じように動作します。Windows デスクトップがハードウェアとのやり取りをすべて処理し、プラグアンドプレイロジックにより適切なドライバーが検出されます。ICA に対応したドライバーが存在する場合、ほとんどの Web カメラを使用できます。汎用 Web カメラモードでは、USB プロトコルにより未圧縮のビデオをネットワーク上で送信するため、はるかに多くの帯域幅（大量の Mbps）が使用されます。

HTML5 マルチメディアリダイレクション

April 26, 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ドライブに保存され、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。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）を探すには、使用するブラウザーの開発者ツールを使用します。

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	高速	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。

以下がサポートされており、ポリシーを使用してこれらを制御します。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。

- 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

Citrix Workspace アプリおよび Citrix Receiver の最小バージョン:

- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.5
- Linux 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Linux 13.5

VDA ブラウザーの最小バージョン	Windows OS のバージョン/ビルド/SP
Internet Explorer バージョン 11.0	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2
Firefox 47。Firefox 証明書ストアに証明書を手動で追加するか、Windows の信頼できる証明書ストアで証明書を探すように Firefox を構成します。詳しくは、「https://wiki.mozilla.org/CA:AddRootToFirefox」を参照してください。	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2

VDA ブラウザーの最小バージョン	Windows OS のバージョン/ビルド/SP
Chrome 51	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2

HTML5 ビデオリダイレクションソリューションのコンポーネント

- **HdxVideo.js** - Web サイト上のビデオコマンドを傍受する JavaScript フック。HdxVideo.js は、セキュア WebSocket（SSL/TLS）を使用して WebSocketService と通信します。
- **WebSocket SSL** 証明書
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp/XenDesktop Engineering、CN = Citrix XenApp/XenDesktop HDX In-Product CA）
    場所：［証明書 - ローカルコンピューター］>［信頼されたルート証明機関］>［証明書］
  - エンドエンティティ（リーフ）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（Citrix Virtual Apps and Desktops 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。

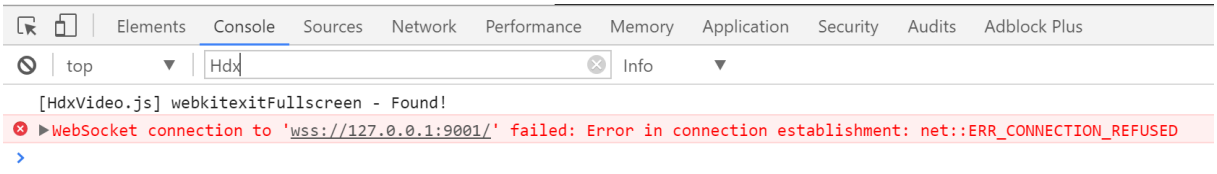
youtube.com のようにアダプティブビットレート技術（HTTP ライブストリーミング（HLS）、Dynamic Adaptive Streaming over HTTP（DASH）など）をベースにした Web サイトは、サポートされていません。

詳しくは、*「[マルチメディアのポリシー設定]」(/ja-jp/citrix-virtual-apps-desktops/2003/policies/reference/ica-policy-settings/multimedia-policy-settings.html)* 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:



Microsoft Teams の最適化

April 26, 2021

> 重要:
>
> Microsoft Teams の最適化には、Microsoft Teams バージョン 1.2.00.31357 以降が必要です。

Citrix では Citrix Virtual Apps and Desktops および Citrix Workspace アプリを通じてデスクトップベースの Microsoft Teams の最適化を提供します。必要なコンポーネントはデフォルトで Citrix Workspace アプリと Virtual Delivery Agent（VDA）に付属しています。

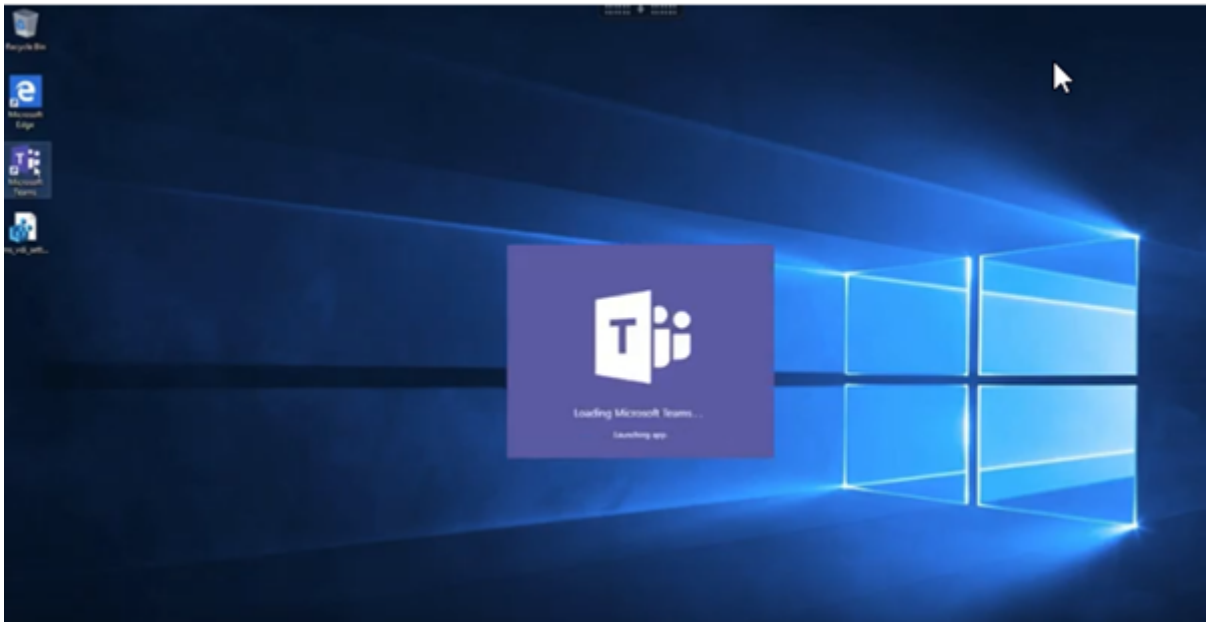
Microsoft Teams の最適化には、Microsoft Teams のホストアプリとのインターフェイスとしてコマンドを受信する、VDA 側の HDX サービスと API が含まれます。これらのコンポーネントにより Citrix Workspace アプリ側のメディアエンジンにつながる制御用の仮想チャネル（CTXMTOP）が開かれます。エンドポイントではマルチメディアがローカルでデコーディングされ、レンダリングされます。リバースシームレスの仕組みにより、Citrix Workspace アプリのローカルウィンドウはホストされている Microsoft Teams アプリにスナップインとして渡されます。

認証とシグナリングは他の Microsoft Teams サービス（チャットやコラボレーションなど）と同様に、Microsoft Teams がホストされているアプリでネイティブに行われます。これらのアプリはオーディオやビデオのリダイレクトによる影響を受けません。

CTXMTOPはコマンドであり、制御用の仮想チャネルです。つまり、Citrix Workspace アプリと VDA の間でメディアは交換されません。

クライアント側で取得/クライアント側でレンダリングのみを利用できます。

このデモ動画をご覧いただければ Microsoft Teams が Citrix の仮想環境でどのように機能するのかがお分かりいただけると思います。



Microsoft Teams のインストール

> 注:
>
> ゴールデンイメージで Teams をインストールする前に、VDA をインストールすることをお勧めします。このインストール順序は、**ALLUSER=1** フラグを有効にするために必要です。VDA をインストールする前に仮想マシンに Teams がインストールされている場合は、Teams をアンインストールして再インストールします。App Layering を使用している場合は、このセクションの最後にある「App Layering」の手順を参照してください。

Microsoft Teams のマシン全体のインストールガイドラインに記載のとおり、AppDataに Teams をインストールする.exe インストーラーを使用しないことをお勧めします。代わりに、コマンドラインで **ALLUSER=1** フラグを使用してC:\Program Files (x86)\Microsoft\Teamsにインストールします。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、**ALLUSERS=1** パラメーターも使用します。このパラメーターを設定すると、Teams のマシン全体のインストーラーが、そのコンピューターのすべてのユーザーのコントロールパネルにある ［プログラムと機能］と Windows 設定にある ［アプリと機能］に表示されます。管理者の資格情報があれば、すべてのユーザーが Teams をアンインストールできます。**ALLUSERS=1** と **ALLUSER=1** の違いを理解することが重要です。**ALLUSERS=1** パラメーターは、非 VDI 環境と VDI 環境で使用できます。マシンごとのインストールを指定するには、VDI 環境でのみ **ALLUSER=1** パラメーターを使用します。

ALLUSER=1 モードでは、Teams アプリケーションのバージョンが新しくなるたびに自動更新されることはありません。非永続環境では、このモードの使用をお勧めします。たとえば、Windows Server または Windows 10 のランダム/プールカタログからホストされた共有アプリまたはデスクトップなどです。詳しくは、「MSI を使用して Microsoft Teams をインストールする」（VDI インストールセクション）を参照してください。

Windows 10 専用の永続 VDI 環境があります。Teams アプリケーションを自動更新し、ユーザーごとにAppdata/Localに Teams をインストールする場合、.exeインストーラーを使用するか、**ALLUSER =1** を設定せずに MSI を使用します。

App Layering の場合:

> 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。
> PortICAという名前の空のレジストリキーを作成します（デフォルトの名前、種類、データはそのままにします）。

Citrix App Layering を使用して VDA と Microsoft Teams インストールを異なるレイヤーで管理する場合、**ALLUSER =1** で Teams をインストールする前に Windows で次のレジストリキーを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix

または

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix

Profile Management の推奨事項

コマンドラインでALLUSER =1フラグを MSI に渡すと、Teams アプリはC:\Program Files（~300MB）にインストールされます。このアプリはログにAppData\Localを、ユーザー独自の構成、ユーザーインターフェイスの要素のキャッシュなどに AppData\Roaming\Microsoft\Teamsを使用します。

システム要件

最小バージョン **- Delivery Controller**（**DDC**）**1906.2**:

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 2019、2016、2012 R2 の Standard Edition、Datacenter Edition、および Server Core オプション付き

最小バージョン **- Virtual Delivery Agent**（**VDA**）**1906.2**:

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 64 ビット版、バージョン 1607 以降。
- Windows Server 2019、2016 および 2012 R2 の Standard および Datacenter エディション

要件:

- BCR_x64.msi - Microsoft Teams の最適化コードが格納された MSI ファイルです。自動的に GUI で起動します。VDA のインストールにコマンドラインインターフェイスを使用する場合は、このファイルを除外しないでください。

推奨バージョン **- Windows** 向け **Citrix Workspace** アプリ **2006.1** および最小バージョン **- Windows** 向け **Citrix Workspace** アプリ **1907**:

- Windows 7、8、および 10 32 ビット版および 64 ビット版（Embedded エディションを含む）
- Windows 10 IoT Enterprise 2016 LTSB（v1607）および 2019 LTSC（v1809）
- サポートされているプロセッサ（CPU）アーキテクチャ：x86 および x64（ARM はサポートされていません）
- エンドポイントの要件：2.1～2.4GHz 程度のデュアル CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応していること。
- デュアルまたはクアッドコア CPU、低い基本速度（約 1.5GHz）で Intel Turbo Boost または AMD Turbo Core を搭載し、少なくとも 2.4GHz までブーストできる。
- 検証済みの HP シンクライアント：t630/t640、t730/t740、mt44/mt45。
- 検証済みの Dell シンクライアント：5070、5470 モバイル TC。
- 検証済みの 10ZiG シンクライアント：4510 および 5810q。
- 検証済みエンドポイントの完全な一覧については、「シンクライアント」を参照してください。
- Citrix Workspace アプリでは、少なくとも 600MB のディスクスペースと 1GB の RAM が必要です。
- Microsoft .NET Framework の最小要件はバージョン 4.6.2 です。システムに.NET Framework が導入されていない場合は、Citrix Workspace アプリにより自動的にダウンロードとインストールが行われます。

最小バージョン **- Linux** 向け **Citrix Workspace** アプリ **2006**:

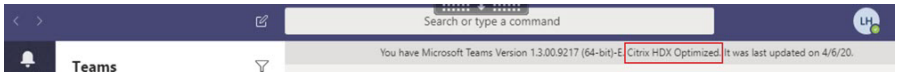
詳しくは、「2006 の新機能」の「*Microsoft Teams* の最適化」を参照してください。

Microsoft Teams の最適化を有効にする

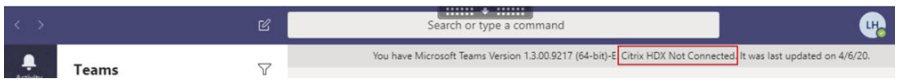
Microsoft Teams の最適化を有効にするには、「Microsoft Teams のリダイレクトポリシー」で説明されている Studio 用ポリシーを使用します（デフォルトは **ON** です）。HDX はこのポリシーが有効になっていることと、Citrix Workspace アプリのバージョンが最低限必要とされるバージョンよりも新しいことを確認します。ポリシーが有効で Citrix Workspace アプリがサポート対象のバージョンである場合は、VDA でレジストリキー **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** の値が **1** に自動的に設定されます。Microsoft Teams アプリケーションはこのレジストリキーを VDI モードで読み取ってロードします。

> 注:
>
> Studio で使用可能なポリシーがない古い Controller バージョン（たとえばバージョン 7.15）でバージョン 1906.2 以上の VDA を使用している場合、その VDA では Microsoft Teams の HDX 最適化がデフォルトで有効になっているため、まだ最適化されていることがあります。

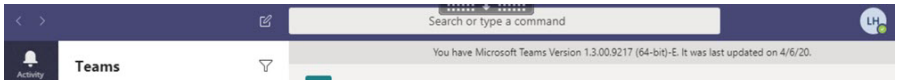
［バージョン情報］をクリックすると、**Citrix HDX Optimized** と表示されます:



代わりに **Citrix HDX Not Connected** と表示される場合は、Citrix API が Teams に読み込まれますが（リダイレクトの最初のステップです）、スタックの後続の部分にエラーがありました。このエラーは、VDA サービスまたは Citrix Workspace アプリで発生する可能性があります。



凡例が表示されない場合、Teams は Citrix API を読み込めませんでした。通知領域のアイコンを右クリックして Teams を終了し、再起動します。Studio ポリシーが ［禁止］に設定されておらず、Citrix Workspace アプリのバージョンがサポートされていることを確認します。



ネットワークの要件

Microsoft Teams は、会議またはマルチパーティ通話で Office 365 のメディアプロセッササーバーに依存します。次のシナリオで Microsoft Teams は Office 365 トランスポートリレーに依存します:

- ピアツーピア通話の 2 つのピアが直接接続できない。
- 参加者がメディアプロセッサに直接接続できない。

そのため、ピアと Office 365 クラウドの間のネットワークの状態が通話のパフォーマンスを左右します。

環境を評価し、クラウド全体のオーディオおよびビデオ環境に影響を与える可能性のあるリスクと要件を特定することをお勧めします。
Skype for Business ネットワーク評価ツールを使用して、ネットワークが Microsoft Teams に対応できるかどうかをテストします。サポート情報については、「サポート」セクションを参照してください。

リアルタイムプロトコル（**RTP**）トラフィックに関する主要なネットワーク推奨事項の要約:

- 可能な限り支社から直接 Office 365 ネットワークに接続します。
- 支社で次のいずれかを使用する必要がある場合は、RTP/UDP の Teams トラフィックが妨げられないことを確認してください。HdxTeams.exe は、エンドポイントで構成された明示的なプロキシを適用しません。
  - プロキシサーバーのバイパス
  - ネットワークの SSL インターセプト
  - ディープパケットインスペクションデバイス
  - VPN ヘアピン（可能な場合は分割トンネリングを使用）
- 十分な帯域幅を計画して提供します。
- 各支社のネットワークの接続性と品質について確認してください。

Workspace アプリ（HdxTeams.exe）の WebRTC メディアエンジンは、クライアントにオフロードされるマルチメディアストリームの Secure Real-time Transport Protocol（SRTP）を使用します。SRTP は、対称キー（128

ビット）を使用してメディアを暗号化しメッセージを制御することにより、RTP に機密性と認証を提供し、カウンターモードで AES 暗号化を使用します。

ポジティブなユーザーエクスペリエンスを保証するために、次の測定基準をお勧めします:

測定基準	エンドポイントから Office 365
遅延（片道）	50 ミリ秒未満
遅延（RTT）	100 ミリ秒未満
パケット損失	15 秒間隔で 1% 未満
パケット到着間ジッタ —	15 秒間隔で 30 ミリ秒未満

詳しくは、「Microsoft Teams 用に組織のネットワークを準備する」を参照してください。

帯域幅の要件に関して、Microsoft Teams 用の最適化では、オーディオ（OPUS/G.722/PCM G711）およびビデオ（H264/VP9）用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル（SDP）のオファー/アンサーを使用して、通話の確立プロセス中にこれらのコーデックをネゴシエートします。
Citrix の最低推奨要件は次のとおりです:

種類	帯域幅	コーデック
オーディオ（片道）	約 90kbps	G.722
オーディオ（片道）	約 60kbps	Opus*
ビデオ（片道）	約 700kbps	H264 360p @ 30 fps 16:9
ビデオ（片道）	約 2,500kbps	VP9 720p @ 30 fps 16:9
画面共有	約 300kbps	H264 1080p @ 15 fps

* Opus は、6kbps～510kbps の固定および可変ビットレートのエンコードをサポートしています。

Opus および VP9 は、最適化された 2 VDI ユーザー間のピアツーピア通話の優先コーデックです。

G.722 および H264 は、会議に参加する VDI ユーザーに推奨されるコーデックです。

通話の確立とメディアフローパス

可能であれば、Citrix Workspace アプリの HDX メディアエンジン（HdxTeams.exe）が、ピアツーピア通話でユーザーデータグラムプロトコル（UDP）上で直接ネットワーク Secure Real-time Transport Protocol（SRTP）接続を確立しようとします。UDP ポートがブロックされている場合、メディアエンジンは TCP 443 にフォールバッ

クします。

HDX メディアエンジンは、ICE、Session Traversal Utilities for NAT（STUN）、Traversal Using Relays around NAT（TURN）をサポートして、候補の検出と接続の確立を行います。

2 つのピア間、またはピアと会議サーバーの間に直接のパスがない（ユーザーがマルチパーティ通話または会議に参加している）場合、HdxTeams.exe は Office 365 の Microsoft Teams トランスポートリレーサーバーを使用して、他のピアまたは（会議がホストされている）メディアプロセッサにアクセスします。ユーザーのクライアントマシンは、2 つの Office 365 サブネット IP アドレス範囲と 4 つの UDP ポートにアクセスできる必要があります。詳しくは、下の「通話のセットアップ」セクションのアーキテクチャ図と「Office 365 の URL と IP アドレスの範囲 ID 11」を参照してください。

ID	カテゴリ	アドレス	ターゲットポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP**：3478、3479、3480、3481、**TCP**：443（フォールバック）

これらの範囲には、トランスポートリレーとメディアプロセッサの両方が含まれます。
Teams トランスポートリレーは、STUN および TURN 機能を提供しますが、ICE エンドポイントではありません。また、Teams トランスポートリレーはメディアを終了せず、トランスコード処理も実行しません。他のピアまたはメディアプロセッサにトラフィックを転送するときに、TCP（HdxTeams.exe が TCP を使用している場合）を UDP に中継できます。

HdxTeams.exe は、Office 365 クラウド内の最も近い Microsoft Teams トランスポートリレーと通信します。HdxTeams.exe は、エニーキャスト IP とポート 3478～3481 UDP（ワークロードごとに異なる UDP ポート、多重化によって発生する場合あり）またはフォールバックに 443 TCP TLSv1.2 を使用します。通話品質は、基盤となるネットワークプロトコルによって異なります。UDP は常に TCP よりも推奨されるため、支社の UDP トラフィックに対応するようネットワークを設計することをお勧めします。

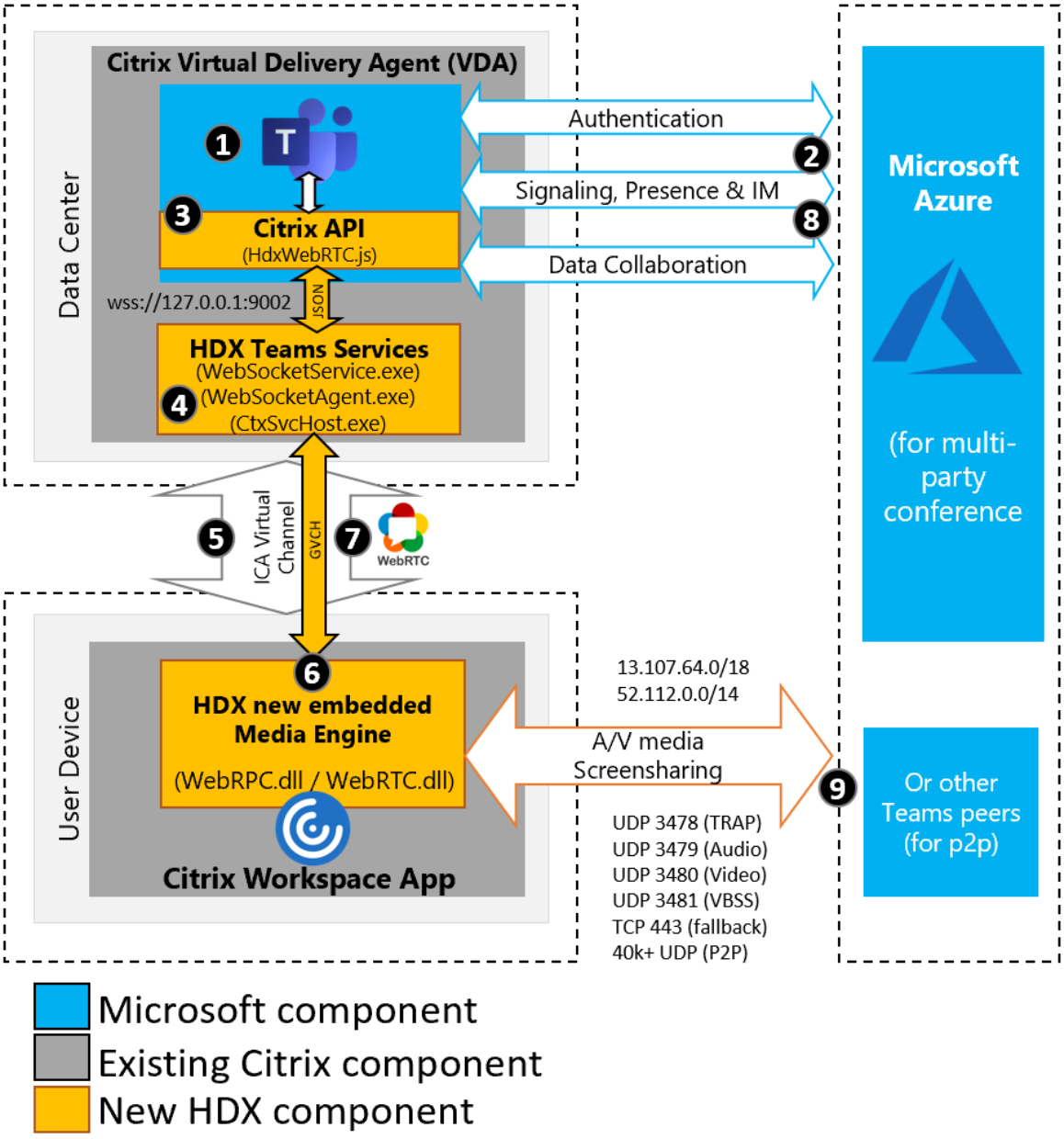
Teams が最適化モードで読み込まれ、HdxTeams.exe がエンドポイントで実行されている場合、対話型接続確立（ICE）の失敗により、通話のセットアップエラーが発生するか、オーディオ/ビデオが一方通行になります。通話を完了できない場合、またはメディアストリームが全二重でない場合は、最初にエンドポイントの **Wireshark** トレースを確認してください。ICE 候補の収集プロセスについて詳しくは、「サポート」セクションの「ログの収集」を参照してください。

> 注：
>
> エンドポイントにインターネットアクセスがない場合でも、同じ LAN 上でピアツーピア通話ができる可能性があります。会議は失敗します。この場合、通話のセットアップが始まる前に 30 秒のタイムアウトがあります。

通話のセットアップ

このアーキテクチャ図は、通知フローシーケンスの視覚的なリファレンスとして使用します。対応する手順が図に示されています。

アーキテクチャ:



1. Microsoft Teams を起動します。
2. Teams が O365 に対する認証を行います。テナントポリシーが Teams クライアントにプッシュダウンされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Teams は VDA で実行されていることを検出し、Citrix JavaScript API への API 呼び出しを行います。

4. Teams 内の Citrix JavaScript は、VDA 上で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き（127.0.0. 1:9002）、ユーザーセッション内で実行される WebSocketAgent.exe を起動します。
5. WebSocketAgent.exe は、Citrix HDX Teams リダイレクトサービス（CtxSvcHost.exe）を呼び出すことによって、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe（HDX エンジン）は、Teams の最適化に使用される新しい WebRTC エンジンである HdxTeams.exe という新しいプロセスを生成します。
7. HdxTeams.exe と Teams.exe は、双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   ——ユーザー呼び出し——

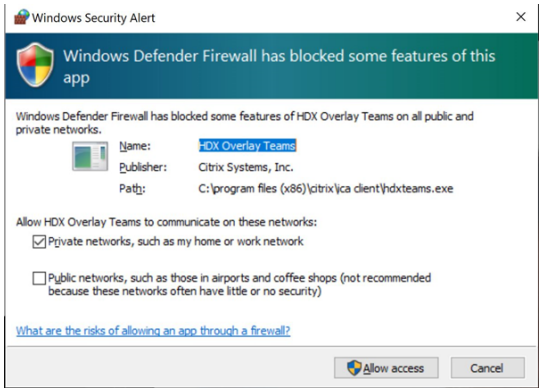
8. ピア **A** が 呼び出しボタンをクリックします。Teams.exe は Office 365 の Teams サービスと通信し、ピア **B** とのエンドツーエンドのシグナリングパスを確立します。Teams は、サポートされている一連の呼び出しパラメーター（コーデック、解像度など、セッション記述プロトコル（SDP）サービスとして知られています）を HdxTeams に要求します。これらの呼び出しパラメーターは、Office 365 の Teams サービスへのシグナリングパスを使用して、そこから他のピアに中継されます。
9. SDP オファーまたは応答（シングルパスネゴシエーション）はシグナリングチャネル経由で実行され、対話型接続確立（ICE）接続チェック（Session Traversal Utilities for NAT（STUN）バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。次に、Secure Real-time Transport Protocol（SRTP）メディアは、HdxTeams.exe と他のピア（または会議の場合は Office 365 会議サーバー）の間で直接やり取りされます。

Microsoft 電話システム

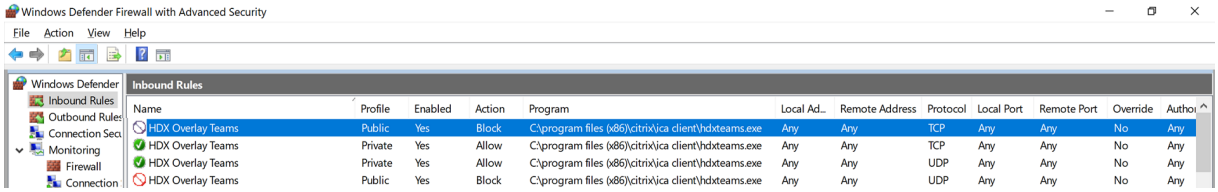
電話システムは、Microsoft Teams を使用して Office 365 クラウドで通話制御機能および PBX 機能を有効にする Microsoft のテクノロジです。Microsoft Teams の最適化は、Office 365 通話プランまたはダイレクトルーティングを使用する電話システムをサポートします。ダイレクトルーティングを使用すると、オンプレミスのソフトウェアを追加しなくても、サポートされている独自のセッションボーダーコントローラーを Microsoft 電話システムに直接接続できます。

ファイアウォールについての考慮事項

ユーザーが初めて Microsoft Teams クライアントを使用して最適化された呼び出しを開始すると、**Windows** ファイアウォール設定の警告が表示される場合があります。この警告は、HdxTeams.exe（HDX Overlay Teams）の通信を許可するようユーザーに求めます。



以下の 4 つのエントリが ［セキュリティが強化された **Windows Defender** ファイアウォール］コンソールの ［受信規則］に追加されます必要に応じて、より制限的な規則を適用できます。

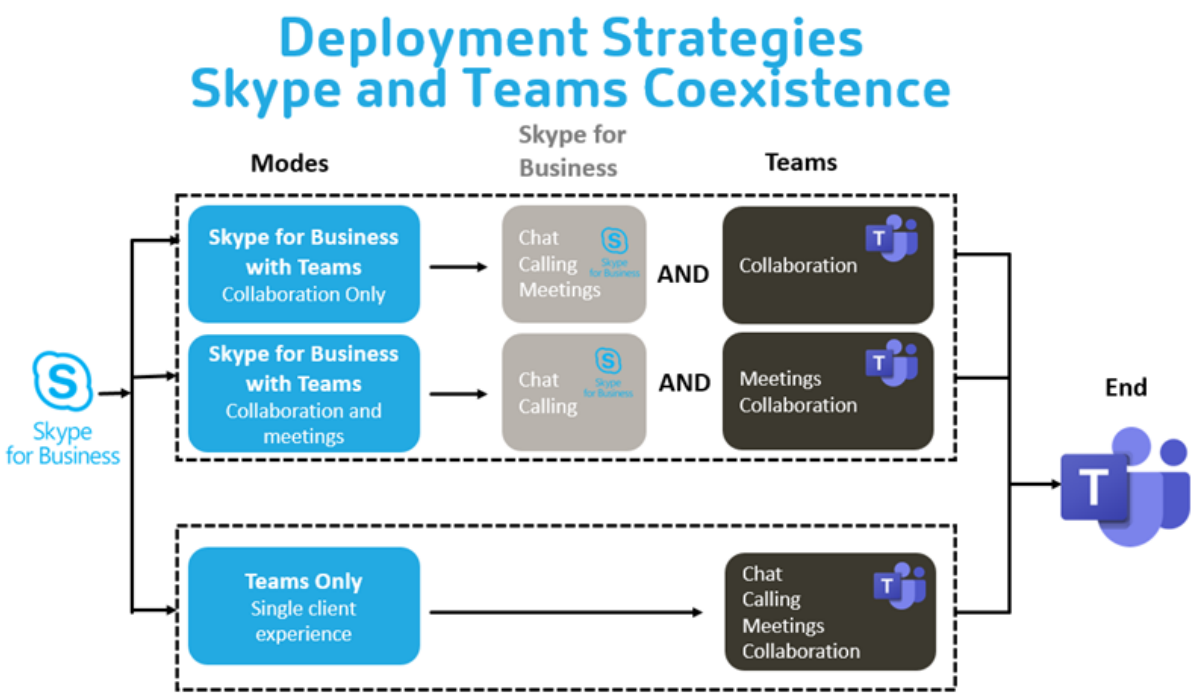


Microsoft Teams と **Skype for Business** の共存

Microsoft Teams と Skype for Business を、機能が重複する 2 つの個別のソリューションとして並べて展開できます。
詳しくは、Microsoft Teams と Skype for Business の共存と相互運用性の理解を参照してください。

Citrix RealTime Optimization Pack と Teams マルチメディアエンジンの HDX 最適化は、環境に設定されている構成をすべて尊重します（たとえば、アイランドモード、Skype for Business と Teams のコラボレーション、Skype for Business と Teams のコラボレーションおよび会議）。

周辺機器アクセス権限は、一度に 1 つのアプリケーションにのみ付与されます。たとえば、通話中に RealTime Media Engine が Web カメラにアクセスすると、通話の間、イメージデバイスがロックされます。デバイスがリリースされると、Teams で使用できるようになります。



Citrix SD-WAN：**Microsoft Teams** 向けに最適化されたネットワーク接続

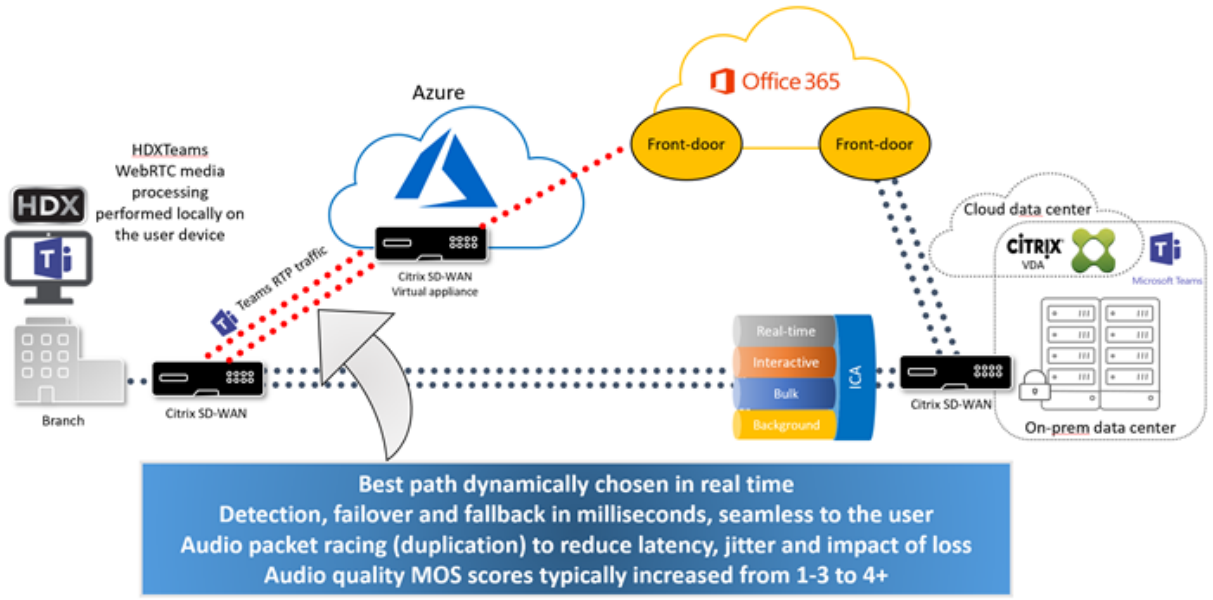
オーディオとビデオの最適な品質には、Office 365 クラウドへのネットワーク接続で低遅延、低ジッター、低パケット損失が必要です。Citrix Workspace アプリユーザーによる支社からデータセンターへの Microsoft Teams 音声ビデオ RTP トラフィックのバックホールで追加の遅延が発生し、WAN リンクの輻輳が発生することがあります。Citrix SD-WAN は Microsoft Office 365 ネットワーク接続の原則に従って、Microsoft Teams の接続を最適化します。Microsoft REST ベースの Office 365 IP アドレスと Web サービス、および近接 DNS を使用して、Citrix SD-WAN が Microsoft Teams トラフィックを識別、分類、および誘導します。

多くの地域のビジネス用ブロードバンドインターネット接続は、断続的なパケット損失、過度のジッター期間、停止に悩まされています。

Citrix SD-WAN は、ネットワークの状態がさまざまに異なる場合、または低下している場合、Microsoft Teams のオーディオ/ビデオ品質を保持する 2 つのソリューションを提供します。

- Microsoft Azure を使用している場合、Azure VNET で導入された Citrix SD-WAN 仮想アプライアンス（VPX）は、高度な接続の最適化を提供します。これらの最適化には、シームレスなリンクフェールオーバーとオーディオパケットトレースが含まれます。
- または、Citrix SD-WAN のお客様は Citrix Cloud Direct サービスを介して Office 365 に接続できます。このサービスは、すべてのインターネットのトラフィックに信頼できる安全な配信を提供します。

支社のインターネット接続の品質が問題にならない場合は、Microsoft Teams トラフィックを Citrix SD-WAN ブランチアプライアンスから最も近い Office 365 フロントドアに直接誘導し、遅延を最小限に抑えることができます。詳しくは、「Citrix SD-WAN Office 365 の最適化」を参照してください。



Microsoft Teams のギャラリービューとアクティブスピーカー

会議またはグループ通話では、単一の受信ビデオストリームのみがサポートされます。ビデオを送信する参加者が複数いる場合、常に主要なスピーカーのビデオのみが表示されます。アクティブなスピーカーが検出されてからビデオフィードが表示されるまでの間に、1、2 秒の遅延が発生することがあります。

Microsoft Teams の画面共有

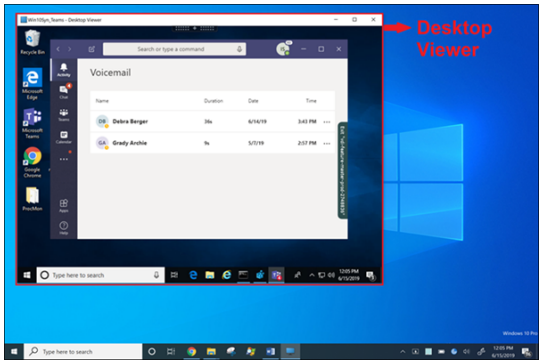
Microsoft Teams は、H264 のようなビデオコーデックで共有されているデスクトップを効果的にエンコードし高画質ストリームを作成する、ビデオベースの画面共有（VBSS）に依存しています。HDX 最適化により、受信画面共有はビデオストリームとして扱われます。そのため、ビデオ通話の最中に他のピアがデスクトップの共有を開始すると、元のカメラのビデオフィードが一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、このピアは手動でカメラ共有を再開する必要があります。

> 重要:
>
> 画面共有は、音声通話またはビデオ通話がアクティブな場合にのみ使用でき、音声やビデオがないチャットウィンドウから直接使用することはできません。

送信画面の共有も最適化され、Citrix Workspace アプリ（バージョン 1907 以降）にオフロードされます。この場合、HdxTeams.exe は、Citrix Desktop Viewer（CDViewer.exe）ウィンドウのみをキャプチャして送信します。クライアントマシンで実行されているローカルアプリケーションを共有する場合は、CDViewer にオーバーレイとして適用することができ、それもキャプチャされます。

マルチモニター：CDViewer が全画面モードでマルチモニターにまたがっている場合、プライマリモニターのみが共有されます。ユーザーは、仮想デスクトップ内の目的のアプリケーションを、通話中の他のピアのプライマリモニタ

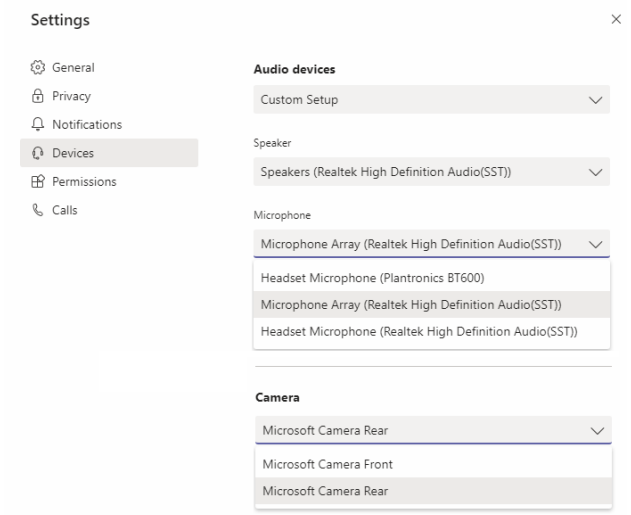
ーにドラッグして表示する必要があります。



> 注:
>
> Teams をスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は、Citrix Workspace アプリのバージョン 1909 以降で物理エンドポイントのローカルデスクトップをキャプチャします。

Microsoft Teams の周辺機器

Microsoft Teams の最適化がアクティブな場合、Citrix Workspace アプリは周辺機器に（ヘッドセット、マイク、カメラ、スピーカーなど）アプリにアクセスします。その後、周辺機器は Microsoft Teams UI に正しく列挙されます（設定 **>** デバイス）。



Microsoft Teams はデバイスに直接アクセスしません。メディアの取得、キャプチャ、処理には、代わりに HdxTeams.exe が使用されます。Microsoft Teams では、ユーザーが選択できるデバイスが一覧表示されます。

推奨事項:

- エコーキャンセルが内蔵されたMicrosoft Teams 認定ヘッドセット。マイクとスピーカーが別のデバイスにある複数周辺機器のセットアップでは、エコーが発生する可能性があります。これは、マイクが Web カメラ

に内蔵されており、スピーカーがモニターに搭載されている場合などです。外部スピーカーを使用する場合は、マイクと、マイクに音を屈折させる可能性のある面から可能な限り離れた場所に配置します。

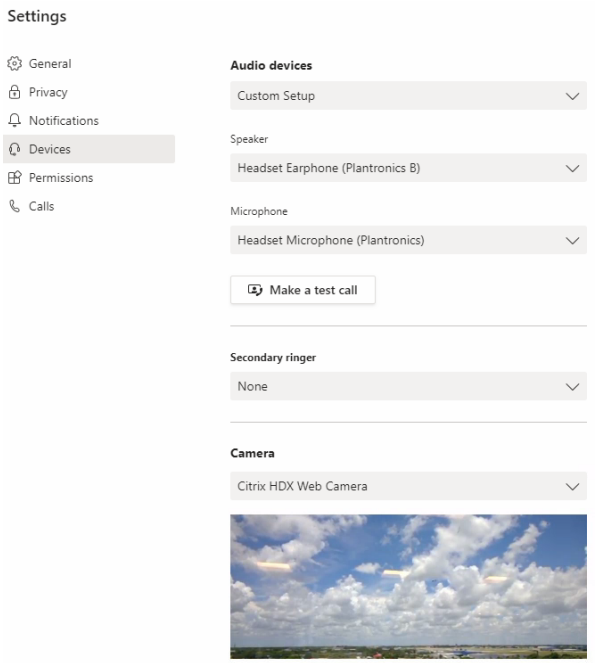
- Skype for Business 認定周辺機器は Microsoft Teams と互換性がありますが、Microsoft Teams 認定カメラ。
- HdxTeams.exe は、オンボード H.264 エンコーディング-UVC 1.1 および 1.5 を実行する Web カメラで CPU オフロードを利用できません。

> 注:
>
> HdxTeams.exe は、特定のオーディオデバイス形式（チャネル、ビット深度、サンプルレート）のみをサポートします:
>
> - 再生デバイス: 最大 2 チャネル、16 ビット、最大 96,000Hz の周波数
> - 録音デバイス: 最大 4 チャネル、16 ビット、最大 96,000Hz の周波数
>
> 1 つのスピーカーまたはマイクが通常の設定と一致しない場合でも、Teams のデバイス列挙は失敗し、［設定］**>**［デバイス］になしが表示されます。
> **HdxTeams.exe** の
> Webrpcログはこのような情報を表示します:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create
> audio module!
> ```
>
> この問題を回避するには、サウンドコントロールパネル（mmsys.cpl）を開き、再生または録音デバイスを選択して、［プロパティ］**>**［詳細設定］でサポートされているモードに変更します。または、特定のデバイスを無効にします。

フォールバックモード

最適化された VDI モードで Microsoft Teams が読み込めない場合、VDA は、Web カメラリダイレクトやクライアントのオーディオとマイクのリダイレクトのような従来の HDX テクノロジを使用します。非最適化モードでは、周辺機器が VDA にマップされます。周辺機器は、Microsoft Teams アプリには仮想デスクトップにローカルで接続されているように表示されます。

Teams の ［設定］**>**［デバイス］タブで表示されるカメラ名の違いで、最適化モードか非最適化モードかを判断できます。Microsoft Teams が非最適化モードで読み込まれた場合、従来の HDX テクノロジが起動します。以下の画像のように、Web カメラ名の冒頭には **Citrix HDX** が表示されます。スピーカーとマイクのデバイス名は、最適化モードと比べてわずかに異なる（または省略される）場合があります。



従来の HDX テクノロジを使用する場合、Microsoft Teams はオーディオ、ビデオ、および画面共有処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジでサーバー側でのレンダリングが使用されます。ビデオをオンにすると、VDA の CPU 消費量が高くなることが予想されます。リアルタイムのオーディオパフォーマンスは最適ではない場合があります。

既知の制限事項

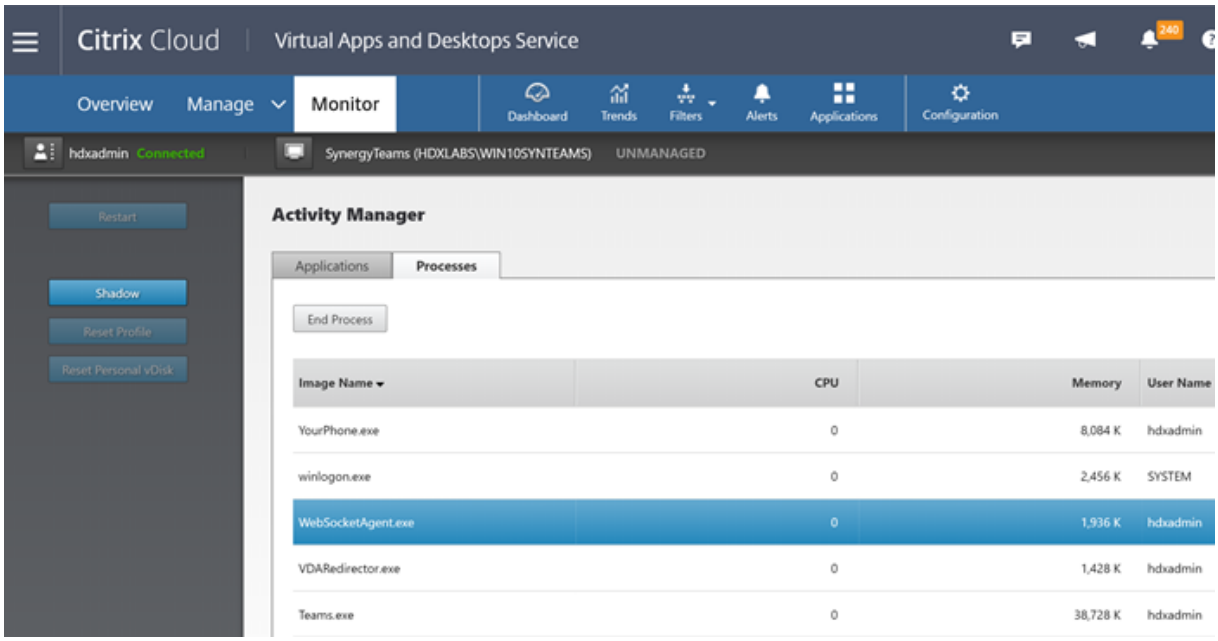
制限事項	コメント
画面の共有 - 画面を共有するにはアクティブな通話が必要です。チャットウィンドウからの画面共有はサポートされていません。	Teams の依存関係 – Microsoft にお問い合わせください
ポップアウトチャット（マルチウィンドウチャットまたは新しい会議エクスペリエンスとも呼ばれます）はサポートされていません。	Citrix と Microsoft の制限
ギャラリービュー - アクティブスピーカーのみ。	Teams の依存関係 – ギャラリービュー（2x2）が必要になる状況については、Microsoft にお問い合わせください
HID ボタン - 応答と通話終了はサポートされていません。音量の増減はサポートされています。	Citrix Workspace アプリの制限
通話中に ［設定］**>** ［デバイス］で周辺機器の入力または出力を切り替えると、通話の途中で 1 秒のオーディオの乱れが発生する場合があります。	

制限事項	コメント
マルチモニター環境で画面共有を行うと、メインモニターのみが共有されます。	Citrix Workspace アプリの制限
Citrix Workspace アプリの高 DPI 設定を ［いいえ、ネイティブ解像度を使用します］に設定すると、モニターの DPI スケールファクターが 100% を超えて設定された場合、リダイレクトされたビデオウィンドウが外れて表示されます。	Citrix Workspace アプリの制限
テレフォニーシステムでの Dual Tone Multi Frequency（DTMF）の使用はサポートしていません。	Citrix Workspace アプリの制限
画面共有を行うと ［システムオーディオを含める］オプションを使用できません。	Citrix と Microsoft の制限
Skype for Business との相互運用性は音声通話に限定され、ビデオのモダリティはありません。	Microsoft の制限
受信および発信ビデオストリームの最大解像度は 720p です。	Teams の依存関係 – 1080p が必要になる状況については、Microsoft にお問い合わせください
受信カメラまたは画面共有ストリームからのビデオストリームは 1 つしかサポートしません。受信画面共有がある場合、優先度の高いスピーカーのビデオではなく、画面共有が表示されます。	Teams の依存関係 – Microsoft にお問い合わせください
発信画面共有：アプリケーション共有はサポートされていません。	Citrix Workspace アプリと VDA の制限
ライブイベントはサポートしていません。	Citrix および Teams の制限
制御を渡すまたは制御を獲得する：画面共有またはアプリケーション共有セッション中はサポートされません。PowerPoint 共有セッション中はサポートされます。	Teams の依存関係 – Microsoft にお問い合わせください
発信画面共有でマウスポインターがキャプチャされません	Citrix の制限
セカンダリ呼び出し（[**Teams**］**>** ［設定］**>** ［デバイス］）はサポートされていません	Citrix の制限
通話中に、ユーザーが Microsoft Teams で共有ファイルを開くと、通話が切断されることがあります。	Microsoft の制限

制限事項	コメント
PSTN 通話の呼び出し音はサポートされていません	Teams の依存関係 – Microsoft にお問い合わせください
Microsoft Teams の通話品質ダッシュボードに VDI ユーザーのデータが表示されない	Teams の制限 — Microsoft に問い合わせてください

Teams の監視

このセクションでは、HDX による Microsoft Teams の最適化を監視するためのガイドラインを提供します。
ユーザーが最適化モードで実行していて、`HdxTeams.exe`がクライアントマシンで実行されている場合、VDA にはセッションで実行されている`WebSocketAgent.exe`というプロセスがあります。Director で ［アクティビティマネージャー］を使用してアプリケーションを表示します。



VDA バージョン 1912 以降では、Citrix HDX Monitor（最小バージョン 3.11）を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品の ISO には、フォルダー`layout\image-full\Support\HDX Monitor`に最新の`hdxmonitor.msi`が含まれます。

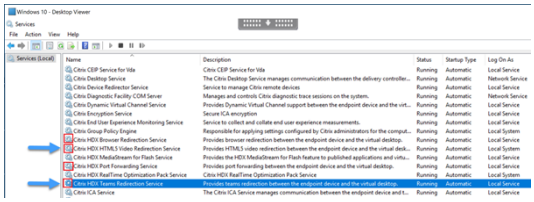
詳しくは、Knowledge CenterCTX253754の *Monitoring* を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を実施する際に想定される問題に対処するためのヒントを提供します。
詳しくは、CTX253754 を参照してください。

Virtual Delivery Agent の状態

BCR_x64.msi. により 4 つのサービスがインストールされています。そのうちの 2 つが、VDA での Microsoft Teams のリダイレクトを担当します。



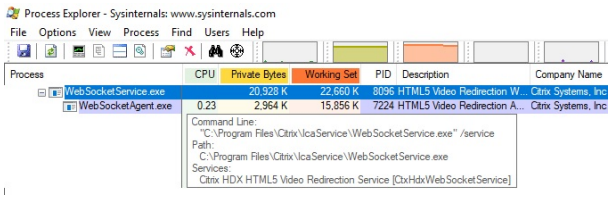
- **Citrix HDX Teams** リダイレクトサービスは Microsoft Teams が使用する仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存します。
- **Citrix HDX HTML 5** ビデオリダイレクトサービスは WebSocketService.exe として実行され、127.0.0.1 の TCP ポート 9002 をリッスンします。WebSocketService.exe には主に 2 つの機能があります。

  i. Microsoft Teams アプリのコンポーネントとして組み込まれている vdiCitrixPeerConnection.js から **WebSocket** のセキュリティを確保する **TLS** ターミネーションに対して、安全な WebSocket 接続が渡されます。この接続はプロセスモニターで追跡可能です。証明書について詳しくは、「Controller と VDA の間の通信」の「TLS および HTML5 ビデオリダイレクション、および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。

  一部のウイルス対策ソフトウェアおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`およびその証明書の適切な動作を妨げます。Citrix HDX HTML5 ビデオリダイレクトサービスは、`services.msc`コンソールで動作している可能性がありますが、localhost `127.0.0.1:9002` TCP ソケットが netstat で表示されるようにリスニングモードになることはありません。サービスを再起動しようとすると、サービスがハングします（「停止しています...」）。`WebSocketService.exe`プロセスで適切な除外を適用するようにしてください。

  ii. ユーザーセッションのマッピング。Microsoft Teams アプリケーションが起動すると、WebSocketService.exe は VDA のユーザーセッションで WebSocketAgent.exe プロセスを起動します。WebSocketService.exe は LocalSystem アカウントの動作として、セッション 0 で実行されます。

  netstat を使用して、WebSocketService.exe サービスが VDA でアクティブなリッスン状態であるかどうかを確認できます。

  管理者特権でのコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します:


```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

接続が成功すると、状態が ESTABLISHED に変わります:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> 重要:
>
> WebSocketService.exe は 127.0.0.1:9001 と 127.0.0.1:9002 の 2 つの TCP ソケットでリッスンします。ポート 9001 はブラウザーコンテンツのリダイレクトと HTML5 ビデオのリダイレクトに、ポート 9002 は Microsoft Teams のリダイレクトにそれぞれ使用されます。VDA の Windows OS に、Teams.exe と WebSocketService.exe の間の直接通信を妨げる可能性があるプロキシ構成がないことを確認してください。Internet Explorer 11（[インターネットオプション] > [接続] > [**LAN** の設定] > [プロキシサーバー]）で明示的なプロキシを構成すると、接続は割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合、[ローカルアドレスにはプロキシサーバーを使用しない] がオンになっていることを確認します。

サービスの場所と説明

サービス	Windows Server OS の実行可能ファイルへのパス	ログオン名	説明
Citrix HTML5 ビデオリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\W /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアのリダイレクトを実行する場合に必要な、複数の HDX マルチメディアサービスの初期のフレームワークを提供します。
Citrix HDX ブラウザーリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs	使用アカウント（ローカ	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトを実行します。

サービス	Windows Server OS の実行可能ファイルへのパス	ログオン名	説明
Citrix ポートフォワーディングサービス	“C:\Program Files (x86)\Citrix\System32\C -g PortFwdSvcs	使用アカウント（ローカルサービス）	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトのポートフォワーディングを実行します。
Citrix HDX Teams リダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間で Microsoft Teams のリダイレクトを実行します。

Citrix Workspace アプリ

Windows 向け Citrix Workspace アプリは、ユーザーのエンドポイント上で HdxTeams.exe という名前の新しいサービスをインスタンス化します。これは、Microsoft Teams が VDA で起動し、ユーザーがセルフプレビューで周辺機器の呼び出しやアクセスを試みたときに行われます。このサービスが表示されない場合は、次の点を確認してください:

1. Windows 向け Workspace アプリのバージョン 1905 以上がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe と webrpc.dll バイナリがあるかを確認します
2. 手順 1 の確認ができたら、次の手順を実行して HdxTeams.exe が起動するかを確認してください。
   a) VDA で Microsoft Teams を終了します。
   b) VDA で services.msc を起動します。
   c) Citrix HDX Teams リダイレクトサービスを停止します。
   d) ICA セッションを切断します。
   e) ICA セッションを接続します。
   f) Citrix HDX チームリダイレクトサービスを起動します。
   g) Citrix HDX HTML5 ビデオリダイレクトサービスを再起動します。
   h) VDA で Microsoft Teams を起動します。
3. これでもクライアントエンドポイントで HdxTeams.exe が起動しない場合は、次の手順を実行してください:
   a) Linux VDA を再起動します。
   b) クライアントエンドポイントを再起動します。

サポート

シトリックスと Microsoft は Citrix Virtual Apps and Desktops での Microsoft Teams の提供について、Microsoft Teams の最適化を通じて共同でサポートしています。この共同サポートは両社の緊密な協力関係により実現したものです。サポート契約の有効期間にこのソリューションで問題が発生した場合は、原因と考えられるコードの担当ベンダーのサポートチケットを開いてください。つまり Teams の場合は Microsoft の、最適化コンポーネントの場合はシトリックスのサポートチケットを開きます。

シトリックスまたは Microsoft はチケットを受け取ると問題の優先度を判断し、必要に応じてエスカレーションします。管理者が各社のサポートチームに連絡する必要はありません。

問題がある場合は、Teams UI の［**Help**］**>**［**Report a Problem**］にアクセスすることをお勧めします。VDA 側のログは Citrix と Microsoft の間で自動的に共有されるため、技術的な問題をより迅速に解決できます。

ログの収集

HDXTeams.exe ログは、ユーザーのマシンの%TEMP% にある **HDXTeams** フォルダー（AppData/Local/Temp）内にあります。「webrpc_Day_Month_timestamp_Year.txt」という名称の.txt ファイルを探します。

通話を確立する場合、次の 4 つの ICE フェーズが必要です：

- 候補の収集
- 候補の交換
- 接続性チェック（STUN バインド要求）
- 候補のプロモーション

HdxTeams.exe ログでは、以下のエントリが関連の対話型接続確立（ICE）エントリです。通知のセットアップを成功させるには、次のエントリが必要です（収集段階に関するこのサンプルスニペットを参照）：

```
RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering
```



```
15
16 [ … ]
17 >>> begin:sdp
18 candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
      generation 0 ufrag oVk6 network-id 1
19 <<< end:sdp
20 [ … ]
21 >>> begin:sdp
22 candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
      raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
      network-cost 10
23 <<< end:sdp
24 [ … ]
25 >>> begin:sdp
26 candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
      raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
      1
27 <<< end:sdp
28 [ … ]
29
30 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
      Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
31 >>> begin:sdp
32 [ … ]
33
34 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
      HaveRemotelOffer
35
36 <!--NeedCopy-->
```

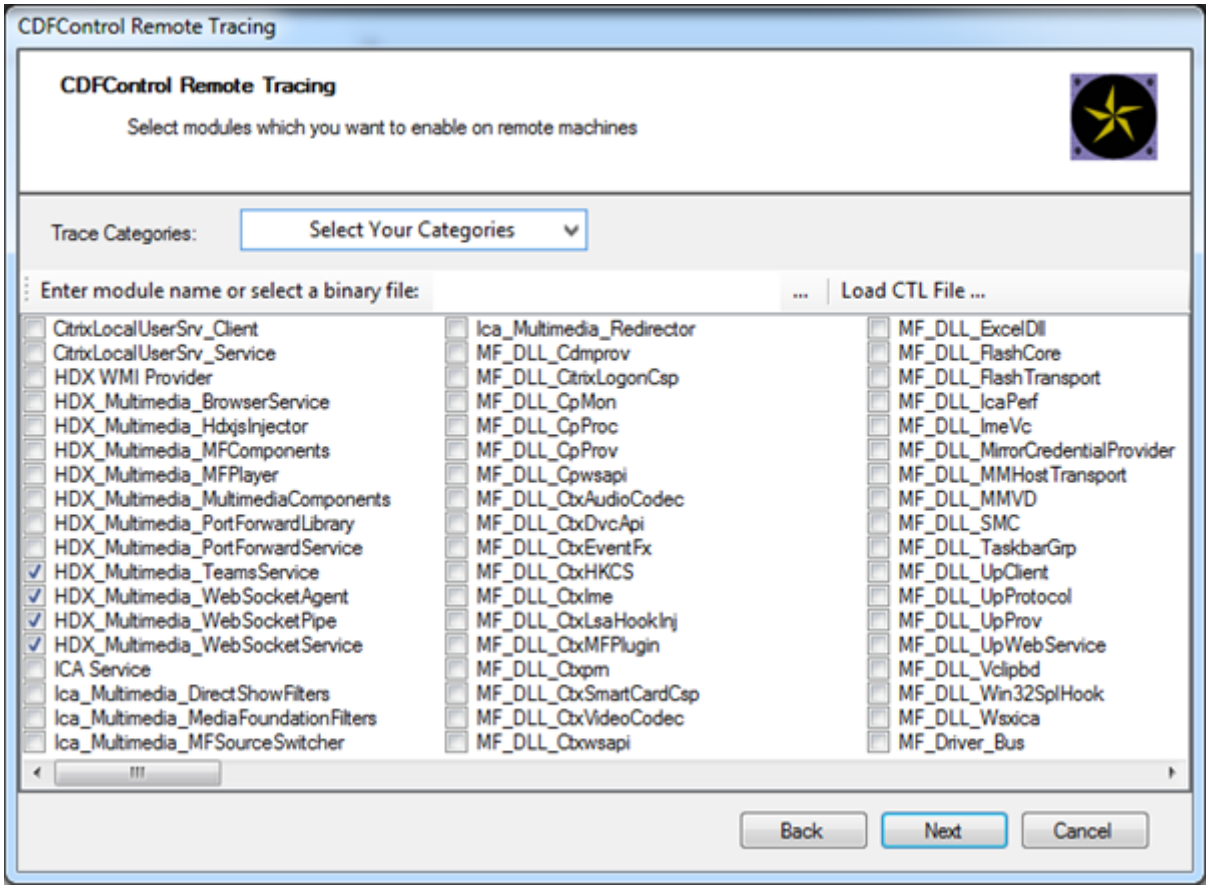
複数の ICE 候補がある場合、優先順位は次のとおりです:

1. host
2. peer reflexive
3. server reflexive
4. transport relay

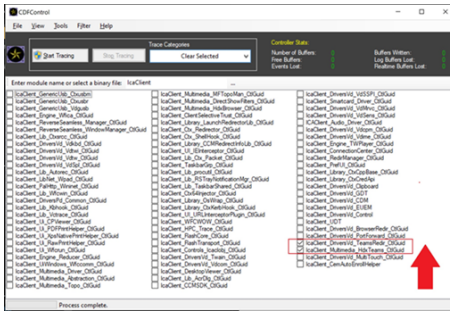
問題が発生し、一貫して再現できる場合は、Teams で［**Help**］**>**［**Report a problem**］にアクセスすることをお勧めします。Microsoft でケースを開いた場合の技術的な問題を解決するために、Citrix と Microsoft の間でログが共有されます。
シトリックスサポートに連絡する前に CDF トレースをキャプチャすることもお勧めします。詳しくは、Knowledge Center のCDFcontrolを参照してください。

CDF トレースを収集する際の推奨事項については、Knowledge Center の記事（Recommendations for Collecting the CDF Traces）を参照してください。

VDA 側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



Workspace アプリ側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



Windows Media リダイレクト

April 26, 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。Citrix Scout 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。詳しくは、「Citrix Scout」を参照してください。

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。

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、画面表示が黒くなることがあります。この黒い画面は、ビデオコンテンツを右クリックし、［プレイビューを常に手前に表示］を選択すると表示されることがあります。

一般コンテンツリダイレクト

April 26, 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。

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、マルチセッション OS VDA でのみサポートされ、シングルセッション OS 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。コンピューター間で切り替えるはありません。

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。

クライアントフォルダーのリダイレクト

April 24, 2021

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。つまり、ユーザーデバイス上のファイルシステム全体が表示されるわけではありません。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 シングルセッション 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 Workspace アプリに含まれています。

要件:

サーバーの場合:

- Windows Server 2019、Standard、および Datacenter 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。

クライアントの場合:

- Windows 10 32 ビット版および 64 ビット版（バージョン 1607 以降）
- Windows 8.1 32 ビット版および 64 ビット版（Embedded エディションを含む）
- Windows 7 32 ビット版および 64 ビット版（Embedded エディションを含む）

> 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. 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 Workspace アプリがインストールされていることを確認します。
    b) Citrix Workspace アプリ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

April 26, 2021

コンテンツのリダイレクトを使用すると、ユーザーが情報にアクセスする方法を制御できます。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。マルチセッション OS VDA でのみサポートされています（シングルセッション OS 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:

パフォーマンスのためにホストからクライアントへのリダイレクトを使用できます。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ると、VDA 上のアプリケーションではなくそのアプリケーションが使用されます。

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（Real Media など）を使用する場合
- 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	コンテンツリダイレクトの機能
タブレット	-	次表のすべての機能
ラップトップ PC	-	次表のすべての機能
デスクトップ PC	ユーザーがユーザーデバイスにインストール済みの多様なアプリケーションを使用する場合	次表のすべての機能
デスクトップ PC	ユーザーが使用するのが、ユーザーデバイスにインストール済みである少数かつ既知のアプリケーションに限られている場合	ローカルアプリアクセス
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
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と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をサポートしている場合	マルチメディアリダイレクト

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	コンテンツリダイレクトの機能
Web ページまたはドキュメント	VDA が URL にアクセスできない場合	ホストからクライアントへのリダイレクト
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

URL リンク	状況または環境	コンテンツリダイレクトの機能
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、以下の Citrix Workspace アプリでサポートされます:

- Windows 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- HTML5 向け Citrix Workspace アプリ
- Chrome 向け Citrix Workspace アプリ

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以下のいずれかである場合、適切なアプリケーションと電源があることを確認します。

- シンクライアント
- ゼロクライアント

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

ホストからクライアントへのリダイレクト機能は、Web ブラウザーの URL には使用されません。つまり、Web ページにあるか、Web ブラウザーのアドレスバーに入力します。

> 注
>
> ユーザーが 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。デフォルトの Web ブラウザーを変更する例では、［デフォルトのプログラムを設定する］を使用しています。

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構成を使用します。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、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
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

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ことで、URL の種類を削除および追加できます。URL タイプにはカスタムタイプが含まれます。

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. 例中の「**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]

    @=""C:\Program Files (x86)\Citrix\HDX\bin\iexplore.exe" %1"
    [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

    @="ServerFTA"
    [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

    "ApplicationDescription"="Server FTA URL."

    "ApplicationIcon"="C:\Program Files (x86)\Citrix\HDX\bin\iexplore.
       exe,0"

    "ApplicationName"="ServerFTA"
    [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\
       URLAssociations]

    "http"="ServerFTAHTML"

    "https"="ServerFTAHTML"
    [HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

    "Citrix.ServerFTA"="SOFTWARE\Citrix\ServerFTA\Capabilities"

    -- Reg file end --
<!--NeedCopy-->
```

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。

```
-- xml file start --

<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>

-- xml file end --
```

現在のグループポリシー管理コンソールで、［コンピューターの構成］>［管理用テンプレート］>［**Windows** コンポーネント］>［エクスプローラー］>［既定の関連付け構成ファイルの設定］の順に開いて、作成した ServerFTAdefaultPolicy.xml ファイルを指定します。

ホストからクライアントへのリダイレクト機能の **URL** タイプリストの変更

ホストからクライアントへのリダイレクト機能の URL タイプのリストを変更するには、サーバー VDA で次のレジストリキーを設定します。

キー: HKLM\Software\Wow6432Node\Citrix\SFTA

リストから URL タイプを削除するには、DisableServerFTA と NoRedirectClasses を設定します。

値の名前：DisableServerFTA

種類：REG_DWORD

データ：1

値の名前：NoRedirectClasses

種類：REG_MULTI_SZ

データ：値の組み合わせを指定します：`http`, `https`, `rtsp`, `rtspu`, `pnm`, `or mms`。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。このワイルドカード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

April 26, 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。
- アプリケーションが仮想デスクトップから個別にホストされている場合、ダブルホップによる遅延を排除します。このために、ユーザーの Windows デバイス上で公開アプリケーションのショートカットを作成します。
- 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。
  - 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。たとえば、DVD バーナーや TV チューナーなどです。

Citrix Virtual Apps and Desktops では、URL のリダイレクトにより、ホストされたデスクトップセッションからローカルアプリケーションアクセスアプリケーションを起動できます。URL リダイレクトでは、複数の URL アドレスでアプリケーションを起動できます。デスクトップセッションで、Web ブラウザー内に埋め込まれたリンクをクリックすると、Web ブラウザーの URL ブラックリストに基づいてローカルの Web ブラウザーが起動します。ブラックリストにない URL をクリックすると、デスクトップセッション内の Web ブラウザーが再度使用されます。

URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できるリダイレクト機能は、サーバー FTA（File Type Association：ファイルタイプの割り当て）リダイレクトの 1 つである「ホストからクライアントへのコンテンツのリダイレクト」のみです。この FTA では、http、http、rtsp、mms など、特定のプロトコルがクライアント側に転送されます。たとえば、http の埋め込みリンクを開くときに、クライアント側のアプリケーションが使用されます。特定の URL のリダイレクトを有効にしたり無効にしたりすることはできません。

ローカルアプリケーションアクセスを有効にすると、ローカルで実行されるアプリケーション、ホストされるアプリケーション、またはデスクトップ上のショートカットからアクセスされた URL を、以下のいずれかの方法でリダイレクトできます。

- ユーザーのコンピューターから、ホストされているデスクトップへ
- Citrix Virtual Apps and Desktops サーバーからユーザーのコンピューターへ
- 起動された環境内で処理（リダイレクトなし）

特定の Web サイトでのリダイレクト方法を指定するには、Virtual Delivery Agent 上の URL ホワイトリストおよび URL ブラックリストを構成します。これらのリストでは、URL リダイレクトのポリシー設定を指定する複数行文字列値を設定します。詳しくは「ローカルアプリケーションアクセスのポリシー設定」を参照してください。

すべての URL を VDA 側の Web ブラウザ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 が表示されるはずですが、代わりに、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。この機能は、Silverlight などの他のメディアの種類のサイトをリダイレクトします。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。FTA により、セッションで特定のファイルを開くときにローカルのアプリケーションが使用されます。ローカルアプリケーションでファイルを開くには、そのローカルアプリケーションがそのファイルにアクセスできる必要があります。つまり、ローカルアプリケーションで開くことができるのは、ネットワーク共有上またはクライアントドライブ上にあるファイル（クライアント側ドライブのマッピング機能）のみです。たとえば、PDF ファイルを開く場合、ローカルにインストールされている PDF リーダーでファイルが表示されます。ローカルアプリケーションはファイルに直接アクセスできるため、ファイルを開くときに ICA によるネットワーク転送は発生しません。

要件、考慮事項、および制限事項

ローカルアプリアクセスは、Windows マルチセッション OS 対応 VDA および Windows シングルセッション OS 対応 VDA 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ています。ローカルアプリケーションアクセスには、バージョン 4.1 以降の Windows 向け Citrix Workspace アプリが必要です。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。
  - ローカルアプリケーションアクセスをウィンドウ表示モードの仮想デスクトップで使用するなど、単一の仮想デスクトップをすべてのモニター上で表示しない場合、ユーザーエクスペリエンスに混乱が生じます。
  - マルチモニター環境で、アプリケーションの表示を 1 つのモニターで最大化すると、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。このデフォルトの状態は、以降のアプリケーションが通常は他のモニターに表示される場合でも発生します。
  - 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。
  - ドライブ文字により、ユーザーが仮想デスクトップの C ドライブとローカルの C ドライブを混同する場合があります。
  - 仮想デスクトップで使用できるプリンターは、ローカルアプリケーションでは使用できません。
  - 管理者特権が必要なアプリケーションは、ローカルアプリケーションアクセスでは起動できません。

  - 単一インスタンスアプリケーション（Windows Media Player など）もほかのアプリケーションと同等に処理されます。
  - ローカルアプリケーションはローカルマシンの Windows テーマで表示されます。
  - 全画面アプリケーションはサポートされません。これらのアプリケーションには、PowerPoint のスライドショーやデスクトップ全体で表示されるフォトビューアーなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリケーションアクセスでは、VDA 上の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］メニューのショートカットなど）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他のプロパティはコピーされません。
  - 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。つまり、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。
  - 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きます。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。また URL リダイレクトのため、URL ホワイトリストとブラックリストポリシー設定を構成できます。詳しくは、「ローカルアプリケーションアクセスのポリシー設定」を参照してください。

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 リダイレクトのホワイトリスト］は、リモートセッションのデフォルトのブラウザーで開く 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 リダイレクトのブラックリスト］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。

   a. 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。

   b. 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。

   c. ［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。

   d. ［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）。

   e. ［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。

   f. ［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。

   g. ［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>*

<browser> には、IE、FF、Chrome、または All を指定します。

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。ブラックリストに追加されていてもリダイレクトされません。

URL リダイレクトが正しく機能するためには、Web ブラウザーに表示されるメッセージに従ってアドオンを有効にする必要があります。インターネットオプションを使用するアドオンやメッセージで示されたアドオンが無効の場合、URL リダイレクトは正しく機能しません。

- Firefox アドオンでは、URL が常にリダイレクトされます。

Firefox では、アドオンのインストールを許可するかどうかを確認するメッセージが新しいタブに表示されます。URL リダイレクトが正しく機能するためには、アドオンのインストールを許可します。

- 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。

汎用 **USB** リダイレクトとクライアント側ドライブの考慮事項

April 26, 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。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は、Android 向け Citrix Workspace アプリで使用できるドライバーがないことがあります。
- 使用しているバージョンの Citrix Workspace アプリで、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利用できないとき。

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。

> 重要:
>
> - 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、シトリックスの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、シトリックス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には該当しません。
> - Citrix ソフトウェアを使用して Azure 仮想マシンにセッションを仲介する場合、Citrix は Azure 仮想マシンへの USB リダイレクトに関するベストエフォートサポートを提供します。Citrix ソフトウェアの問題の修正をサポートしていますが、基盤となる Azure 仮想マシンはサポートしていません。

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 デバイスで汎用 USB リダイレクトを使用する場合、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）。帯域幅を増やすことができない場合には、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用状況を調整することで、問題を緩和できます。詳しくは、クライアント USB デバイスのリダイレクトの「帯域幅のポリシー設定」、および「マルチストリーム接続のポリシー設定」を参照してください。

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 デバイスのリスクは、Citrix Workspace アプリと Citrix Virtual Apps and Desktops の構成により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。こうした状況は、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発生します。

> 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。
>
> USB デバイスの安全な使用についての以下のようなガイダンスをユーザーに提供してください。
>
> - 信頼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 ドライブを置きっぱなしにしない）。

> • 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。

汎用 USB リダイレクトは、次の Citrix Workspace アプリでサポートされます:

- Windows 向け Citrix Workspace アプリについては、アプリケーション配信の構成を参照してください。
- Mac 向け Citrix Workspace アプリについては、Mac 向け Citrix Workspace アプリを参照してください。
- Linux 向け Citrix Workspace アプリについては、最適化を参照してください。
- Chrome 向け Citrix Workspace アプリについては、Chrome 向け Citrix Workspace アプリを参照してください。

Citrix Workspace アプリの各バージョンについては、『Citrix Workspace アプリの機能マトリックス』を参照してください。

過去のバージョンの Citrix Workspace アプリを使用している場合は、Citrix Workspace アプリ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。サポート対象の USB デバイスのタイプに関する制限事項については、Citrix Workspace アプリのドキュメントを参照してください。

汎用 USB リダイレクトはシングルセッション OS 対応 VDA 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 リダイレクトはマルチセッション OS 対応 VDA のバージョン 7.6 以上のデスクトップセッションでサポートされますが、以下の制限事項があります。

- VDA は Windows Server 2012 R2 または Windows Server 2016 で動作している必要があります。
- シングルホップのシナリオだけがサポートされます。デスクトップでホストされるアプリケーションセッションでは、ダブルホップ汎用 USB リダイレクトはサポートされません。
- USB デバイスドライバーには、完全仮想化サポートなど、VDA OS（Windows 2012 R2）のリモートデスクトップセッションホスト（RDSH）との完全な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、Citrix Ready Marketplace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し、個別に構成できます。

- 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「クライアント側の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 Workspace アプリで、Citrix Workspace アプリに依存するメカニズムを使用して設定します。たとえば、管理用テンプレートは、Windows 向け Citrix Workspace アプリを構成するレジストリ設定を制御できます。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、Windows 向け Citrix Workspace アプリのドキュメントの「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:

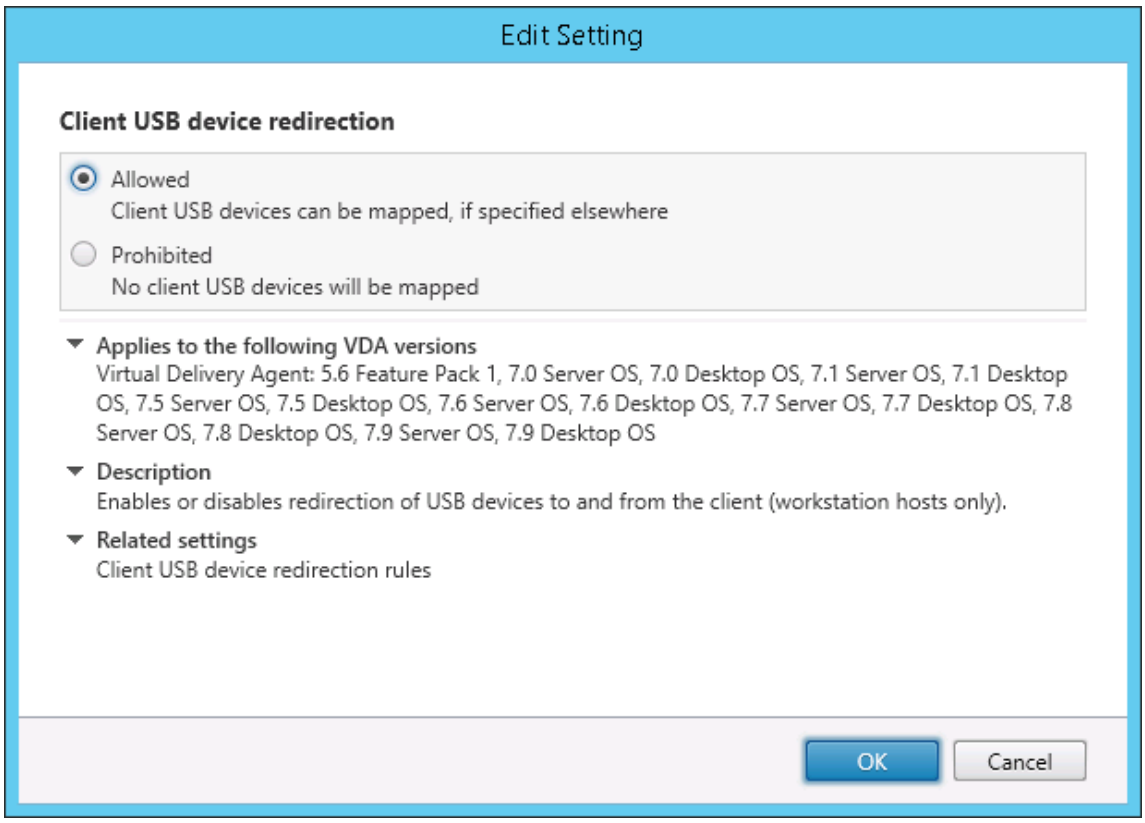
- 2 つの異なる組織または部門が Citrix Workspace アプリと VDA を担当している場合に、それぞれが別に制御を実行できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスするときにも適用されます。
- Citrix ポリシー設定では、特定のユーザー、または（Citrix Gateway 経由ではなく）LAN 経由で接続しているユーザーのみに許可された USB デバイスを制御できます。

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化して、ユーザーの手動リダイレクトを不要にするには、Citrix ポリシー設定と Citrix Workspace アプリの接続設定の両方を構成します。

Citrix ポリシー設定で、次の手順に従います:

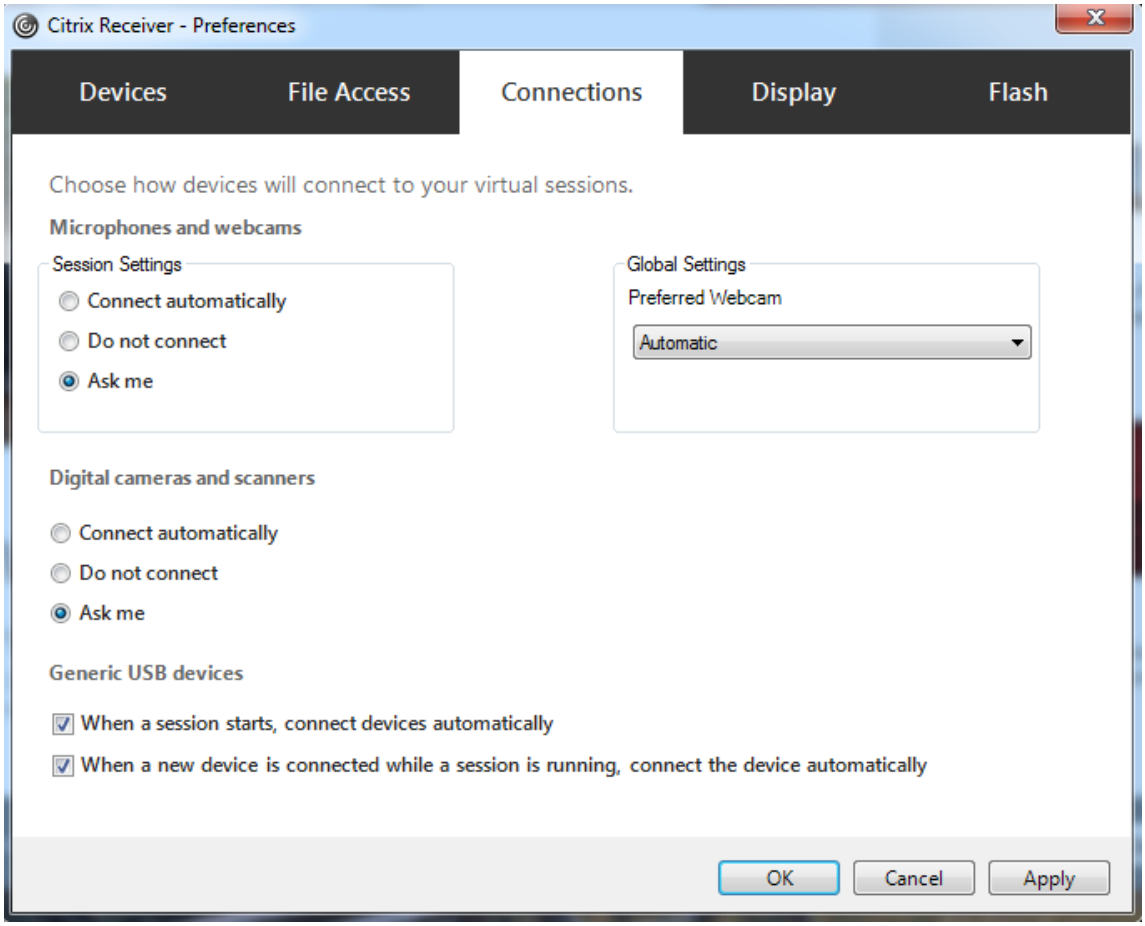
1. ポリシーに［クライアント USB デバイスリダイレクト］を追加して、値を ［許可］に設定します。



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 Workspace アプリで、次の手順を実行します:

3. デバイスが手動リダイレクトなしで自動的に接続されるように設定します。この設定は、管理用テンプレートを使うか、Windows 向け Citrix Workspace アプリの［基本設定］>［接続］で実行できます。



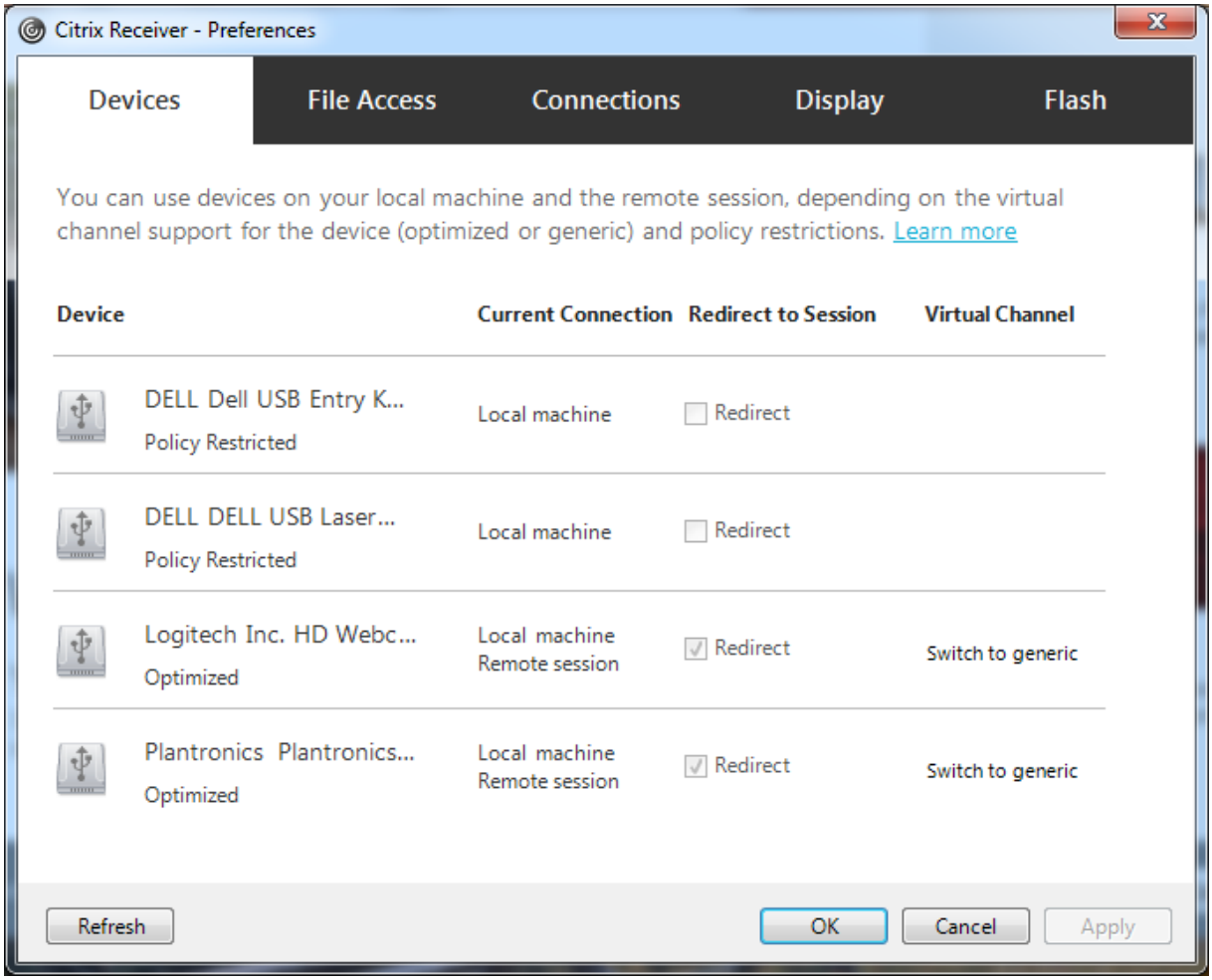
前の手順で VDA の USB ポリシー規則を指定した場合は、Citrix Workspace アプリにも同じポリシー規則を指定します。

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。接続バーが表示されていない場合も、USB デバイスは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。詳しくは、Windows 向け Citrix Workspace アプリのユーザーヘルプの「Desktop Viewer でのデバイスの表示」を参照してください。



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 Workspace アプリで、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］タブで ［汎用に切り替え］をオンにします。
- 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、「USB デバイスの自動リダイレクトを構成する」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。

Citrix Workspace アプリおよび VDA のデバイス規則を定義して、USB デバイスを一覧に表示しないようにしたり、リダイレクトできないようにしたりできます。

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 を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 Workspace アプリ両方の 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可能な 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、マルチセッション 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

Windows 向け Citrix Workspace アプリの場合:

- 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

タグ	説明
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http://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

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
```

- 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
```


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。

Windows 向け Citrix Workspace アプリでは、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］メニューに直ちに追加されます。
- 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。このサポートは、Citrix Virtual Apps and Desktops のクライアント側ドライブのマッピング機能に含まれています。ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップのドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。クライアント側ドライブのマッピングを構成するには、［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。この設定は、ICA ポリシー設定の「ファイルリダイレクトのポリシー設定」セクションにあります。

USB マスストレージデバイスでは、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。これらは Citrix ポリシーを使って制御されます。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	はい
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーがオペレーティングシステムで推奨される手順に従う場合）

汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効な場合、セッション開始前または後に装着されたマスストレージデバイスがクライアント側ドライブのマッピングによりリダイレクトされます。汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効で、自動リダイレクトが構成されている場合、セッション開始前または後に装着されたマスストレージデバイスが汎用 USB リダイレクトによりリダイレクトされます。詳しくは、Knowledge Center の記事CTX123015を参照してください。

> 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。ただし、大きなファイルはコピーできません。

クライアント側ドライブのマッピングを使うファイルアクセスの制御

管理者は、ユーザーが仮想環境のファイルをユーザーデバイス上にコピーすることを許可したり禁止したりできます。デフォルトでは、マップされたクライアント側ドライブ上のフォルダーやファイルに対するセッション内での読み取りや書き込みが許可されます。

マップされたクライアント側デバイス上でのフォルダーおよびファイルの追加や変更を禁止するには、［クライアント側ドライブへの読み取り専用アクセス］設定を有効にします。この設定項目をポリシーに追加するときは、［クライアントドライブのリダイレクト］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

April 26, 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、マルチセッション 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。

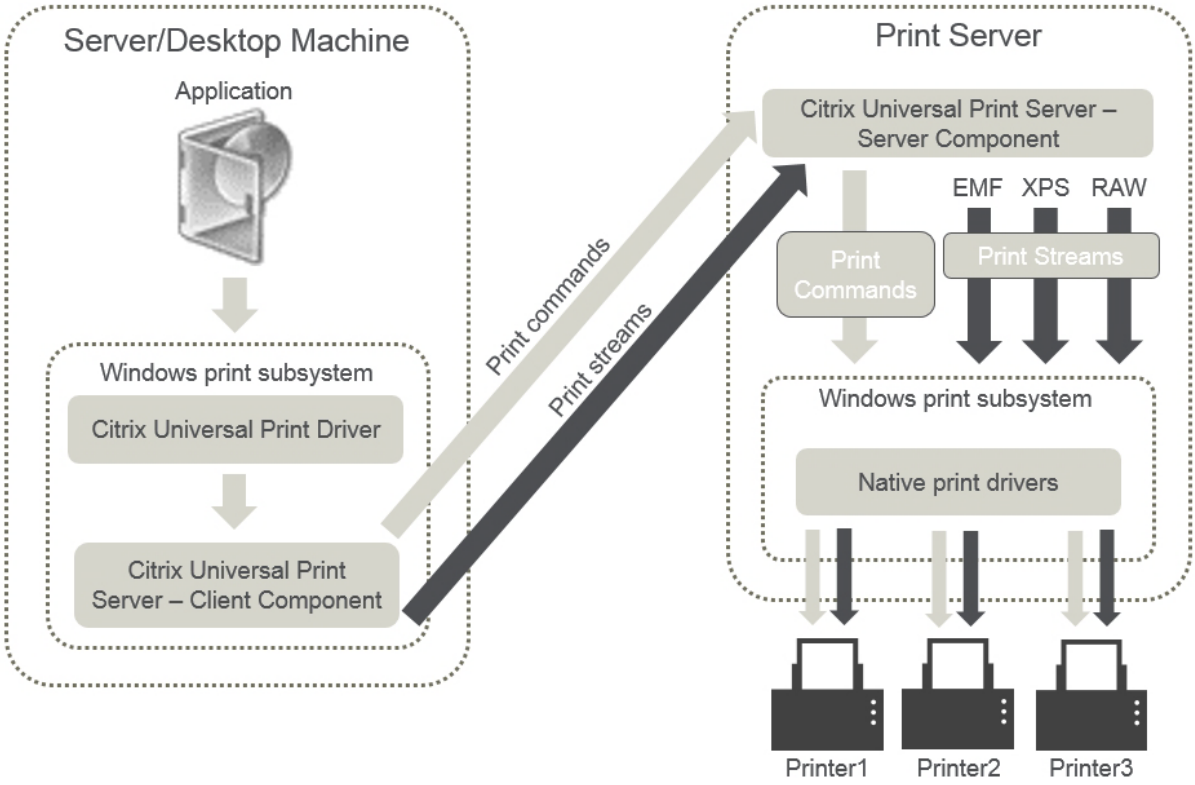
クライアントコンポーネント、ユニバーサルプリントクライアント - 各マルチセッション OS マシンでユニバーサルプリントクライアントを有効にして、セッションネットワークプリンターをプロビジョニングし、ユニバーサルプリ

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、マルチセッション 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］設定ですべてのマルチセッション OS マシンにドライバーを追加します。

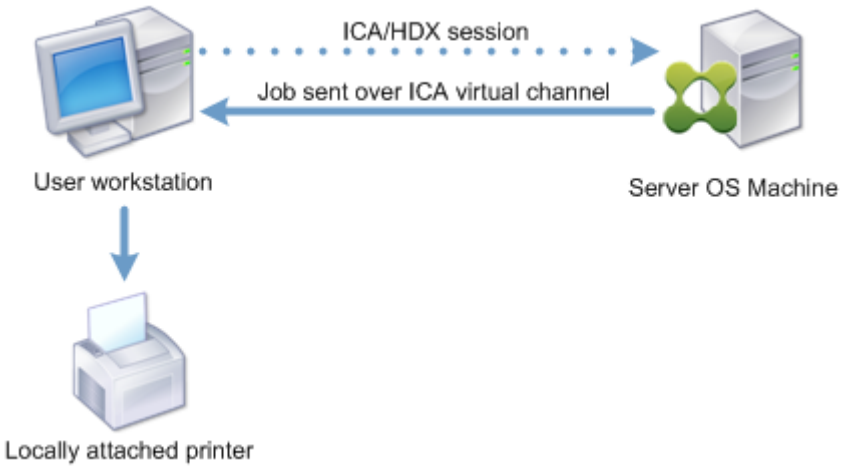
印刷ジョブの送信

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、マルチセッション 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。



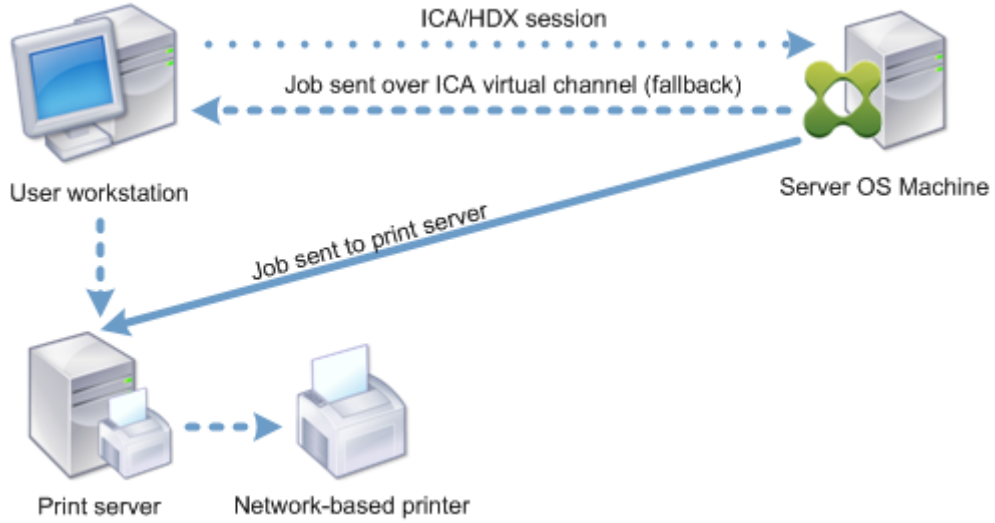
ネットワークベースのプリンター

デフォルトでは、マルチセッション 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マルチセッション 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、Citrix Virtual Apps and Desktops 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

VDA インストーラーでは、ユニバーサルプリントサーバー PDF プリンタードライバーのインストールを制御するオプションは提供されなくなりました。PDF プリンタードライバーは、必ず自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされているバージョン）にアップグレードすると、以前にインストールされた Citrix PDF プリンタードライバーが自動的に削除されて最新バージョンに置き換えられます。

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 Workspace アプリ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、Citrix Virtual Apps and Desktops 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 は次の印刷形式をサポートします。

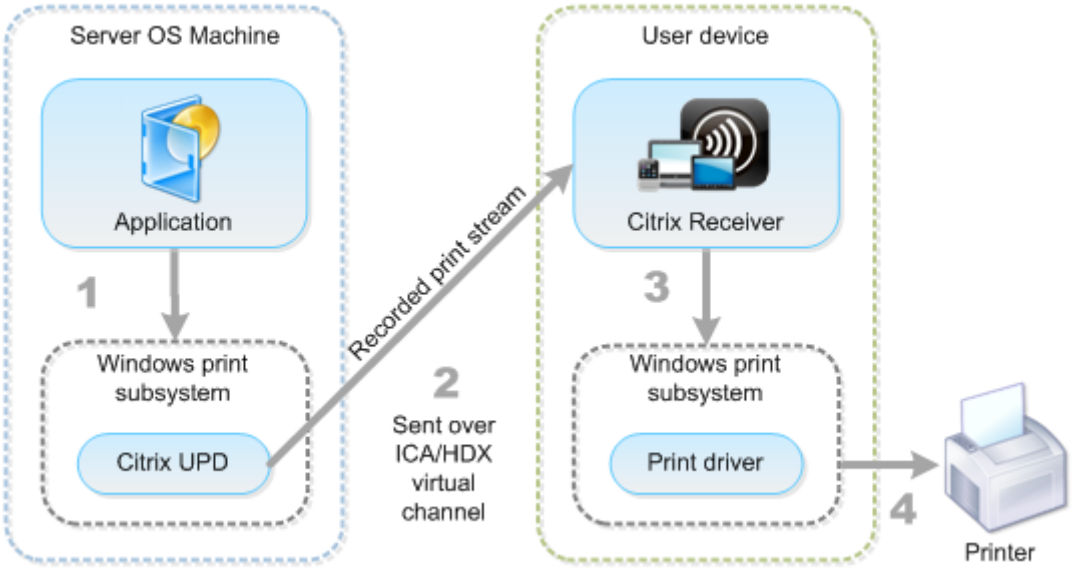
- 拡張メタファイル形式（**EMF**）、デフォルト。EMF は 32 ビットバージョンの Windows Metafile（WMF）形式です。EMF ドライバーは、Windows ベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPS ドライバーでは XML が使用され、Adobe PDF に似た、プラットフォームに依存しない「電子ペーパー」が作成されます。
- プリンターコマンド言語（**PCL5c** および **PCL4**）。PCL は、もともとインクジェットプリンターのために Hewlett-Packard によって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。

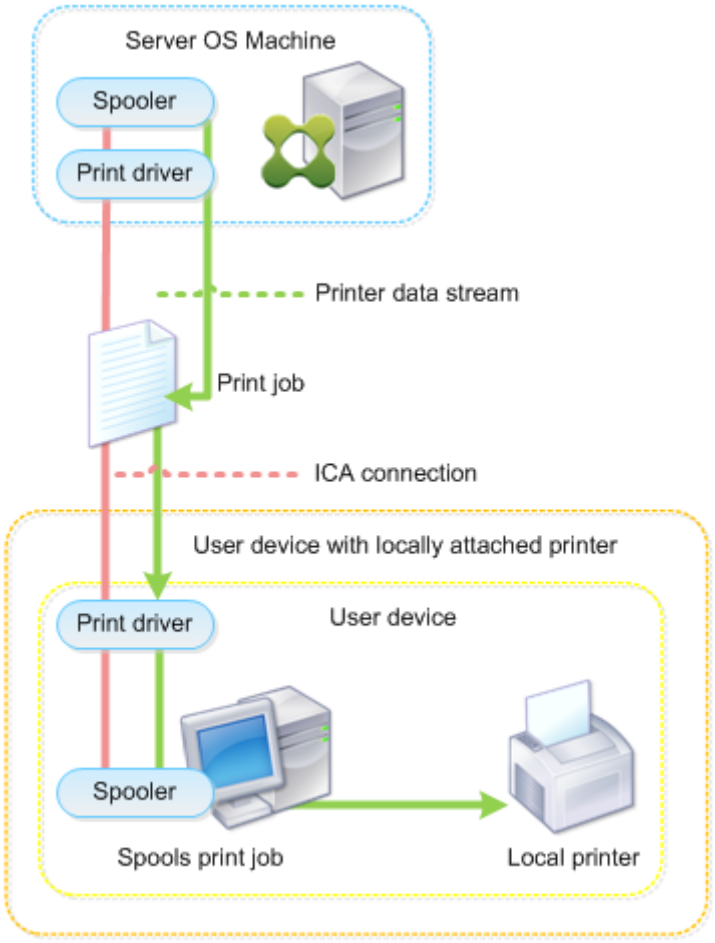
次の図は、ユニバーサルプリンタードライバーコンポーネントとデバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



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マルチセッション 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、マルチセッション 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。
- マルチセッション 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

April 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。

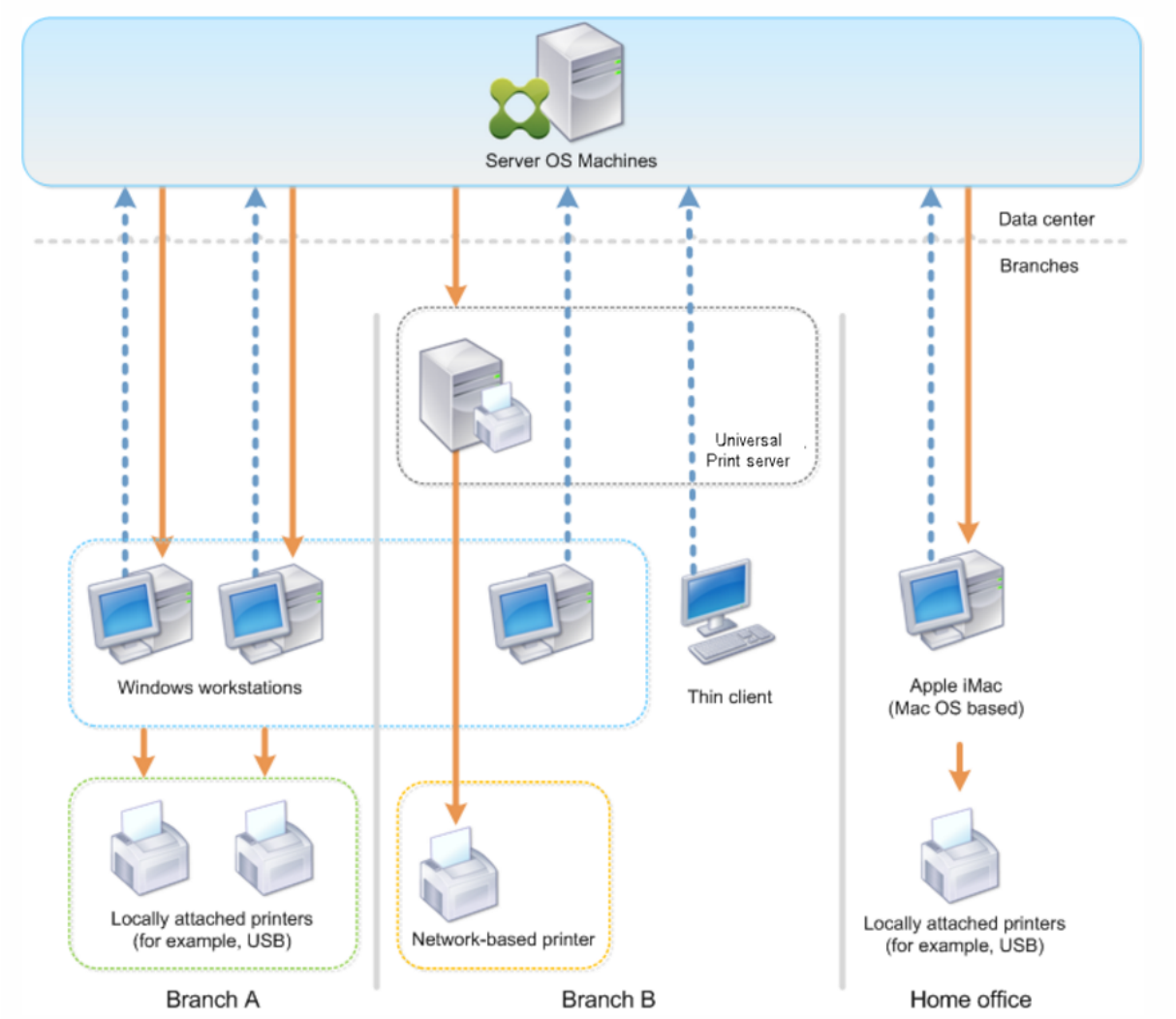
- 組織のセキュリティポリシー。人事部用のプリンターなど、特定のユーザー用に予約されたプリンターがあるかどうかを確認します。
- メインのワークステーションとは離れた場所で印刷するユーザーがいるかどうか。たとえば、複数のワークステーション間を移動しながら作業したり、出張先で印刷したりするユーザーがいるかどうかを確認します。

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支社。すべてのユーザーワークステーションは共有されていないプリンターにローカルで接続されています。
- 支社 **B** - シンクライアントおよび Windows ベースのワークステーションが複数台ある大規模な支社。効率を上げるため、この支店のユーザーはネットワーク上のプリンターを（各階で 1 台）共有しています。支店内に置かれている Windows ベースのプリントサーバーが印刷キューを管理します。
- 社員の自宅 - Mac OS ベースのユーザーデバイスで自宅から会社の Citrix インフラストラクチャにアクセスしています。ユーザーデバイスはプリンターにローカルで接続されています。



以降のセクションでは、各印刷環境をシンプルにして簡単に管理するための構成について説明します。

自動作成されるクライアントプリンターと **Citrix** ユニバーサルプリンタードライバー

支社 A のすべてのユーザーは Windows ベースのワークステーションを使用しており、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。この構成には以下のメリットがあります。

- パフォーマンス - 印刷ジョブは ICA 印刷チャネル上で配信されます。このため、印刷データの圧縮により帯域幅を節約できます。

  サイズの大きなドキュメントを印刷しているユーザーがほかのユーザーのセッションパフォーマンスを低下させることがないように、最大印刷帯域幅を指定する Citrix ポリシーを構成します。

  代替策として、マルチストリーム ICA 接続を使用して、印刷トラフィックが優先度の低い専用の TCP 接続で転送されるように構成することもできます。マルチストリーム ICA は、WAN 接続にサービス品質（QoS）が実装されていない場合のオプションです。

- 柔軟性 - Citrix ユニバーサルプリンタードライバーを使用しているため、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

支社 B のすべてのプリンターはネットワークに接続されており、その印刷キューは Windows プリントサーバー上で管理されます。このため、Citrix 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。

- マルチセッション 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。マルチセッション 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。
- 支社 B の各階に個別の［セッションプリンター］設定が構成されており、その階のすべてのシンクライアントに適用されます。
- 支社 B には QoS が実装され、優れたユーザーエクスペリエンスが提供されています。

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

April 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。
- マルチセッション 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、マルチセッション 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、マルチセッション 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。

- VDA バージョン 7.16 以降では、V3 インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrix ポリシー設定「受信トレイプリンタードライバーの自動インストール」は Windows 8 以降の Windows オペレーティングシステムのバージョンには影響しません。

- 7.16 より前の VDA では、セッション内でプリンターが自動作成されるときに、そのマルチセッション 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

April 26, 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、シトリックスの「印刷のポリシー設定」にある以下の設定で制御できます。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 Workspace アプリのデフォルトでは、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）またはマルチセッション 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、つまりマルチセッション 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。
- マルチセッション **OS** マシン上 - マルチセッション 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、マルチセッション 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、自動的にマルチセッション 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

April 26, 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。このドライバーはマ

ルチセッション 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 シングルセッション OS または Windows マルチセッション OS 用の Citrix Virtual Apps and Desktops 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。

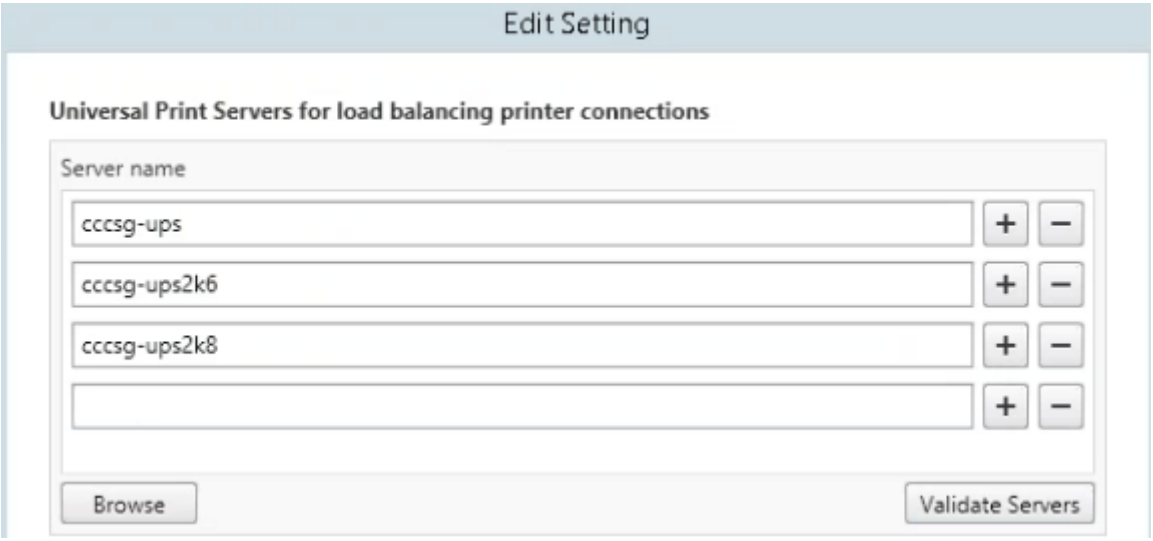
- ユニバーサルプリントサーバーの有効化。ユニバーサルプリントサーバーはデフォルトでは無効になっています。ユニバーサルプリントサーバーを有効にする場合、ユニバーサルプリントサーバーを使用できないときに Windows 印刷プロバイダーにフォールバックするかどうかを選択できます。ユニバーサルプリントサーバーを有効にすると、Windows 印刷プロバイダーと Citrix プロバイダーのインターフェイスを介してネットワークプリンターを追加して列挙できます。
- ユニバーサルプリントサーバー印刷データストリーム（**CGP**）ポート。ユニバーサルプリントサーバー印刷データストリーム CGP（Common 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。

Citrix Virtual Apps and Desktops VDA へのユニバーサルプリントサーバーの通信用ポートをデフォルトの HTTP 8080 から変更するには、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。

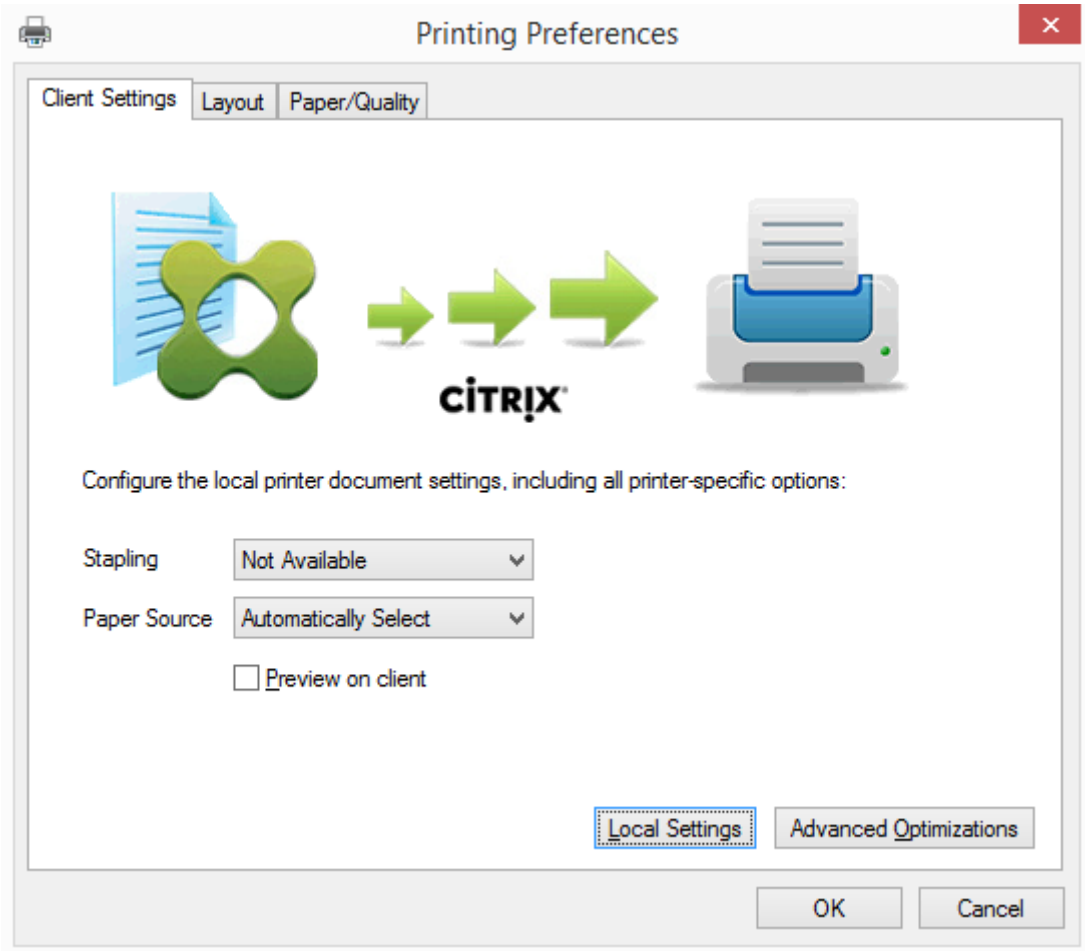
ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターを自動作成する	ユニバーサルプリントサーバーが有効な場合、ネイティブドライバーの代わりにユニバーサルプリンタードライバーを使ってクライアントネットワークプリンターが作成されます。ユーザー側には、同じプリンター名が表示されます。
セッションプリンター	Citrix ユニバーサルプリントサーバーソリューションを使用する場合、ユニバーサルプリンタードライバー関連のポリシー設定によりセッションプリンターが構成されます。

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。
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 Workspace アプリ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。

  Windows 以外の Citrix Workspace アプリ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。

ポリシーの詳細については、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色設定、両面印刷、部数などのデフォルト設定を変更する方法については、CTX113148を参照してください。

ユーザーデバイスからのプリンターの自動作成 — デフォルトでは、セッションの開始時にユーザーデバイス上で設定されているすべてのプリンターが自動作成されます。管理者は、セッション内でユーザーに提供するプリンターの種類を制御して、自動作成を無効にできます。

自動作成機能を制御するには、Citrix ポリシーの［クライアントプリンターを自動作成する］設定を使用します。以下のオプションを選択できます。

- ローカル接続されているプリンターやネットワークプリンターを含め、ユーザーデバイス上で設定されているすべてのプリンターがセッション開始時に自動作成されるようにする（デフォルト）。
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動作成されるようにする。
- ユーザーデバイス上で設定されているデフォルトプリンターだけが自動作成されるようにする。
- 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

April 26, 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設定の詳細については、「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、マルチセッション 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 — マルチセッション 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、マルチセッション 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 — マルチセッション 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、各マルチセッション 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	位置情報
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］。
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（マルチセッション 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］

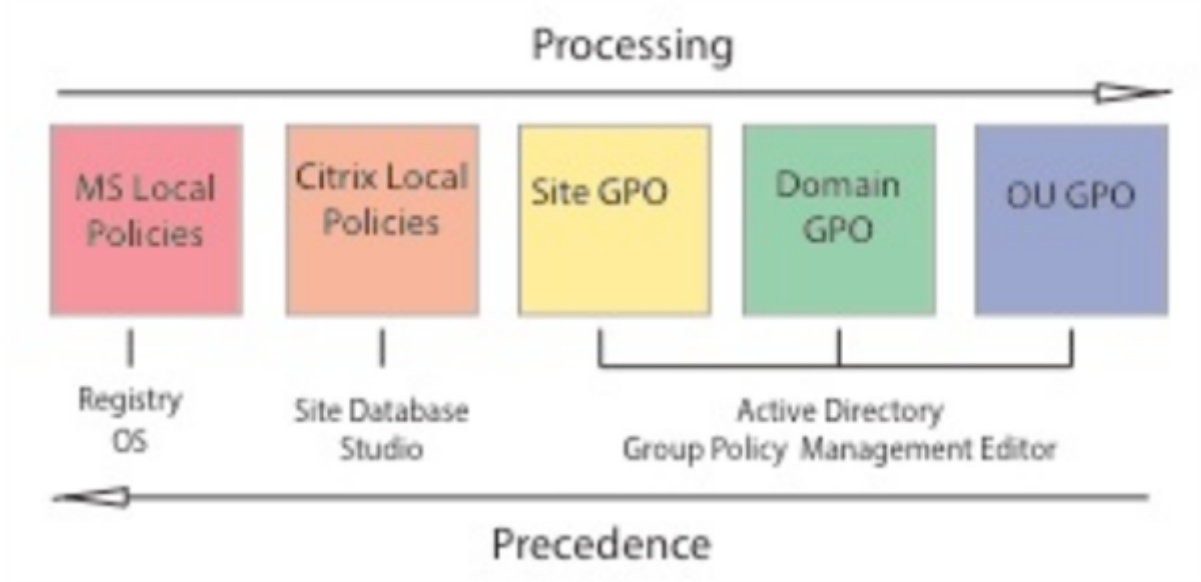
> 注:
>
> ネットワーク印刷経路で実行されたネットワークプリンターへの印刷キューは「プライベート」であり、システムで管理することはできません。

ポリシー

April 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 内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 Citrix Workspace アプリ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

April 26, 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、ポリシーの一部の設定項目を構成するには、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。

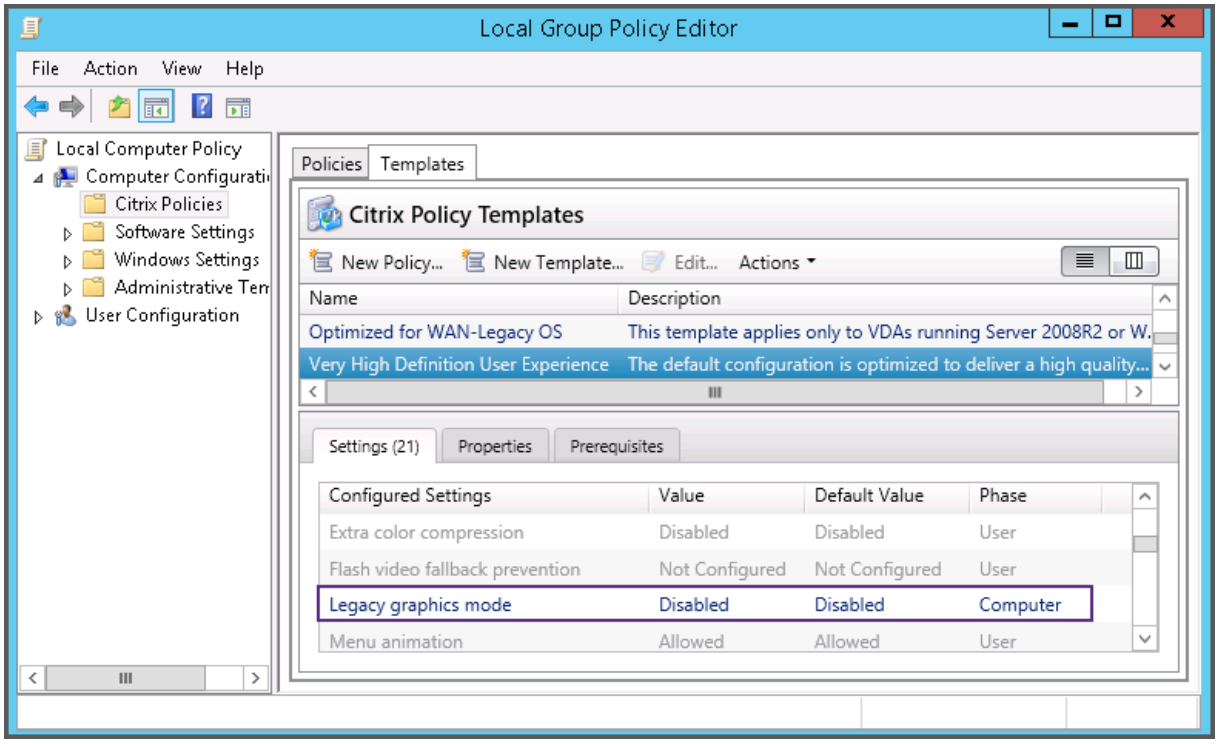
特定の製品バージョンや設定項目のカテゴリを選択することで、検索範囲を限定できます。すべての設定項目を検索対象にするには、［すべての設定］を選択します。

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

April 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。

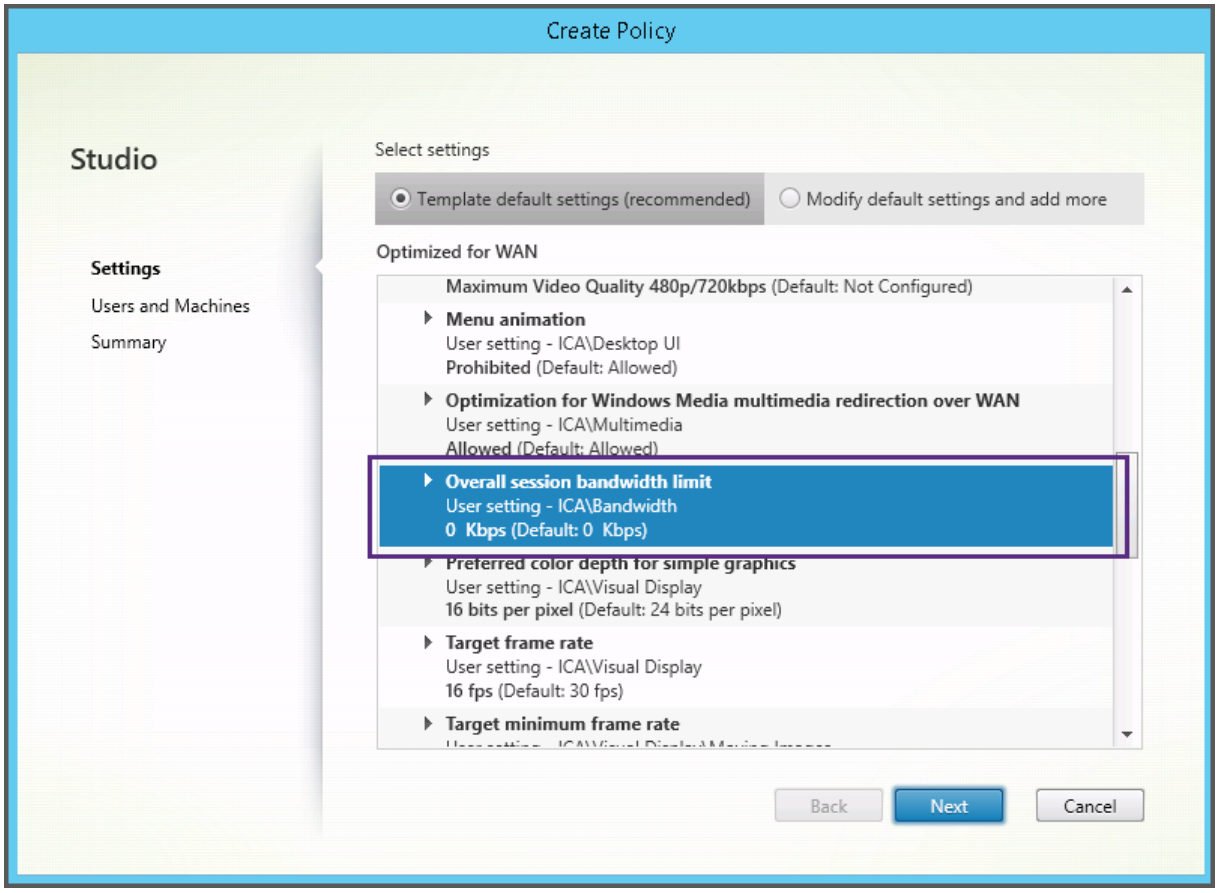
テンプレートを使用してポリシーを作成する際の考慮事項については、Knowledge Center のCTX202330を参照してください。

組み込みの **Citrix** テンプレート

使用できるポリシーテンプレートは以下のとおりです。

- 最高品位ユーザーエクスペリエンス。このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。
- 高サーバースケーラビリティ。サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増大させながら、良質のユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防ぎます。
- 高サーバースケーラビリティ **-** レガシ **OS**。この高サーバースケーラビリティテンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **NetScaler SD-WAN** に最適化。これは、NetScaler SD-WAN が展開された支店などのユーザーに適用して Citrix Virtual Desktops の配信を最適化するテンプレートです。(NetScaler SD-WAN は、CloudBridge の新しい名前です)。
- **WAN** の最適化。このテンプレートは、共有 WAN 接続を使用している支店や、低帯域幅接続を実行する遠隔地にいて、マルチメディアコンテンツがほとんどない視覚的に簡素なユーザーインターフェイスのアプリケーションにアクセスするタスクワーカーを対象としたものです。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。
- **WAN** の最適化 **-** レガシ **OS**。この *WAN* の最適化テンプレートは、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。Citrix Virtual Apps and Desktops 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、その設定には特定の推奨値はありません。たとえば、WAN の最適化テンプレートにはセッション全体の最大帯域幅があります。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:
>
> Citrix が組み込みテンプレートを開発およびアップデートします。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。属していない既存の設定を削除します。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。属していない既存の設定を削除します。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`.gpt`ファイルがエクスポートされます。

グループポリシーエディターでテンプレートを作成および管理する

グループポリシーエディターの［コンピューターの構成］または［ユーザーの構成］を開きます。［ポリシー］ノードを開き、［**Citrix** ポリシー］を選択します。適切な操作を行います。

タスク	手順
既存のポリシーから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。
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。

タスク	手順
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、Citrix Virtual Apps and Desktops 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

April 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、設定の構成を制限できます。これによって設定の構成が無効になり、ポリシーが適用されるとその前に入力された値が無視され、設定項目のデフォルト値しか使用できなくなります。

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。
NetScaler SD-WAN	ユーザーセッションで NetScaler SD-WAN が使用されているかどうか。注：ポリシーに追加できる NetScaler SD-WAN 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 の場合は 12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24 など。IPv6 の場合は、2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54 など。
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。ワイルドカード文字を使用する場合、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。注：プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.x でのみ使用できます。詳しくは、「CTX219153」を参照してください。
組織単位（OU）	組織単位。
タグ	マシンのタグ。注：このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれていません。

割り当て名	ポリシーの適用対象
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の［コンピューターの構成］または［ユーザーの構成］を開きます。［ポリシー］ノードを開き、［Citrix ポリシー］を選択します。以下の操作を行います。

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。

タスク	手順
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。ポリシーに複数のフィルターを追加する場合、適用するポリシーですべてのフィルター条件が満たされている必要があります。
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

April 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、シングルセッション OS VDA がマルチセッション OS VDA に接続すると、シングルセッション OS 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シングルセッション OS 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

April 26, 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

Name	デフォルト設定	VDA
アダプティブトランスポート	[オフ]、[可能であれば使用]	VDA 7.13～7.15、VDA 7.16 以降
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
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
デスクトップの起動	禁止	マルチセッション OS 対応 VDA 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	マルチセッション OS 対応 VDA 7 以降
損失耐性モード	許可	VDA 2003。注：損失耐性モードはまだ利用できません。利用可能になった際、VDA のこのバージョンでサポートされます。
損失耐性モードのしきい値	損失耐性モードが利用可能な場合：パケット損失：5%、遅延：300 ミリ秒（RTT）	VDA 2003 以降
ランデブープロトコル	有効	Citrix Cloud 経由で確立された HDX セッションにのみ適用されます。
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
タブレットモードの切り替え	有効	VDA 7.16 以降。VDA 7.14 および 7.15 LTSR では、この設定はレジストリで構成します。

ICA/Adobe Flash デリバリー/Flash リダイレクト

Name	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

Name	デフォルト設定	VDA
オーディオプラグアンドプレイ	許可	マルチセッション OS 対応 VDA 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

Name	デフォルト設定	VDA
UDP でのオーディオリアルタイムトランスポート	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	許可	すべてのバージョンの VDA
クライアントの自動再接続時の認証	認証を必要としない	すべてのバージョンの VDA
クライアントの自動再接続のログ	自動再接続イベントをログに記録しない	すべてのバージョンの VDA
クライアントの自動再接続のタイムアウト	120 秒	VDA 7.13 以降
再接続 UI の透過レベル	80%	VDA 7.13 以降

ICA/帯域幅

Name	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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 およびシングルセッション OS 対応 VDA 7 から最新のマルチセッション OS 対応 VDA およびシングルセッション OS 対応 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

Name	デフォルト設定	VDA
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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/コンテンツの双方向リダイレクト

Name	デフォルト設定	VDA
コンテンツの双方向リダイレクトを許可する	禁止	VDA 7.13 以降
クライアントへのリダイレクトを許可する URL	empty	VDA 7.13 以降
VDA へのリダイレクトを許可する URL	empty	VDA 7.13 以降
クライアントからホスト（VDA）およびクライアント間の双方向リダイレクト		Citrix Workspace アプリのグループポリシーオブジェクト管理用テンプレートを使用してください。

ICA/Web ブラウザーコンテンツのリダイレクト

Name	デフォルト設定	VDA
Web ブラウザーコンテンツのリダイレクト	許可	VDA 7.16 以降
Web ブラウザーコンテンツリダイレクトの ACL 構成	`https://www.youtube.com/*`	VDA 7.16 以降
Web ブラウザーコンテンツリダイレクトのプロキシ構成	empty	VDA 7.16 以降

ICA/クライアントセンサー

Name	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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/デスクトップ **UI**

Name	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、シングルセッション OS 対応 VDA 7～7.15
デスクトップコンポジションリダイレクトの画質	中	VDA 5.6、シングルセッション OS 対応 VDA 7～7.15
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

Name	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

Name	デフォルト設定	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/拡張デスクトップエクスペリエンス

Name	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	マルチセッション OS 対応 VDA 7 以降

ICA/ファイルリダイレクト

Name	デフォルト設定	VDA
クライアントドライブに自動接続する	許可	すべてのバージョンの VDA
クライアントドライブリダイレクト	許可	すべてのバージョンの VDA
クライアント側固定ドライブ	許可	すべてのバージョンの VDA
クライアント側フロッピードライブ	許可	すべてのバージョンの VDA
クライアント側ネットワークドライブ	許可	すべてのバージョンの VDA
クライアント側光学式ドライブ	許可	すべてのバージョンの VDA
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	マルチセッション OS 対応 VDA 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、シングルセッション OS 対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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。マルチセッション OS 対応 VDA 7 以降

Name	デフォルト設定	VDA
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

Name	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、シングルセッション OS 対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
従来のグラフィックモード	無効	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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	マルチセッション OS 対応 VDA 7 以降
3D 画像ワークロードの最適化	無効	VDA 7.17 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

Name	デフォルト設定	VDA
固定キャッシュしきい値	3000000bps	マルチセッション OS 対応 VDA 7 以降

ICA/グラフィック/Framehawk

Name	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

Name	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

Name	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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/モバイルデバイスでの動作

Name	デフォルト設定	VDA
キーボードの自動表示	禁止	VDA 5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション OS 対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/マルチメディア

Name	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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
Microsoft Teams リダイレクト	許可	マルチセッション OS 対応 VDA 1906 以降、シングルセッション対応 VDA 1906 以降
マルチメディア会議	許可	すべてのバージョンの VDA
WAN 接続での Windows Media マルチメディアリダイレクトの最適化	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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

Name	デフォルト設定	VDA
Windows Media のクライアント側でのコンテンツ取得	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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 以降
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 以降

ICA/マルチストリーム接続

Name	デフォルト設定	VDA
UDP を使用したオーディオ	許可	マルチセッション OS 対応 VDA 7 以降
オーディオ UDP ポートの範囲	16500、16509	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
マルチストリーム仮想チャネルのストリーム割り当て設定	デフォルトのストリーム割り当てについては、「マルチストリーム仮想チャネルの割り当て設定」を参照	VDA 2003

ICA/ポートリダイレクト

Name	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

Name	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

Name	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

Name	デフォルト設定	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	VDA 5.6
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

Name	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

Name	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
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

Name	デフォルト設定	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

Name	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］の各項目は［必要なイメージ品質］=［標準品質］、［ヘビーウェイト圧縮を有効にする］=［いいえ］。［イメージおよびフォントのキャッシュ］の各項目は、［埋め込みイメージのキャッシュを許可する］=［はい］、［非管理者によるこれらの設定の変更を許可する］=［いいえ］。	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

Name	デフォルト設定	VDA
SecureICA の最低暗号化レベル	基本	マルチセッション OS 対応 VDA 7 以降

ICA/サーバーの制限

Name	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	マルチセッション OS 対応 VDA 7 以降

ICA/セッションの制限

Name	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、シングルセッション OS 対応 VDA 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、シングルセッション OS 対応 VDA 7 以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 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、シングルセッション OS 対応 VDA 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、シングルセッション OS 対応 VDA 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、シングルセッション OS 対応 VDA 7 以降

ICA/セッション画面の保持

Name	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

Name	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

Name	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	マルチセッション OS 対応 VDA 7 以降
セッションの切断時またはログオフ時にシングルセッション OS のタイムゾーンを復元する	有効	最新の VDA バージョン
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

Name	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、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
TWAIN 圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/USB デバイス

Name	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

Name	デフォルト設定	VDA
クライアント USB デバイスリダイレクト規則	規則の指定なし	すべてのバージョンの VDA
クライアント USB プラグアンドプレイデバイスリダイレクト	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/視覚表示

Name	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	中	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/視覚表示**/**動画

Name	デフォルト設定	VDA
画質の下限レベル	Normal	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
プログレッシブ圧縮のレベル	なし	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
プログレッシブ圧縮のしきい値	2147483647Kbps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

Name	デフォルト設定	VDA
保持する最低フレーム数	10fps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/視覚表示/静止画

Name	デフォルト設定	VDA
エクストラ色圧縮	無効	すべてのバージョンの VDA
エクストラ色圧縮しきい値	8192Kbps	すべてのバージョンの VDA
ヘビーウェイト圧縮	無効	すべてのバージョンの VDA
非可逆圧縮のレベル	中	すべてのバージョンの VDA
非可逆圧縮のしきい値	2147483647Kbps	すべてのバージョンの VDA

ICA/WebSocket

Name	デフォルト設定	VDA
WebSocket 接続	禁止	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
WebSocket ポート番号	8008	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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）	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

負荷管理

Name	デフォルト設定	VDA
同時ログオントレランス	2	マルチセッション OS 対応 VDA 7 以降

Name	デフォルト設定	VDA
CPU 使用率	無効	マルチセッション OS 対応 VDA 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	マルチセッション OS 対応 VDA 7 以降
ディスク使用率	無効	マルチセッション OS 対応 VDA 7 以降
最大セッション数	250	マルチセッション OS 対応 VDA 7 以降
メモリ使用率	無効	マルチセッション OS 対応 VDA 7 以降
基本メモリ使用量	負荷なし：768MB	マルチセッション OS 対応 VDA 7 以降

Profile Management/上級設定

Name	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

Name	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

Name	デフォルト設定	VDA
ユーザーストアへのパス	Windows	すべてのバージョンの VDA
ローカル管理者のログオン処理	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

Name	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。[処理済みグループ] で指定したすべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA
クロスプラットフォーム設定の有効化	無効	すべてのバージョンの VDA
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのバージョンの VDA
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CM が使用されます。	すべてのバージョンの VDA
クロスプラットフォーム設定を作成するためのソース	無効	すべてのバージョンの VDA

Profile Management/ファイルシステム/除外

Name	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

Name	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

Name	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**）

Name	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

Name	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

Name	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

Name	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

Name	デフォルト設定	VDA
ダウンロードパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ダウンロードのリダイレクト設定	［ダウンロードパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**お気に入り

Name	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

Name	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

Name	デフォルト設定	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

Name	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

Name	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

Name	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

Name	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

Name	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

Name	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

Name	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

Name	デフォルト設定	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

Name	デフォルト設定	VDA
キャッシュしたプロファイルを削除する前の待ち時間	0	すべてのバージョンの VDA
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	すべてのバージョンの VDA
ローカルプロファイル競合の制御	ローカルプロファイルを使用	すべてのバージョンの VDA
既存のプロファイルの移行	ローカルおよび移動	すべてのバージョンの VDA
テンプレートプロファイルへのパス	無効。ユーザーが最初にログオンするコンピューター上のデフォルトのユーザープロファイルから新しいユーザープロファイルが作成されます。	すべてのバージョンの VDA
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのバージョンの VDA
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのバージョンの VDA
すべてのログオンで Citrix 固定プロファイルとして使用されるテンプレートプロファイル	無効	すべてのバージョンの VDA

Profile Management/レジストリ

Name	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

Name	デフォルト設定	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

Name	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
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

Name	デフォルト設定	VDA
StoreFront アカウント一覧	ストアの指定なし	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ユーザー個人設定レイヤー

Name	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12 以降のバージョン
ユーザーレイヤーサイズ（GB）	0GB（デフォルトは 10GB の最小レイヤーサイズです）	VDA 19.12 以降のバージョン

Virtual Delivery Agent

Name	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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
IPv6 コントローラー登録のみを使用する	無効	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 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

Name	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

Name	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

Name	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

Name	デフォルト設定	VDA
仮想 IP ループバックプログラムー覧	なし	VDA 7.6 以降

ポリシー設定リファレンス

April 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。

すべてのポリシー設定の完全な一覧は、.CHM（コンパイル済み HTML）形式と.CSV 形式で利用できます。これらのファイルは、ブローカー（Delivery Controller）がインストールされているサーバー上の`\program files\citrix\grouppolicy`フォルダーにあります。また、ここをクリックして、ポリシー設定の最新バージョンをダウンロードすることもできます。

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]、[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

> 重要:
>
> Flash ポリシーは、以前の VDA を使用しているお客様が新しい Controller（バージョン 1912 Controller など）を使用し、引き続き Flash を使用できるようにするためにのみ残されます。この VDA バージョンは Flash をサポートしていません。

目的	使用するポリシー設定
仮想デスクトップがクライアント側に送信されるときの、1 秒あたりのフレームの最大数を設定する	ターゲットフレーム数
ユーザーデバイス側に表示されるイメージの表示品質を制御する	表示品質
セッションで特定の 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

目的	使用するポリシー設定
クライアントプリンターおよびネットワークプリンターの自動作成時に、Windows に付属のプリンタードライバーを自動的にインストールするかどうかを制御する	付属のプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーの使用を制御する	ユニバーサル印刷の使用
ローミングユーザーの接続方法に応じて自動作成されるプリンターを制御する	デフォルトプリンター
負荷を分散し、Universal Print Server のフェールオーバーしきい値を設定する	[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:
> デスクトップまたはアプリケーションセッションでは、ポリシーを使用してスクリーンセーバーを有効にすることはできません。スクリーンセーバーが必要なユーザーの場合は、ユーザーデバイスにスクリーンセーバーを実装できます。

ICA のポリシー設定

April 26, 2021

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が有効になり（[優先]）、可能な場合は EDT が使用されて、TCP にフォールバックします。無効になっていて有効にしたい場合は、次の手順に従います。

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。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。

［許可］に設定した場合は、クライアント接続でクリップボードが使用できる最大帯域幅を構成します。これには、［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（**%**）］を使用します。

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、Citrix Virtual Apps and Desktops 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] に設定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。

カスタム定義のデータ形式を追加できます。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。

> 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に含まれるあらゆるスクリプトが、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。

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、Citrix Virtual Apps and Desktops 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］に設定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］に設定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。

カスタム定義のデータ形式を追加できます。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。

> 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に含まれるあらゆるスクリプトが、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。

デスクトップを起動する

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 コネクションでの VDA 上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

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 Workspace アプリ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。

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。

損失耐性モード

> 重要:
>
> - この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。利用可能になった際、VDA のこのバージョンでサポートされます。
> - 損失耐性モードは、Citrix Gateway または Citrix Gateway サービスではサポートされていません。このモードでは、直接接続でのみ使用可能です。

この設定は、損失耐性のモードを有効または無効にします。

デフォルトでは、損失耐性のモードは ［許可］になっています。

許可の場合、パケット損失および遅延がしきい値を超えると、このモードに移行します。損失耐性モードのしきい値ポリシーを使用してしきい値を設定できます。

詳しくは、「損失耐性モード」を参照してください。

損失耐性モードのしきい値

損失耐性モードを使用できる場合、この設定はセッションが損失耐性モードに切り替わるネットワーク指標のしきい値を指定します。

デフォルトのしきい値は次のとおりです:

- パケット損失：5%
- 遅延：300 ミリ秒（RTT）

詳しくは、「損失耐性モード」を参照してください。

ランデブープロトコル

この設定により、Citrix Gateway Service の使用時に HDX セッションがプロキシ接続される方法が変更されます。この設定を有効にすると、HDX トラフィックは Citrix Cloud Connector を経由しなくなります。代わりに、VDA

の発信接続は、Citrix Gateway サービスに対して直接確立されるようになります（Cloud Connector のスケーラビリティが向上します）。

> 重要：
>
> この機能は、Citrix Cloud の機能トグルと HDX ポリシー設定によって制御されます。HDX 設定はデフォルトで無効ですが、Citrix Cloud の機能トグルはデフォルトで有効になっています。HDX 設定の影響を受けるのは、Citrix Gateway サービスを介して確立された HDX セッションのみです。クライアントと VDA 間で直接確立されたセッションまたはオンプレミス Citrix Gateway 経由のセッションはこの設定の影響を受けません。

詳しくは、ランデブープロトコルを参照してください。

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。

タブレットモードの切り替えのポリシー設定

タブレットモードの切り替えでは、VDA 上でのストアアプリ、Win32 アプリ、および Windows シェルの外観と動作を最適化します。これは、電話やタブレット（またはタッチ対応デバイス）などの小型のフォームファクタデバイスから接続するときに、仮想デスクトップからタブレットモードに自動的に切り替えることによって行われます。

このポリシーを無効にすると、VDA はクライアントの種類に関係なく、ユーザーが設定したモードになり、ずっと同じモードを維持します。

クライアントの自動再接続のポリシー設定

April 24, 2021

［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 以降および Citrix Workspace アプリ 1808 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 Workspace アプリの 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。

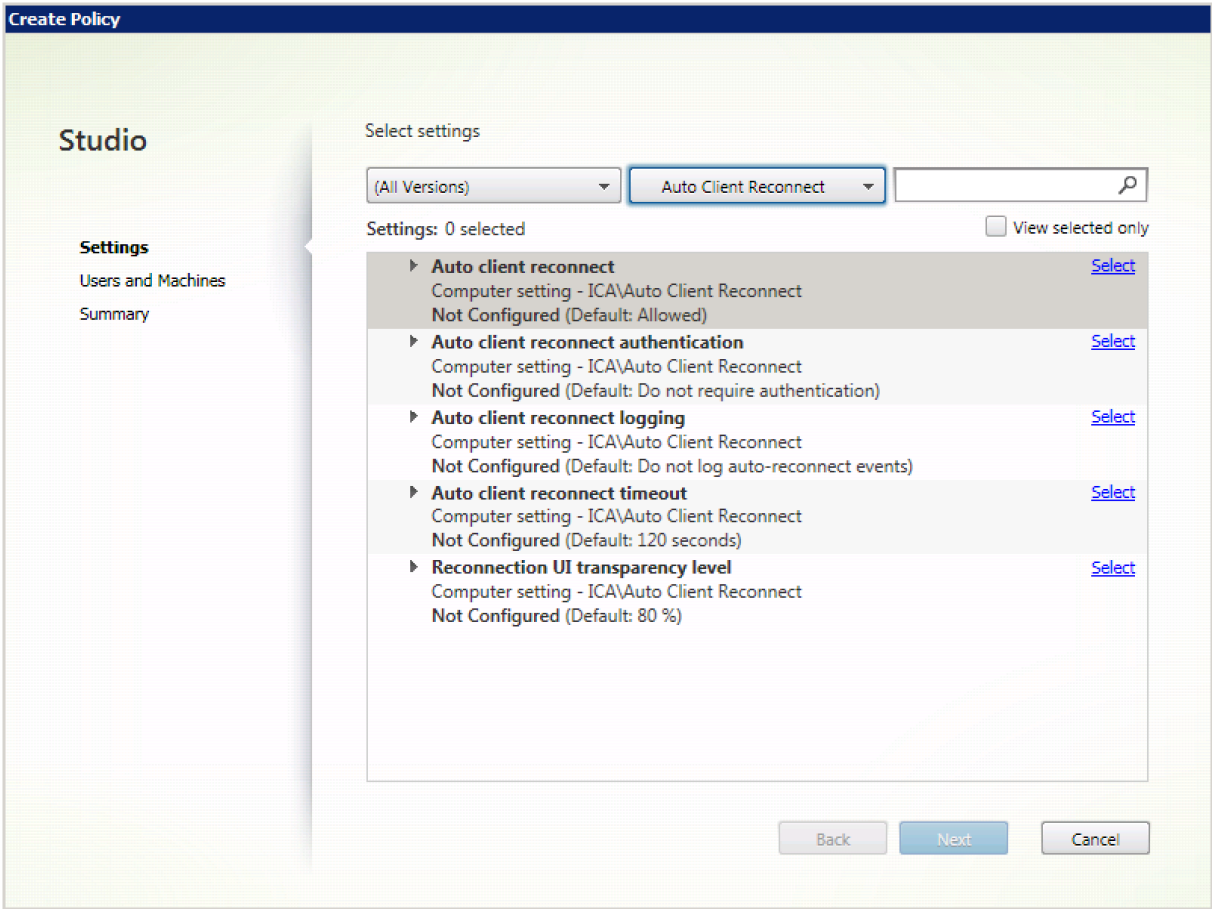
アプリケーションセッションで自動再接続が許可されている場合は、セッションが再接続するまでの残り時間を指定するカウントダウンタイマーが通知領域に表示されます。Citrix Workspace アプリによる再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。

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 Workspace アプリは、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 Workspace アプリに送信されます。この設定を構成すると、Cookie は使用されなくなります。その代わりに、Citrix Workspace アプリが切断セッションに再接続するときに、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**］を選択します。

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**］を選択します。

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**］を選択します。

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**］を選択します。

オーディオのポリシー設定

April 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 マルチセッション 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。
- ボイスオーバー 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。

  この設定では、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。ボイスオーバー IP 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、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 マルチセッション 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 Workspace アプリ側で無効にできます。

Windows マルチセッション 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

April 26, 2021

［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（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。

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

April 26, 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 Workspace アプリの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、Citrix Virtual Apps and Desktops 1808 以降か XenApp または XenDesktop 7.13 以降に加えて、Citrix Workspace アプリ 1808 以降か 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。
> - Windows 向け Citrix Workspace アプリ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。

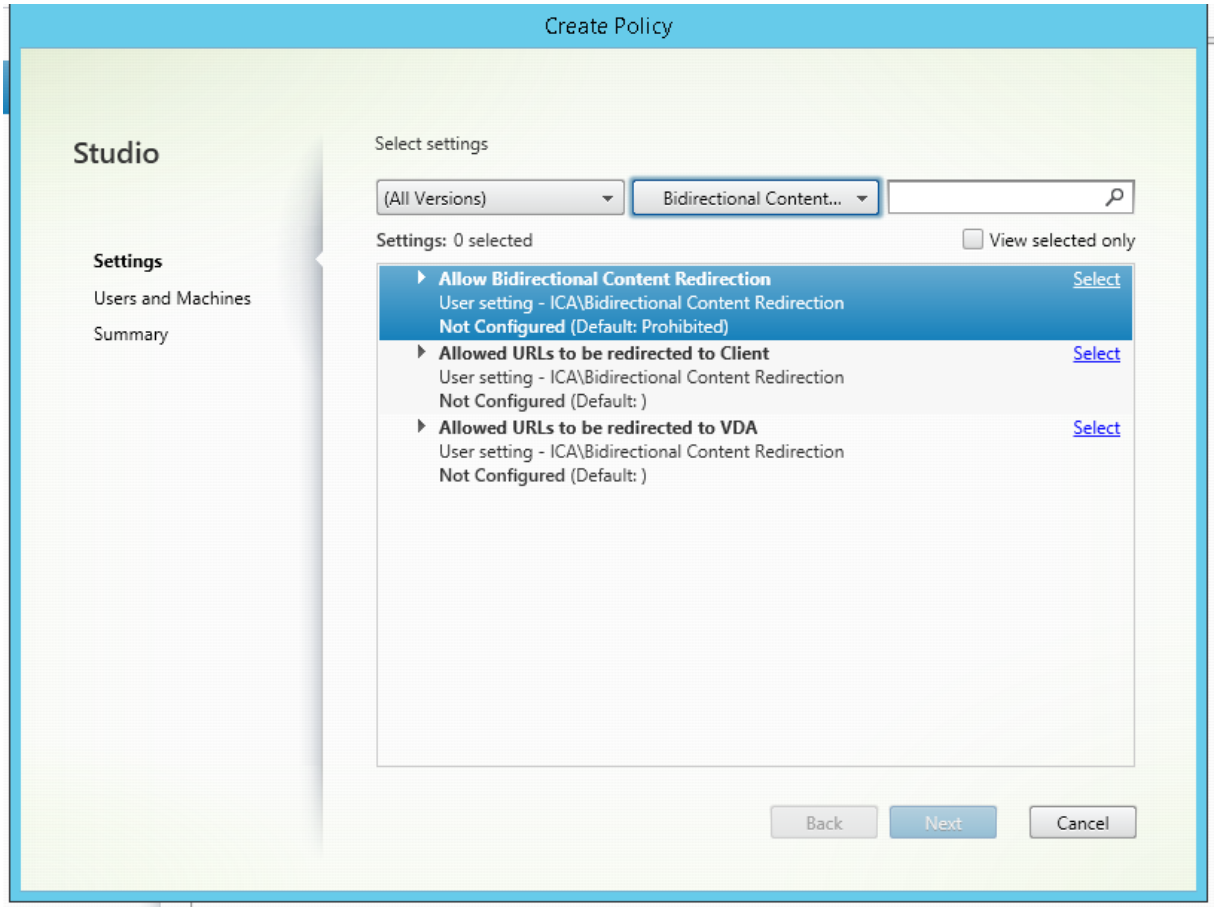
デフォルトでは、双方向のコンテンツリダイレクトは禁止されています。

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：

http://*.citrix.com、http://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。



Citrix Workspace アプリでのクライアント側の双方向コンテンツリダイレクト構成については、Windows 向け Citrix Workspace アプリのドキュメントの「コンテンツの双方向リダイレクト」を参照してください。

セッションとクライアント間のコピーと貼り付け

セッションからクライアントへのコピーと貼り付け機能を構成するには、次のポリシーを設定します:

- [クライアントクリップボードリダイレクト] を許可します。
- [クライアントクリップボードの書き込み制限] でクリップボードからクライアントへのすべての形式の貼り付けを制限します。
- [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] でクリップボードからクライアントにファイルを貼り付ける場合の例外を指定します（この機能を有効にするには CFX_FILE 形式を使用します）。
- [セッションクリップボードの書き込み制限] でクリップボードから VDA セッションへのすべての形式の貼り付けを制限します。
- [セッションクリップボードに書き込みを許可する形式] でクリップボードから VDA にファイルを貼り付ける場合の例外を指定します（この機能を有効にするには CFX_FILE 形式を使用します）。

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 Workspace アプリ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、Windows マルチセッション OS VDA 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

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

April 26, 2021

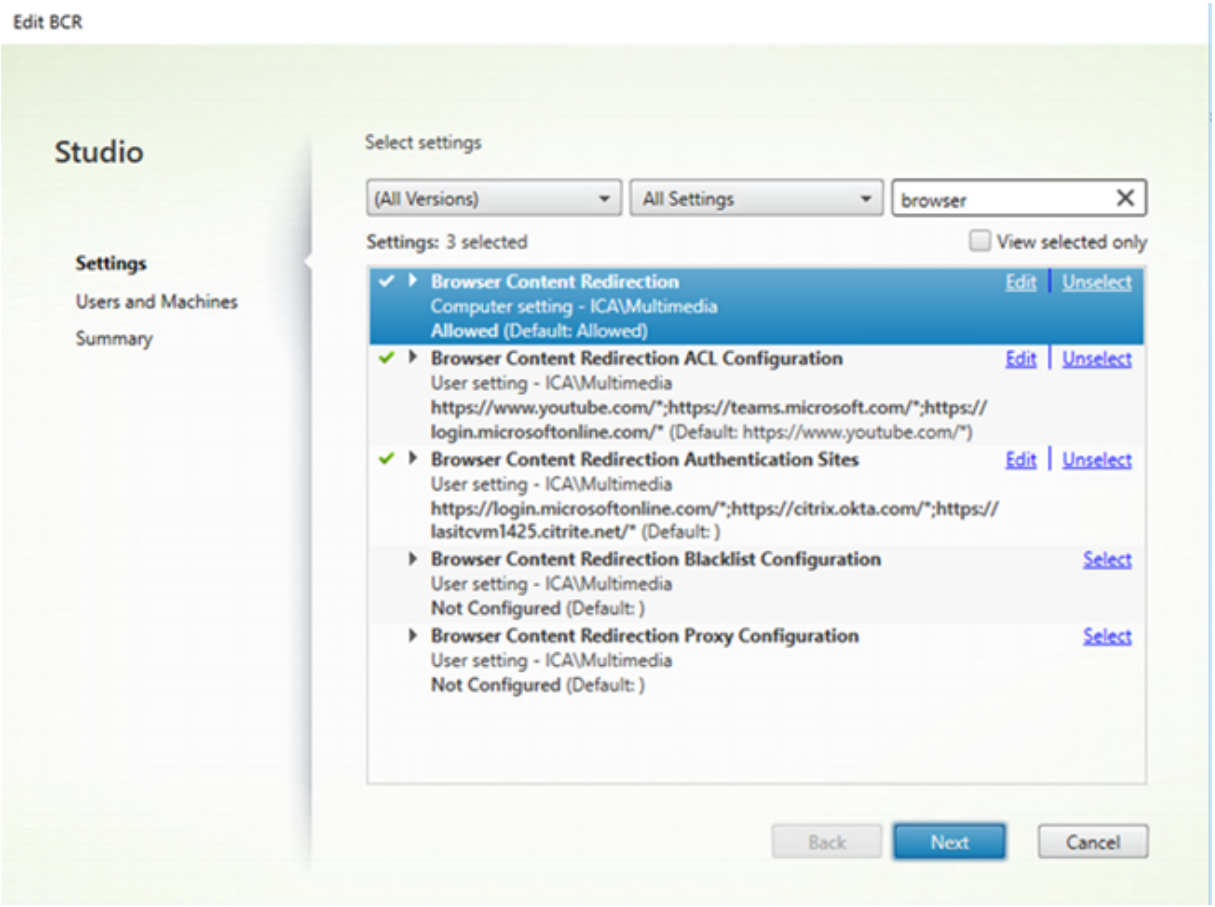
[Web ブラウザーコンテンツリダイレクト]には、この機能を構成するためのポリシー設定が含まれています。

Web ブラウザーコンテンツのリダイレクトでは、Citrix Virtual Apps and Desktops が Web ブラウザーコンテンツ(HTML5 など)をユーザーに配信する方法を制御し、最適化します。コンテンツが表示されている Web ブラウザーの表示領域のみがリダイレクトされます。

HTML5 ビデオリダイレクションと Web ブラウザーコンテンツリダイレクトは、独立した機能です。この機能の使用には HTML5 ビデオリダイレクションのポリシーは必要ありませんが、Citrix HDX HTML5 ビデオリダイレクションサービスは、Web ブラウザーコンテンツリダイレクトのために使用されます。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。

ポリシー設定:

Citrix Studio の Web ブラウザーコンテンツリダイレクト機能では、次のポリシー設定を使用できます。これらのポリシーは VDA 上でレジストリキーにより上書きできますが、レジストリキーはオプションです。



TLS および Web ブラウザーコンテンツリダイレクト

Web ブラウザーコンテンツリダイレクトを使用して、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。

Web ブラウザーコンテンツのリダイレクト

デフォルトでは、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントでクライアントフェッチとレンダリングが失敗すると、サーバー側のレンダリングが試行されます。Web ブラウザーコンテンツのリダイレクトプロキシ設定ポリシーも有効にすると、Citrix Workspace アプリはサーバーフェッチとクライアントレンダリングだけを試みます。

デフォルトでは、［許可］に設定されています。

Web ブラウザーコンテンツのリダイレクトのアクセス制御リスト（ACL）のポリシー設定

Web ブラウザーコンテンツリダイレクトを使用できる URL、またはブラウザーコンテンツリダイレクトへのアクセスを拒否する URL のアクセス制御リスト（ACL）を構成するには、この設定を使用します。

承認済み URL は、コンテンツがクライアントにリダイレクトされるホワイトリストに登録された URL です。

ワイルドカード文字「*」は使用可能ですが、この文字は URL のプロトコルおよびドメインアドレスには使用できません。

使用可能:`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

使用不可: `http://*.xyz.com/`

URL にパスを指定することにより、より細分化することができます。たとえば、`https://www.xyz.com/sports/index.html`を指定すると、index.html ページのみがリダイレクトされます。

デフォルトでは、この設定は`https://www.youtube.com/*`に設定されています。

詳しくは、Knowledge Center のCTX238236を参照してください。

Web ブラウザーコンテンツリダイレクト認証サイト

URL の一覧を構成するには、この設定を使用します。Web ブラウザーコンテンツリダイレクトによりリダイレクトされたサイトは、この一覧を使用してユーザーを認証します。この設定では、ホワイトリストに登録済みの URL から移動するときに、Web ブラウザーコンテンツリダイレクトをアクティブ（リダイレクトあり）のままにする URL を指定します。

一般的なシナリオとしては、ID プロバイダー（IdP）を利用して認証を行う Web サイトが考えられます。たとえば、Web サイト`www.xyz.com`をエンドポイントにする必要があるものの、Okta（`www.xyz.okta.com`）などのサードパーティ IdP が認証を処理しているとします。この場合、管理者が Web ブラウザーコンテンツリダイレクトの ACL 構成ポリシーで`www.xyz.com`をホワイトリストに登録し、さらに Web ブラウザーコンテンツリダイレクト認証サイトで`www.xyz.okta.com`をホワイトリストに登録します。

詳しくは、Knowledge Center の CTX238236を参照してください。

Web ブラウザーコンテンツリダイレクトのブラックリスト設定

この設定は、Web ブラウザーコンテンツリダイレクトの ACL 構成の設定と連携しています。Web ブラウザーコンテンツリダイレクトの ACL 構成設定とブラックリスト構成設定に URL が存在する場合、ブラックリスト構成が優先され、その URL のブラウザーコンテンツはリダイレクトされません。

承認されていない **URL**: Web ブラウザーコンテンツがクライアントにリダイレクトされずサーバーでレンダリングされる、ブラックリストに登録する URL を指定します。

ワイルドカード文字「*」は使用可能ですが、この文字は URL のプロトコルおよびドメインアドレスには使用できません。

使用可能:`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

使用不可: `http://*.xyz.com/`

URL にパスを指定することにより、より細分化することができます。たとえば、`https://www.xyz.com/sports/index.html`を指定すると、index.html ページのみがブラックリストに登録されます。

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

この設定は、Web ブラウザーコンテンツリダイレクト用の VDA でのプロキシ設定のオプションです。有効なプロキシアドレスとポート番号、PAC/WPAD URL、または直接/透過型の設定を指定して有効にすると、Citrix Workspace アプリはサーバーフェッチとクライアントレンダリングだけを試行します。

無効にするか構成しないで、デフォルト値を使用すると、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、禁止に設定されています。

明示的なプロキシで許可されたパターン:

`http://\<hostname/ip address\>:\<port\>`

例:

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

PAC/WPAD ファイルで許可されたパターン:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

例: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接または透過型のプロキシで許可されたパターン:

ポリシーテキストボックスに「**DIRECT**」と入力します。

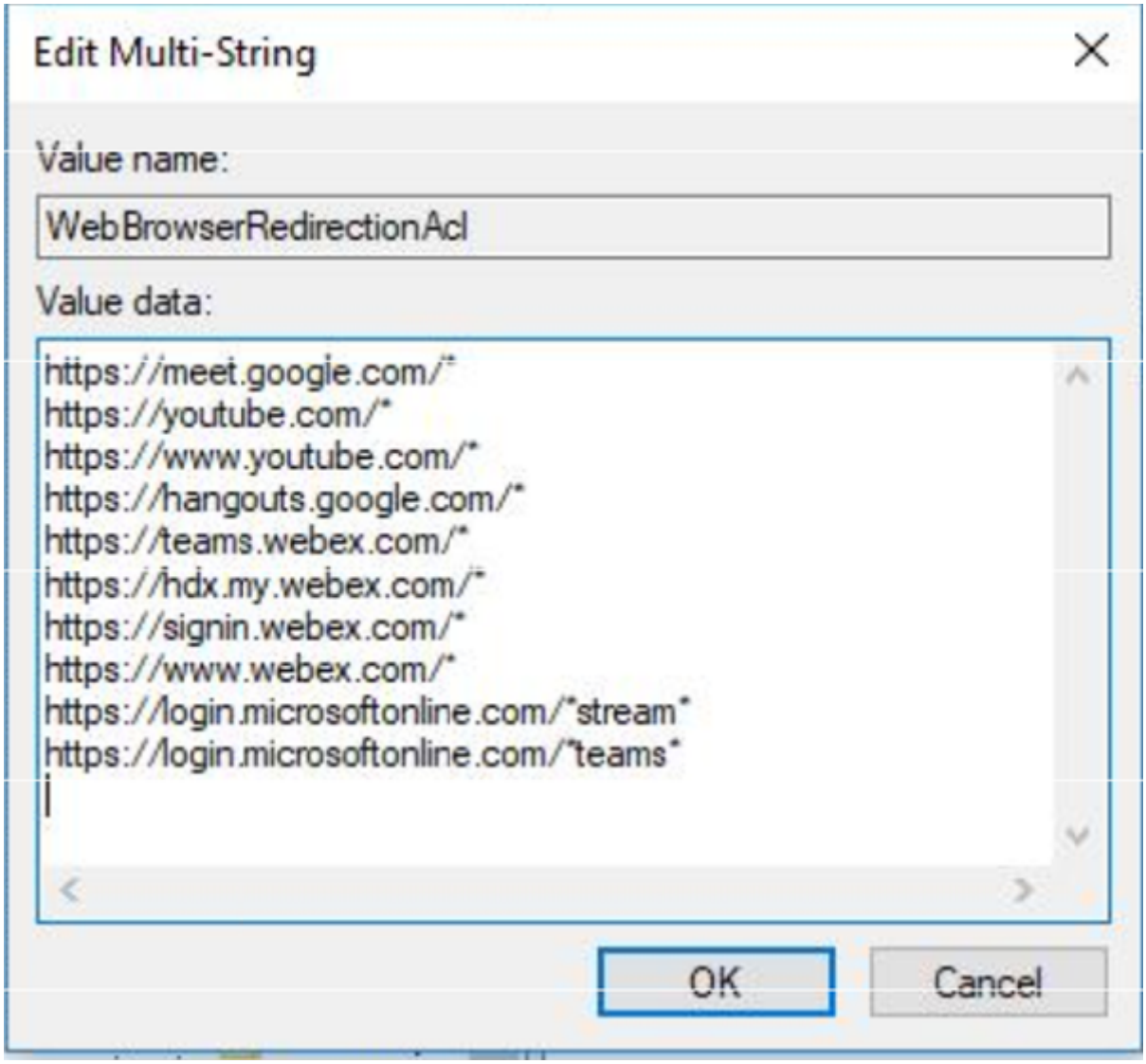
Web ブラウザーコンテンツリダイレクトのレジストリキーの上書き

> 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

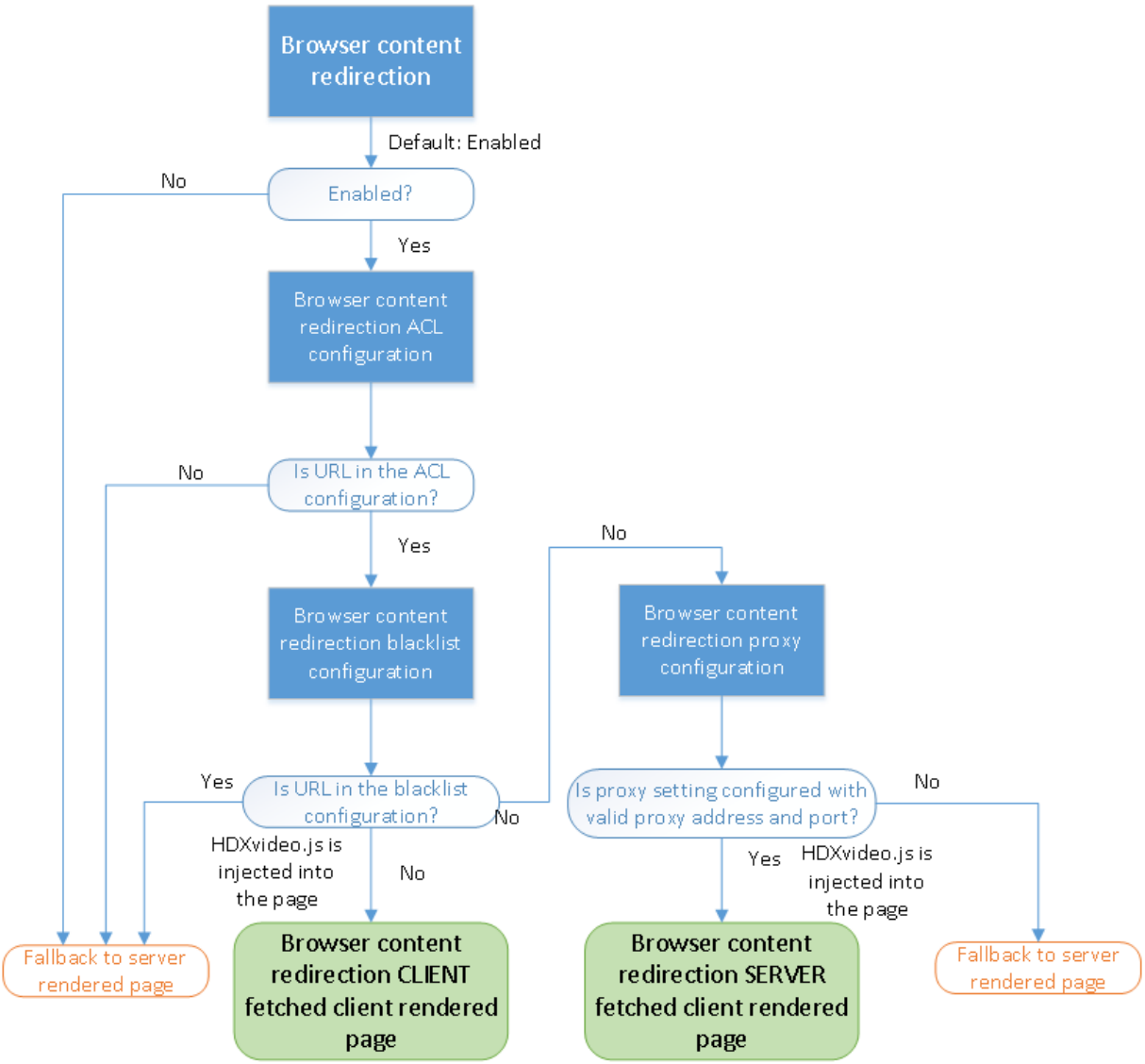
> では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
>
> ポリシー設定を上書きするレジストリ設定を以下に示します:

\HKLM \SOFTWARE\Wow6432Node\Citrix\HdxMediastream

Name	種類	値
WebBrowserRedirection	DWORD	1= 許可、0= 禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthen	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	http://myproxy.citrix.com:8080 または http://10.10.10.10:8888
WebBrowserRedirectionBlacklis	REG_MULTI_SZ	



Web ブラウザーコンテンツのリダイレクト用の **HDXVideo.js** 挿入



HdxVideo.js は、Chrome の Web ブラウザーコンテンツリダイレクト拡張機能または Internet Explorer Browser Helper Object（BHO）を使用して Web ページに挿入されます。BHO は、Internet Explorer のプラグインモデルです。Web ブラウザー API のフックを提供し、プラグインがナビゲーションを制御するためにページの DOM（Document Object Model）にアクセスできるようにします。

BHO は、特定のページに HdxVideo.js を挿入するかどうかを決定します。この決定は、上記のフローチャートに示した管理ポリシーに基づいています。

JavaScript の挿入とクライアントへの Web ブラウザーコンテンツのリダイレクトが決定されると、VDA 上の Internet Explorer ブラウザーの Web ページが消去されます。**document.body.innerHTML** を空に設定すると、VDA 上では Web ページの本文全体が削除されます。ページがクライアントに送信され、クライアントのオーバーレイ Web ブラウザー（Hdxbrowser.exe）に表示される準備が整います。

クライアントセンサーのポリシー設定

April 24, 2021

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 Workspace アプリ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らないことにご注意ください。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。
  - アプリケーションがキャッシュした位置情報データをユーザーが消去できる（ただし、Citrix Workspace アプリ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 Workspace アプリを信頼できるサーバーに接続してください。
- 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

April 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。

> 重要
>
> このリリースでは、従来のグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートしていません。このポリシーは、Windows 7 および Windows 2008 R2 で XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、および以前の VDA リリースを使用している場合の後方互換性のためにのみ含まれています。

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。

デフォルト値は［高］です。

［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。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ている場合、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

April 24, 2021

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

April 24, 2021

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

April 24, 2021

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、自動接続する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。

> 注:
>
> ［クライアントドライブのリダイレクト］ポリシー設定は、汎用 USB リダイレクトを使用するセッションにマッピングされているドライブには適用されません。

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 Workspace アプリや 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 Workspace アプリ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。

ファイル転送速度が良好な遠隔接続が必要で、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。

グラフィックのポリシー設定

April 26, 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。

グラフィックス状態インジケーター

この設定では、グラフィックス状態インジケーターがユーザーセッションで実行されるように構成されます。使用中のグラフィックモードの詳細を確認できます。グラフィックプロバイダー、エンコーダー、ハードウェアエンコーディング、イメージ品質、進行表示状態、および無損失テキストなどです。

デフォルトでは、グラフィックス状態インジケーターは無効になっています。この設定は、無損失インジケーターを置き換えます。Citrix Virtual Apps and Desktops の以前のリリースでは、無損失インジケーターは有効になります。

Microsoft の待ち時間による制限:

グラフィックス状態インジケーターを有効にした後、ユーザーが最初に Citrix Virtual Apps and Desktops にログオンしたときに問題が発生する可能性があります。状態インジケーターのアイコンがシステムトレイに表示されるまでに 4 時間かかります。

表示メモリの制限

この設定では、セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。

デフォルトの表示メモリ制限は、65536 キロバイトに設定されます。

セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。キロバイト単位の容量指定は、128 から 4,194,303 です。最大値 4,194,303 によって表示メモリが制限されることはありません。デフォルトでは、65536 キロバイトに設定されます。ウィンドウサイズを大きくしたり、表示色数を多くしたりすると、必要なメモリの量が増えます。従来のグラフィックモードでは、この最大値に達すると、［メモリが不足したときの表示モード］設定に基づいて色数または解像度が低下します。

高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は、次の式で算出できます。

必要とされるメモリ（バイト単位）＝（1 ピクセルあたりのビット数を 8 で割った色数）x（垂直方向のピクセル単位の解像度）x（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）x（600 ピクセル）x（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、次のシームレスウィンドウの表示を有効または無効にします:

- フリップ
- フリップ 3D
- タスクバープレビュー
- ピークウィンドウプレビュー

Windows Aero プレビューオプション	説明
タスクバープレビュー	Windows タスクバー上のアイコン上にマウスポインターを合わせると、そのウィンドウの縮小版がプレビューとして表示されます。
ピークウィンドウプレビュー	Windows タスクバー上に開いた縮小版上にマウスポインターを合わせると、そのウィンドウがフルサイズで表示されます。
フリップ	Alt+Tab キーを押すと、開いているすべてのウィンドウの縮小版が一覧表示されます。
フリップ 3D	Tab+Windows ロゴキーを押すと、開いているすべてのウィンドウが立体的に重なって一覧表示されます。

デフォルトでは、有効になっています。

イメージキャッシュ

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定項目では、セッション内のイメージのセクションキャッシュおよび取得を有効または無効にします。必要な場合にセクションのイメージをキャッシュし、そのセクションを取得すると、スクロールがよりスムーズになり、ネットワーク上のデータ伝送量が減少して、ユーザーデバイス上で必要とされる処理が少なくなります。

デフォルトでは、イメージのキャッシュ設定は有効になっています。

> 注:
>
> イメージのキャッシュ設定は、イメージがどのようにキャッシュおよび取得されるかを制御します。この設定では、イメージをキャッシュするかどうかは制御されません。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 - サポートされていません。後方互換性のためにのみ

> 重要:
>
> このリリースでは、従来のグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートしていません。このポリシーは、Windows 7 および Windows 2008 R2 で XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、および以前の VDA リリースを使用している場合の後方互換性のためにのみ含まれています。

この設定では、リッチなグラフィック表示が無効になります。この設定を使用すると、従来のグラフィック表示が取り消され、WAN やモバイル接続での帯域幅の使用量が削減されます。XenApp および XenDesktop 7.13 に導入された帯域幅の削減によって、このモードは廃止されます。

この設定はデフォルトで無効になっており、リッチなグラフィック表示が提供されます。

Windows 7 および Windows Server 2008 R2 VDA では、従来のグラフィックモードがサポートされます。

Windows 8.x、10、または Windows Server 2012、2012 R2、2016 では、従来のグラフィックモードはサポートされていません。

XenApp および XenDesktop 7.6 FP3 以降でのグラフィックモードおよびポリシーの最適化について詳しくは、CTX202687を参照してください。

許可される最大表示色数

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、セッションで許可される最大表示色数を指定します。

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シングルセッション 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 マルチセッション 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。

3D 画像ワークロードの最適化

この設定では、グラフィックの負荷が過剰なワークロードに合わせて適切なデフォルト設定を構成します。グラフィックワークロードの負荷が大きいアプリケーションのユーザーに対してこの設定を有効にします。このポリシーは、セッションで GPU が利用可能な場合にのみ適用してください。その他の設定がこのポリシーのデフォルト設定を明示的に上書きする場合、そちらが優先されます。

デフォルトでは、3D 画像ワークロードの最適化は無効になっています。

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。［領域をアクティブに変更］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、またはビデオコーデックを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。［可能であれば使用］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、［可能であれば使用］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、［可能であれば使用］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。

ビデオデコーディングをサポートする Citrix Workspace アプリはすべて、ハードウェアエンコーディングで使用できます。

NVIDIA

NVIDIA GRID GPU の場合、ハードウェアエンコーディングはマルチセッション OS 対応 VDA およびシングルセッション OS 対応 VDA でサポートされています。

NVIDIA GPU は、NVENC ハードウェアエンコーディングをサポートする必要があります。サポートされている GPU の一覧については、「NVIDIA ビデオコーデック SDK」を参照してください。

NVIDIA GRID には、ドライバーのバージョン 3.1 以上が必要です。NVIDIA Quadro には、ドライバーのバージョン 362.56 以上が必要です。NVIDIA リリース R361 ブランチからのドライバーをお勧めします。

無損失テキストは、NVENC ハードウェアエンコーディングと互換性がありません。無損失テキストを有効にした場合、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。

［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。

視覚的無損失圧縮（YUV 4:4:4）がサポートされています。視覚的無損失（グラフィックポリシー設定「視覚的無損失の圧縮を使用する」）には、Citrix Workspace アプリ 1808 以降または Citrix Receiver for Windows 4.5 以降が必要です。

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シングルセッション OS 対応 VDA およびマルチセッション OS 対応 VDA でサポートされています。

サポート対象は、Intel Broadwell プロセッサーファミリの 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。

無損失テキストは、ビデオコーデックポリシーが画面全体に対して設定され、**3D** グラフィック用に最適化されたワークロードポリシーが無効になっている場合にのみサポートされます。

視覚的無損失（YUV 4:4:4）はサポートされていません。

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提供します（たとえば、1 人のユーザーが 8 つのモニターを使用したり、8 人のユーザーが各自 1 つのモニターを使用したりするなど）。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。

AMD

AMD の場合、ハードウェアエンコーディングはシングルセッション OS 対応 VDA でサポートされています。

AMD GPU が RapidFire SDK をサポートしている必要があります。たとえば、AMD Radeon Pro GPU や FirePro GPU です。

エンコーディングを行うには、最新の AMD ドライバーをインストールします。これらのドライバーはhttps://www.amd.com/en/supportからダウンロードできます。

無損失テキストは、AMD ハードウェアエンコーディングと互換性がありません。無損失テキストを有効にした場合、無損失テキストは AMD ハードウェアエンコーディングよりも優先されます。

［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。

キャッシュのポリシー設定

April 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

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。その代わりにThinwireでアダプティブトランスポートを有効にします。

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

April 24, 2021

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

April 24, 2021

［ローカルアプリケーションアクセス］カテゴリには、ホストされるデスクトップ環境で、ユーザーデバイス上にインストールされたローカルアプリケーションとホスト上のアプリケーションをシームレスに使用できるようにするための設定項目が含まれています。

ローカルアプリ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

April 24, 2021

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、Citrix Workspace アプリのインターフェイスの全体的な動作を指定します。

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、

iOS 向け Citrix Workspace アプリのユーザーは、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

April 26, 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。

> 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。

マルチメディアポリシー

デフォルトでは、Delivery Controller で設定されたすべてのマルチメディアポリシーは、次のレジストリに格納されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

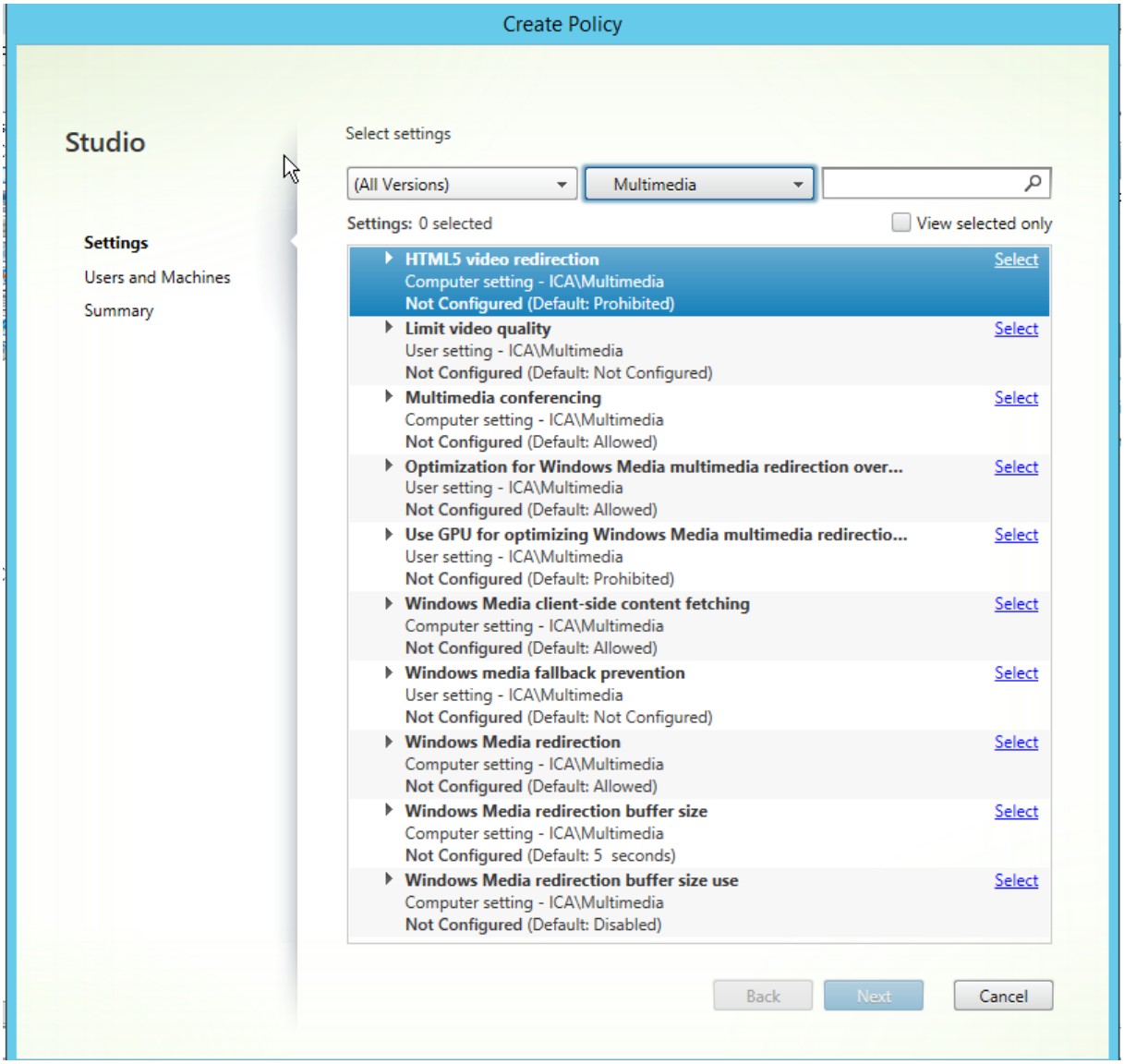
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッション ID}\User\MultimediaPolicies

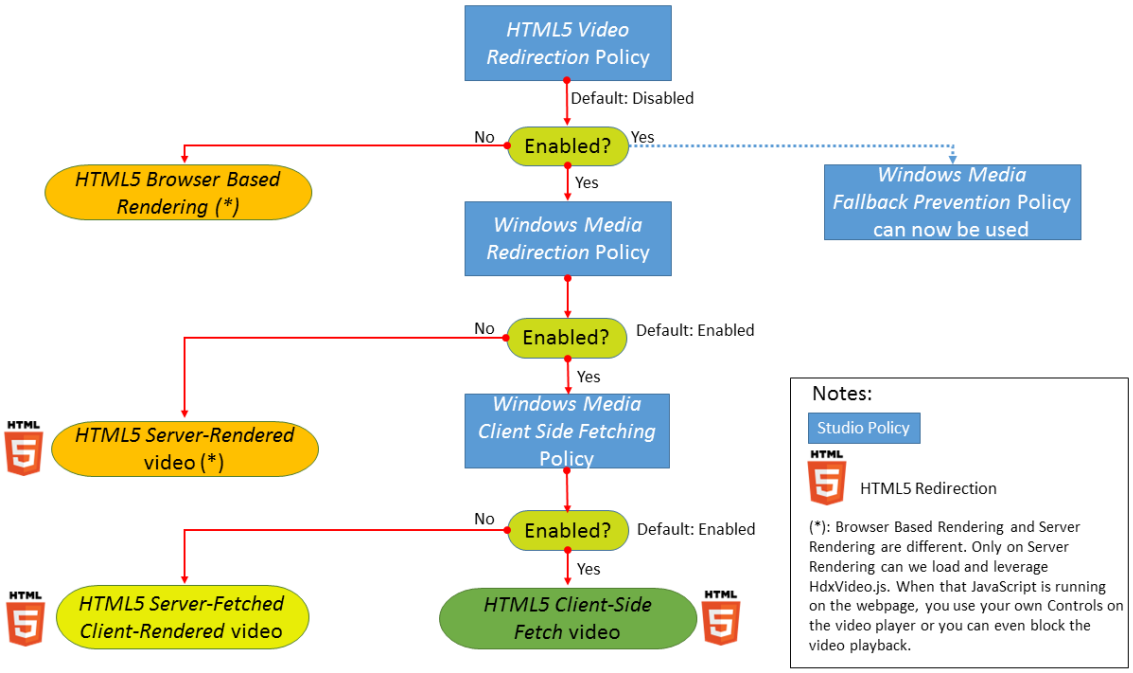
現行のユーザーセッション ID を見つけるには、Windows コマンドラインで **qwinsta** コマンドを実行します。

HTML5 ビデオリダイレクト

Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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、**HTML5** ビデオリダイレクト、**Web** ブラウザーコンテンツのリダイレクト

HTML5 ビデオリダイレクトを使用して HTTPS Web サイトからビデオをリダイレクトしたり、Web ブラウザーコンテンツのリダイレクトを使用して Web サイト全体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アカウントとして動作し、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。

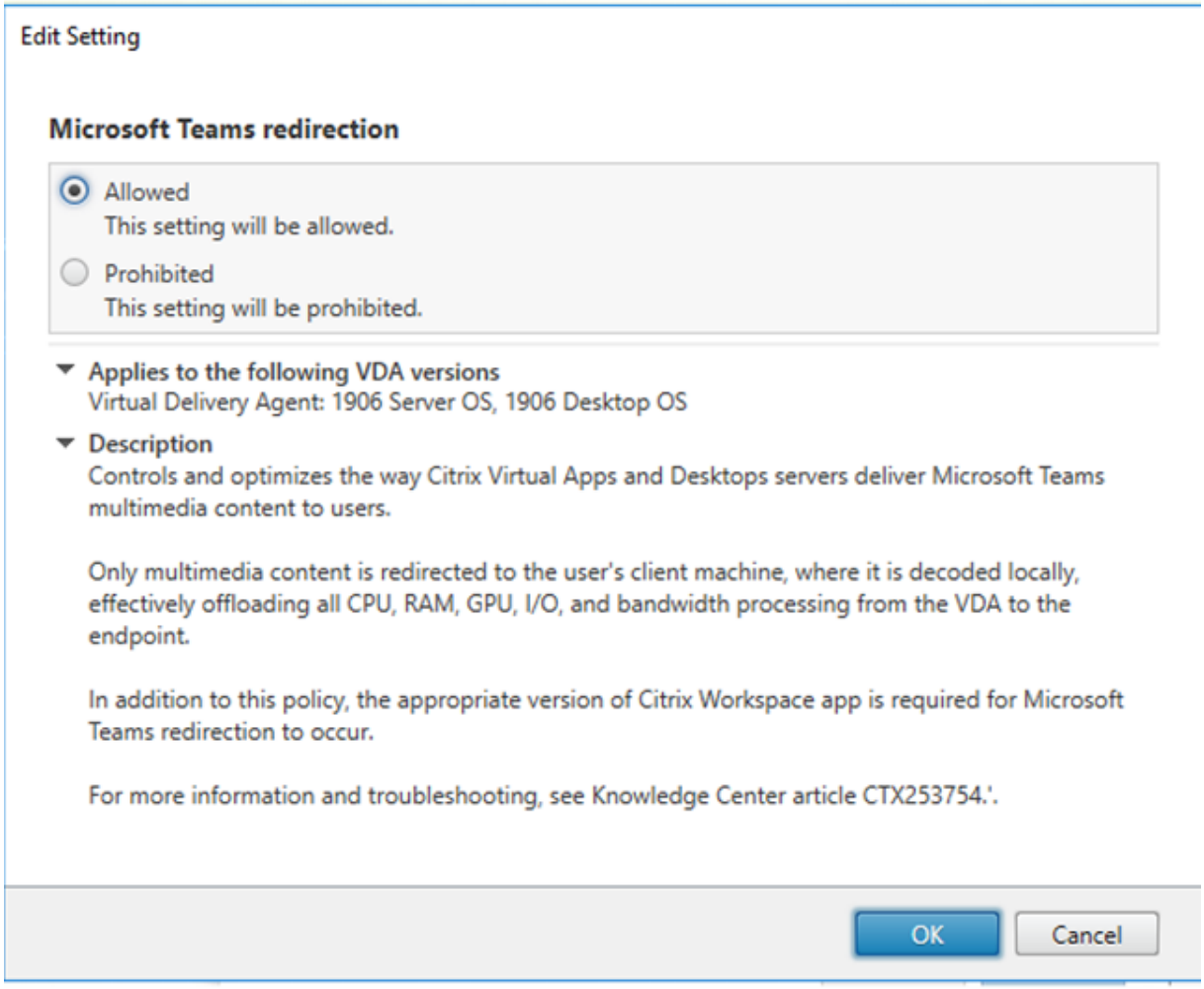
- 1080p/8.5mbps

- 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。

Microsoft Teams リダイレクト

この設定により、HDX テクノロジに基づいて Microsoft Teams を最適化できます。



このポリシーが有効でサポート対象のバージョンの Citrix Workspace アプリを使用している場合、VDA でこのレジストリキーの値は **1** に設定されます。Microsoft Teams アプリケーションはこのレジストリキーを VDI モードで読み取ってロードします。
レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

値の名前：MSTeamsRedirSupport

値：DWORD（1 - オン、0 -オフ）

> 注：
>
> Studio で使用可能なポリシーがない古い Controller バージョン（たとえばバージョン 7.15）でバージョン 1906.2 以上の VDA を使用している場合、HDX 最適化は VDA でデフォルトで有効になります。Workspace アプリのバージョンが 1907 以降の場合、Teams は最適化モードで起動します。
>
> この場合、特定のユーザーに対してこの機能を無効にするには、グループポリシーを使用して対象ユーザーの組織単位にログオンスクリプトを適用し、レジストリ設定を上書きします。

Microsoft Teams のリダイレクト機能はデフォルトでは有効になっています。

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、Web ブラウザーコンテンツのリダイレクト、HTML 5、Windows Media 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。

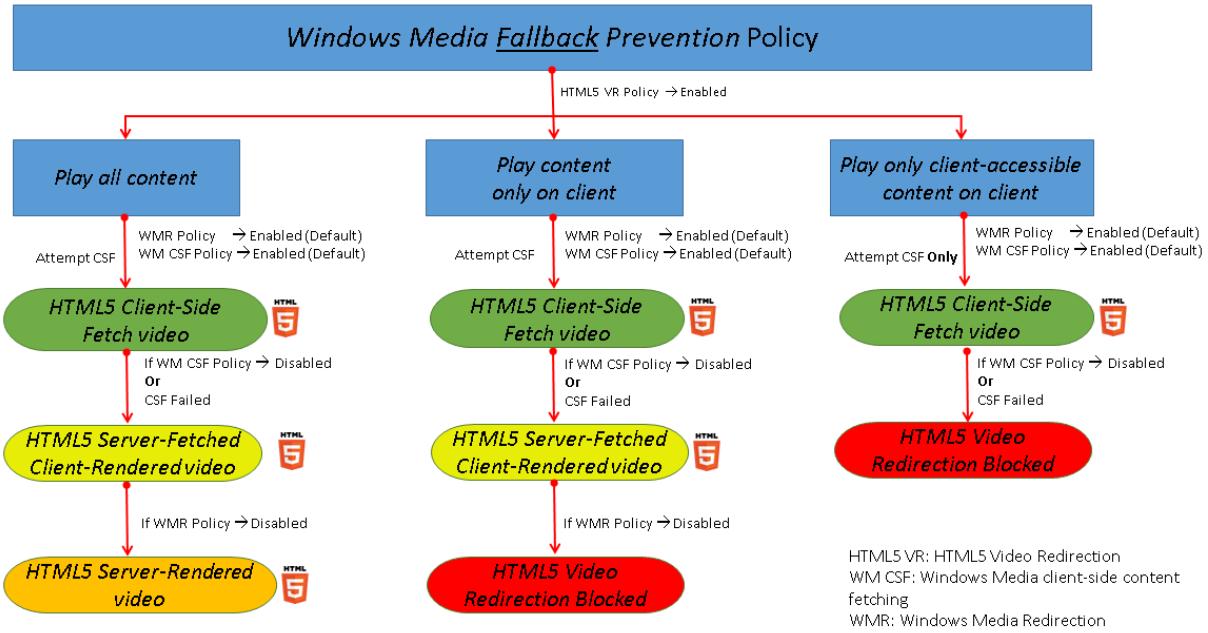
管理者はこの Windows メディアバック防止ポリシー設定を使って、ユーザーへのストリーム配信コンテンツの配信方法を指定できます。

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。

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。

Citrix Workspace アプリでは、オーディオはデフォルトで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 Workspace アプリ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

April 26, 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（サービス品質）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（最小ポート番号、最大ポート番号）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」の範囲が設定されています。

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（サービス品質）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。

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。

マルチストリーム仮想チャネルの割り当て設定

マルチストリーム使用時に仮想チャネルが割り当てられる ICA ストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルを ICA ストリームに割り当てるには、仮想チャネル名の横の［ストリーム番号］一覧から目的のストリーム番号（0、1、2、3）を選択します。

使用環境にカスタム仮想チャネルがある場合、［追加］をクリックして［仮想チャネル］の下のテキストボックスに仮想チャネル名を入力し、その隣の［ストリーム番号］一覧からストリーム番号を選択します。実際の仮想チャネル名を入力し、フレンドリ名は使用しないでください。例：Citrix Browser Acceleration ではなく CTXSBR と入力します。

これらの設定は、マルチストリームコンピューター設定を有効にしたときのみ機能します。

デフォルトの仮想チャネルおよびストリーム割り当ては次のとおりです：

- AppFlow：2
- オーディオ：0
- Web ブラウザーコンテンツリダイレクト：2
- クライアント側 COM ポートのマッピング：3
- クライアントドライブマッピング：2
- クライアント側プリンターのマッピング：3
- クリップボード：2
- CTXDND：1（注：新しいドラッグアンドドロップ機能を評価するお客様に向けて、CTXDND を追加しました。詳しくは、「新機能」の「Citrix セッションとローカルエンドポイント間でファイルをドラッグアンドドロップ（評価専用）」を参照してください。
- DVC プラグイン（DVC プラグインのフレンドリ名から自動的に生成された、または管理者によって割り当てられた静的 VC 名）：2
- End User Experience Monitoring：1
- ファイル転送（HTML5 Receiver）：2
- 汎用データ転送：2
- ICA コントロール：1
- Input Method Editor：1
- 従来のクライアント側プリンターのマッピング（COM1）：1、3
- 従来のクライアント側プリンターのマッピング（COM1）：2、3
- 従来のクライアント側プリンターのマッピング（LPT1）：1、3
- 従来のクライアント側プリンターのマッピング（LPT2）：2、3
- ライセンス管理：1
- Microsoft Teams/WebRTC リダイレクト：1
- モバイルデバイス上の Receiver：1
- マルチタッチ：1
- ポート転送：2
- リモートオーディオおよびビデオ拡張機能（RAVE）：2
- シームレス（透過型ウィンドウ統合）：1
- センサーおよび位置情報：1
- スマートカード：1
- Thinwire グラフィック：1
- 透過型 UI 統合/ログオン状態：2
- TWAIN リダイレクト：2

- USB：2
- 遅延のないフォントとキーボード：2
- 遅延のないデータチャネル：2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center のCTX131001を参照してください。

ポートリダイレクトのポリシー設定

April 26, 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。VDA のバージョンが **7.0**～**7.8** の場合は、これらの設定をレジストリで構成します。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

April 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。ICA/HDX セッションでは、Citrix Print Manager サービス（CpSvc.exe）によって、セッションプリンターポリシー設定で指定されたネットワークプリンターごとに、セッションログオン時にネットワークプリンター接続が作成されます。プリンターは、セッションのログオフ時に削除されます。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターは Windows プリントサーバーまたは Citrix ユニバーサルプリントサーバー上に存在します。

- **Windows** プリントサーバー： 1 つまたは複数のネットワークプリンターを共有します。ネットワークプリンターを使用するために必要なネイティブのプリンタードライバーも用意されています。
- 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ソフトウェアがインストールされている Windows プリントサーバーです。

Windows プリントサーバーを使用する場合、Citrix Print Manager サービスはネイティブのプリンタードライバーを使用してネットワークプリンターの接続を作成します。Citrix Virtual Apps サーバーには、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ている必要があります。

Citrix ユニバーサルプリントサーバーを使用する場合、Citrix Print Manager サービスはネイティブの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、または Citrix Universal XPS プリンタードライバーのいずれかを使用してネットワークプリンターの接続を作成します。使用するドライバーは、ユニバーサルプリントドライバーの使用ポリシー設定によって制御されます。

現在、すべての Windows プリンタードライバーのバージョンは、v3 または v4 のいずれかです。詳しくは、「Support for the Microsoft V3 and V4 Printer Driver Architectures」を参照してください。

セッションプリンターを追加してからセッションに表示されるかどうかを確認するには、以下の手順を実行します：

1. Citrix Studio で、［ポリシー］タブに移動します。
2. ［ポリシーの編集］ダイアログボックスでセッションの印刷ポリシーを有効にします。
3. このポリシーに、セッションプリンターを追加します。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。セッションプリンターが一覧に表示されている必要があります。
4. ポリシーの設定後、公開アプリケーションにセッションプリンターが表示されないことがあります。この問題は、Citrix Virtual Apps サーバーのプリンタードライバーがないか、ポリシーが作成されているが有効になっていない場合に発生する可能性があります。

> 注:
>
> Citrix Virtual Apps サーバーにプリンタードライバーがインストールされていない原因として多いのが、管理者が Citrix Virtual Apps サーバーにプリンタードライバーをインストールするのを失念しているケースです。

5. 公開デスクトップを起動して、手動で［デバイスとプリンター］**>**［コントロールパネル］からセッションプリンターを追加します。
6. これが失敗する場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP でのテストの実行を検討してください。

プリンターの自動作成を待機する

Citrix Virtual Desktops 用か Citrix Virtual Apps 用かに応じてこの機能を有効にします。Citrix Virtual Desktops でこの機能を有効にするには、Delivery Controller のポリシーを有効にします。Citrix Virtual Apps でこの機能を有効にするには、Delivery Controller の PowerShell コマンドレットを使用します。

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、クライアントがリダイレクトされた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ことができます。

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。

プリンターの自動作成を待機する（**Citrix Virtual Apps**）:

次の PowerShell コマンドレットを設定すると、クライアントがリダイレクトされたプリンターが自動作成されるまでサーバーデスクトップ上に作成された Virtual Apps への接続を遅延させることができます。

```
Set-BrokerApplication -Name <VirualAppName> -WaitForPrinterCreation $true
```

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

April 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

PDF ユニバーサルプリンターを自動作成する

この設定では、Citrix Workspace アプリ（VDA 7.19 以降）、HTML5 向け Citrix Workspace アプリ、または Chrome 向け Citrix Workspace アプリを使用するセッション用の Citrix PDF プリンターの自動作成を有効または無効にします。

デフォルトでは、Citrix PDF プリンターは自動作成されません。

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後方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、従来のバージョンの XenApp および XenDesktop との後方互換性を保持する場合に使用します。このオプションは、新しいバージョンの Citrix Virtual Apps and Desktops で使用できます。

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、また、作成されたプリンターがユニバーサルプリンタードライバーのみを使用することを許可できます。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、プリンターのプロパティを保存するかどうか、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 Citrix Virtual Apps 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。

Citrix PDF ユニバーサルプリンタードライバー

Citrix PDF ユニバーサルプリンタードライバーを使用すると、ホストされているアプリケーション、または Citrix Virtual Apps and Desktops で配信された仮想デスクトップ上で実行中のアプリケーションで開かれているドキュメントを印刷できます。ユーザーが ［**Citrix PDF** プリンター］オプションを選択すると、ドライバーがファイルを PDF に変換して、これをローカルデバイスに転送します。その後、PDF を表示したり、ローカルに接続されたプリンターで印刷したりできます。PDF は、（EMF および XPS に加えて）Citrix ユニバーサル印刷でサポートされている形式の 1 つです。
Citrix ポリシーを使用して、PDF プリンターを有効化および構成できるほか、デフォルトとして設定できます。［**Citrix PDF** プリンター］オプションは、Windows、Chrome、および HTML5 向けの Citrix Workspace アプリで利用できます。

> 注:
>
> Windows エンドポイントには、PDF ビューアーが必要です。クライアントには、PDF ファイルを開くため、Windows でファイルタイプの関連付けを登録済みのアプリケーションが必要です。

ドライバーのポリシー設定

April 24, 2021

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

> 注
>
> このポリシーは、このリリースの VDA をサポートしていません。

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

April 24, 2021

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。

SSL 暗号の組み合わせ

この設定は、暗号化印刷データストリーム（CGP）でユニバーサルプリントクライアントが使用する SSL/TLS 暗号の組み合わせセットを指定します。

暗号化印刷 Web サービス（HTTPS/SOAP）接続でユニバーサルプリントクライアントが使用する暗号の組み合わせを制御するには、[SCHANNEL] を参照してください。

デフォルト値：ALL

この設定の値は、ALL、COM、または GOV です。

それぞれの値は、以下の暗号の組み合わせに関連しています：

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL 準拠モード

この設定は、暗号化印刷データストリーム（CGP）でユニバーサルプリントクライアントが使用する NIST Special Publication 800-5 への準拠レベルを指定します。

デフォルト値：なし。

この設定では以下の値を指定できます：

なし。

暗号化印刷データストリーム（CGP）接続はデフォルトの準拠モードを使用します。

SP800-52。

暗号化印刷データストリーム（CGP）接続は NIST Special Publication 800-52 準拠モードを使用します。

SSL が有効

この設定は、印刷データストリーム（CGP）接続と Web サービス（HTTP/SOAP）接続でユニバーサルプリントクライアントが使用する SSL/TLS 暗号の組み合わせセットを指定します。

［ユニバーサルプリントサーバーの有効化］を ［有効。**Windows** のリモート印刷機能にフォールバックする］に設定すると、フォールバック接続は Microsoft Windows ネットワーク印刷プロバイダーによって確立されます。この設定によって、フォールバック接続が影響を受けることはありません。

デフォルト値：無効

この設定では以下の値を指定できます：

有効。

ユニバーサルプリントクライアントはユニバーサルプリントサーバーへの接続に SSL/TLS を使用します。

無効。

ユニバーサルプリントクライアントはユニバーサルプリントサーバーへの接続に SSL/TLS を使用します。

SSL FIPS モード

この設定は、印刷データストリーム（CGP）接続でユニバーサルプリントクライアントが使用する SSL/TLS 暗号モジュールが FIPS モードで実行されるかを指定します。

デフォルト値：無効

この設定では以下の値を指定できます：

有効。

FIPS モードは有効になっています。

無効。

FIPS モードは無効になっています。

SSL プロトコルバージョン

この設定はユニバーサルプリントクライアントが使用する SSL/TLS プロトコルのバージョンを指定します。

デフォルト値：ALL

この設定では以下の値を指定できます：

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

TLSv1。

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL ユニバーサルプリントサーバー暗号化印刷データストリーム（**CGP**）ポート

この設定では、ユニバーサルプリントサーバー暗号化印刷データストリーム（CGP）ポートが使用する TCP ポート番号を指定します。このポートは印刷ジョブのデータを受信します。

デフォルト値：443

SSL ユニバーサルプリントサーバー暗号化 **Web** サービス（**HTTP/SOAP**）ポート

この設定では、ユニバーサルプリントサーバー暗号化 Web サービス（HTTPS/SOAP）ポートが使用する TCP ポート番号を指定します。このポートは印刷コマンドのデータを受信します。

デフォルト値：8443

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、Citrix Virtual Apps and Desktops 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。この設定を行うと、Citrix Virtual Apps and Desktops 上の VDA が変更されます。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、サーバーの一覧に重複するサーバー名が含まれていないか、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

April 24, 2021

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

April 24, 2021

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 Citrix Virtual Apps and Desktops 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

April 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。

このポリシーを表示するには、［複数のバージョン］を選択してシングルセッション OS バージョンの選択をオフにし、［サーバーの制限］を選択します。

> 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。Citrix ポリシー設定では、この Microsoft のダイアログボックスメッセージは制御されません。詳しくは、http://support.citrix.com/article/CTX118618を参照してください。

セッションの制限のポリシー設定

April 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、1,440 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、1,440 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せん。

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、1,440 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

April 24, 2021

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機能およびクライアントの自動再接続機能によって、ネットワークの中断からの回復後、ユーザーは Citrix Workspace アプリ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 Workspace アプリ 1808 以降および 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。

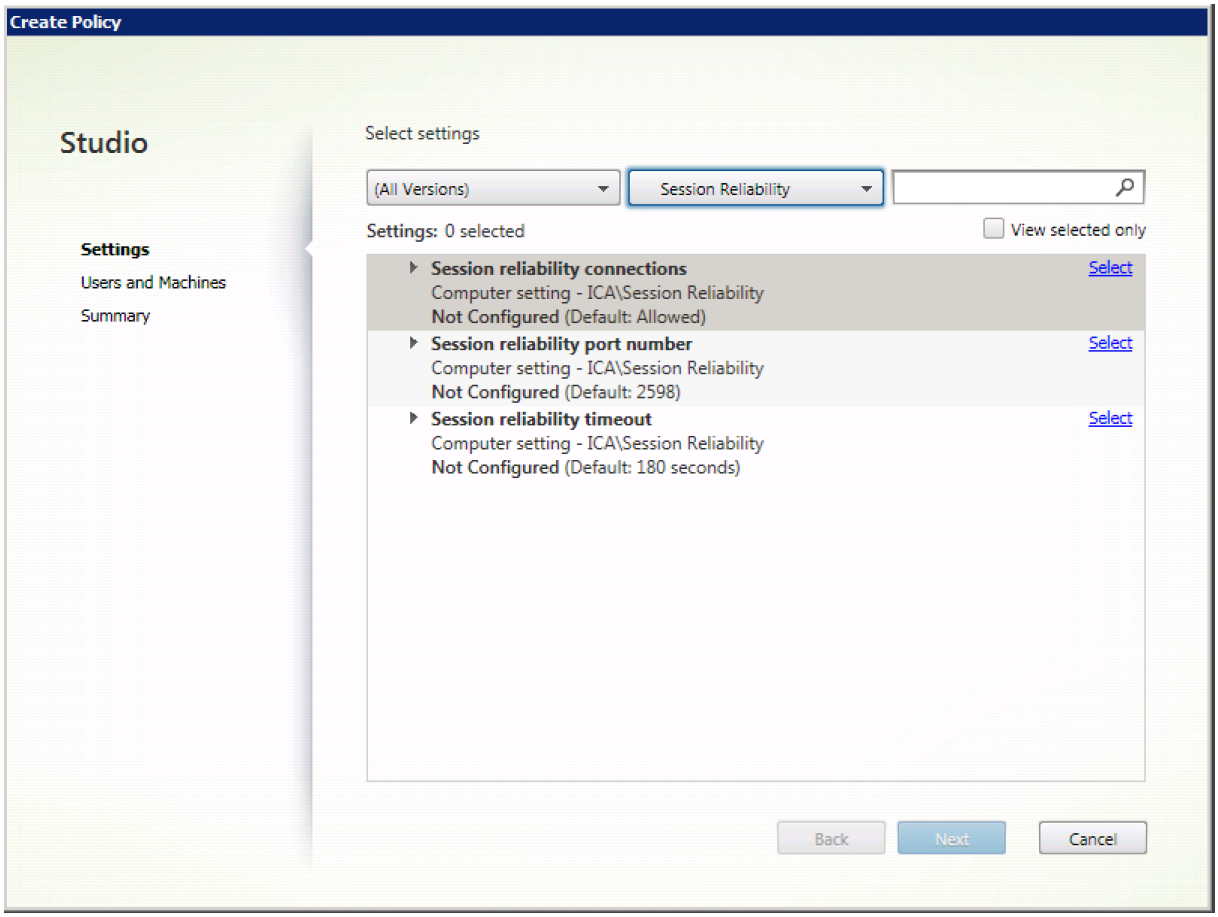
セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。接続が失われると、ユーザーの表示は不透明になります。中断中、ユーザーにはセッションが停止しているように見えることがあり、ネットワーク接続が回復するとアプリケーションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

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。

セッションウォーターマークのポリシー設定

April 24, 2021

［セッションウォーターマーク］セクションには、この機能を構成するためのポリシー設定が含まれています。
この機能を有効にすると、VDA マシンによるネットワーク帯域幅と CPU の使用率が大幅に上昇します。使用可能なハードウェアリソースに基づいて、選択した VDA マシンのセッションウォーターマークを構成することをお勧めします。

> 重要
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。ユーザーエクスペリエンスを向上させるためには、ウォーターマークのテキスト項目を 3 つ以上有効にしないようにしてください。

セッションウォーターマークを有効化

この設定を有効にすると、セッション画面に、セッション固有の情報を示す不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、これが有効になっているかどうかで異なります。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアント **IP** アドレスを含む

この設定を有効にすると、セッションで、現在のクライアント IP アドレスがウォーターマークとして表示されます。

デフォルトでは、［クライアント IP アドレスを含む］は無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式は、yyyy/mm/dd hh:mm です。表示される時間は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、［接続時間を含める］は無効になっています。

ログオンユーザー名を含む

この設定を有効にすると、セッションで、現在のログオンユーザー名がウォーターマークとして表示されます。表示形式は、USERNAME@DOMAINNAME です。ユーザー名は 20 文字までにすることをお勧めします。ユーザー名が 20 文字を超えている場合は、文字が極端に小さく表示されるか、一部が表示されず、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、[ログオンユーザー名を含む] は有効になっています。

VDA ホスト名を含む

この設定を有効にすると、セッションで、現在の ICA セッションの VDA ホスト名がウォーターマークとして表示されます。

デフォルトでは、[VDA ホスト名を含む] は有効になっています。

VDA の **IP** アドレスを含む

この設定を有効にすると、セッションで、現在の ICA セッションの VDA IP アドレスがウォーターマークとして表示されます。

デフォルトでは、[VDA の IP アドレスを含む] は無効になっています。

セッションウォーターマークスタイル

この設定は、1 つのウォーターマークテキストラベルを表示するか複数のラベルを表示するかを制御します。[値] ドロップダウンメニューで [複数] または [単一] を選択します。

[複数] の場合は、セッションに 5 つのウォーターマークラベルが表示されます。中央に 1 つ、隅に 4 つです。

[単一] の場合は、セッションの中央にウォーターマークラベルが 1 つ表示されます。

デフォルトでは、[セッションウォーターマークスタイル] は [複数] になっています。

ウォーターマークのカスタムテキスト

この設定では、セッションウォーターマークで表示するカスタムテキスト文字列（社名など）を指定します。空でない文字列を構成すると、ウォーターマークに、新しい行でそのテキストが表示され、有効になっているその他の情報が付け加えられます。
ウォーターマークのカスタムテキストの最大値は、25 文字の Unicode です。長い文字列を構成すると、25 文字に切り捨てられます。

デフォルトのテキストはありません。

ウォーターマークの透明度

ウォーターマークの不透明度を 0〜100 の範囲で指定できます。指定された値が大きいほど、ウォーターマークが不透明になります。

デフォルトでは、値は 17 です。

タイムゾーン制御のポリシー設定

April 24, 2021

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。

セッションの切断時またはログオフ時にデスクトップ **OS** のタイムゾーンを復元する

この設定は、ユーザーが切断またはログオフしたときに、シングルセッション OS VDA のタイムゾーン設定をコンピューターの元のタイムゾーンに復元するかどうかを指定します。この設定を有効にした場合、VDA はユーザーが切断またはログオフしたときにマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、［クライアントのタイムゾーンを使用する］に ［クライアントのローカルタイムゾーンを使用する］を設定します。

デフォルトでは、有効になっています。

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。選択できるオプションは、ユーザーセッションのタイムゾーン（サーバータイムゾーン）とユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

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。

この設定を反映するには、グループポリシーエディターで ［タイムゾーンのリダイレクトを許可する］設定を有効にします。この設定は、［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] > [デバイスとリソースのリダイレクト] にあります。

シングルセッション OS VDA をマルチセッション OS 上で実行している場合は、[すべてのユーザー] にローカルのユーザー権限 [タイムゾーンの変更] を設定します。このユーザー権限は、[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] > [**Windows** の設定] > [セキュリティの設定] > [ローカルポリシー] > [ユーザー権利の割り当て] にあります。

> 注:
>
> シングルセッション OS の場合は、[ユーザー権利の割り当て] の [タイムゾーンの変更] で [**Users**] を追加しますが、マルチセッション OS ではこの設定は行いません。マルチセッション OS では、次のグループポリシーでタイムゾーンを同期します: [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] > [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] > [タイムゾーンのリダイレクトを許可する]。このポリシーは、サーバーがマルチセッション OS VDA のリモートデスクトップセッションホストでない（インストール時に`/ServerVDI`コマンドを使用していない）場合は適用されません。マルチセッション OS では、設計上、デフォルトではユーザーにタイムゾーンを変更できるローカル権限は付与されません。

TWAIN デバイスのポリシー設定

April 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（%）

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

April 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、ホストは、そのデバイスが ［**USB** ポリシー］設定で許可されているかどうかをチェックします。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。遅延が大きい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。使用可能なモードの説明については、この記事の表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。スクリーンセーバーを無効にする手順については、このセクションの最後で説明しています。
- 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、Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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 では、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアが提供されています。http://www.wacom.com/を参照してください。
- 描画用タブレット。PCI/ACPI バス上の HID デバイスとして表示される特定の描画入力デバイスはサポートされていません。これらのデバイスは、Citrix Virtual Desktops セッション内でリダイレクトするクライアント上の USB ホストコントローラーに接続します。

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）
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. ［**Change**］を選択し、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 ［**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
PID	デバイス記述子の製品 ID
REL	デバイス記述子のリリース ID
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

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。
- 使用可能な 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 # 別のメーカーの別のフラッシュドライブ
- DENY: Class=08 subclass=05 # Mass Storage
- すべての USB デバイスを拒否する規則を作成するには、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。

USB デバイスの自動リダイレクトを構成する

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。

> 注:
>
> Citrix Receiver for Windows 4.2 では、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。以前のバージョンの Citrix Receiver for Windows では、デスクトップアプライアンスモードで動作しているか、仮想マシン（VM）ホストアプリケーションで実行している場合、USB デバイスが自動的にリダイレクトされます。

一部の USB デバイスはリダイレクトしない方が良い場合もあります。ユーザーは、USB デバイスリストから、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。USB デバイスのリスト表示とリダイレクトを禁止するには、クライアントエンドポイントまたは Virtual Desktop Agent（VDA）で DeviceRules を適用します。詳しくは、「管理ガイド」を参照してください。

> 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。

USB デバイスの自動リダイレクトのユーザー設定

ポリシー:

1. ローカルグループポリシーエディターを開き、[管理用テンプレート] **>** [**Citrix** コンポーネント] **>** [**Citrix Receiver**] **>** [クライアントデバイスをリモート処理します] **>** [一般的な **USB** のリモート処理] の順に選択します。
2. [新しい **USB** デバイス] を開いて [有効] を選択し、[**OK**] をクリックします。
3. [既存の **USB** デバイス] を開いて [有効] を選択し、[**OK**] をクリックします。

Citrix Receiver:

1. [**Citrix Receiver** 環境設定] **>** [接続] の順に選択します。
2. 次のオプションを選択します:
   - セッションが開始されると、自動的にデバイスに接続します
   - セッションの実行中に新しいデバイスが接続されると、自動的にデバイスに接続します
3. [**OK**] をクリックします。

レジストリキーとポリシーに対するすべての変更が、Windows クライアントデバイスに適用されます。

プレーン **USB** プリンターのリダイレクト

プレーン USB プリンターを利用する場合の最適な方法は、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を行うことです。デフォルトでは、プレーン USB プリンターは自動的にはリダイレクトされません。

プレーンプリンターはヒューリスティックスを使用して検出されるため、スキャン機能を備えた高度なプリンターなどを完全に動作させるには、USB サポートを使用してリダイレクトする必要のある場合があります。

プレーンプリンターを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は 0 です（自動リダイレクトは行われません）。この値を 0 より大きい任意の値にすると、USB サポートが有効になり、プレーン USB プリンターがリダイレクトされるようになります。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前: AutoRedirectAudio

種類: DWORD

データ：00000000

プレーンオーディオデバイスのリダイレクト

プレーンプリンターと同様に、ICA の専用オーディオ仮想チャネルを使用してプレーンオーディオデバイスから音声データすることで、ユーザーエクスペリエンスを最適化できます。ただし、一部の特殊なデバイスは、USB サポートを使用してリダイレクトする必要のある場合があります。どのデバイスがプレーンオーディオデバイスであるかは、ヒューリスティックスにより判別されます。

プレーンオーディオデバイスを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectAudio

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、USB サポートによりプレーン USB オーディオデバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectVideo

種類：DWORD

データ：00000000

プレーンストレージデバイス（大容量記憶装置デバイス）のリダイレクト

プレーンストレージデバイスでは、クライアントドライブマッピングなど、最適化も行える専用の仮想チャネルを使用することでユーザーエクスペリエンスを最適化できます。ただし、ファイルの単純な読み取りまたは書き込みだけでなく、CD/DVD の作成や暗号化済みファイルシステムデバイスへのアクセスなどの特殊な操作も行う場合には、汎用 USB サポートによりデバイスをリダイレクトする必要のある場合があります。

どのデバイスがプレーンストレージデバイスであるかは、ヒューリスティックスにより判別されます。プレーンストレージデバイスを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectStorage

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、汎用 USB サポートによりプレーン USB ストレージデバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectStorage

種類：DWORD

データ：00000000

> 注：
>
> 汎用 USB サポートを使用する場合、プレーンストレージデバイスへの読み取り専用アクセスを構成することはできませんが、CDM を使用する場合はこのアクセスを構成可能です。

ハードウェア暗号化機能付き **USB** フラッシュドライブのリダイレクト

一般的なハードウェア暗号化機能付き USB フラッシュドライブは、暗号化済みのストレージパーティションと、この暗号化済みパーティションのロック解除用ユーティリティが含まれるユーティリティパーティションで構成されています。USB フラッシュデバイスでは、クライアントドライブマッピング/動的サムドライブマッピングの専用 HDX 仮想チャネルを使用することで、ユーザーエクスペリエンスを最適化できます。このチャネルにより、最適化も行われます。

Windows 以外のクライアント（Linux クライアントなど）や、搭載されているローカル機能へのユーザーアクセスを顧客が制限（締め出し）しているクライアントでは、汎用 USB リダイレクトが必要になります。汎用 USB リダイレクトを使用すると、ハードウェア暗号化のないすべての USB ストレージデバイスを、シングルセッション OS VDA とマルチセッション OS VDA の両方にリダイレクトできます。

バージョン 7 1808 以前の Citrix Virtual Apps and Desktop では、ハードウェア暗号化機能付きの USB フラッシュドライブを、シングルセッション OS VDA セッションおよびマルチセッション OS VDA セッションへ簡単にリダイレクトすることはできませんでした。Citrix Virtual Apps and Desktops 7 1808 で実施された新しい機能強化により、汎用 USB リダイレクトを使用して、シングルセッション OS VDA セッションやマルチセッション OS VDA セッションにハードウェア暗号化機能のある USB フラッシュドライブをリダイレクトできるようになりました。
デバイスがリダイレクトされると、そのドライブはローカルクライアントに表示されません。このため、ドライブのロックを解除する必要がある場合は、セッション内で実行してください。この機能を使用するには、Windows 更新プログラム KB4074590 が必要です。

プレーン静止画デバイス（スキャナーおよびデジタルカメラ）

プレーン静止画デバイスでは、最適化も行える専用の仮想チャネル（TWAIN 仮想チャネルなど）を使用することでユーザーエクスペリエンスを最適化できます。これらのデバイスは、業界標準に準拠している必要があります。デバイスが業界標準に準拠していない場合、または当初の意図と異なる方法で使用されている場合、このデバイスを使用

する唯一の方法は汎用 USB リダイレクトです。どのデバイスがプレーン静止画デバイスであるかは、ヒューリスティックスにより判別されます。

プレーン静止画デバイスを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectImage

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、汎用 USB サポートによりプレーン USB 静止画デバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectImage

種類：DWORD

データ：00000000

デバイス固有の設定

Citrix で最適化可能なデバイス（プリンター、オーディオデバイス、ビデオデバイス、ストレージデバイス、静止画デバイス）を選択するためのヒューリスティックスでは、目的と一致しないデバイスが選択されることがあります。また、上記に記載のないデバイスについて、自動リダイレクトを制御する必要のある場合もあります。自動リダイレクトの制御は、デバイスごとに行うことができます。

たとえば、DemoTech 2,000 バーコードリーダーを、USB サポートによりリダイレクトする必要がないとします。この製品のベンダー ID は 12AB、製品 ID は 567B です。これらの 16 進数値は、デバイスマネージャーで確認できます。

このバーコードリーダーが自動リダイレクトされないようにするには、デバイス固有のレジストリキーを作成します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

値の名前：AutoRedirect

種類：DWORD

データ：00000000

値が 0 のため、デバイスは自動リダイレクトされません。ゼロ以外の値を指定すると、このデバイスは（ユーザー設定に応じて）自動リダイレクトの対象とみなされます。ベンダー ID と製品 ID の間には、スペース文字を 1 つ挿入します。

Active Directory ポリシーを使用して、この値をレジストリキーに設定することもできます。ポリシー以外により値が設定されている場合は、ポリシーで設定した値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

値の名前：AutoRedirect

種類：DWORD

データ：00000000

デバイス固有の AutoRedirect 設定は、上述した対象デバイスの幅が広い AutoRedirectXXX の値よりも優先されます。Citrix の最適化対象デバイスを選択するデフォルトのヒューリスティックスでは、デバイスが汎用デバイスであると誤解される場合があります。このため、自動リダイレクトが行われるようにするには、デバイス固有の AutoRedirect の値を 1 に設定します。

視覚表示のポリシー設定

April 26, 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。

この設定のデフォルト値は［中］です。

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 - イメージデータの画質を優先する必要がある場合には、［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。たとえば、品質の低下が許容されない X 線画像を表示する場合などに選択します。

動画のポリシー設定

April 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

April 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 Workspace アプリでサポートされていますが、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

April 24, 2021

[WebSocket] セクションには、仮想デスクトップおよびホストアプリケーションへの、HTML5 向け Citrix Workspace アプリを使用した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 Web 向け Citrix Workspace アプリ）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、Web 向け Citrix Workspace アプリのすべての 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 である必要があります。<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

April 24, 2021

負荷管理セクションには、Windows マルチセッション OS 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

April 26, 2021

[Profile Management] カテゴリには、Profile Management 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 のポリシー」を参照してください。

上級設定のポリシー設定

April 24, 2021

FSLogix プロファイルコンテナへのマルチセッションライトバックを有効にする

Profile Management は、FSLogix プロファイルコンテナのマルチセッションシナリオで変更を保存するソリューションを提供します。同じユーザーが異なるマシンで複数のセッションを開始すると、各セッションに加えられた変更は同期され FSLogix プロファイルコンテナに保存されます。マルチセッションライトバック機能は、[**FSLogix** プロファイルコンテナへのマルチセッションライトバックを有効にする] ポリシーを実装すると使用できます。ポリシーをここでまたは INI ファイルで構成しない場合、デフォルト値が使用されます。

ロックされたファイルにアクセスする場合の試行数

ロックされたファイルにアクセスする場合の試行数を設定します。

このポリシーが無効の場合は、デフォルト値の 5 回が使用されます。このポリシー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、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

一部の展開環境では、Index.dat ファイルでは参照されない余分なインターネット Cookie がそのまま残ります。ブラウズ実行後にファイルシステムに余分な Cookie が残ると、プロファイルが膨張化することとなります。このポリシーを有効にすると、Index.dat の処理が強制的に実行され、余分な Cookie が削除されます。このポリシーを有効にするとログオフに時間がかかるため、問題がある場合にのみ設定を有効にします。

このポリシー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、Index.dat の処理は実行されません。

自動構成を無効にする

Profile Management では、あらゆる Citrix Virtual Desktops 環境（Personal vDisk の存在など）が検査され、それに応じてグループポリシーが構成されます。調整されるのは［未構成］状態の Profile Management ポリシーのみなので、ユーザーによるカスタマイズは保持されます。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、Citrix Virtual Apps 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:

	マルチセッション OS	シングルセッション 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。

Profile Management 1909 以降、Windows 10（バージョン 1607 以降）および Windows Server 2016 以降の［スタート］メニューの操作性が向上しました。これは、次のポリシーの自動構成によって達成されました:

- 「Appdata\Local\Microsoft\Windows\Caches」および「Appdata\Local\Packages」を［ミラーリングするフォルダー］に追加します。
- 「Appdata\Local\Microsoft\Windows\UsrClass.Dat*」を［同期するファイル］に追加します。

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、環境が変わると自動構成が有効になって Profile Management 設定が変更されることがあります。

問題が発生する場合にユーザーをログオフ

このポリシーが無効、またはこれを構成しない場合、問題が発生すると（ユーザーストアが使用できないなど）、ユーザーに一時プロファイルが提供されます。このポリシーが有効な場合は、エラーメッセージが表示されて、ユーザーはログオフされます。この手順により、問題のトラブルシューティングが容易になります。

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。

カスタマーエクスペリエンス向上プログラム

カスタマーエクスペリエンス向上プログラムは、デフォルトで有効になっており、匿名の統計および使用状況情報を送信して、Citrix 製品の品質とパフォーマンスを向上させるために役立てます。

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。

Outlook で検索インデックスの移動を有効にする

Outlook 検索データをユーザープロファイルと一緒に自動的に移動することで、ユーザーベースの Outlook の検索エクスペリエンスを実現します。このためには、ユーザーストアに Outlook の検索インデックスを保存するための追加の領域が必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンする必要があります。

Outlook 検索インデックスデータベース–バックアップと復元

この設定では、[Outlook で検索インデックスの移動を有効にする] が有効になっている場合、ログオン時に Profile Management が実行する処理を構成します。

この設定を有効にすると、Profile Management は、データベースがログオン時に正常にマウントされるたびに、検索インデックスデータベースのバックアップを保存します。Profile Management は、バックアップを検索インデックスデータベースの完全な状態に近い正常なコピーとして扱います。データベースが破損したために検索インデックスデータベースのマウントが失敗すると、Profile Management は、検索インデックスデータベースを前回認識された正常なコピーに自動的に戻します。

注：Profile Management は、新しいバックアップが正常に保存された後に、以前に保存されたバックアップを削除します。バックアップは、VHDX ファイルの使用可能なストレージ領域を消費します。

基本設定のポリシー設定

April 24, 2021

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。

Profile Management の有効化

デフォルトでは、展開を促進するため、Profile Management はログオンまたはログオフを処理しません。必ずほかのすべてのセットアップタスクを実行し、環境内で Citrix ユーザープロファイルの実行をテストした後で、Profile Management を有効にします。

このポリシー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、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。

処理済みグループ

コンピューターのローカルグループとドメイングループ（ローカル、グローバル、およびユニバーサル）の両方を使用できます。ドメイングループは、次の形式で指定する必要があります：ドメイン名\グループ名。

ここでポリシーを構成しない場合は、Profile Management はユーザーグループのメンバーのみを処理します。このポリシーが無効な場合は、Profile Management はすべてのユーザーを処理します。このポリシー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、すべてのユーザーグループのメンバーが処理されます。

除外グループ

コンピューターのローカルグループとドメイングループ（ローカル、グローバル、およびユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。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。

ここでこの設定を構成する場合、これらのユーザーグループのメンバーが除外されます。この設定が無効な場合は、どのユーザーも除外されません。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。この設定をここでまたは INI ファイルで構成しない場合、どのグループのメンバーも除外されません。

ローカル管理者のログオン処理

BUILTIN\Administrators グループのメンバーのログオンが処理されるかどうかを指定します。Citrix Virtual Apps 環境など、このポリシーがマルチセッション OS で無効な場合、または構成されていない場合は、ローカル管理者ではなくドメインユーザーによるログオンが処理されたと Profile Management は推定します。シングルセッション OS（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンも処理されます。このポリシーにより、ローカル管理者権限があるドメインユーザー（通常は仮想デスクトップが割り当てられている Citrix Virtual Desktops ユーザー）は、すべての処理、ログオン、および Profile Management で問題があるデスクトップのトラブルシューティングをパイパスできます。

注：ドメインユーザーのログオンは、一般的には製品ライセンスに確実に準じるためグループのメンバーシップにより制限を受けることがあります。
このポリシーが無効の場合、Profile Management ではローカル管理者によるログオンは処理されません。このポ

リシー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、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリ変更および同期済みファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

以下のパスを設定できます:

- 相対パス。（Active Directory のユーザーの #homeDirectory# 属性として通常構成される）ホームディレクトリに相対する必要があります。
- 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。

次の種類の変数をこのポリシーに使用できます。

- パーセントで囲まれたシステム環境変数（%ProfVer% など）。システム環境変数には通常、追加のセットアップが必要です。
- 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、製品ドキュメントサイトの「Profile Management variables」を参照してください。

ユーザー環境変数は、%username% および%userdomain% を除いては使用できません。またカスタム属性を作成し、場所またはユーザーなどで組織変数を完全に定義することができます。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$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS!」と指定した場合、「\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64」に展開する可能性があります。

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、このファイルが\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile にある場合は、ユーザーストアのパスとして「\server\profiles$\JohnSmith.Finance\Win8x64」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。

ユーザーストアへのパスの指定での変数使用について詳しくは、次のトピックを参照してください:

- 複数のファイルサーバー上の Citrix ユーザープロファイルの共有
- 組織単位（OU）内および複数の OU 間でのプロファイルの管理
- Profile Management での高可用性と障害復旧

［ユーザーストアへのパス］が無効の場合は、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。

このポリシーが無効の場合は、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。このポリシー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、ホームドライブの Windows ディレクトリが使用されます。

ユーザーストアを移行する

ユーザー設定（レジストリ変更および同期ファイル）が以前に保存されていたフォルダーへのパス（以前に使用したユーザーストアのパス）を指定します。

この設定を構成すると、以前のユーザーストアに保存されたユーザー設定は、［ユーザーストアへのパス］ポリシー設定により指定される現在のユーザーストアに移行されます。

パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。

いずれの場合でも、次の種類の変数を使用できます：パーセント記号で囲まれたシステム環境変数と、ハッシュ記号で囲まれた Active Directory ユーザーオブジェクトの属性。

例：

- フォルダー`Windows\\%ProfileVer%`は、ユーザーストアの`Windows\W2K3`という名称のサブフォルダーにユーザー設定を保存します（W2K3 に解決されるシステム環境変数が%ProfileVer% の場合）。
- `\\server\share\##SAMAccountName##`は、UNC パス`\\server\share\<JohnSmith>`にユーザー設定を保存します（`##SAMAccountName##`が現在のユーザーの JohnSmith に解決される場合）。

パスには、%username% および%userdomain% 以外のユーザー環境変数を使用できます。

この設定が無効な場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.ini ファイルの対応する設定が使用されます。

この設定がここまたは.ini ファイルで構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更される（レジストリエントリ以外の）ファイルおよびフォルダーをセッション中にログオフする前にユーザーストアに同期できます。

このポリシー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、有効になります。

オフラインプロファイルサポート

このポリシーにより、プロファイルをできるだけ早い段階でユーザーストアと同期できます。これは、ラップトップコンピューターやモバイルデバイスを使ってローミングを実行するユーザーに向けた機能です。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はラップトップコンピューターまたはモバイルデバイス上にそ

のまま保持されます。モバイルユーザーが作業する際、プロファイルはローカルで更新されて、ネットワーク接続が再度確立されたらユーザーストアと同期されます。

このポリシー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、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

このポリシーを「アクティブライトバック」とともに使用します。変更されるレジストリエントリをセッション中にユーザーストアに同期できます。

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、アクティブライトバックレジストリは無効になります。

オフラインプロファイルサポート

オフラインプロファイル機能を有効にします。これは、一般的にネットワークから削除されるコンピューター（通常はサーバーやデスクトップではないノートブックやモバイルデバイス）を対象としています。

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、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。

クロスプラットフォームのポリシー設定

April 24, 2021

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の有効化

展開を簡素化するため、デフォルトではクロスプラットフォーム設定は無効になっています。この機能の計画とテストが完了した後後にのみ、このポリシーを有効にしてクロスプラットフォーム設定を有効にします。

このポリシー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、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ユーザーグループ

1 つ以上の Windows ユーザーグループを入力します。たとえば、このポリシーを使ってテストユーザーグループのプロファイルのみを処理するとします。このポリシーを構成すると、Profile Management のクロスプラットフォ

ーム設定機能によりこれらのユーザーグループのメンバーのみが処理されます。このポリシーが無効な場合、［処理済みグループ］ポリシーで指定されたユーザーのすべてが処理されます。

このポリシー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定義へのパス

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の場所です。このパスは、UNC パスである必要があります。ユーザーにはこの場所への読み取りアクセス権限、管理者には書き込みアクセス権限が必要です。この場所は、サーバーメッセージブロック（SMB）または Common Internet File System（CIFS）ファイル共有である必要があります。

このポリシー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、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

クロスプラットフォーム設定ストアへのパスを設定します。このフォルダーには、ユーザーのクロスプラットフォーム設定が保存されています。ユーザーには、このフォルダーに対する書き込みアクセス権限が必要です。パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。

この領域は、複数のプラットフォームにより共有されるプロファイルデータがあるユーザーストアの共有領域である必要があります。ユーザーには、このフォルダーに対する書き込みアクセス権限が必要です。パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。［ユーザーストアへのパス］と同じ変数を使用できます。

このポリシーが無効な場合は、パスに Windows\PM_CP が使用されます。このポリシー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、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

プラットフォームの OU でこのポリシーが有効な場合、基本プラットフォームとしてプラットフォームを指定します。このポリシーは、基本プラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

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。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使用してクロスプラットフォーム設定ストアをシード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。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、または単一のプラットフォームプロファイルのキャッシュデータを含んでいる場合、このポリシーを無効にしない限りは Profile Management が単一のプラットフォームプロファイルからストアにデータを移行します。

> 重要:
>
> このポリシーを複数の 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。
> デフォルトでは、このポリシーは有効になっています。

ファイルシステムのポリシー設定

April 24, 2021

［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

April 24, 2021

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 - ファイル

同期時に無視されるファイルの一覧。ファイル名は、ユーザープロファイル（%USERPROFILE%）に対する相対パスで指定する必要があります。ワイルドカードを使用でき、またこれは再帰的に適用されます。

例:

- 「デスクトップ\Desktop.ini」と指定した場合、デスクトップフォルダーの Desktop.ini ファイルは同期されません。
- 「%USERPROFILE%*.tmp」と指定した場合、プロファイル全体で.tmp 拡張子を持つすべてのファイルを無視します。
- 「AppData\Roaming\MyApp*.tmp」と指定した場合、プロファイルのある一部で.tmp 拡張子を持つすべてのファイルを無視します。

このポリシーが無効の場合、ファイルは除外されません。このポリシー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、ファイルは除外されません。

デフォルトの除外一覧の有効化 - ディレクトリ

同期時に無視されるディレクトリのデフォルトの一覧。このポリシーは、手動で記入しないで GPO 除外ディレクトリを指定するために使用します。

このポリシーを無効にすると、デフォルトで Profile Management は、いかなるディレクトリも除外しません。このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、デフォルトで Profile Management は、いかなるディレクトリも除外しません。

除外の一覧 - ディレクトリ

同期時に無視されるフォルダーの一覧。フォルダー名は、ユーザープロファイル（%USERPROFILE%）に対する相対パスで指定する必要があります。

例:

- 「Desktop」と指定した場合、ユーザープロファイルの Desktop フォルダーを無視します。

このポリシーが無効の場合、フォルダーは除外されません。このポリシー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、フォルダーは除外されません。

ログオン時の除外チェック

この設定は、ユーザーストアのプロファイルに除外されたファイルまたはフォルダーが含まれる場合に Profile Management がこれをどのように処理するかを構成します。

この設定を無効にするかデフォルト値の［ログオン時に除外されたファイルまたはフォルダーを同期］に設定すると、Profile Management はログオン時にユーザーストアの除外されたファイルまたはフォルダーをローカルプロファイルに同期します。

この設定を［ログオン時に除外されたファイルまたはフォルダーを無視］にすると、Profile Management はログオン時にユーザーストアの除外されたファイルまたはフォルダーを無視します。

この設定を［ログオン時に除外されたファイルまたはフォルダーを削除］にすると、Profile Management はログオン時にユーザーストアの除外されたファイルまたはフォルダーを削除します。

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。

この設定をここで構成しない、または INI ファイルからの値がない場合、除外されたファイルまたはフォルダーはログオン時にユーザーストアからローカルプロファイルに同期されます。

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

より快適にログオンしたり大きなサイズのファイルを処理したりするために、この一覧のファイルをコピーするのではなくシンボリックリンクが作成されます。

ポリシーでは、ファイルを参照するワイルドカードを使用できます。例：!ctx_localappdata!\Microsoft\Outlook*.OST。

Microsoft Outlook でオフラインフォルダーファイル（*.ost）を処理するために、Outlook フォルダーが Profile Management から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスできないことに注意してください。

同期のポリシー設定

April 24, 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

Profile Management は、プロファイルがインストールされたシステムおよびユーザーストア間で各ユーザーのプロファイル全体を同期します。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。

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。

このポリシーを無効にすると、これを有効にして空の一覧を構成するのと同じ結果になります。

このポリシー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、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

Profile Management は、プロファイルがインストールされたシステムおよびユーザーストア間で各ユーザーのプロファイル全体を同期します。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。

このポリシーを使用して除外フォルダーのファイルを含めることができます。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。ファイル名に対してのみ、ワイルドカードを使用できます。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。

このポリシーを無効にすると、これを有効にして空の一覧を構成するのと同じ結果になります。

このポリシー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、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

このポリシーは、（参照フォルダーとしても知られる）任意のトランザクションフォルダーが関連する問題の解決に役立ちます。このフォルダーには、あるファイルがほかのファイルを参照する相互依存ファイルが含まれています。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。このような状況では、最後の書き込みが優先されます。そのため、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ます。

たとえば、ユーザーがインターネットをブラウズする間に Index.dat がどのように Cookie を参照するかを考えます。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ます。したがって、Index.dat が最新の状態で維持されます。

このポリシー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。

プロファイルコンテナ

プロファイルコンテナは、プロファイルディスクに含めるフォルダーを指定できる VHDX ベースのプロファイルソリューションを提供します。プロファイルコンテナは、これらのフォルダーを含むプロファイルディスクを接続するため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナを使用するには、このポリシーを有効にし、フォルダーの相対パスを一覧に追加します。一覧には、大きなサイズのキャッシュファイルを含むフォルダーを含めることをお勧めします。たとえば、Citrix Files のコンテンツキャッシュフォルダーを一覧に追加します：`AppData\Local\Citrix\Citrix Files\PartCache`。

次の 2 つのシナリオに注意する必要があります：

- プロファイルコンテナは、複数のセッションによる同時アクセスをサポートしていません。
- プロファイルコンテナには、プロファイル全体を含むことはできません。

このポリシー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または INI ファイルで構成しない場合、無効になります。

フォルダーリダイレクトのポリシー設定

April 24, 2021

［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。

> 注:
>
> この設定により、ドメインに完全かつ無制限にアクセスできる管理者に権限が付与されます。

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

April 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

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

アドレス帳のリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

デスクトップのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

デスクトップのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ドキュメントのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ファイルを 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ダウンロードのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ダウンロードのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

お気に入りのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

お気に入りのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

リンクのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

リンクのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ミュージックのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ミュージックのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ピクチャのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ピクチャのリダイレクト設定

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

保存したゲームのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

保存したゲームパス

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

スタートメニューのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

スタートメニューパス

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

検索のポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

検索パス

この設定では、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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ビデオのポリシー設定

April 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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

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。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ログのポリシー設定

April 24, 2021

［ログ］カテゴリには、Profile Management のログ機能の構成に関するポリシー設定が含まれています。

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

April 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用に保持し、ユーザーストアから Citrix ユーザープロファイルをインポートします。

この設定をここで構成しない場合、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。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間での既存のアプリケーションプロファイルの自動移行を有効または無効にします。アプリケーションプロファイルには、AppData フォルダー内のアプリケーションデータと HKEY_CURRENT_USER\SOFTWARE のレジストリエントリの両方が含まれます。この設定は、アプリケーションプロファイルを異なるオペレーティングシステム間で移行する場合に役立ちます。

たとえば、オペレーティングシステム（OS）を Windows 10 バージョン 1803 から Windows 10 バージョン 1809 にアップグレードするとします。この設定を有効にすると、Profile Management は、各ユーザーの初回ログオン時に、既存のアプリケーション設定を Windows 10 バージョン 1809 に自動的に移行します。その結果、AppData フォルダー内のアプリケーションデータと HKEY_CURRENT_USER\SOFTWARE のレジストリエントリが移行されます。

既存のアプリケーションプロファイルが複数ある場合、Profile Management は、次の優先度に従って移行を実行します:

1. 同じ種類の OS のプロファイルから移行します（シングルセッション OS からシングルセッション OS またはマルチセッション OS からマルチセッション OS）。
2. 同じ Windows OS ファミリの OS のプロファイルから移行します（Windows 10 から Windows 10、Windows Server 2016 から Windows Server 2016 など）。
3. 以前の OS のプロファイルから移行します（Windows 7 から Windows 10、Windows Server 2012 から Windows 2016 など）。
4. 最も近い OS のプロファイルから移行します。

注：ユーザーストアパスに変数「!CTX_OSNAME!」を含めてオペレーティングシステムの短い名前を指定する必要があります。これによって、Profile Management が既存のアプリケーションプロファイルを見つけることができます。

この設定をここで構成しない場合、INI ファイルの設定が使用されます。

この設定をここで構成しない、または.ini ファイルからの設定がない場合、デフォルトで無効になります。

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

April 24, 2021

［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

ログオフ時に無視される HKEY_CURRENT_USER ハイブのレジストリキーの一覧です。

例：Software\Policies

このポリシーが無効の場合、レジストリキーは除外されません。このポリシー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、レジストリキーは除外されません。

包含の一覧

ログオフ時に処理される HKEY_CURRENT_USER ハイブのレジストリキーの一覧です。

例：Software\Adobe

このポリシーが有効な場合、この一覧のキーのみが処理されます。このポリシーが無効な場合、すべての HKEY_CURRENT_USER ハイブが処理されます。このポリシー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、すべての HKEY_CURRENT_USER ハイブが処理されます。

デフォルトの除外の一覧の有効化 **- Profile Management 5.5**

ユーザーのプロファイルに同期しない HKCU ハイブのレジストリキーのデフォルトの一覧。このポリシーは、手動で記入しないで GPO 除外ファイルを指定するために使用します。

このポリシーを無効にすると、デフォルトで Profile Management は、いかなるレジストリキーも除外しません。このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、デフォルトで Profile Management は、いかなるレジストリキーも除外しません。

NTUSER.DAT のバックアップ

破損の場合には、健全とわかっている最新の NTUSER.DAT のコピーのバックアップを有効化し、ロールバックします。

このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーム配信ユーザープロファイルのポリシー設定

April 26, 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、「ユーザープロファイルのストリーム配信」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。

ユーザー個人設定ポリシーの設定

April 26, 2021

Virtual Delivery Agent 内のユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します:

- ユーザーレイヤーにアクセスするネットワーク上の場所。
- 新しいユーザーレイヤーのディスクが拡大できるサイズ。

このために、次の 2 つのポリシーが利用可能なポリシーの一覧に表示されます:

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「server name or address\folder name」の形式でパスを入力します。
- ユーザーレイヤーサイズ（GB）- デフォルト値の 0 からユーザーレイヤーが拡大できる最大サイズ（GB）に変更します。デフォルト値を保持する場合、最大ユーザーレイヤーサイズは 10GB です。

> 注:
>
> ポリシーでユーザーレイヤーサイズを変更しても、既存のレイヤーのサイズは変更されません。

デフォルトのレイヤーサイズは 0 です。

詳しくは、「ユーザー個人設定レイヤー」を参照してください。

Virtual Delivery Agent のポリシー設定

April 24, 2021

[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

April 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

April 26, 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 およびディスク待ち時間のデータは、データベースに 1 時間間隔で適用されます。

CPU とメモリデータ

CPU とメモリデータは、デフォルトで ［有効］に設定されています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
5 分データ	1 日
10 分データ	7 日間
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］に設定されています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
時間単位のデータ	3 日
日単位のデータ	90 日間

上記のデータ保持設定では、1 つの VDA の CPU、メモリ、IOPS、およびディスク遅延のデータを 1 年間格納するのに約 276KB の容量が必要です。

マシン数	必要なストレージ
1	276KB
1,000	270MB
40,000	10.6GB

プロセスデータ

デフォルトでは、プロセスデータは無効になっています。プロセスデータは、必要に応じてマシンのサブセットで有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データの粒度	日数
10 分のデータ	1 日
時間単位のデータ	7 日間

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、マルチセッション OS 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。

シングルセッション **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、マルチセッション 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。シングルセッション OS 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っ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

April 24, 2021

> 重要:
>
> Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化（仮想 IP）がサポートされていないため、Windows 10 Enterprise マルチセッションでは、仮想 IP も仮想ループバックもサポートしていません。

［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。

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

April 26, 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、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

レジストリキー	説明	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

April 24, 2021

[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 で管理するマルチセッション 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。手動管理のシングルセッション 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 で管理するシングルセッション 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

April 26, 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。

仮想 IP および仮想ループバック

Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

Delivery Controller

この記事では、Controller をサイトに追加およびサイトから削除する場合の考慮事項と手順を説明します。また、Controller を別のゾーンやサイトに移動する方法、および VDA を別のサイトに移動する方法についても説明します。

Delivery Controller 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

April 26, 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。

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。

ここ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
Citrix Virtual Apps	Premium、Advanced、Standard	同時使用
Citrix Virtual Desktops	Premium、Advanced、Standard	ユーザー/デバイスおよび同時使用

詳しくは、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

以下の表に、Citrix Virtual Apps and Desktops、XenApp および XenDesktop 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。

最新リリース	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
2003	11.16.3.0 ビルド 28000	16.0.0.28000
1912	11.16.3.0 ビルド 28000	16.0.0.28000
1909	11.16.3.0 ビルド 28000	16.0.0.28000
1906	11.15.0.0 ビルド 24100	15.4.0.24100
1903	11.15.0.0 ビルド 24100	15.4.0.24100
1811	11.15.0.0 ビルド 24100	15.4.0.24100
1808	11.15.0.0 ビルド 24100	15.4.0.24100
7.18	11.15.0.0 ビルド 24100	15.4.0.24100

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 21103	14.2.0.21103
7.6 LTSR	11.14.0.1 ビルド 21103	14.2.0.21103

> 重要:
>
> 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。

ライセンス情報の表示

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。

製品の種類、ライセンスのエディション、ライセンスモデルなどのサイトのライセンス設定と、設定済みのライセンスサーバーが使用しているライセンスが一致するようにしてください。一致していない場合は既存のライセンスをダウンロードするか、または割り当てるかしてサイトのライセンス設定に合わせなければならない場合があります。

Citrix Studio を使ってライセンスをダウンロードしてインストールします

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、ライセンスの購入後または更新後にシトリックス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］を選択します。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。そのコードで他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の追加

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の変更

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の選択

- 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の変更

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。

ライセンス管理者の追加

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の変更またはライセンス管理者の削除

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の追加

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の変更またはライセンス管理者グループの削除

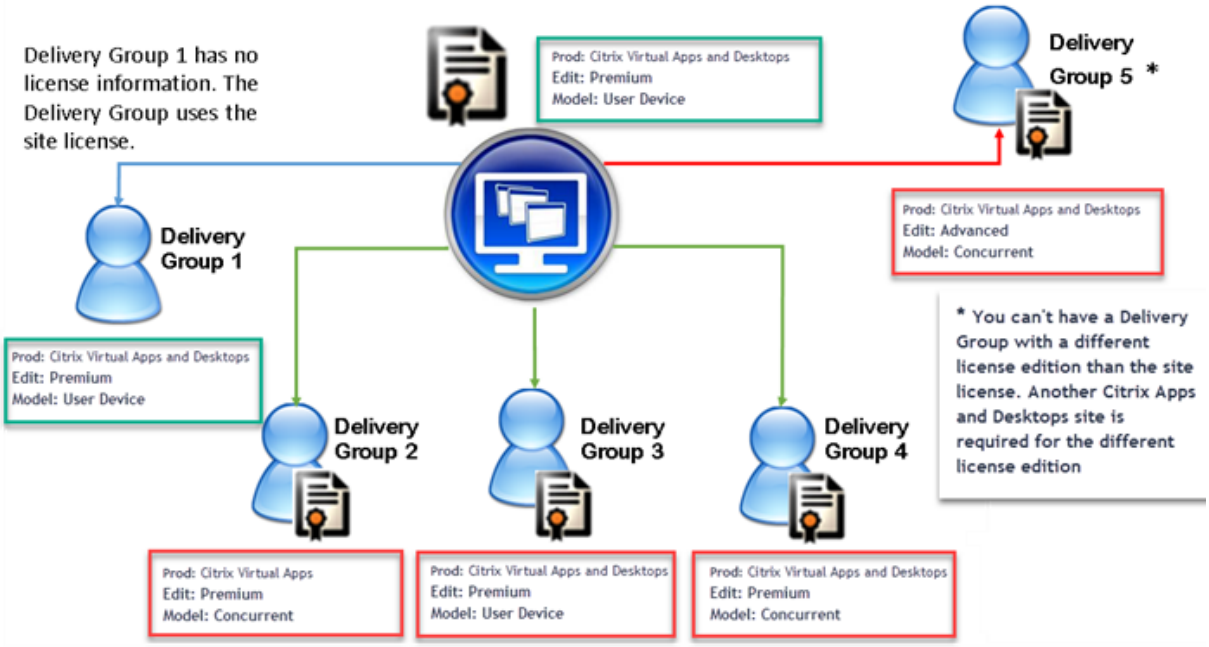
1. Studio のナビゲーションペインで ［構成］**>**［ライセンス］の順に選択します。
2. 中央ペインで［ライセンス管理者］タブを選択し、目的の管理者グループを選択します。
3. ［操作］ペインで、［ライセンス管理者グループの編集］または ［ライセンス管理者グループの削除］を選択します。

マルチタイプのライセンス

April 26, 2021

マルチタイプのライセンスでは、単一の Citrix Virtual Apps and Desktops 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 または MPS）とモデル（ユーザーデバイスまたは同時使用）の組み合わせのことです。デリバリーグループは、サイトレベルでの構成と同じ製品エディション（PLT/Premium または ENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops 展開のマルチタイプライセンスを構成する場合は、この記事の最後の「特殊考慮事項」に注意してください。

マルチタイプのライセンスが構成されていない場合は、個別の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。マルチタイプのライセンス構成時の重要な通知制限については、「特殊考慮事項」を参照してください。



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

カスタマーサクセスサービスの有効期間は、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カスタマーサクセスサービス有効期間は異なる場合があります。

ライセンスの互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を示しています。互換性の 4 つの列では、マルチタイプライセンスに互換性がある製品とライセンスモデルの組み合わせを指定します。たとえば、列 **1** の下に **X** があるすべての種類に互換性があります。CCU と CCS は同時ライセンスであり、UD はユーザー/デバイスライセンスです。

Old Name	New Name	Feature	Multi-type licensing compatibility 1	2	3	4
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
CSP - Citrix XenApp Base	Citrix Virtual Apps Base	XDT_ADV_UD		X		
CSP Premium	Citrix Virtual Apps and Desktops Premium	XDT_PLT_UD				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops - Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

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。

Name	値	制限事項
LicenseModel	グループのライセンスモデルを指定するパラメーター（同時使用またはユーザーデバイス）です。何も指定されていない場合、サイト全体のライセンスモデルが使用されます。	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。
ProductCode	グループのライセンス製品 ID を指定する XDT（Citrix Virtual Desktops の場合）または MPS（Citrix Virtual Apps の場合）のテキスト文字列です。何も指定されていない場合、サイト全体の製品コードが使用されます。	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。

LicenseModel および ProductCode について詳しくは、about_Broker_Licensingを参照してください。

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

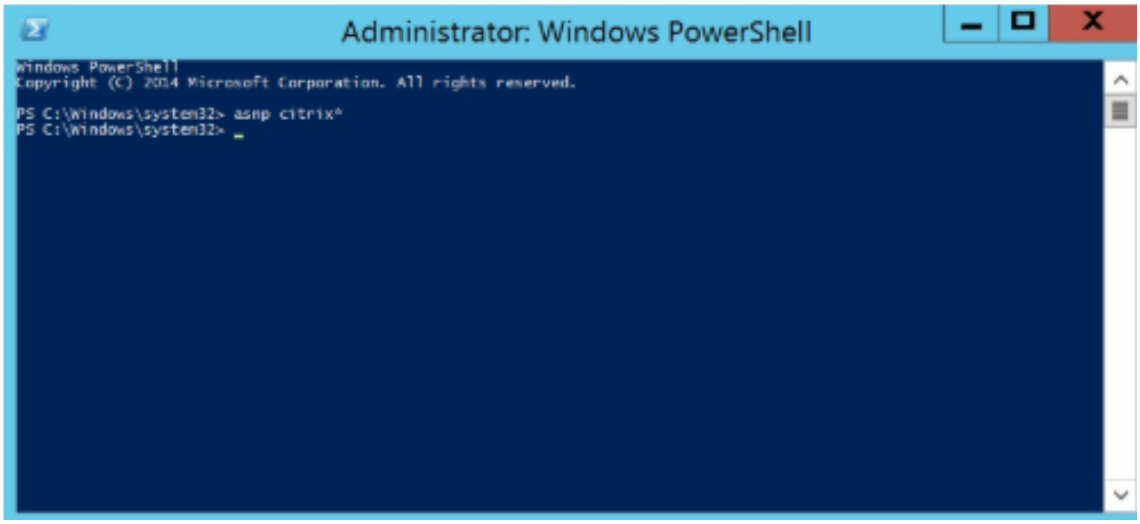
既存のブローカーデスクトップグループの有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

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。

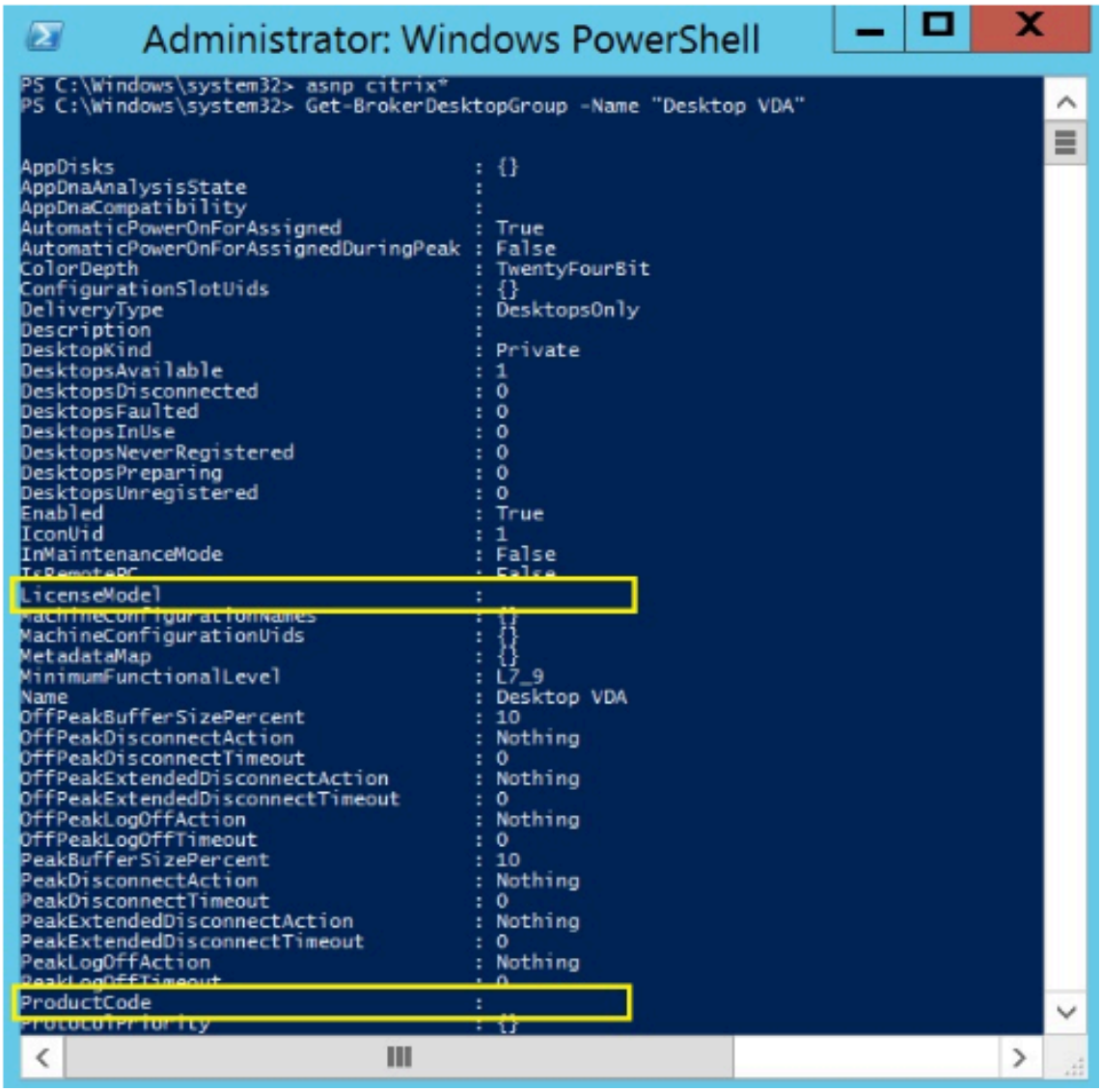
デリバリーグループごとに異なるライセンス製品とモデルを構成する

1. 管理者権限で PowerShell を開き、Citrix スナップインを追加します。

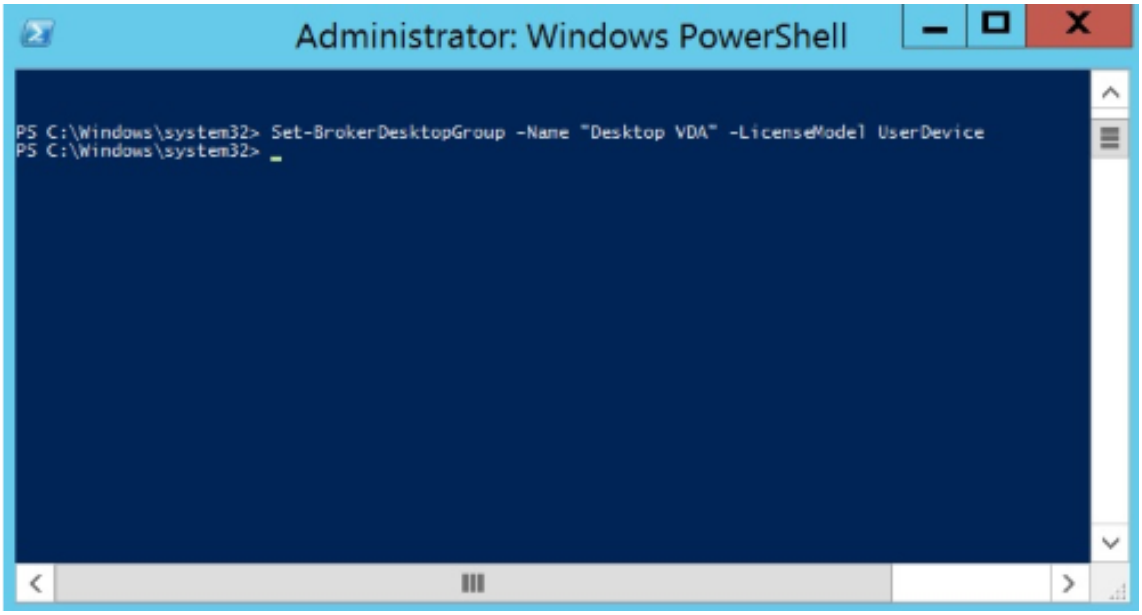


2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して最新のライセンス構成を表示します。パラメーター **LicenseModel** および **ProductCode** を参照します。これらのパラメーターを以前に構成してない場合、空白の可能性があります。

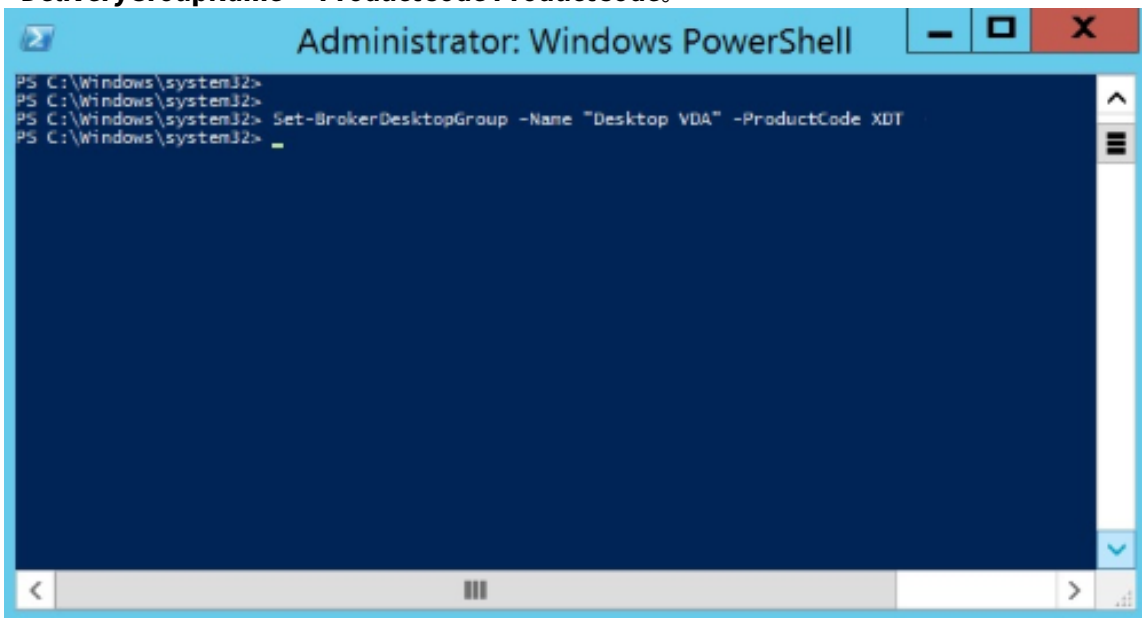
> 注:
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトの **Site level Site license** が適用されます。



3. 次のコマンドを実行してライセンスモデルを変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**。

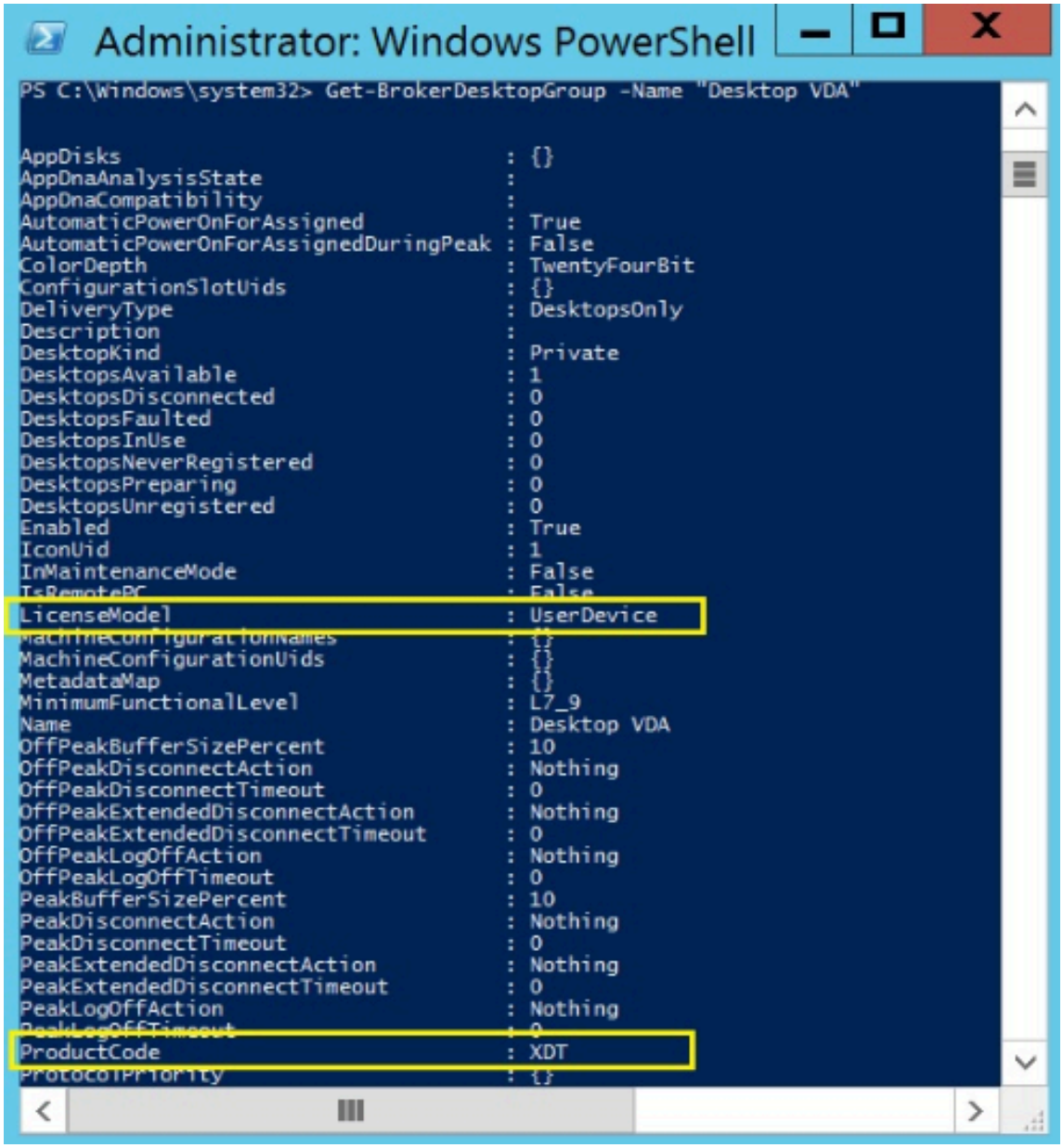


4. 次のコマンドを実行してライセンスモデルを変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



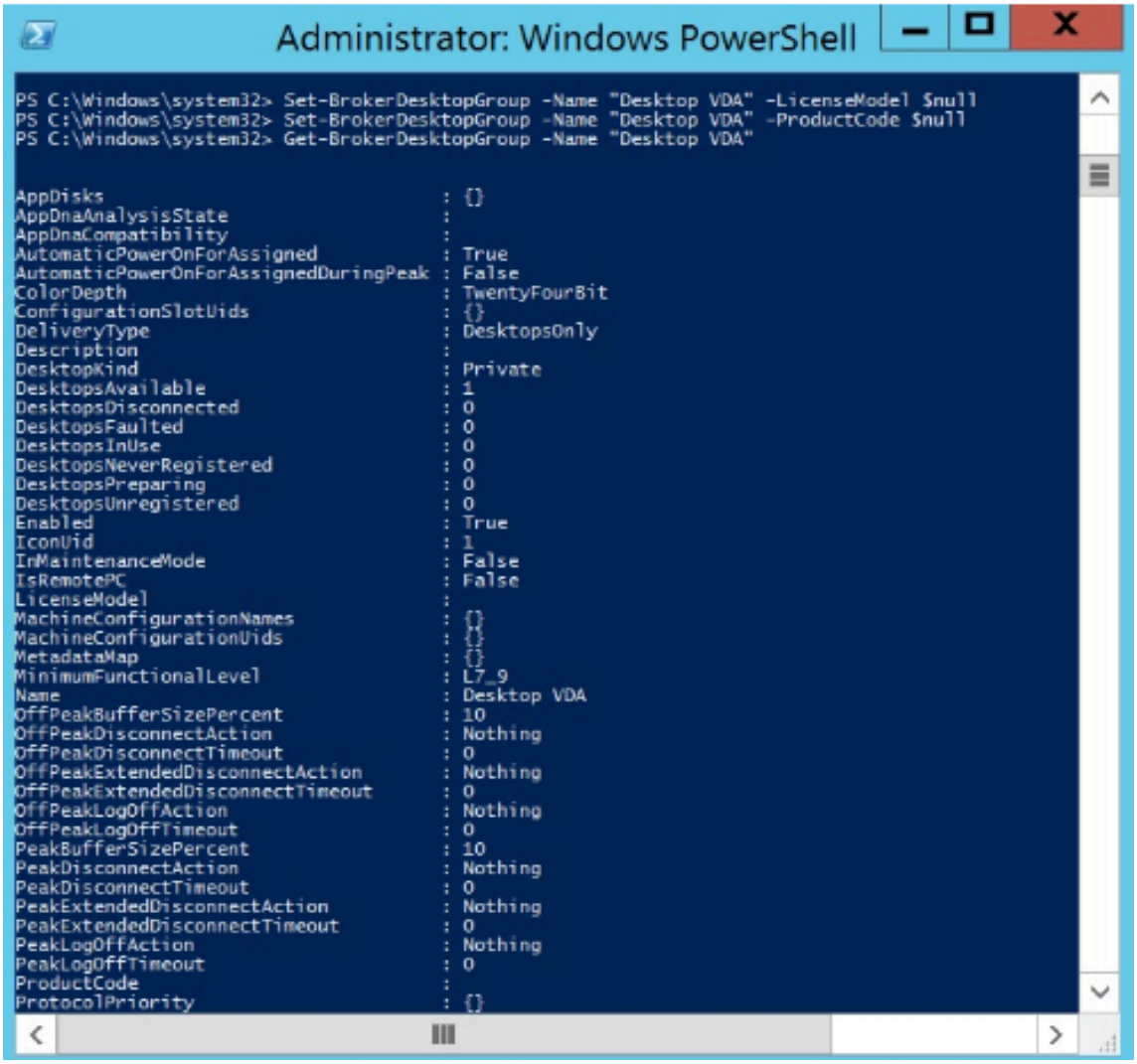
5. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力して変更を確認します。

> 注:
>
> 同じサイトで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。たとえば、Premium ライセンスと Advanced ライセンスなどの場合です。異なるエディションのライセンスがある場合は、複数のサイトが必要です。



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 コマンドレットの例では、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 Citrix Virtual Apps Premium 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 Citrix Virtual Desktops Premium 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 Citrix Virtual Desktops Premium 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 Citrix Virtual Apps and Desktops 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。

マルチタイプのライセンス用に構成されたデリバリーグループは、そのライセンスの種類のみを消費し、完全に消費したあとはサイト構成にフォールバックしません。

Citrix Virtual Apps Standard および Citrix Virtual Desktops Standard のライセンスエディション名は、どちらも Standard であることを示していますが、同じエディションではありません。マルチタイプのライセンスは、Citrix Virtual Apps Standard および Citrix Virtual Desktop Standard のライセンスでは機能しません。

ライセンスについてよく寄せられる質問

July 19, 2021

> 注:
>
> - 新型コロナウイルス（COVID-19）感染拡大に対応したビジネス継続性に関する情報については、CTX27055を参照してください。
> - ビジネス継続性の維持に関する一般的な情報については、ビジネスを継続。今すぐ始めるテレワークを参照してください。
> - 最新の Citrix ライセンスサーバーについて詳しくは、「ライセンス」を参照してください。

Citrix Virtual Apps and Desktops のライセンスはどのように割り当てられますか

Citrix Virtual Apps and Desktops のライセンスでは、ユーザー/デバイスモデルと同時使用ライセンスモデルが提供されています。

ユーザー/デバイス:

柔軟性の高いユーザー/デバイスモデルは、以下に適しています:

- エンタープライズ規模でのデスクトップの使用。
- 基盤となる Microsoft デスクトップ仮想化ライセンス。
- ユーザーが仮想デスクトップと仮想アプリにアクセスする頻度が低い顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスでは、ユーザーが仮想デスクトップと仮想アプリにアクセスできるデバイスの数に制限がありません。デバイスライセンスでは、1 台のデバイスから仮想デスクトップとアプリにアクセスできるユーザーの数に制限がありません。このアプローチは柔軟性を最大化し、Microsoft デスクトップ仮想化ライセンスに適しています。

> 重要:
>
> ユーザーまたはデバイスにライセンスを手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスによってライセンスが割り当てられます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは 90 日間非アクティブになるまで別のユーザーに割り当てることができません。

同時使用:

同時使用ライセンスでは、ユーザーおよびデバイスに対し、数に制限のない仮想アプリおよびデスクトップへの接続が 1 つ許可されます。ライセンスは、アクティブなセッション中にのみ使用されます。セッションが切断または終了している間、ライセンスはプールにチェックインされます。

ユーザー/デバイスライセンスについて詳しくは「ユーザー/デバイスライセンス」、同時使用ライセンスについて詳しくは「同時使用ライセンス」を参照してください。

ライセンスを購入する前に **Citrix Virtual Apps and Desktops** を試用できますか

はい。Citrix Virtual Apps and Desktops ソフトウェアをダウンロードして、試用モードで実行できます。試用モードでは、Citrix Virtual Apps and Desktops オンプレミスをライセンスなしで 30 日間、10 接続まで使用できます。

Citrix Cloud 用の Citrix Virtual Apps and Desktops Services は、承認に基づいて試用サービスを利用できます。詳しくは、Citrix の担当者にお問い合わせください。

Citrix では、**Citrix Virtual Apps and Desktops** の同時使用をどのように定義していますか

Citrix Virtual Apps and Desktops の同時使用モデルでは、ユーザーおよびデバイスに対し、数に制限のない仮想アプリおよびデスクトップへの接続が 1 つ許可されます。ライセンスは、アクティブなセッション中にのみ使用されます。セッションが切断または終了している間、ライセンスは再発行に備えてプールにチェックインされます。

Citrix では、ユーザー/デバイスライセンスモデルでユーザーにどのようにライセンスを割り当てますか

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーによってライセンスが一意のユーザー ID に割り当てられます。1 人のユーザーに対するデバイスと接続の数に関する制限はありません。デスクトップまたはデバイスに接続するユーザーには、仮想デスクトップまたはアプリケーションにアクセスするために 1 つのライセンスが割り当てられている必要があります。ライセンスサーバーまたはクラウドサービスによってライセンスが割り当てられます。

これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなくユーザーに割り当てられます。一度割り当てられたライセンスは、90 日間非アクティブになるまで別のユーザーに割り当てることができません。

Citrix では、ユーザー/デバイスライセンスモデルでライセンスが割り当てられたデバイスをどのように定義していますか

ライセンスが割り当てられたデバイスでは、一意のエンドポイントデバイス ID が必要です。ユーザー/デバイスモデルでは、デバイスとは Citrix Virtual Apps and Desktops のインスタンスにアクセスするために個人が使用を許可された機器を指します。共有デバイスの場合、1 つの Citrix Virtual Apps and Desktops ユーザー/デバイスライセンスが、デバイスを共有する複数のユーザーに適用されます。たとえば、共有デバイスにはクラスルームワークステーションや病院の臨床ワークステーションが含まれます。

Citrix Virtual Desktops Standard Edition の同時使用ライセンスをユーザー/デバイスモデルに変換できますか

Citrix Virtual Desktops Standard Edition の同時使用ライセンスを Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Edition のユーザー/デバイスモデルを Citrix Virtual Desktops Standard Edition の同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Edition の同時使用ライセンスを所有しており、ユーザー/デバイスライセンスモデルを希望する場合は、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードします。

ライセンス	Standard の同時接続	Standard のユーザー/デバイス	Advanced のユーザー/デバイス	Premium のユーザー/デバイス
Citrix Virtual Desktops Standard Edition の同時使用ライセンス	-	同時使用からユーザー/デバイスへの変換は不可	ライセンスモデルは変換できませんが、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードできます。	ライセンスモデルは変換できませんが、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードできます。

ライセンス	Standard の同時接続	Standard のユーザー/デバイス	Advanced のユーザー/デバイス	Premium のユーザー/デバイス
Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンス	ユーザー/デバイスから同時使用への変換は不可	-	-	-

同時使用ライセンスとユーザー/デバイスライセンスはどこが違いますか

同時使用ライセンスは、同時デバイス接続に基づいています。同時使用ライセンスは、デバイスでアクティブ接続が確立されている間にのみ使用されます。接続が終了すると、同時使用ライセンスはライセンスプールに戻ります。戻ったライセンスはすぐに使用できます。ライセンスの使用頻度が高くない場合は、このライセンスモデルをお勧めします。ユーザー/デバイスライセンスは一定期間リースされ、リースの期限が切れるまで他のユーザーは使用できません。

ユーザー/デバイスモデルで、同じ企業内のユーザーとデバイスの両方にライセンスを割り当てることはできますか

はい。1 つの企業内で 2 つのタイプを併用できます。ライセンスサーバーは、使用状況に基づいてライセンスをユーザーまたはデバイスに最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを割り当てるユーザーやデバイスの数はどのようにして決定しますか

ユースケースの要件を評価し、適切なライセンス数を決定します。ユーザー/デバイスライセンスでは、仮想デスクトップと仮想アプリの数にも、それらにアクセスできるデバイスの数にも制限がなく、無制限でアクセスできます。同時使用ライセンスでは、仮想デスクトップと仮想アプリの数に制限がなく、無制限でアクセスできます。アクセスできるデバイスは 1 つだけですが、デバイスを使用できるユーザーの数に制限はありません。下の式を考慮してください:

```
(Number of total users) - (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 - 700 + 300 = 600 licenses.
<!--NeedCopy-->
```


ユーザー/デバイスモデルでは、ライセンスが割り当てられたユーザーによる環境への接続に最大いくつのデバイスを使用できますか

ライセンスが割り当てられた各ユーザーが使用できる接続デバイスまたはオフラインデバイスの数に、制限はありません。

ユーザー/デバイスモデルでは、ライセンスが割り当てられたデバイスに最大何人のユーザーがアクセスできますか

ライセンスが割り当てられた各デバイスを使用できる組織内のユーザー数に制限はありません。

ユーザー/デバイスモデルでは、ライセンスが割り当てられたユーザーが最大いくつの仮想デスクトップまたは **Secure Browser Web** アプリケーションを同時に使用できますか

ライセンスが割り当てられた各ユーザーが接続できる仮想デスクトップや Web アプリケーションの数に、制限はありません。

ライセンスが割り当てられたユーザーは、最大でいくつの仮想アプリケーションを同時に使用できますか

ライセンスが割り当てられた各ユーザーが接続できる仮想アプリケーションの数に、制限はありません。

ライセンスが割り当てられたユーザーが組織を離れるとどうなりますか

ライセンスが割り当てられた既存ユーザーが組織を離れた場合、シトリックスに通知せずにそのユーザーのライセンスを解放できます。ライセンスの解放には、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、非アクティブの状態が 90 日続くと、ライセンスサーバーによってライセンスが自動的に解放されます。この情報は、EULA で指定された条件に準拠します。

ライセンスが割り当てられたユーザーが長期間不在にするとどうなりますか

ライセンスが割り当てられた既存ユーザーが長期間不在にする場合、シトリックスに通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、`udadmin`ユーティリティを使用します。

組織内でライセンスを割り当てたデバイスを交換するとどうなりますか

ライセンスが割り当てられた既存デバイスを交換する場合、シトリックスに通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、`udadmin`ユーティリティを使用します。

ライセンスを割り当てたデバイスが長期間使用できなくなった場合はどうなりますか

ライセンスが割り当てられた既存デバイスが長期間使用できなくなった場合、シトリックスに通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、udadminユーティリティを使用します。ライセンスを解放しない場合、非アクティブの状態が 90 日続くと、ライセンスサーバーによってライセンスが自動的に解放されます。この情報は、EULA で指定された条件に準拠します。

デバイスまたはユーザーにライセンスを割り当てた後、ユーザーライセンスとデバイスライセンスを切り替えることはできますか

はい。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてライセンスをユーザーまたはデバイスに割り当てます。使用パターンが変化した場合、新しい使用状況に基づき、ライセンスサーバーによって割り当てが切り替えられることがあります。ライセンスサーバーは、常に顧客にとっての経済性を最優先にしてライセンスを割り当てます。また、ライセンスサーバーはライセンスを監視し、90 日の割り当て期間後に未使用ライセンスを特定します。90 日の割り当て期間後に未使用として特定されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用モデルでは、**Citrix Virtual Apps and Desktops** のライセンスが割り当てられたユーザーが最大いくつの仮想デスクトップを同時に使用できますか

エンドポイントは多数のユーザーに対応でき、無制限の接続が可能です。

Citrix Virtual Apps and Desktops のライセンスを購入して、既存の **Citrix Virtual Apps and Desktops** 環境でより多くのユーザー/デバイスにライセンスを割り当てることができますか

はい。Citrix Virtual Apps and Desktops のライセンスを購入することで、既存の Citrix Virtual Apps and Desktops 環境でライセンスを割り当てるユーザー/デバイスの数を増やすことができます。

1 つのライセンスサーバーに、旧バージョンの **Citrix Virtual Apps and Desktops** の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時接続ライセンスを展開できますか

はい。引き続き同じライセンスサーバーを使用して、ユーザー/デバイスライセンスまたは同時使用ライセンスの環境に対応できます。

1 つのライセンスサーバーに、同時使用ライセンスとユーザー/デバイスライセンスまたは同時接続ライセンスを展開できますか**?**

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスの環境に対応できます。

1 つのライセンスサーバーに、複数のエディションの **Citrix Virtual Apps and Desktops** ライセンスを展開できますか

はい。ライセンスサーバーは、両方の Citrix Virtual Apps and Desktops のライセンスを同時に管理できます。最新バージョンのライセンスサーバーをインストールすることをお勧めします。ライセンスサーバーのバージョンが適正かどうかわからない場合は、シトリックスのダウンロードサイトにあるバージョン番号を参照して調べることができます。

1 つのサイトで **Citrix Virtual Apps** と **Citrix Virtual Apps and Desktops** の両方のライセンスを使用できますか

バージョンによっては、1 つの Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトでユーザー/デバイスと同時接続の両方のライセンスモデルに対応できます。1 つの Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトで対応できるエディションは、1 つのみです。詳しくは、「マルチタイプのライセンス」を参照してください。

複数のタイプのライセンスに対応するのは、XenApp および XenDesktop 7.15 長期サービスリリース（LTSR）および Citrix Virtual Apps and Desktops 7 1808 以上のバージョンです。

ライセンスサーバーに **Citrix Virtual Apps and Desktops** のユーザー/デバイスライセンスまたは **Citrix Virtual Apps and Desktops** の同時使用ライセンスがインストールされている場合、製品モデルとして **Citrix Virtual Apps** 同時使用を選択できますか

Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition の機能として Citrix Virtual Apps を使用する場合、Citrix Virtual Apps のライセンスモデルは Citrix Virtual Apps and Desktops の Advanced Edition または Premium Edition と同じになります。Citrix Virtual Apps and Desktops を購入した場合は、Citrix Virtual Apps の機能のみを使用する予定であっても、ライセンスを Citrix Virtual Apps and Desktops として構成します。Citrix Virtual Apps 同時使用スタンドアロンライセンスがライセンスサーバーにインストールされている場合にのみ、Citrix Virtual Apps を製品モデルとして選択します。

超過使用保護ライセンス

このセクションでは、超過使用保護ライセンスに関する質問に回答します。

超過使用保護ライセンスを取得するにはどうすればよいですか**?** ライセンスの超過使用保護は、すべてのユーザー/デバイスライセンスに含まれます。ユーザーまたはデバイスライセンスを購入すると、10% の超過使用保護を取得します。この超過使用保護は、購入済みライセンスと評価ライセンスをすべて割り当て終えたら利用できるようになります。超過使用保護機能は、ライセンス使用権には関係なく便宜上提供されています。超過使用保護ライセンスを頻繁に使用する場合は、追加のライセンスを購入することをお勧めします。

ライセンスの超過使用はどのようにして特定できますか**?** Citrix Licensing Manager で、超過使用のライセンス数を含む使用状況の情報を表示できます。Studio にも、超過使用情報が含まれています。

超過使用保護ライセンスが使用されるとどうなりますか?
ライセンスはインストールされたライセンスから割り当てられ、Citrix Virtual Apps and Desktops 環境へのアクセスが許可されます。この超過使用保護ライセンスでは、他のライセンスと同様のアクセス権と機能が提供されます。

超過使用保護ライセンスが使用された場合に、通知を受け取ることはできますか?
現時点では、超過使用保護ライセンスが使用されても特定の通知は送信されません。

超過使用保護ライセンスは何日間使用できますか?
超過使用保護ライセンスは、最初の使用から 30 日以内に購入していただく必要があります。

Citrix Virtual Apps と **Citrix Virtual Apps and Desktops** の各エディションにはどの製品コンポーネントが含まれていますか

エディション別の完全な機能マトリックスについては、「Citrix Virtual Apps and Desktops の機能」を参照してください。

Citrix Virtual Apps and Desktops のライセンス契約書に準拠して **Citrix Virtual Desktops** 環境のライセンスを取得するにはどうすればよいですか

Citrix Virtual Apps and Desktops のライセンス契約書に準拠し、ユーザー/デバイスライセンスモデルまたは同時使用ライセンスモデルで Citrix Virtual Apps and Desktops を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーによって、ライセンスのコンプライアンスが制御および監視されます。購入内容に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premium を購入するものの、Citrix Virtual Apps の機能のみを使用する場合は、コンプライアンスのため製品を Citrix Virtual Apps and Desktops に構成します。詳しくは「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps and Desktops のライセンス契約書に準拠して **Citrix Virtual Apps** 環境のライセンスを取得するにはどうすればよいですか

Citrix Virtual Apps のライセンス契約書に準拠し、同時使用ライセンスモデルで Citrix Virtual Apps を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーによって、ライセンスのコンプライアンスが制御および監視されます。

Citrix Virtual Apps and Desktops Advanced Edition および **Premium Edition** には、**Citrix Virtual Apps** の同時使用ライセンスが含まれていますか

Citrix Virtual Apps and Desktops Advanced Edition および Premium Edition のユーザー/デバイスライセンスには、互換性のみを目的として Citrix Virtual Apps の同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスとの互換性がない旧製品バージョンにのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、6.5 より前の XenApp バージョンと 5.0 Service Pack 1 より前の XenDesktop バージョンのみで許可されます。

ライセンスファイルを取得するにはどうすればよいですか

ライセンスアクセスコードをメールでお送りします。ライセンスアクセスコードを使用してライセンスファイルを生成するには、次の 3 つの方法があります:

- citirix.com の［マイアカウント］ページにある［ライセンスの管理］ツールボックス
- Citrix Studio における購入の割り当てと Citrix ライセンスサーバーへのライセンスファイルの自動インストール
- Citrix ライセンスサーバー内の Citrix Licensing Manager における購入の割り当てとライセンスファイルのインストール

詳しくは、Citrix ライセンスサーバードキュメントの「ライセンス」と Citrix Virtual Apps and Desktops ドキュメントの「ライセンス」を参照してください。

Citrix ライセンスサーバーはどの **TCP** ポートが使用されますか

- ライセンスサーバー：27000
- ベンダーデーモン：7279
- 管理コンソール Web ポート：8082
- Web Services for Licensing ポート：8083

Citrix ライセンスサーバーとは何ですか

Citrix ライセンスサーバーは、ネットワークを介したライセンスの共有を可能にするシステムです。詳しくは、「ライセンス処理の概要」を参照してください。

Citrix ライセンスサーバーを仮想化またはクラスター化できますか

はい。Citrix ライセンスサーバーは仮想化することも、クラスター化することもできます。詳しくは、「ライセンスサーバーのクラスター化」を参照してください。

Citrix ライセンスサーバーを仮想化すると、どのようなメリットがありますか

Citrix ライセンスサーバーを仮想化すると、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバーを切り替えることが可能になります。

Citrix ライセンスサーバーを仮想化する場合に考慮する必要がある制限はありますか

いいえ。

Citrix ライセンスサーバーでは、**Citrix Virtual Apps and Desktop** 環境のライセンスがすべて管理されますか

Citrix ライセンスサーバーは、Citrix Gateway で使用される Premium Edition のライセンスを除き、Citrix Virtual Apps and Desktops で受け取るすべてのライセンスを管理します。これらの Premium Edition のライセンスは、セキュリティ指向のネットワークデバイスで必要とされるネットワークアプライアンスに組み込まれたライセンスサーバーによって管理されます。

Citrix Licensing Manager とは何ですか

Citrix Licensing Manager がインストールされているライセンスサーバーからライセンスファイルをダウンロードし、割り当てることができます。Citrix Licensing Manager はライセンスサーバーの推奨管理手段であり、以下を実行できます:

- 短いコードを使用してライセンスサーバーを Citrix Cloud に登録でき、登録解除も簡単です。
- ユーザーアカウントとグループアカウントを構成します。
- ダッシュボードを使用して、インストールされたライセンス、使用中のライセンス、期限切れのライセンス、使用可能なライセンス、カスタマーサクセスサービス日を表示します。
- レポートで使用するため、ライセンス使用データをエクスポートします。
- 使用履歴データの保持期間を構成。デフォルトのデータ保有期間は 180 日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスファイルをライセンスサーバーに簡単にインストールできます。
- 追加猶予期間を有効または無効にする。
- カスタマーエクスペリエンス向上プログラム（CEIP）と Call Home を構成します。
- カスタマーサクセスサービス更新ライセンスを自動または手動で確認し、ライセンスが見つかると通知またはインストール。
- 次のライセンスサーバーの状態を通知 - 起動ライセンスの不足、時間の問題、アップローダの失敗。
- 以下のポートの変更:
  - ライセンスサーバー（デフォルトは 27000）
  - ベンダーデーモン（デフォルトは 7279）
  - Web Services For Licensing（デフォルトは 8083）

詳しくは、「Citrix Licensing Manager」を参照してください。

Citrix ライセンス管理コンソールとは何ですか

ライセンス管理コンソールは、Citrix インフラストラクチャのライセンスを管理できるインターフェイスです。また、ライセンス管理コンソールでは、ライセンスサーバーの設定を構成し、現在のライセンスの使用状況を表示することもできます。

ライセンスサーバーが Studio と同じドメインまたは信頼済みドメインにある場合、Studio を使用してライセンスを管理および追跡できます。

詳しくは、「ライセンス管理コンソール」を参照してください。

ライセンス割り当て期間とは何ですか

ライセンス割り当て期間は、Citrix Virtual Apps and Desktops ライセンスがユーザーまたはデバイスに割り当てられる期間です。デフォルトのライセンス割り当て期間は 90 日です。

付与されたユーザー/デバイスライセンスを解放するにはどうすればよいですか

付与されたユーザー/デバイスライセンスを解放するには、ライセンス契約書に従って`udadmin`ユーティリティを使用します。それにより、ライセンスサーバーによって該当する次のユーザー/デバイスにライセンスが割り当てられます。

組織が購入したライセンスの数を確認するにはどうすればよいですか

https://www.citrix.comの［マイアカウント］ページにある安全な［ライセンスの管理］ツールボックスで、購入したすべてのライセンスを 24 時間 365 日いつでもレビューでき、またそれらにアクセスできます。

特定の時点で使用されているライセンスの数を確認するにはどうすればよいですか

Citrix Licensing Manager、ライセンス管理コンソール、Studio では、ライセンスの使用に関する詳細がリアルタイムで提供されます。

購入したユーザー/デバイスライセンスの数を超えた場合はどうなりますか

ユーザー/デバイスライセンスでは、ライセンスが生成されるときに 10%の超過使用保護ライセンスも含まれます。超過使用保護ライセンスはインストール済みライセンス数に含まれます。使用の急増によって超過使用保護を含めたインストール数を超過した場合、これ以上のユーザーアクセスは拒否されます。追加のユーザーがアクセスできるようにするには、新しいライセンスを購入して展開する必要があります。

すべてのライセンス（超過使用保護分も含む）が使用されると、追加猶予期間で無制限のアクセスが許可されます。追加猶予期間中に、ユーザーの作業を中断させることなく最大ライセンス数を超過した原因を調査し、さらにライセンスを購入するかを検討することができます。追加猶予期間は、15 日経過するまで、または他の製品版ライセンスを追加するまで継続します。どちらか一方が発生した時点で終了します。詳しくは、「追加猶予期間」を参照してください。

Director は、猶予期間の状態を表示します。詳しくは、「Director のダッシュボードのパネル」を参照してください。

購入した同時使用ライセンス数を超えた場合はどうなりますか

すべてのライセンスが使用されると、追加猶予期間で無制限のアクセスが許可されます。追加猶予期間中に、ユーザーの作業を中断させることなく最大ライセンス数を超過した原因を調査し、さらにライセンスを購入するかを検討す

ることができます。追加猶予期間は、15 日経過するまで、または他の製品版ライセンスを追加するまで継続します。どちらか一方が発生した時点で終了します。詳しくは、「追加猶予期間」を参照してください。

Director は、猶予期間の状態を表示します。詳しくは、「Director のダッシュボードのパネル」を参照してください。

Citrix Virtual Apps and Desktops のサービスオプションである長期サービスリリース（**LTSR**）または最新リリース（**CR**）に関するライセンス要件はありますか

長期サービスリリースなどの Citrix Virtual Apps and Desktops のサービスオプションは、カスタマーサクセスサービスプログラムの特典です。LTSR の特典を受けるには、カスタマーサクセスサービスがアクティブである必要があります。詳しくは、「Citrix Virtual Apps、Citrix Virtual Apps and Desktops、Citrix Hypervisor のサービスオプション」を参照してください。

Secure Browser Standard Service のプール時間とはどのようなものですか

購入したサービスユーザーの数が 25 以上である場合、5,000 時間のサービス使用権が付与され、すべてのユーザーによって共有されます。後でユーザーの権利を追加購入しても、プール時間は追加で付与されません。サービス使用権の時間を増やすには、アドオンパックを購入する必要があります。

ライセンスサーバーの障害回復とメンテナンス

ライセンスサーバーの障害回復とメンテナンスについては、Citrix ライセンスサーバードキュメントの「障害回復とメンテナンス」を参照してください。

CCU ライセンスをリモート **PC** アクセスで使用することはできますか

はい。

リモート PC アクセスについて詳しくは、「リモート PC アクセス」を参照してください。

その他の製品固有のライセンス情報

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor
- Citrix ライセンスサーバー

アプリケーション

April 26, 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むように自分の権限を拡張してください。

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 Workspace アプリに同じ名前が 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。

詳しくは、次のページを参照してください：

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

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バージョン 7.9 以前の XenDesktop 7.x 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

実行できるアクションは次のとおりです:

- 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。

プロパティ	ページ
Citrix Workspace アプリでアプリケーションを表示するカテゴリ/フォルダー	配信
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を参照）	位置情報
アプリケーションを使用できるデリバリーグループおよびアプリケーショングループ	グループ
説明	識別
ファイル拡張子とファイルタイプの関連付け：アプリケーションが自動的に開く拡張子	ファイルタイプの関連付け
アイコン	配信
StoreFront 用のキーワード	識別
制限（「アプリケーション制限の設定」を参照）	配信

プロパティ	ページ
名前：ユーザーと管理者に表示される名前	識別
実行可能ファイルへのパス（「公開アプリケーションにパラメーターを渡す」を参照）	位置情報
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	配信
表示できるユーザー：Citrix Workspace アプリ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も起動可能です。非表示にすると同時に起動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	位置情報

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 Workspace アプリや 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。アプリケーション制限設定は複数あり、そのいずれかまたはすべてを構成できます：

- デリバリーグループのすべてのユーザーが実行でき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ユーザーごとに 1 つのアプリケーションインスタンス
- マシンごとの最大同時実行アプリケーションインスタンス数（PowerShell のみ）

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。複数の制限が構成されている場合、最初の制限に達するとエラーが報告されます。

アプリケーション制限の使用例

- 最大同時インスタンス数を制限する：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。
- ユーザーごとにアプリケーションインスタンスを **1** つのみに制限する：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。
- 最大同時インスタンス数を制限し、ユーザーごとにアプリケーションインスタンスを **1** つのみに制限する：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。
- マシンごとの最大同時インスタンス数の制限とタグによる制限を組み合わせる：アプリケーション Charlie には、特定のサーバーで同時に実行可能なインスタンス数、およびサイト内のすべてのサーバーで同時に実行可能なインスタンス数に関するライセンスとパフォーマンス上の要件があります。

  マシンごとアプリケーションインスタンス数に関する制限は、（指定したデリバリーグループ内のマシンだけでなく）サイト内のすべてのサーバーに影響します。たとえば、サイトに 3 つのサーバーがあるとします。アプリケーション Charlie の場合、マシンごとのアプリケーションインスタンス数の上限を 2 に設定します。このようにすると、サイト全体で起動できるアプリケーション Charlie のインスタンスは、6 個以下に制限されます（3 つのサーバーそれぞれでは、Charlie のインスタンスは 2 個までに制限されます）。

  （サイト全体のマシンすべてでのインスタンス数の制限に加えて）デリバリーグループ内の特定のマシンでのみアプリケーションを使用できるようにするには、それらのマシンにタグ付け機能を使用し、対象のアプリケーションについてマシンごとの最大インスタンス数制限を構成します。

アプリケーションインスタンスが Controller を介さない方法（Controller が停止モードの場合など）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。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとにインスタンス 1 つのみ制限を構成するには:

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、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. ［配信］ページで、次のいずれかのオプションを選択します。
   - 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
4. 変更を適用してダイアログボックスを閉じる場合は ［**OK**］をクリックし、変更を適用してダイアログボックスを開いたままにするには ［適用］をクリックします。

マシンごとの最大インスタンス数制限（PowerShell のみ）を構成するには:

- PowerShell（Citrix Cloud 環境の場合はリモート PowerShell SDK、オンプレミス環境の場合は Power-Shell SDK）で、MaxPerMachineInstances パラメーターを使用して適切な BrokerApplication コマンドレットを入力します。
- 詳しくは、Get-Help コマンドレットを使用してください。例:

```
Get-Help Set-BrokerApplication -Parameter MaxPerMachineInstances
```

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）には:「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: 目的のフォルダーを選択し、［操作］ペインで ［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。（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：目的のフォルダーを選択し、［操作］ペインで ［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：目的のフォルダーを選択し、［操作］ペインで ［フォルダーの削除］を選択します。アプリケーションや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：アプリケーションを 1 つまたは複数選択します。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、追加し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。

公開デスクトップ上のアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップで公開アプリケーションを起動する場合、そのデスクトップセッションでアプリケーションを起動するのか、同じデリバリーグループ内の公開アプリケーションとして起動するのかを制御できます。デフォルトでは、公開されたデスクトップセッションのアプリケーションが起動されます。この操作は、PowerShell（Citrix Cloud 環境の場合はリモート PowerShell SDK、オンプレミス環境の場合は PowerShell SDK）で変更できます。

New-Broker Application または Set-BrokerApplication コマンドレットで、LocalLaunchDisabled オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値は false です（-LocalLaunchDisabled $ false）。公開デスクトップ内で公開アプリケーションを起動すると、そのデスクトップセッションでアプリケーションが起動されます。

オプションの値を true に設定すると（-LocalLaunchDisabled $ true）、公開アプリケーションが起動します。この場合、公開されたデスクトップ（Windows 用 Citrix Workspace アプリを使用）で、公開アプリケーションとの別の追加セッションが作成されます。

要件および制限：

- このオプションは、同じ配信グループ内の公開デスクトップおよびアプリケーションにのみ適用されます。
- アプリケーションの ApplicationType 値は、HostedOnDesktop である必要があります。
- このオプションは、適切な PowerShell SDK でのみ使用できます。Studio のグラフィカルユーザーインターフェイスでは現在使用できません。
- このオプションを使用するには、最低でも StoreFront 3.14、Citrix Receiver for Windows 4.11、および Delivery Controller 7.17 が必要です。

ユニバーサル **Windows** プラットフォームアプリ

April 26, 2021

Windows 10 および Windows Server 2016 マシン上の Citrix Virtual Apps and Desktops では、VDA によりユニバーサル Windows プラットフォーム（UWP）アプリを使用できます。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 Citrix Virtual Apps and Desktops 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。

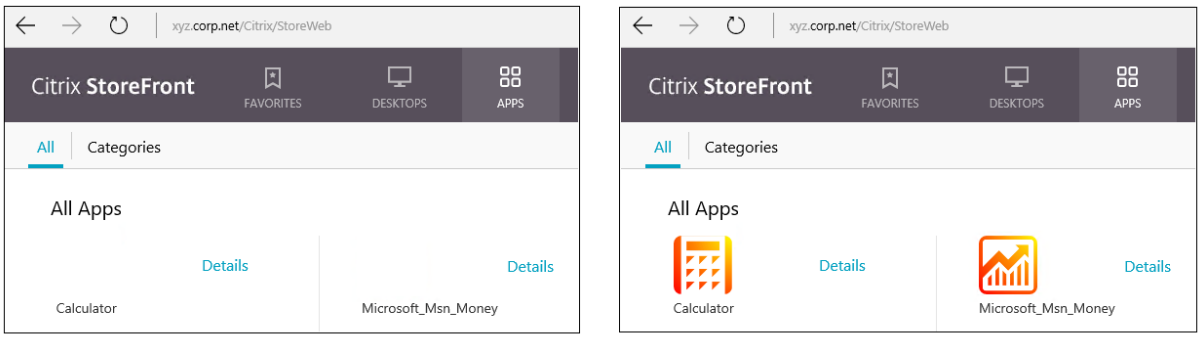
シームレスウィンドウまたは固定ウィンドウで起動された公開ユニバーサルアプリから正常にログオフすると、セッションが終了せずにユーザーがログオフしている状態になることがあります。このような場合は、セッションに残っ

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、「オフラインアプリの配布」を参照してください。

- アプリのサイドロード。詳しくは、「Windows 10 で LOB アプリをサイドロードする」を参照してください。

Citrix Virtual Apps または Citrix Virtual Desktops にユニバーサルアプリを 1 つ以上追加（公開）するには、次の手順を実行します:

1. 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。［アプリケーション］ページの ［追加］メニューで、[［スタート］メニューから］を選択します。
2. 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を選択します。
3. ウィザードを先に進めるか、編集ダイアログを閉じます。

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

April 26, 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 Citrix Virtual Apps 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、Citrix Virtual Apps サイトまたは Citrix Virtual Desktops 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。

ゾーンのネットワーク待機時間が 250 ミリ秒（RTT）を超える場合は、ゾーンではなくサイトを複数展開することをお勧めします。

このアーティクルを通じ、「ローカル」という用語は、対象となるゾーンを指しています。たとえば、「VDA はローカル Controller に登録されます」という場合、VDA が存在するゾーンの Controller に登録されることを意味します。

このリリースでのゾーンは、XenApp Version 6.5 以前と大きな違いはありませんが、同一ではありません。たとえば、このゾーン実装では、データコレクターが存在しません。サイトのすべての Controller が、プライマリゾーンの 1 つのサイトデータベースと通信します。また、このリリースではフェールオーバーおよび優先ゾーンの機能が異なります。

ゾーンの種類

1 つのサイトには、必ず 1 つのプライマリゾーンがあります。また、サイトにはオプションで 1 つまたは複数のサテライトゾーンを含めることもできます。サテライトゾーンは、障害回復、地理的に離れたデータセンター、支社、クラウド、またはクラウドのアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「プライマリ」です。これには、SQL Server サイトデータベース（および使用している場合は高可用性 SQL Server）、Studio、Director、Citrix StoreFront、Citrix ライセンスサーバー、および Citrix 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。

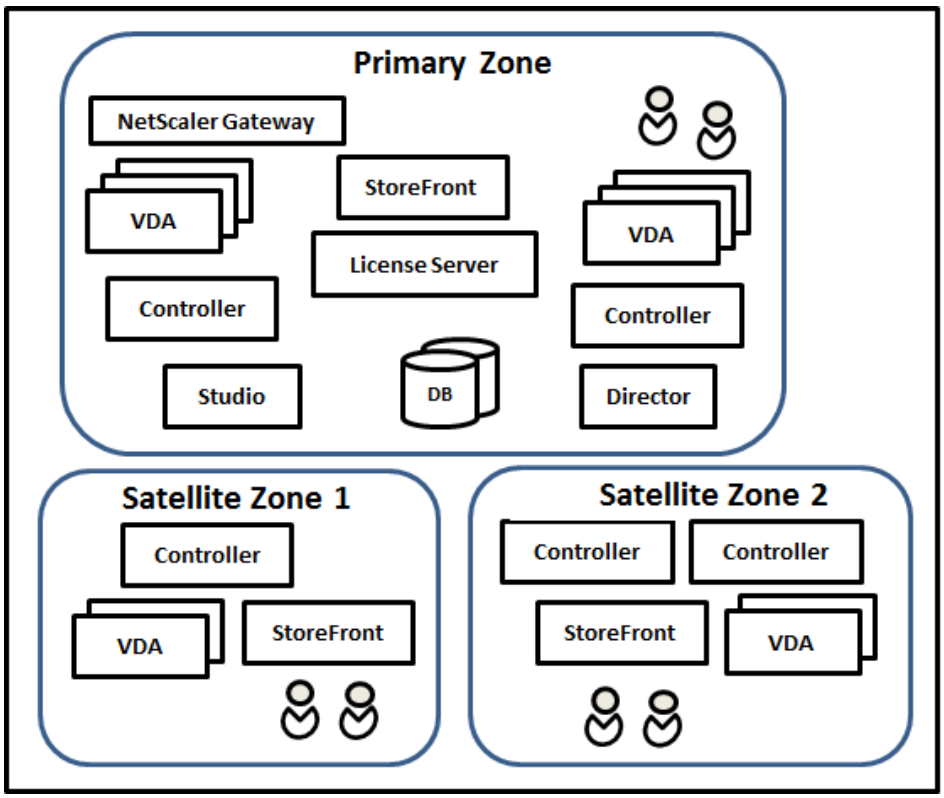
また、プライマリゾーンには、冗長性確保のために少なくとも 2 つの Controller が含まれている必要があります。また、データベースおよびインフラストラクチャと密結合されたアプリケーションを含む 1 つまたは複数の VDA が含まれる場合があります。

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 Citrix 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。



この図の内容は次のとおりです:

- プライマリゾーン: Controller が 2 つ、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 Citrix Gateway も含まれています。
- サテライトゾーン **1**（**VDA** と **Controller**）: サテライトゾーン 1 には、1 つの Controller、複数の VDA、1 つの 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。

  ローカルホストキャッシュ機能を使用すると、WAN で障害が発生した場合に、サテライトゾーン内の Controller がそのゾーン内の VDA への接続を引き続き仲介できるようになります。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** と冗長性用 **Controller**）: サテライトゾーン 2 には、2 つの Controller、複数の VDA、1 つの 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（カタログを別のゾーンに移動するときは、このゾーンと、関連付けられたホスト接続のあるゾーンとが正しく接続されていることを確認します。帯域幅が制限されているか遅延が長い場合は、ホスト接続を、関連付けられたマシンカタログを含む同じゾーンに移動します。

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

ゾーン優先度機能を使用するには、StoreFront 3.7 以上および Citrix 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、

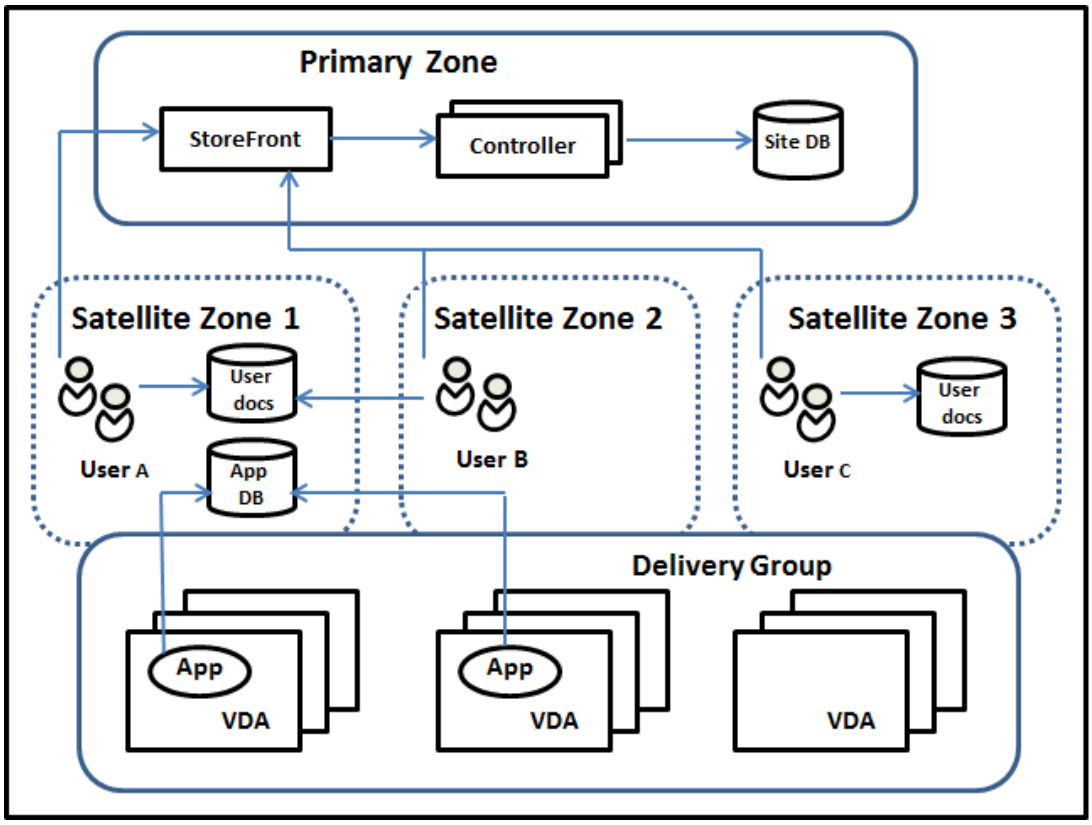
ゾーンの優先度機能によってより柔軟に制御できます。

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 Workspace アプリが実行されている）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 Workspace アプリエンドポイントを実行できる場所の数が示しています。ユーザー A はサテライトゾーン 1 で、Citrix Workspace アプリを搭載した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）。次の操作を実行できます：

- 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。この順序は調整可能です。「ゾーン優先度の調整」を参照してください。ユーザーがアプリケーションを起動すると、優先ゾーンは次のように選択されます：

- 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 Workspace アプリ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 Workspace アプリを実行中の）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、デバイス接続で経由されている Citrix Gateway により、エンドポイントデバイス上の Citrix Workspace アプリが検出される必要があります。Citrix Gateway 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が使用される場合、カタログと接続の両方が同じゾーンに含まれている必要があります。（ただし、遅延が少ない高帯域幅接続を利用可能な場合は、異なるゾーンに存在できます。）
- 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。
  - Citrix 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、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 Citrix 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、初期段階ではプライマリゾーンにはコントローラのみが含まれます。マシンカタログとデリバリーグループグループの作成前または作成後に、サテライトゾーンを作成することができます）。
- 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 Citrix 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：ゾーン優先度機能を使用するには、StoreFront 3.7 以上および Citrix 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。

Citrix Provisioning を使用する場合：このリリースに付属する Citrix Provisioning 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、Citrix Provisioning 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（Citrix Provisioning 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の作成、アプリケーショングループの作成、または既存のグループへのアプリケーションの追加を行う場合は、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

April 26, 2021

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2003 の場合、最新リリースは次のホストで VDA をサポートしません:
>
> - Amazon Web Services（AWS 上の VMWare Cloud を含む）
> - CloudPlatform（元の Citrix ソフトウェアプラットフォームを参照）
> - Microsoft Azure（Azure Resource Manager および Azure Classic を含む）
>
> 詳しくは、「最新リリースのホストサポートの変更点」を参照してください。

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、Citrix Virtual Apps や Citrix Virtual Desktops 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のホストや、仮想マシンのプロビジョニングを行うことができます。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 Azure Resource Manager**:
  - Microsoft Azure Resource Manager 仮想化環境の記事
  - Microsoft 社のドキュメント
- アマゾンウェブサービス（**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。接続にはリージョン、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、および資格情報を含めます。
  - **role_based_auth** をアクセスキーおよび秘密キーフィールドの値として入力し、AWS ホスト接続で IAM ロールを使用するように構成します。Citrix で必要なポリシーとアクセス許可を定義する IAM ロ

ールを、AWS でホストされる Delivery Controller または Cloud Connector インスタンスに付与する必要があります。
  - AWS コンソールから取得するルート AWS アカウント用の資格情報ファイルでは、標準的な AWS ユーザーのものとは異なる形式が使用されています。このため、このファイルを Studio で使用して **API** キーと秘密キーの情報を入力することはできません。AWS IAM 形式の資格情報ファイルを使用してください。

- **Citrix Hypervisor**（旧称 **XenServer**）:
  - Citrix Hypervisor 仮想化環境。
  - Citrix Hypervisor ドキュメント。
- **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:
- **Microsoft Hyper-V**:
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事
  - Microsoft 社のドキュメント
- **Microsoft Azure**（**Classic**）:
  - このホストタイプは廃止済みです。
  - Microsoft Azure 仮想化環境の記事
  - Microsoft 社のドキュメント
- **CloudPlatform**:
  - このホストタイプは廃止済みです。
  - 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。

ホストストレージ

ストレージ製品は、サポートされているハイパーバイザーで管理される場合にサポートされます。Citrix サポートでは、これらのストレージ製品ベンダーによる問題のトラブルシューティングと解決をサポートし、必要に応じて Knowledge Center でそれらの問題をドキュメント化します。

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には、1 つまたは複数の Windows Server 2012 クラスターストレージボリューム（接続されたストレージありまたはなし）、ストレージベンダーからのアプライアンスなどがあります。中央ストレージには、ハイパーバイザーのストレージ制御パスやパートナープラグインからの直接アクセスなど、独自の最適化が備わっていることもあります。

一時データをローカルに保存することにより、共有ストレージへのアクセスでネットワークを経由する必要がなくなります。さらに、共有ストレージデバイスの負荷（IOPS）も軽減されます。共有ストレージは費用が高いため、ローカルにデータを保存することによってコストを抑えられます。こうした利点は、ハイパーバイザーサーバー上で十分なストレージを使用できることよりも重要になるでしょう。

接続の作成時、ストレージをハイパーバイザー間で共有するか、またはストレージをハイパーバイザーのローカルに配置する 2 つのストレージ管理方法からいずれかを選択してください。

1 つまたは複数の Citrix Hypervisor 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、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。この方法では、永続性や共有ストレージ内のデータほどの復元性は必要ありません。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。たとえば、Citrix Hypervisor では IntelliCache を使用できます。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

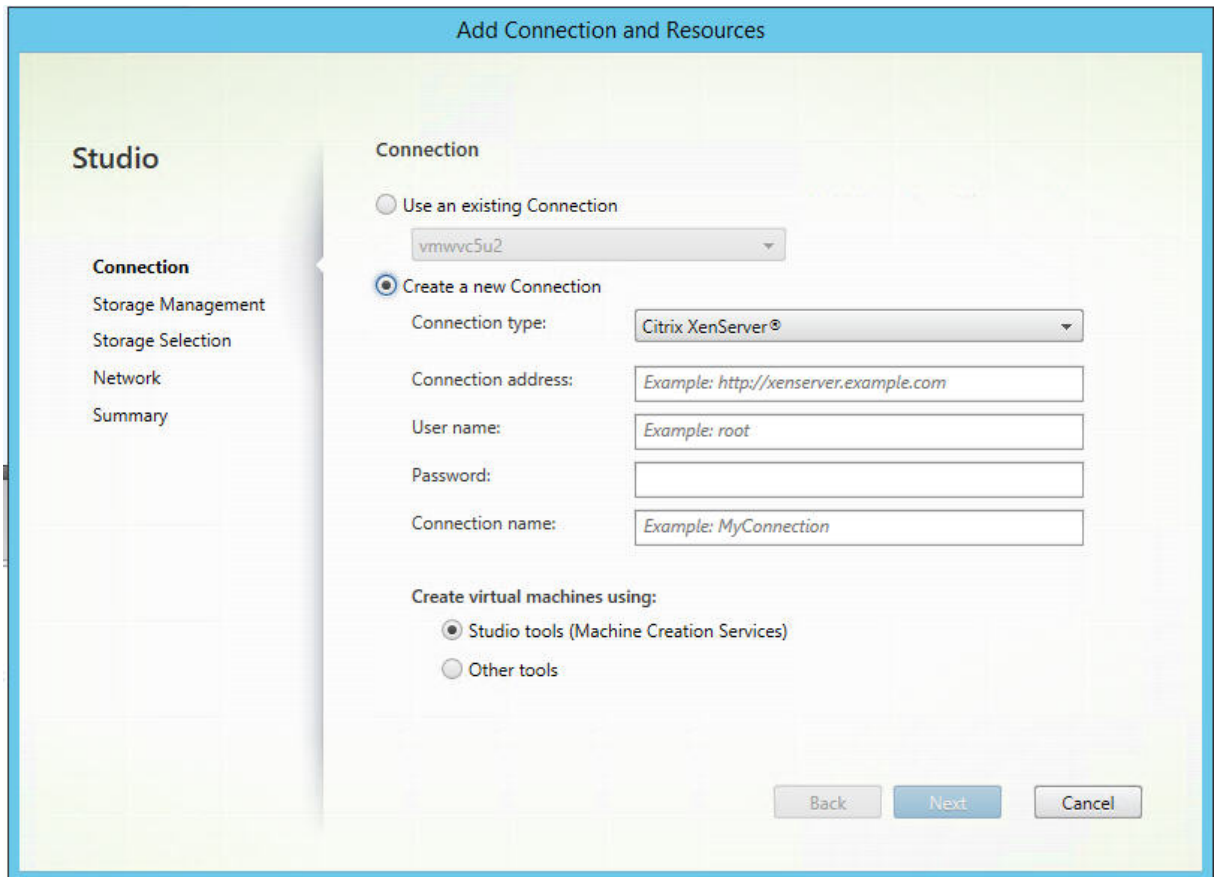
管理者は、サイトを作成するときに、オプションで最初の接続を作成できます。サイト作成ウィザードには、［接続］、［ストレージの管理］、［ストレージの選択］、［ネットワーク］といった接続関連のページがあります。

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。

1. Studio の ［ナビゲーション］ペインで ［構成］ **>** ［ホスト］の順に選択します。
2. ［操作］ペインの ［接続およびリソースの追加］を選択します。
3. 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。

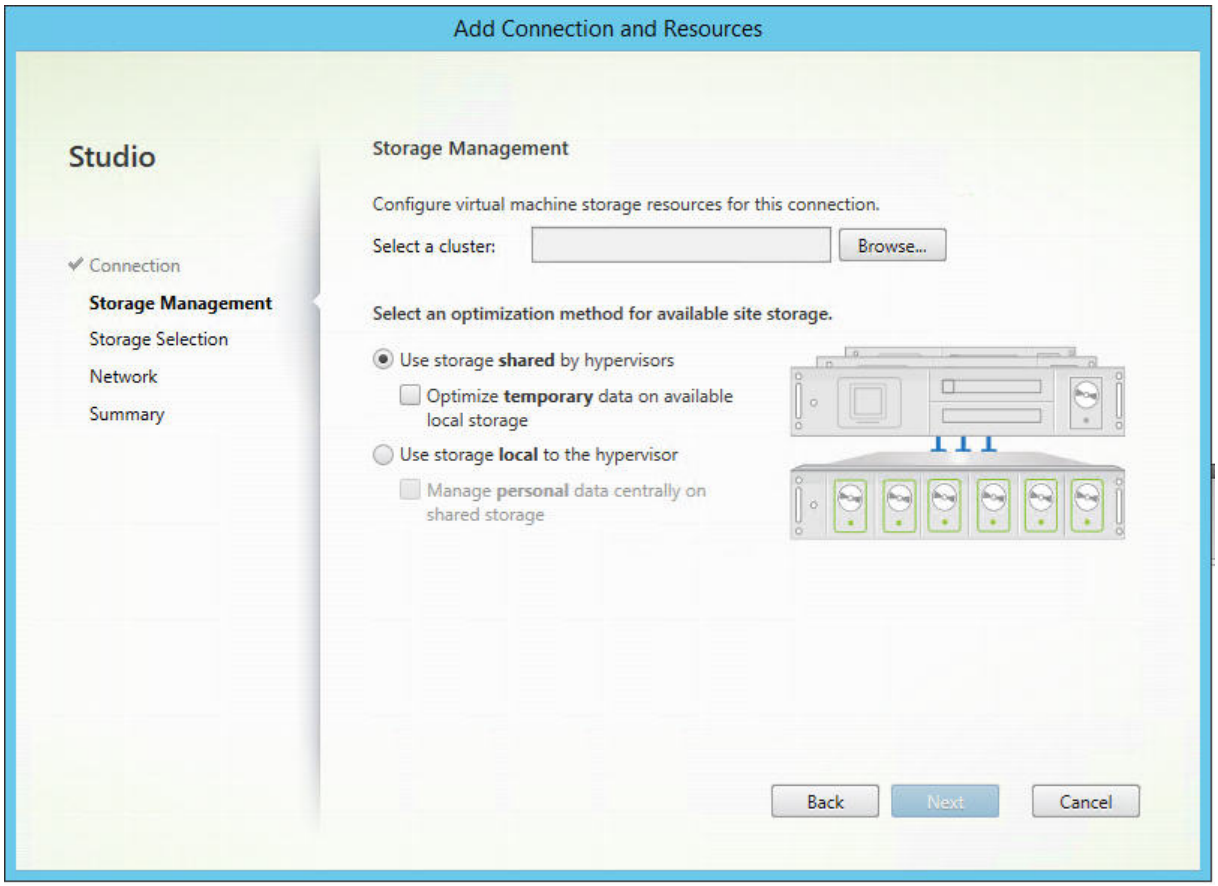
接続



［接続］ページで以下を実行します：

- 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 Citrix Provisioning 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。

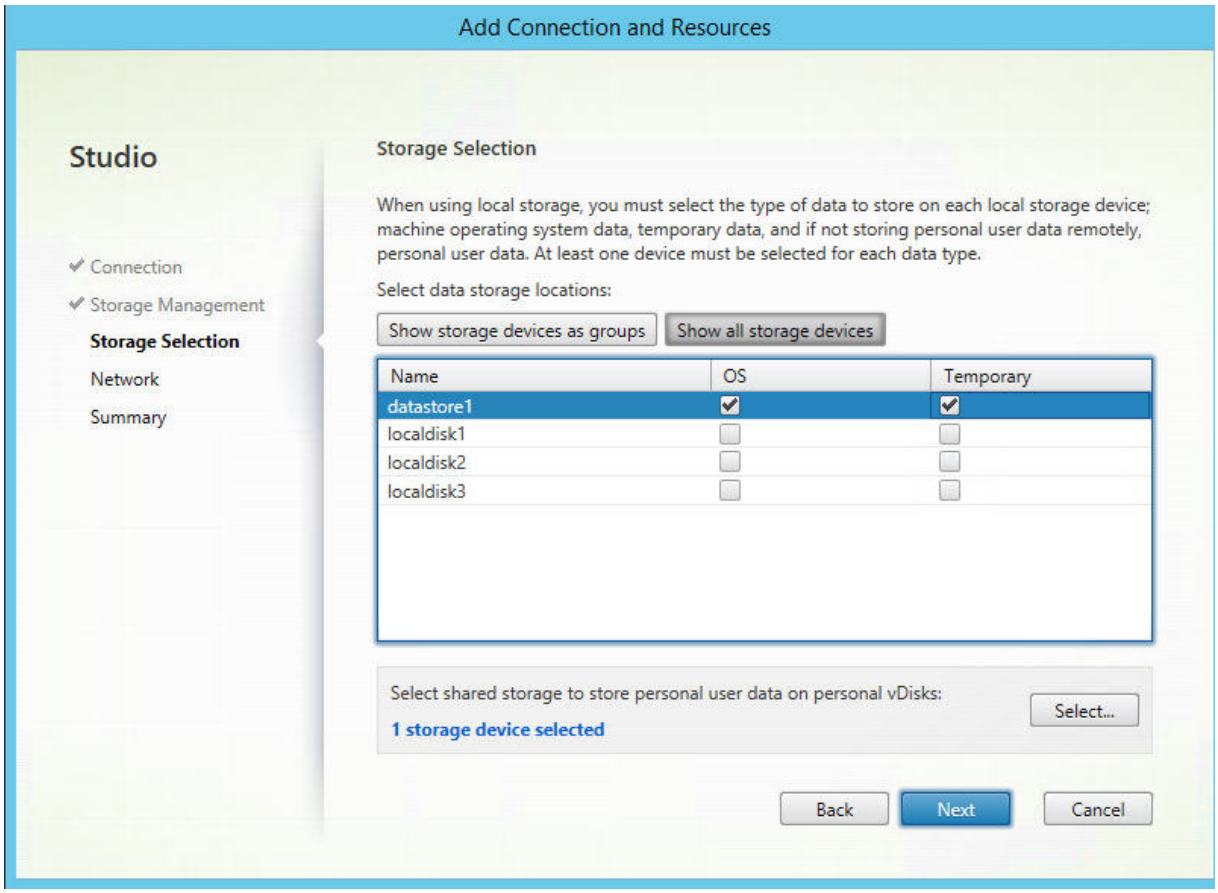
Hyper-V または VMware ホストに対する接続を構成している場合は、クラスター名を参照してから選択します。他の接続の種類では、クラスター名は要求されません。

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。

Citrix Hypervisor のプール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。「Citrix Hypervisor 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] ページ下部には他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

［ネットワーク］ページで、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

［概要］ページで、選択した内容を確認します。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。接続の作成

1. Studio の ［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。
2. 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。
- Citrix Hypervisor 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 Citrix Hypervisor 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が必要です。実際に適用される制限は、いずれか値の小さい方になります。

  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。
- ［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か、ドキュメントで明示的に指示を受け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

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ません。

操作（アクション）	説明
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。

操作（アクション）	説明
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で使用するマシンカタログからは削除されません。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなります。また、そのマシンはマシンカタログから削除されます。マシンを削除する前に、必要なユーザーデータをすべてバックアップしておいてください。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。

マシンのシャットダウンを伴う操作でマシンが 10 分以内にシャットダウンしない場合、電源が切れ、強制的にシャットダウンされます。シャットダウン中に Windows が更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

ストレージの編集

接続を使用する仮想マシンのオペレーティングシステムデータ、一時データ、および個人（PvD）データの保存に使用されているサーバーの状態を表示できます。データの種類それぞれの保存に使用するサーバーを指定することもできます。

1. Studio の ［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。

2. 接続を選択し、［操作］ペインの ［ストレージの編集］を選択します。
3. 左ペインでデータの種類（オペレーティングシステムデータ、Personal vDisk データ、一時データ）を選択します。
4. 選択したデータの種類に対し、1 つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
5. ［**OK**］をクリックします。

一覧の各ストレージデバイスには、デバイス名とストレージの状態が表示されます。有効なストレージの状態の値は次のとおりです。

- 使用中：ストレージは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、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］。

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。

トラブルシューティング

このセクションの情報を使用して、ホストの接続に関連する問題をトラブルシューティングします。

ホスティングリソースに **AWS EC2** の **URL** を追加する際に発生するアクセスキーエラー

Citrix Studio の ［ホストノード］画面で、ホスティング接続として AWS EC2 を追加し、**API** キー、秘密キー、接続名を指定すると SSL エラーが発生します。「**API** キーと秘密キーの組み合わせが正しくありません。入力内容を確認してください。」というエラーメッセージが表示されます。

この問題の原因は次のようなものです:

- 外部ネットワークへの接続にプロキシサーバーを使用。
- 接続先がAmazon AWS サーバーの URL とは異なる EC2 接続を使用。

Studio の ［ホストノード］画面では、EC2 接続のデフォルトのアドレス文字列は`https://ec2.amazonaws.com`のようにハードコードされています。このアドレス文字列はエンドポイントのグローバル URL を表します。AWS サービスがエンドポイントの URL を指定の URL にルーティングできない場合、アクセスキー（アクセスキー ID やシークレットアクセスキーを含む）が正しいことを確認できません。

この問題を解決するには、別の URL を使用する EC 接続を追加するか、プロキシサーバーを使用したインターネット接続を使用します。また、Citrix Studio は使わずに、次のように PowerShell を使用して手作業で EC2 ホスティング接続を作成します:

1. DDC ホストから PowerShell を起動し、`asnp Citrix`コマンドを使用してすべてのシトリックスモジュールを読み込みます。
2. プロキシサーバーとそのポートを環境変数に設定します:

```
$server = "<PROXY_SERVER>"
$port = "<PROXY_SERVER_PORT>"
$options = "ProxyHost=$server,ProxyPort=$port"
<!--NeedCopy-->
```

以下のコマンドを実行して、EC2 ホスティング接続を追加します:

```
$hyp= New-Item -Path xdhyp:\Connections -AdminAddress "localhost" -Name
      “AWSEC2”  -ConnectionType "AWS" -HypervisorAddress @[AWS URL](
    https://<AWS_URL>) -UserName "APIkey" -Password "Secret key" -
    Metadata @{
  "Citrix_MachineManagement_Options" = $options  }
  -Persist
<!--NeedCopy-->
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $hyp.
   HypervisorConnectionUid
<!--NeedCopy-->
```


Citrix Studio を起動し、ホスト接続を確認して AWS EC2 サイトが正しく生成されることを確認します。

ローカルホストキャッシュ

April 26, 2021

Citrix Virtual Apps and Desktops 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（SQL Server のサポートされる高可用性機能については、「データベース」を参照してください）。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：Local Host Cache）機能を使用すると、停止状態が発生しても、サイトの接続仲介操作を続行できます。オンプレミスの Citrix 環境で 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。

XenApp および XenDesktop 7.16 より、接続リース機能（以前のリリースでの高可用性機能）は削除され、使用できなくなりました。

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：

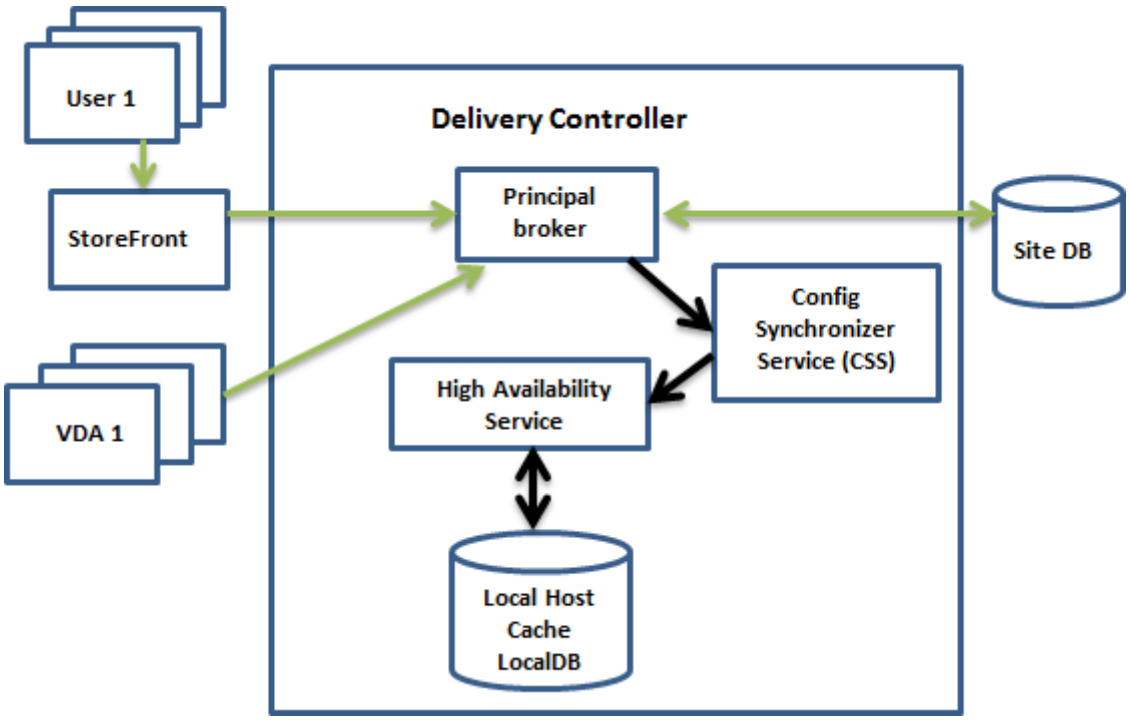
- サイトから公開されたリソースに対する権限が割り当てられているユーザーおよびグループの ID
- サイトの公開リソースを現在使用しているか、最近使用したユーザーの ID
- サイトに構成されている VDA マシン（リモート PC アクセスマシンを含む）の ID
- 公開リソースへの接続で頻繁に使用されている Citrix Receiver クライアントマシンの ID（名前と IP アドレス）

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

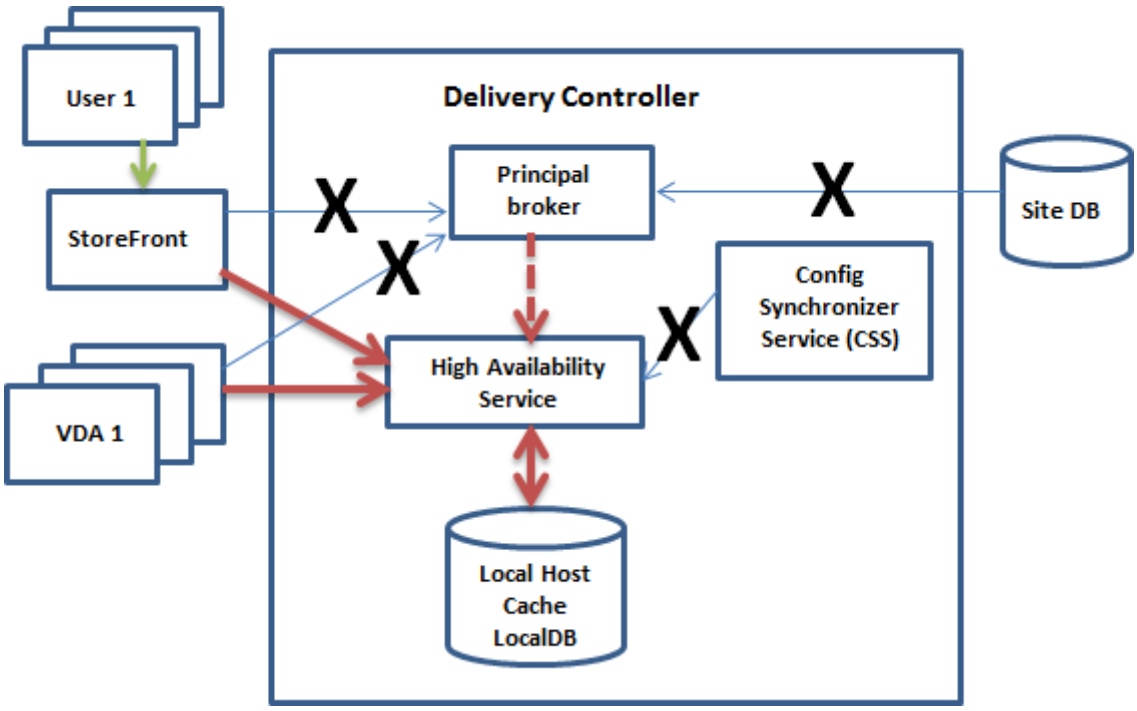
次の図は、通常の操作中のローカルホストキャッシュコンポーネントと通信経路を示しています。



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。
- 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するために、定期的（前のチェックが完了してから 1 分後）にチェックが行われます。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、Citrix Config Synchronizer Service（CSS）は、Controller 上の Citrix High Availability Service に情報を同期（コピー）します。（ドキュメントによっては、High Availability Service はセカンダリブローカーと呼ばれます）。前回のチェック以降に変更された項目のみでなく、すべてのブローカー構成データがコピーされます。High Availability Service 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、LocalDB データベース内の情報がサイト構成データベース内の情報と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。

次の図に、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（停止状態が開始された）場合の通信径路の変化を示します。



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、High Availability Service に指示します。High Availability Service は、CSS からのすべてのコールを破棄します。
- 停止状態の開始時には、High Availability Service にその時点の VDA 登録データはありませんが、VDA との通信時に再登録処理がトリガーされます。その処理中に、High Availability Service は、その VDA に関する現在のセッション情報も取得します。
- High Availability Service が接続を処理する間、プリンシパルブローカーは、サイト構成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、High Availability Service に接続情報のリスニングを停止するように指示し、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。High Availability Service は、前の停止状態時の VDA 登録が残っていればそれを削除し、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。

通常モードと停止モードとの間の移行は、既存のセッションには影響しません。新しいセッションの起動にのみ影響します。

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、監視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」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 に関する情報を定期的に High Availability Servicegへ提供します（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 High Availability Service は、同じ立場にあるすべての High Availability Service を認識します。

High Availability Service 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 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 High Availability Service がゾーン内の仲介操作を担当するかを決定（選出）します。停止状態の間に、すべての VDA が、選出された High Availability Service に再登録されます。ゾーン内の選出されていない High Availability Service は、着信接続と VDA 登録要求を能動的に拒否します。

停止状態の間に、選出された High Availability Service で障害が発生した場合は、引き継ぐために別の High Availability Service が選出され、VDA は新しく選出された High Availability Service に再登録されます。

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に影響が生じることがあります。

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。「監視」を参照してください。

設計に関する考慮事項および要件

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、およびその他の相違点

- 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、現在アクティブな選出された High Availability Service 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。停止状態の間は、ゾーン間での起動（あるゾーン内の High Availability Service から別のゾーン内の VDA へ）はサポートされません。
- デリバリーグループ内の VDA に対してスケジュールされた再起動が開始される前にサイト構成データベースの停止が発生した場合、停止が終了すると再起動が開始されます。これは意図しない結果につながる可能性があります。詳しくは、「データベースの停止によるスケジュールされた再起動の遅延」を参照してください。

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、および静的な（割り当て済み）デスクトップでサポートされています。

デフォルトでは、停止状態が発生した場合、「ShutdownDesktopsAfterUse」プロパティが有効なプールされたデリバリーグループ内で電源管理されているデスクトップ VDA（MCS または Citrix Provisioning によって作成）は、メンテナンスモードになります。このデフォルトの設定を変更して、停止状態中にこれらのデスクトップを使用できるようにすることができます。ただし、停止状態中は電源管理が機能しないことがあります。（通常の操作を開始すると電源管理が始まります）。また、これらのデスクトップは再起動していないため、前のユーザーのデータが含まれている可能性があります。

- デフォルトの動作を上書きするには、サイト全体で、影響を受けるデリバリーグループごとに、これを有効にする必要があります。次の PowerShell コマンドレットを実行します。

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  Set-BrokerDesktopGroup -Name "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 サイズの考慮事項

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に関する考慮事項

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。

ストレージの考慮事項

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、停止状態の間のデータベース増大を考慮に入れ、LocalDB がインストールされるドライブ上に、十分な空き領域がある必要があります。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）。

パフォーマンスについての考慮事項

停止状態の間は 1 つの High Availability Service がすべての接続を処理するため、通常操作時に複数の Controller に負荷を分散するサイト（またはゾーン）では、停止状態時に、選出された High Availability Service が通常よりはるかに多くの要求を処理しなければならない場合があります。このため、CPU への要求が高くなります。選出された High Availability Service が停止状態時に変更される可能性があるので、サイト（ゾーン）内のすべての High Availability Service が、LocalDB と影響を受けるすべての VDA から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 を High Availability Service に再登録する間は、High Availability Service では現在のセッションの情報を完全には把握でき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」High Availability Service 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を受けることはありませんが、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ります。

この期間は、VDA の再登録が必要なときには必ず発生します:

- 停止状態の開始：プリンシパルブローカーから High Availability Service に移行するとき。

- 停止状態時の High Availability Service の障害：障害の発生した High Availability Service から、新しく選出された High Availability Service 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
```

ハートビート値を変更するときは注意が必要です。頻度を増やすと、通常モードと停止モードのどちらの間でも、Controller の負荷が増加します。

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。

High Availability Service 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）の数とともに増加します。たとえば、5,000 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、「監視」を参照してください。

XenApp 6.x リリースとの相違点

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。

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、Remote-Signed、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。High Availability Service のみ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を必要とし、High Availability Service 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。

以前のバージョンの SQL Server Express LocalDB を新しいバージョンに置き換える方法について詳しくは、「SQL Server Express LocalDB の置き換え」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktops（バージョン 7.16 以降）の新規インストール時に、ローカルホストキャッシュが有効になります。

アップグレード（バージョン 7.16 以降へ）後は、展開全体に 10,000 個未満の VDA が存在する場合に、ローカルホストキャッシュが有効になります。

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
  ```

  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、`Get-BrokerSite`を入力します。`LocalHostCacheEnabled`プロパティが`True`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にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意：XenApp および XenDesktop 7.16 より、接続リース機能（バージョン 7.6 以降に提供されていた、ローカルホストキャッシュに先行する機能）は削除され、使用できなくなりました。

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。イベントログで確認してください。
- 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`が作成されたことを確認します。

- Delivery Controller で停止状態の強制を実行します。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。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を作成して`REG_DWORD`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。

監視

イベントログに、同期および停止状態が発生した時刻が示されます。

Config Synchronizer Service:

通常操作時に、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 を使用して LocalDB にインポートするときに、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、「トラブルシューティング」を参照してください。
- 507: 未解決の停止が原因で、インポートが中止されました。同期中に停止状態が開始されると、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。

High Availability Service:

- 3502: 停止状態が発生し、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 High Availability Service が選出されたかと、選出に関わった他の High Availability Service 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には、次のトラブルシューティングツールが役立ちます。

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: 障害ポイントを詳しく説明したレポートを生成し、提供できます。このレポート機能は同期速度に影響するため、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、次のように入力します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML レポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`に格納されます。

レポートが生成されたら、レポート機能を無効にします。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグのために正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

たとえば、`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`などです。

仮想 IP および仮想ループバック

April 26, 2021

> 重要:
>
> Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化（仮想 IP）がサポートされていないため、Windows 10 Enterprise マルチセッションでは、仮想 IP も仮想ループバックもサポートしていません。

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 Citrix Virtual Apps 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、Citrix Virtual Apps 上にある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。Windows ポリシーについて詳しくは、「RDS IP Virtualization in Windows Server」を参照してください。

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。

- 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
- 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

April 26, 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 登録について詳しくは、「Delivery Controller による VDA 登録」を参照してください。

Controller の追加、削除、または移動

Controller の追加、削除、移動を行うには、データベースのデータベース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。

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。

   データベースの初期化スクリプトを生成する場合は、その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 Citrix Provisioning 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は、アップグレード時、またはテストサイトで作成された VDA イメージを実稼働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 の完全修飾ドメイン名（DNS エントリ）を指定してこの Controller を追加します。

Controller のポリシー設定を使用しない場合にのみ、インストーラーで Controller を指定してください。

グループポリシーエディター

次の例では、複数の VDA をほかのサイトに移動します。

1. サイト 1 でポリシーを作成して以下のように設定し、そのポリシーを VDA 移行を行うデリバリーグループに割り当てます。
    - Controller：サイト 2 の 1 つまたは複数の Controller の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

April 26, 2021

はじめに

> 注：
>
> オンプレミス環境で VDA を Delivery Controller に登録します。Citrix Cloud サービス環境で VDA を Cloud Connector に登録します。ハイブリッド環境では、一部の VDA が Delivery Controller に登録し、それ以外は Cloud Connector に登録する場合があります。

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。VDA は *ListOfDDCs* と呼ばれる一覧をチェックして Controller または Connector 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

- セキュリティの観点から、登録は慎重に行う必要があります。Controller または Cloud Connector と VDA 間の接続を確立することになるからです。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。

Citrix Virtual Apps and Desktops では、VDA のインストール中に構成済みの Controller または Cloud Connector に対する接続が自動でテストされます。Controller または Cloud Connector に接続できない場合は、エラーが表示されます。Controller または Cloud Connector に接続できないことを示す警告を無視した場合（または VDA のインストール中に Controller または Cloud Connector のアドレスを指定しなかった場合）は、メッセージが表示されます。

Controller または **Cloud Connector** のアドレスの構成方法

VDA の初めての登録時（初回登録と呼びます）に、管理者は使用する構成方法を選択します。初回登録中に、VDA 上に永続キャッシュが作成されます。以降の登録では、構成の変更が検出されない限り、VDA はこのローカルキャッシュから Controller または Cloud Connector のリストを取得します。

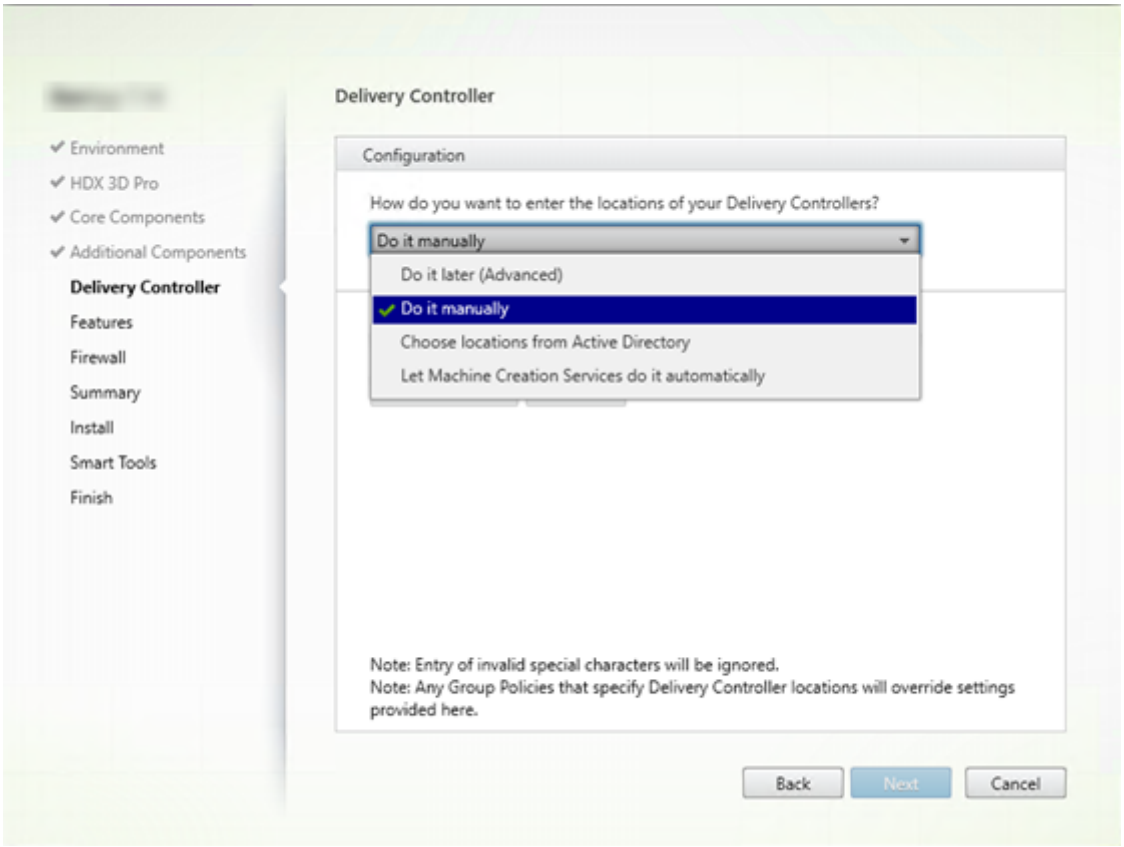
以降の登録時にこのリストを取得する一番簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳しくは、「自動更新」を参照してください。

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、グループポリシーの基本設定（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 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（リスト上では自動更新が最優先となっていますが、自動更新は初回登録後にのみ使用します）。ポリシーベースの登録には、構成にグループポリシーを使用できるという集中化のメリットがあります。

この方法を指定するには、次の手順の両方を実行します。

- VDA インストールウィザードの ［**Delivery Controller**］ページで、［あとで実行（上級）］を選択します。VDA のインストール中に Controller のアドレスの指定は行いませんが、ウィザードからこれらのアドレスを指定するように複数回促されます（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、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 サイトの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のキーが両方ある場合、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「ListOfSIDs」を参照してください）：

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs （REG_SZ）

注：Citrix ポリシーによりポリシーベースの 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連携します。マシンカタログの作成時、MCS は初回プロビジョニングで Controller または Cloud Connector の一覧を`Personality.ini`ファイルに書き込みます。自動更新により、この一覧が最新状態に保たれます。

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

この方法を使用する場合は、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。
- Controller が利用不能な場合に登録の問題が発生しないようにするため、`ListOfDDCs`レジストリキーで複数の Controller をスペースで区切って指定します。例:

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs (REG_SZ)
<!--NeedCopy-->
```

- 起動時に登録が速やかに行われるようにするため、ListOfDDCs に指定する値はすべて有効な完全修飾ドメイン名と対応させてください。

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。このプロセスは、VDA ごとに実行されます。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 Citrix Provisioning 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。Citrix Provisioning サーバーのキャッシュは除外されます。これは、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。

- `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`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。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。

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。

> 重要:
>
> この情報は説明のみを目的として紹介しています。このファイルは変更しないでください。このファイルまたはフォルダーを変更すると、構成はサポート対象外となります。

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation” -Class “Citrix_VirtualDeskt
” -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。このプロセスは、（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

VDA 登録に影響を与える可能性のある設定を構成するときは、次の点を考慮してください。

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
- Kerberos を使用した相互認証

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

特定のシナリオでは、優先グループと、すべての Controller/Cloud Connector で障害が発生した場合のフェールオーバーに使用する別のグループを用意して、Controller または Cloud Connector をグループで処理できます。Controller または Cloud Connector はリストからランダムに選択されるものであるため、グループ化すると優先的な使用を指定しやすくなります。

これらのグループは、単一のサイト内（複数のサイトではなく）での使用を目的としています。

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。

XenDesktop 7.0 以降では、登録グループ機能を使用する場合、追加の手順を実施する必要があります。Citrix Studio で、［**Controller** の自動更新を有効にする］ポリシーを無効にしてください。

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、信頼されている 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。

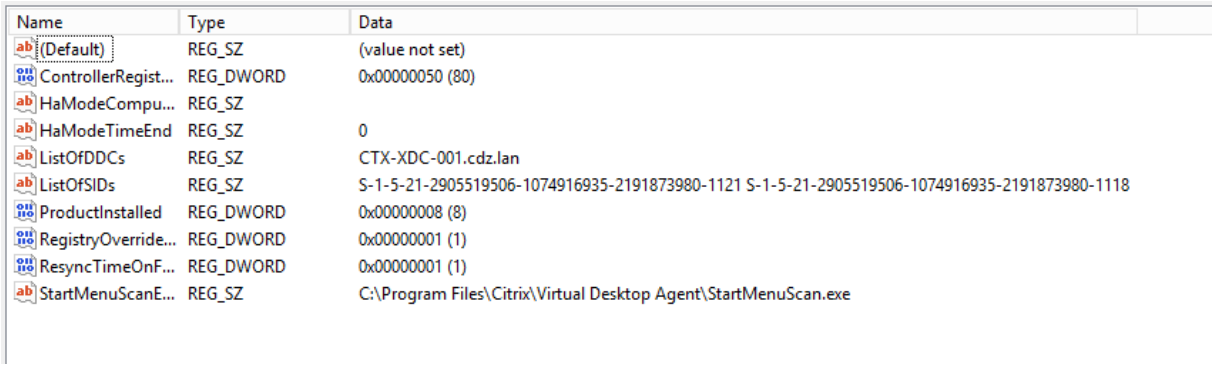
一般には、ListOfSIDs を手動で変更する必要はありません。ただし、いくつかの例外があります。最初の 2 つの例外は、新しいテクノロジーが使用可能になったため有効ではなくなりました。

- **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。これは典型的な構成や推奨される構成ではありません。最新の環境では使用しないでください。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ていました。しかし、自動更新機能では永続キャッシュに SID が含まれるようになったため、この作業を行う必要はなくなりました。自動更新機能は有効にしておくことを 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、`HKLM\Software\Citrix\VirtualDesktopAgent` に `ListOfSIDs`（`REG_SZ`）という名前のレジストリキーを作成します。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 または Cloud Connector 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、（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が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、登録の必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードでないはないのに、Controller に現在登録されていないマシンが 1 台または複数台存在することが考えられます。「未登録だが登録する必要がある」マシンが表示された場合は、［詳細］ペインの ［トラブルシューティング］タブで、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。

VDA 登録のトラブルシューティングの詳細

- 機能レベルについて詳しくは、「VDA バージョンと機能レベル」を参照してください。

- 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

April 26, 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。

この記事で説明する機能では、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。

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 Workspace アプリのユーザーは、Controller 側の設定を上書きできません。

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 Citrix 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 Workspace アプリが検出して、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 Workspace アプリは、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 Workspace アプリは、指定された時間にわたり、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 Workspace アプリ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 Citrix Workspace アプリに送信されます。Citrix Workspace アプリは、再接続時にこのキーをサーバーへ送信します。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］設定を有効にした場合、Cookie は使用されません。その代わりに、Citrix Workspace アプリの切断セッションへの自動再接続時に、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。

Windows 向け Citrix Workspace アプリ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、該当するバージョンの Windows 向け Citrix Workspace アプリ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 Citrix Workspace アプリまたはプラグインから正しくない認証情報が提供された場合、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。

> 重要:
>
> 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 Workspace アプリユーザーが 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。オプションで、「LeasingBehavior」プロパティを指定することもできます。

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。

ほかの設定の影響：

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。

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。

この設定は、デスクトップ（ワークステーション）VDA を搭載した仮想マシンにのみ適用されます。サーバー VDA を搭載したマシンのログオンタイムアウトは、Microsoft 社により制御されます。

Studio での検索の使用

April 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。

   ［マシンカタログ］タブや［デリバリーグループ］タブでは、［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、［検索の展開］アイコン（2 重の下向き山括弧）をクリックすると、検索プロパティのメニューが表示されます。このメニューのプロパティで式を作成することで、高度な検索を行うことができます。

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

April 26, 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。

- 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。具体例と詳細については、「デリバリーグループの管理」を参照してください。

- デ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。

タグは次のものに適用できます:

- マシン
- アプリケーション
- マシンカタログ（PowerShell のみ、「マシンカタログのタグ」を参照）
- 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

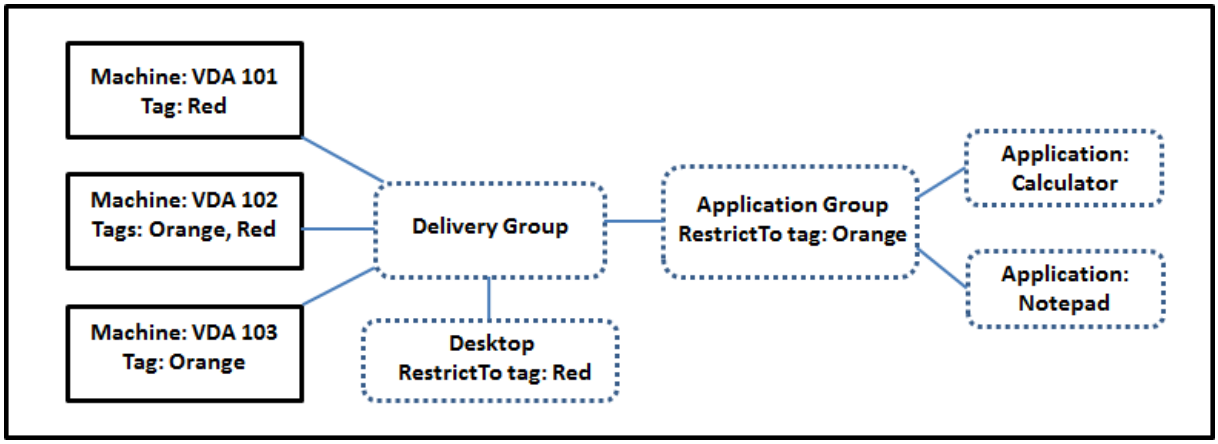
タグ制約には、いくつかの手順があります:

- 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**: 単純なレイアウト

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。



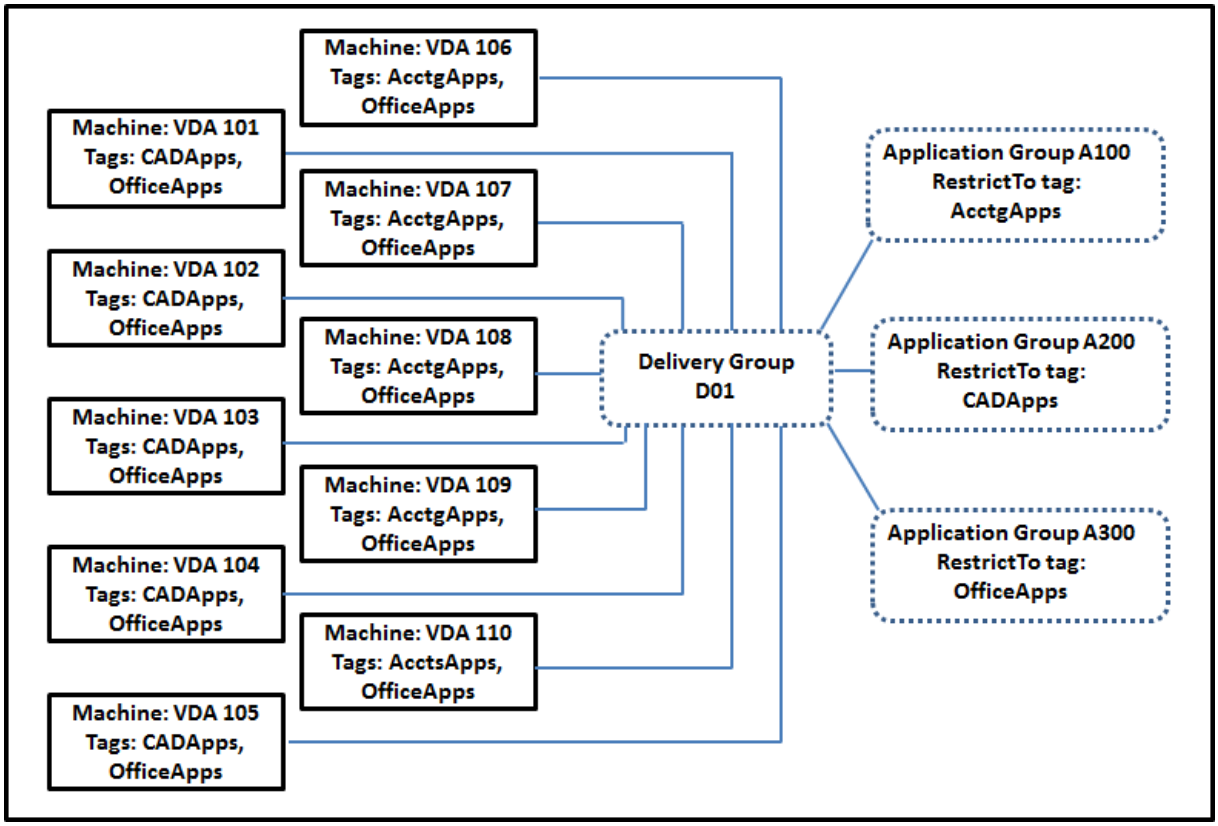
- 3 台のマシン（VDA 101～103）それぞれにタグが追加されています。
- 共有デリバリーグループのデスクトップは「Red」という名前のタグ制約を付けて作成されているため、デリバリーグループの、「Red」という名前のタグを持つマシン（VDA 101 および 102）上でのみ起動できます。
- アプリケーショングループは「Orange」のタグ制約で作成されているので、各アプリケーション（計算機とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン：VDA 102 および 103 上でのみ起動できます。

マシン VDA 102 は両方のタグ（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ます。

例 **2**：複雑なレイアウト

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

（タグを作成、適用し、この例のタグ制約を構成するための手順については、「例 2 を構成する方法」に示しています）。



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

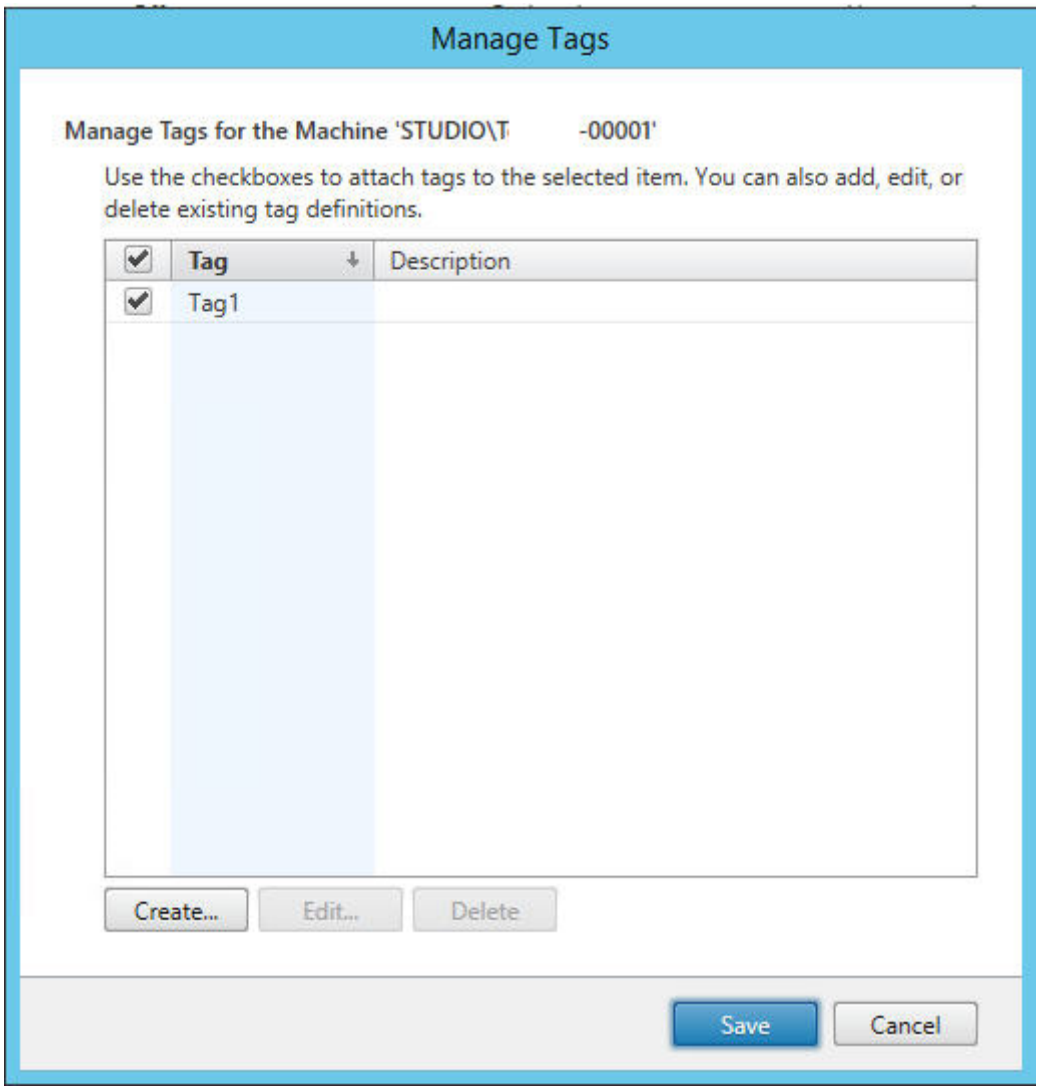
（例外：ポリシー割り当てに使用するタグは、Studio の ［タグの管理］操作を使用して作成、編集、削除します。ただし、タグが適用される（割り当てられる）のはポリシーの作成時です。詳しくは、「ポリシーの作成」を参照してください。）

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。

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。必ず「タグを使用する場合の注意事項」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。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）、このチェックボックスをオンにすると、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。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）、その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、この操作により起動対象となるマシンに影響が及ぶ可能性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。

マシンにタグが適用されているかを確認するには、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、［タグでマシンの起動を制限します:］を選択し、メニュー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。

タグを使用する場合の注意事項

項目に適用されるタグはさまざまな目的に使用できるため、タグの追加や削除が意図しない結果になる可能性があることに注意してください。タグを使用して Studio 検索フィールドのマシン表示を並べ替えることができます。アプリケーショングループまたはデスクトップの構成時に同じタグを制約として使用すると、そのタグが付いている指定されたデリバリーグループのマシンだけに起動対象を制限できます。

タグがデスクトップまたはアプリケーショングループのタグ制約として構成されている場合に 1 つまたは複数のマシンにタグを追加しようとすると、それらのマシンでその他のアプリケーションやデスクトップの起動が可能になることがあるという警告が表示されます。それが意図どおりであれば続行します。そうでない場合は、操作を取り消すこともできます。

たとえば、「Red」というタグ制約を持つアプリケーショングループを作成するとします。後から、そのアプリケーショングループによって使用される同じデリバリーグループに、他のマシンをいくつか追加します。それらのマシンに「Red」というタグを追加すると、おおむね次のようなメッセージが表示されます:「タグ「Red」は、次のアプリケーショングループ上の制約として使用されています。このタグを追加すると、選択されたマシンからこのアプリケーシ

ョングループのアプリケーションが起動可能になる可能性があります」。次に、それらの追加のマシンへのそのタグの追加を確認またはキャンセルできます。

同様に、アプリケーショングループで起動を制限するためにタグが使用されている場合、グループを編集してタグ制約を削除するまで、そのタグを削除できないという警告が表示されます（アプリケーショングループの制約として使用されているタグの削除を許可されている場合、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動を許可することになる可能性があります）。デスクトップ起動の制約として現在タグが使用されている場合も、タグの削除は同様に不可能です。アプリケーショングループまたはデリバリーグループ内のデスクトップを編集してタグ制約を削除すれば、タグを削除できます。

すべてのマシンが同一セットのアプリケーションを持つとは限りません。1 人のユーザーが、それぞれ異なるタグ制約を持ち、デリバリーグループのマシン構成が異なるか重なり合っている複数のアプリケーショングループに属する場合があります。次の表に、対象マシンがどのように決まるかを示します。

アプリケーションの追加先	選択したデリバリーグループ内で起動対象となるマシン
タグ制約を持たない 1 つのアプリケーショングループ	すべてのマシン
タグ制約 A を持つ 1 つのアプリケーショングループ	タグ A が適用されているマシン
2 つのアプリケーショングループ。タグ制約 A を持つグループとタグ制約 B を持つグループ	タグ A とタグ B を持っているマシン。存在しない場合、タグ A またはタグ B を持っているマシン
2 つのアプリケーショングループ。タグ制約 A を持つグループとタグ制約を持たないグループ	タグ A を持つマシン。存在しない場合、すべてのマシン

マシン再起動スケジュールでタグ制約を使用している場合、タグ適用またはタグ制約に影響する変更はすべて、次回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

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。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用は、PowerShell インターフェイスを介してのみサポートされます。Studio を使用して、タグをカタログに適用したり、カタログからタグを削除したりすることはできません。Studio のカタログ表示では、タグが適用されているかどうかは示されません。

概要：Studio または PowerShell を使用して、カタログで使用するタグを作成または削除できます。タグをカタログに適用するには、PowerShell を使用する必要があります。

カタログでタグを使用する例を次に示します：

- デリバリーグループには複数のカタログのマシンがありますが、操作（再起動スケジュールなど）を特定のカタログ内のマシンのみに適用する必要があります。該当するカタログにタグを適用することで、それが実現します。
- アプリケーショングループで、アプリケーションセッションを特定のカタログ内のマシンに制限する必要があります。該当するカタログにタグを適用することで、それが実現します。

影響を受ける PowerShell コマンドレット：

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`で、タグを含むカタログの数が表示されます。

- `Get-BrokerCatalog`には`Tags`というプロパティがあります。

たとえば、次のコマンドレットにより、`fy2018`という名前のタグが`acctg`という名前のカタログに追加されます：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`（タグは以前に Studio または PowerShell を使用して作成されました）

ガイダンスと構文の詳細については、PowerShell コマンドレットのヘルプを参照してください。

詳細情報

ブログ記事：How to assign desktops to specific servers。

IPv4/IPv6 サポート

April 24, 2021

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。

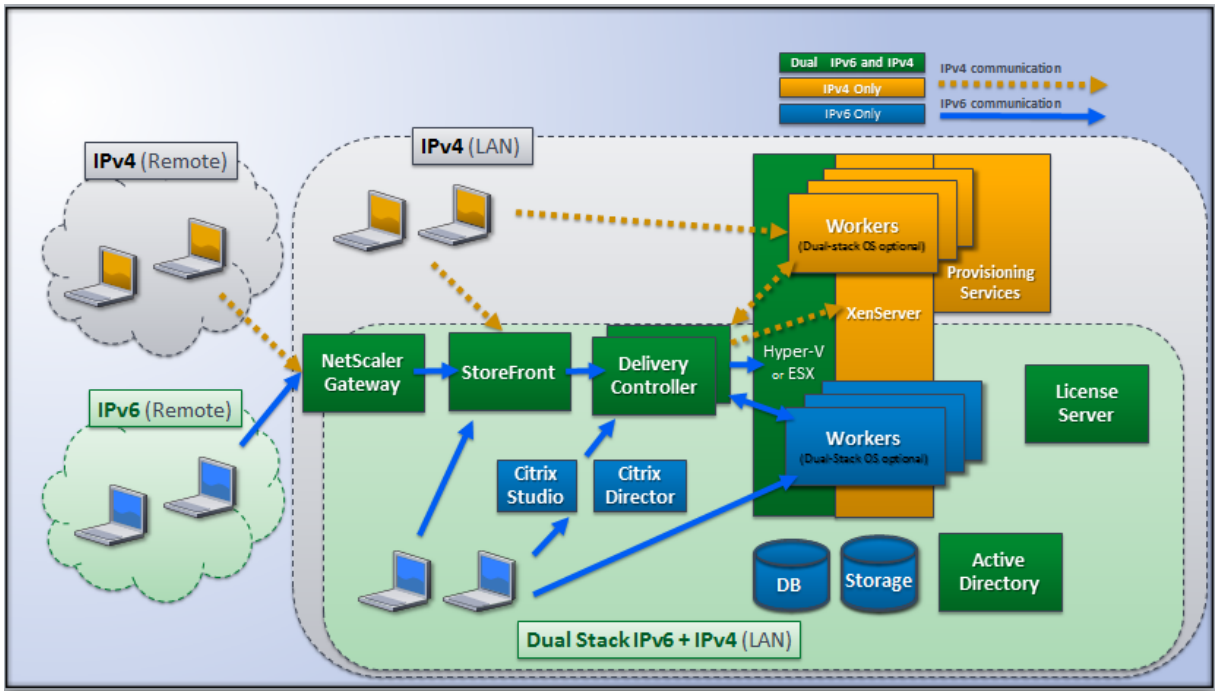
IPv6 通信は、Virtual Delivery Agent（VDA）接続関連の 2 つの Citrix ポリシー設定で制御されます。

- 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。

- Citrix Provisioning
- XenServer
- [**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

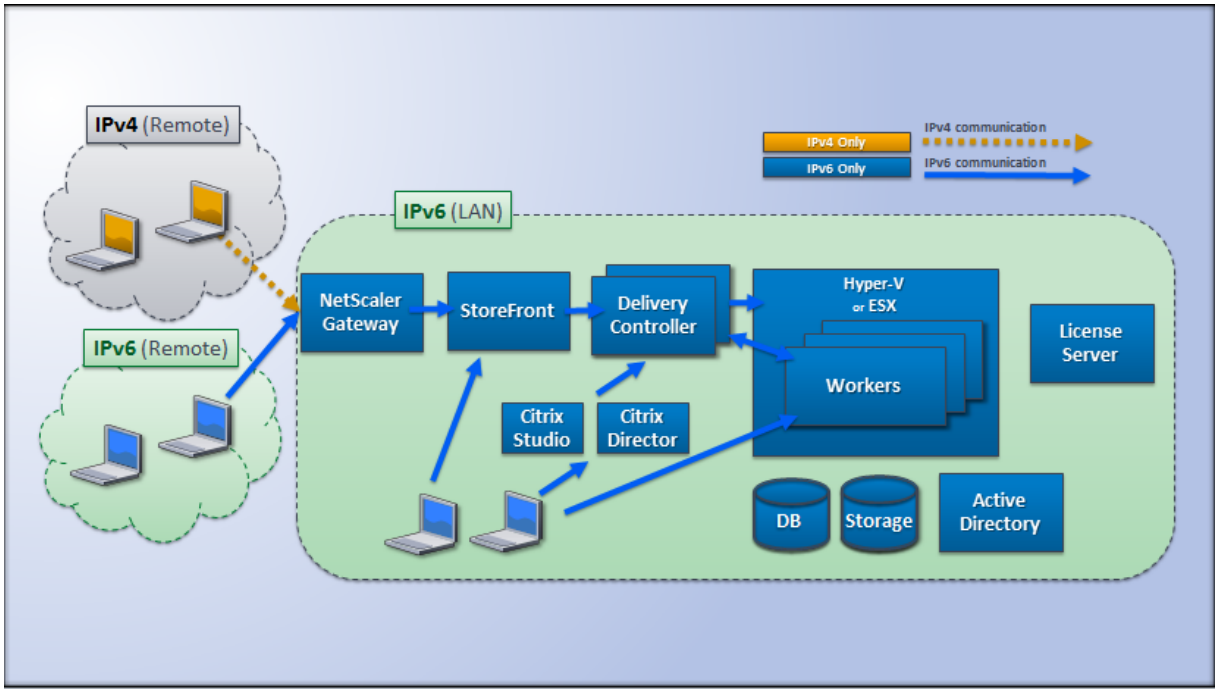
この展開は、以下のように管理されます。

- 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。

これらの設定項目によってのみ、VDA で使用されるアドレスの形式（IPv4 または IPv6）が決定されます。つまり、VDA で IPv6 アドレスが使用されるようにするには、[**IPv6** コントローラー登録のみを使用する] 設定を有効にしたポリシーを適用する必要があります。

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

April 26, 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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］ノードにある Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps and Desktops 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 Citrix Provisioning 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 で作成されるシングルセッション 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、およびノートブックコンピューターなど。
- 固定かつ共有－ Machine Creation Services で作成されるマルチセッション OS マシンなど。
- プロビジョニングかつ専用－ Citrix Provisioning で作成されるシングルセッション 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－ Citrix Provisioning で作成されるシングルセッション 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、Citrix Virtual Apps 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、Citrix Virtual Apps and Desktops 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。

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のみ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。

高度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、「フォルダーのリダイレクト」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、「項目を包含および除外するには」を参照してください。

システム起動時に **Citrix Diagnostic Facility**（**CDF**）トレースを収集する

April 24, 2021

CDFControl ユーティリティはイベントトレースコントローラー、つまりコンシューマーであり、各種 Citrix トレースプロバイダーに表示される Citrix Diagnostic Facility（CDF）トレースメッセージを記録します。このユーティリティは、Citrix に関連する複雑な問題のトラブルシューティング、フィルターサポートの解析、パフォーマンスデ

ータの収集を行うためのものです。CDFControl ユーティリティのダウンロード方法については、CTX111961を参照してください。

ローカルシステムアカウントを使用する

CDF COM サーバーサービスのローカルシステムアカウントを使用するには、次の手順を実行します:

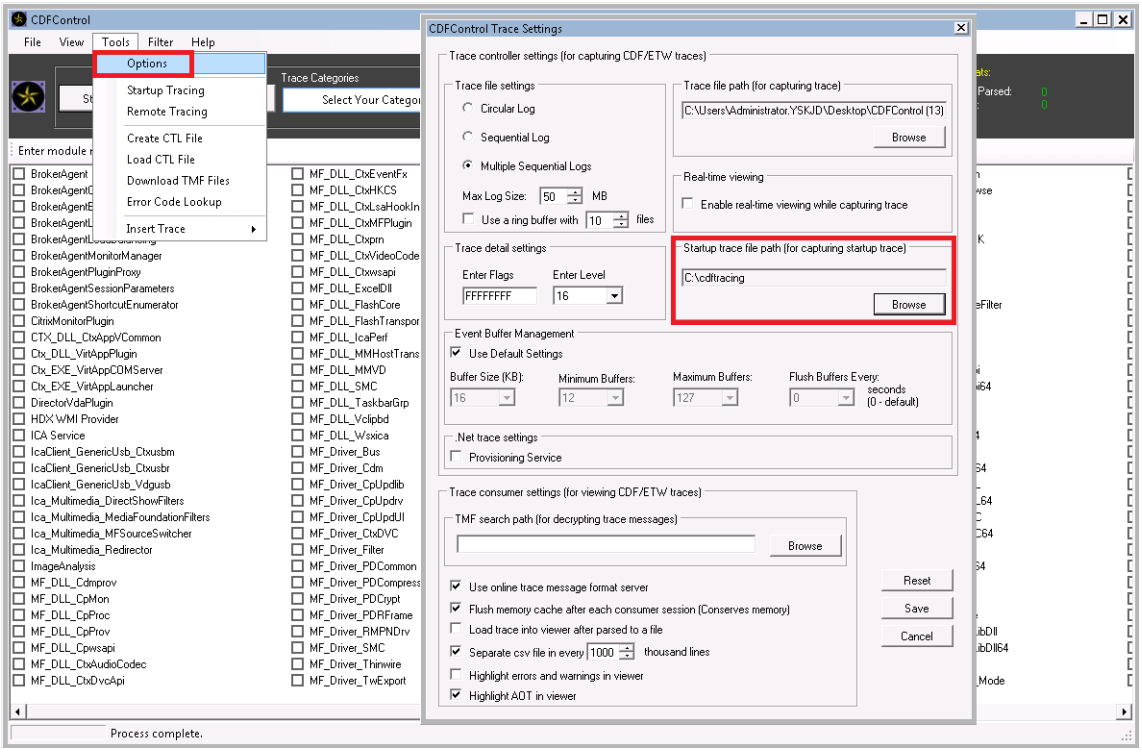
1. ［スタート］メニューで ［実行］をクリックします。
2. ダイアログボックスに「`services.msc`」と入力し、［**OK**］をクリックします。
3. **Citrix Diagnostics Facility COM Server** サービスを選択して、［プロパティ］を選択します。
4. ［ログオン］タブをクリックして、［ローカルシステムアカウント］をオンにします。［**OK**］をクリックします。

5. サービスを再起動します。

システムの起動時にトレースを収集する

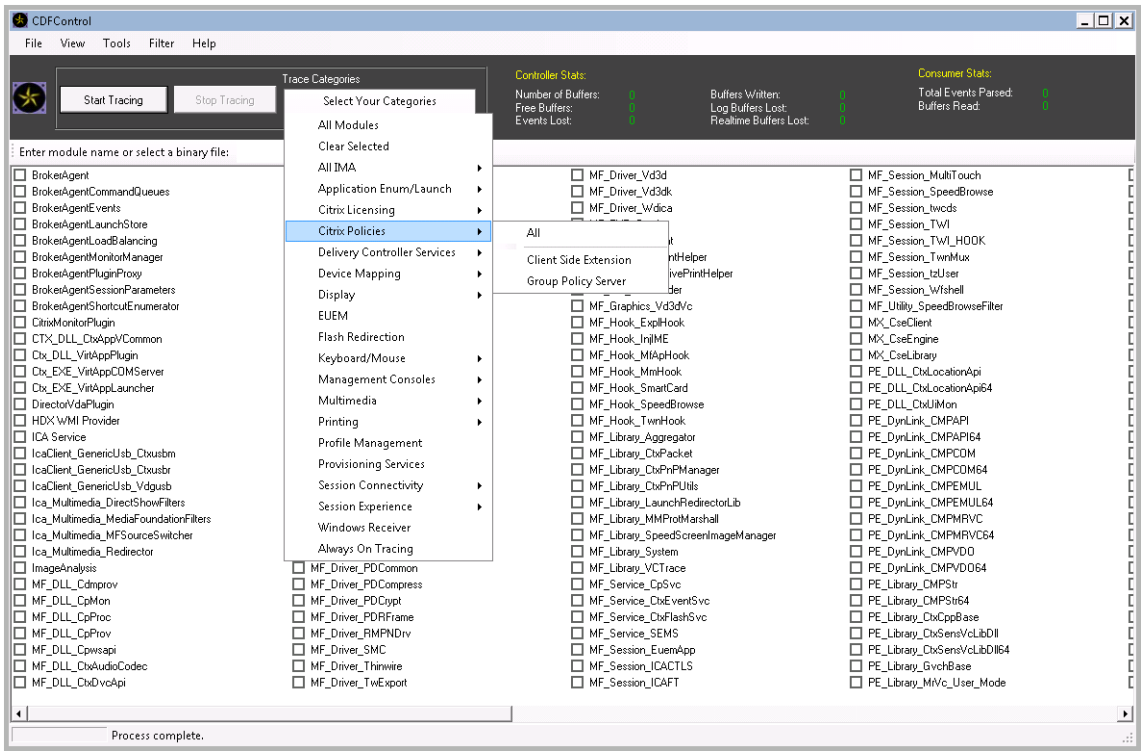
システムの起動時に CDF トレースを収集するには、次の手順に従います:

1. **CDFControl** を起動し、［ツール］メニューで ［オプション］を選択します。
2. ［起動トレースを記録する起動トレースファイルのパス］セクションで、トレースファイルのパスを指定します。次に、［保存］をクリックします。



3. Citrix テクニカルサポートから推奨されたトレースカテゴリを選択します。この例では、［**Citrix** ポリシー］が選択されています。

以下で選択されている［**Citrix** ポリシー］は、起動トレースの一例として示したものです。トラブルシューティングでは、特定の問題に関するプロバイダーを有効にすることをお勧めします。



4. 管理者権限で ［ツール］メニューの ［起動トレース］を選択し、［有効化］をクリックします。

   ［有効化］をクリックすると、バーのスクロール表示が始まります。ただし、これは手順には影響しません。手順 5 に進んでください。

5. ［起動トレース］が有効になったら、**CDFControl** ユーティリティを閉じてシステムを再起動します。

6. **CDFControl** ユーティリティを起動します。システムの再起動後にエラーが表示された場合は、［無効化］をクリックして起動トレースを無効にします。

   手順 4 および 5 の説明に従い、［ツール］メニューで ［起動トレース］を選択し、［無効化］をクリックして起動トレースを無効にします。

7. **Citrix Diagnostics Facility COM Server** サービスを停止します。

8. 手順 1 および 2 を実行して、分析用のトレースログファイル（.etl）を指定したファイルパスに収集します。

9. **Citrix Diagnostics Facility COM Server** サービスを開始します。

Citrix Insight Services

April 26, 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 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

Citrix Virtual Apps and Desktops のリリースでは、以下の技術がサポートされます。

- Citrix Virtual Apps and Desktops のインストールとアップグレードの分析機能
- Citrix カスタマーエクスペリエンス向上プログラム（CEIP）
- Citrix Call Home
- Citrix Scout

CIS および Citrix Analytics に追加（および別途）：Studio をインストール（またはアップグレード）すると、Google Analytics が自動的に収集され（後でアップロードされ）ます。Studio をインストールした後、レジストリキー HKLM\Software\Citrix\DesktopStudio\GAEnabled でこの設定を変更できます。値 1 で収集とアップロードを有効にし、0 で収集とアップロードを無効にします。

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 Citrix Virtual Apps and Desktops 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。

自動アップロードの制御：

- 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：HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall
  - 値の名前：SendExperienceMetrics
  - 値：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
<!--NeedCopy-->
```

- 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

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

CEIP には、サイトの作成時に自動で登録されます（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。登録は、サイトの作成後にいつでも取り消すことができます。Studio のナビゲーションペイン（[製品サポート] タブ）で ［構成］ ノードを選択してガイダンスに従って操作します。

Citrix Virtual Apps and Desktops 環境をアップグレードする場合:

- 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：HKEY_LOCAL_MACHINE\Software\Citrix\Telemetry\CEIP
値の名前：Enabled
値：0 = 無効、1 = 有効

デフォルトでは、レジストリにEnabledプロパティは表示されません。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。

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

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（Citrix Provisioning、AppDNA、Citrix ライセンスサーバー、Windows 向け Citrix Workspace アプリ、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 Call Home

Citrix Virtual Apps and Desktops 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）。

Citrix Virtual Apps and Desktops 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。AOT ログは C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT に保存されます。

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:

- Citrix Virtual Apps and Desktops によって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`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
- インストールとアップグレードの情報これには、製品全体の Metainstaller ログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront ログ、ライセンスの互換性チェックログ、サイトの事前アップグレードテストの結果が含まれます。

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 キーデータポイント」に記載された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。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にすることができます。

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。

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、参加確認のメッセージは表示されません。

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、Citrix に自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

```
1  $cred = Get-Credential
2  Enable-CitrixCallHome -Credential $cred
3  <!--NeedCopy-->
```


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-CitrixCallHomeGet-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での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 }

  <!--NeedCopy-->
  ```

例：

次のコマンドレットでは、毎日午後 10 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
<!--NeedCopy-->
```

スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上記の例では、「StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily」が返される必要があります。

以下のコマンドレットでは、毎週水曜日の午後 10 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
<!--NeedCopy-->
```

スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上記の例では、「StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly」が返される必要があります。

Call Home の無効化

Call Home を無効にするには、PowerShell コマンドレットか Citrix Scout を使用します。

AOT ログは、Call Home のスケジュールによるアップロードが無効な場合でも収集されディスクに保存されます。（スケジュールによるアップロードが無効な場合、AOT ログは自動的に Citrix にアップロードされません。）AOT ログの収集およびローカル保存は無効化できます。

PowerShell で **Call Home** を無効にする

以下のコマンドレットを実行すると、診断データは自動的に Citrix にアップロードされません。（キャンセル後も、Citrix Scout または Telemetry の PowerShell コマンドレットを使用した診断データのアップロードは実行できます）。

```
Disable-CitrixCallHome
```

Call Home が無効になったことを確認するには、`Get-CitrixCallHome`を入力します。無効な場合は、「`IsEnabled=False`」および「`IsMasterImage=False`」が返されます。

Citrix Scout を使用して収集スケジュールを無効にする

Citrix Scout を使用して診断収集スケジュールを無効にするには、「収集スケジュールの設定」のガイドに従います。手順 3 で、［**Off**］をクリックして選択したマシンのスケジュールをキャンセルします。

AOT ログの収集を無効にする

以下のコマンドレットを実行すると（`Enabled`フィールドを**`false`**に設定）、AOT ログは収集されません。

```
Enable-CitrixTrace -Listen '{ "trace":{ "enabled":false,"persistDirectory"
:"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300 } }
'
```

`Listen`パラメーターには JSON 形式の引数が含まれます。

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。

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。
2. PowerShell で「`netsh winhttp import proxy source=ie`」を実行します。


```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

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。以下の赤い枠内の情報を追加します。

```
TelemetryService.exe - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
                <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
    </startup>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
          <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
        </dependentAssembly>
        <probing privatePath="TelemetryModule" />
      </assemblyBinding>
    </runtime>
<system.net>
<defaultProxy>
<proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
</defaultProxy>
</system.net>

</configuration>
```

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、診断情報のパッケージを手動で収集して CIS にアップロードします。(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、診断情報のパッケージをローカルに保存します。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、パッケージのコピーを手動で 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。

データを収集して **CIS** へパッケージをアップロードする:

```
1 Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
     string] [-Description string] [-IncidentTime string] [-SRNumber
     string] [-Name string] [-UploadHeader string] [-AppendHeaders string
     ] [-Collect string] [<CommonParameters>]
2 <!--NeedCopy-->
```

データを収集してローカルに保存する:

```
1 Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
     Description string] [-IncidentTime string] [-SRNumber string] [-Name
      string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
     strings] [<CommonParameters>]
2 <!--NeedCopy-->
```

使用できるパラメーターは次のとおりです。

- **Credential**: アップロード先を CIS に設定します。
- **InputPath**: パッケージに含める 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**: 診断情報を保存する場所。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 **Incident Time**: アップロードに関する自由形式の情報。
- **SRNumber**: Citrix テクニカルサポートのインシデント番号。
- **Name**: パッケージの識別名。
- **UploadHeader**: CIS にアップロードす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 にアップロードす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 の値は以下のとおりです。

  - 'wmi'
  - 'process'
  - 'registry'
  - 'crashreport'
  - 'trace'
  - 'file'
  - 'msi'
  - 'localdata'
  - 'sitedata'
  - 'sfb'

  デフォルトでは、'sfb' 以外のすべての collector が有効です。

  'sfb' collector は、Skype for Business の問題を診断するためにオンデマンドで使用するよう設計されています。'sfb' collector は、'enabled' パラメーターに加えて、ターゲットユーザーを指定する'account' パラメーターと'accounts' パラメーターをサポートします。以下のいずれかの形式を使用します。

  - "-Collect "{'sfb':{'account':'domain\\user1'}}"
  - "-Collect "{'sfb':{'accounts': ['domain\\user1', 'domain\\user2']}}"

- **CommonParameters**: PowerShell のヘルプを参照してください。

ローカルに保存されているデータをアップロードする:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters
>]
```

Pathパラメーターにより、以前保存されたパッケージ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、Citrix Provisioning VDA の登録エラーに関連するものです。アップロード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。

```
1 C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
     zip" -Description "Registration failures with Citrix Provisioning
     VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
     RegistrationFailure-021812016" -Collect "{
2  'wmi':{
3  'enabled':false }
4   }
5  " -UploadHeader "{
6  'key1':'value1' }
7  " -AppendHeaders "{
8  'key2':'value2' }
```



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

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Citrix Scout

April 26, 2021

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開環境での予防的な保守に使用できます。シトリックスでは、Citrix Insight Services を通じて、収集した診断データの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 サポート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 では以下の機能が利用できます:

- 収集: サイト内の選択したマシン上で一度だけ診断情報収集を実行します。その後、ユーザーはファイルを Citrix にアップロードするか、ローカルに保存できます。
- 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。Scout はその他の診断情報を収集し、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。ファイルは自動で Citrix にアップロードされます。
- ヘルスチェック：サイトとそのコンポーネントの正常性および可用性を測定するチェックを実行します。Delivery Controller、VDA、StoreFront サーバー、および Citrix ライセンスサーバーのヘルスチェックを実行できます。チェック中に問題が見つかった場合は、Scout で詳細レポートが提供されます。Scout は起動時に必ず最新のヘルスチェックスクリプトがあるかを確認します。新しいバージョンがある場合は自動的に Scout がダウンロードし、次回のヘルスチェックで使用します。

> 注：
>
> トレースと再現、スケジュール、ヘルスチェックは現在 Linux VDA で利用できません。

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 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：

- オンプレミスの展開環境では、Delivery Controller から Scout を実行して診断情報を収集するか、1 つまたは複数の Virtual Delivery Agent（VDA）、Delivery Controller、StoreFront サーバー、ライセンスサーバーでチェックを実行します。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。
- Citrix Virtual Apps and Desktops 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。

Scout アプリケーションのログは、`C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`に保存されます。このファイルはトラブルシューティングに使用できます。

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。

収集には以下が含まれます：

- Citrix Virtual Apps and Desktops によって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`に作成されたレジストリエントリ
- **Citrix** 名前空間の Windows Management Instrumentation（WMI）情報。
- 実行中のプロセス
- %PROGRAMDATA%\Citrix\CDF に保存されている Citrix プロセスのクラッシュダンプ。
- CSV 形式の Citrix ポリシー情報
- インストールとアップグレードの情報収集には、製品全体の Metainstaller ログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront ログ、ライセンスの互換性チェックログ、サイトの事前アップグレードテストの結果が含まれます。

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保持します。
- Citrix Virtual Apps and Desktops 7 1808 より、AOT のトレース情報はデフォルトでローカルディスク上に保存されるようになりました。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811 より、ネットワーク共有に保存された AOT トレースは、他の診断と一緒に収集されます。
- 最大サイズ（デフォルト値は 10MB）とスライス時間は、`Enable-CitrixTrace`コマンドレットを使用するか、または`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を指定することで変更できます。
- トレース情報は、ファイルサイズが`MaxSize`の 10% になるまでファイルに追加されます。

Scout で収集されるデータポイントの一覧については、「Call Home キーデータポイント」を参照してください。

Scout の構成

Scout は、Linux VDA で機能するように構成できます。Linux VDA および Telemetry について詳しくは、「Citrix Telemetry Service との統合」を参照してください。

Linux VDA では、自動的に`ctxtelemetry`ソケットポートや Telemetry Service のポートが変更される場合があります。その場合は、手動でポートを構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Service に移動します。
2. ScoutUI.exe.config ファイルを開きます。
3. LinuxVDATelemetryServicePort または LinuxVDATelemetryWakeupPort の値を Linux VDA で構成された値に変更します：

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. Scout を再度開いて、最新の構成が読み込まれているのを確認します。

ヘルスチェックについて

ヘルスチェックデータは`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトのヘルスチェックは、FlexCast Management Architecture（FMA）サービスを総合的に評価する Environment Test Service の機能の 1 つです。このチェックではサービスの可用性を確認するだけでなく、正常性を示す他

の指標（データベース接続など）も確認します。

サイトのヘルスチェックは Delivery Controller で実行されます。サイトの規模によっては、チェックが完了するまでに最大 1 時間程度かかることがあります。

Delivery Controller 構成チェック

サイトヘルスチェックの一部として行います。Delivery Controller 構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、次の問題が存在するかどうかを確認します：

- 1 つ以上の Delivery Controller でエラーが発生している。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

ヘルスチェックで権限と要件を満たすことに加え、Delivery Controller 構成チェックでは以下が必要とされます：

- 1 つ以上の Controller の電源がオンになっている。
- Broker Service が Controller で実行されている。
- Controller からサイトデータベースへの有効な接続がある。

VDA のヘルスチェック

VDA のヘルスチェックは、VDA 登録、セッションの起動、タイムゾーンリダイレクトの問題を引き起こす原因となるものを見つけ出します。

VDA への登録について、Scout は以下をチェックします：

- VDA ソフトウェアのインストール状況
- VDA マシンドメインへの参加状況
- VDA の通信ポートの可用性
- VDA サービスの状態
- Windows ファイアウォールの構成
- Controller との通信
- Controller との時刻同期
- VDA の登録状態

VDA でのセッション起動について、Scout は以下をチェックします：

- セッション開始時の通信ポートの可用性
- セッション開始時のサービスの状態
- セッション開始時の Windows ファイアウォールの構成
- VDA リモートデスクトップサービスのクライアントアクセスライセンス
- VDA のアプリケーション起動パス

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします：

- Windows の Hotfix のインストール状況
- シトリックスの Hotfix のインストール状況
- Microsoft のグループポリシー設定
- シトリックスのグループポリシー設定

StoreFront ヘルスチェック

StoreFront チェックでは以下が確認されます:

- Citrix デフォルトドメインサービスが実行されている
- Citrix Credential Wallet サービスが実行されている
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFront サーバーから Active Directory ポート 389 への接続
- ベース URL の FQDN が有効である
- ベース URL からの正しい IP アドレスを取得できる
- IIS アプリケーションプールで.NET 4.0 を使用している
- 証明書がホスト URL の SSL ポートにバインドされているかどうか
- 証明書チェーンが完全かどうか
- 証明書の有効期限が切れているかどうか
- 証明書の有効期限切れが近いかどうか（30 日以内）

ライセンスサーバーチェック

ライセンスサーバーチェックでは以下が確認されます:

- Delivery Controller からのライセンスサーバー接続
- ライセンスサーバーファイアウォールのリモートアクセスのステータス
- Citrix ライセンスサーバーサービスのステータス
- ライセンスサーバーの猶予期間の状態
- ライセンスサーバーのポート接続
- Citrix ベンダーデーモン（CITRIX）が実行されているかどうか
- システムクロックが同期されているかどうか
- Citrix Licensing サービスがローカルサービスアカウントで実行されていません
- `CITRIX.opt` ファイルの存在
- カスタマーサクセスサービスの有効期限
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書が Delivery Controller の信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加え、ライセンスサーバーがドメインに参加している必要があります。参加していないと、ライセンスサーバーは検出されません。

権限と要件

アクセス許可:

- 診断情報を収集するには、以下の条件を満たしている必要があります:
  - 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。
- ヘルスチェックを実行するには、以下の条件を満たしている必要があります:
  - ドメインユーザーグループのメンバーである必要があります。
  - すべての権限を持つ管理者であるか、対象サイトに対する読み取り専用の権限と ［環境テストの実行］権限があるカスタムロールを付与されている必要があります。
- Scout の起動時には ［管理者として実行］を使用してください。

診断情報の収集元またはヘルスチェックの実行元になる各マシンは、次の条件を満たしている必要があります:

- 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。
- Windows Management Infrastructure（WMI）へのアクセスが有効になっている必要があります。
- 診断収集のスケジュールを設定するには、マシンで互換性のある Scout バージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号（$）を使用しないでください。この記号があると、診断情報を収集できません。

Scout により、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

診断情報の収集またはヘルスチェックの開始前に、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、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。

- **Scout** はこのマシンに接続できません：次のことを確認してください:
  - マシンの電源が入れられていること。
  - ネットワーク接続が正しく動作していること（これにはファイアウォールが正しく構成されていることを含みます。）
  - ファイルおよびプリンターの共有が設定されていること。手順については、Microsoft 社のドキュメントを参照してください。

- **PSRemoting** および **WinRM** を有効にする：PowerShell リモート処理と Windows リモート管理は同時に有効にできます。`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。
- **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、開始していることを確認してください。
- スケジュールを取得できません：マシンを XenApp および XenDesktop 7.14 以上にアップグレードしてください。
- **WMI** がマシン上で実行されていません：Windows Management Instrumentation（WMI）アクセスが有効になっていることを確認してください。
- **WMI** 接続がブロックされました：Windows ファイアウォールサービスで WMI を有効にします。
- **Citrix Telemetry Service** の新しいバージョンが必要です：バージョンの確認は［収集］と［トレースおよび再現］の処理でのみ行われます。対象のマシンで Telemetry Service のバージョンをアップグレードしてください（「インストールとアップグレード」を参照してください）。サービスをアップグレードしていないマシンは、［収集］と ［トレースおよび再現］の対象になりません。
- **Scout** はこのマシンの **systemd** ソケットに接続できません：次を確認します：
  - ポート 7503 が開いている。systemd ctxtelemetry.socket がマシンのポート 7503 でリスンしていることを確認します。ctxtelemetry.socket のポートが変更された場合、異なるポートの可能性があります。ポートを変更するには、「Scout の構成」を参照してください。
  - ネットワーク接続が正しく動作していること（ファイアウォールが正しく構成されていることの確認も含まれる場合があります）。
- このマシンでは、**Linux VDA Telemetry Service** が開始されていません：次を確認します：
  - ポート 7502 が開いている。Linux VDA Telemetry Service がマシンにインストールされ、開始されていることを確認します。Telemetry Service のポートが変更された場合、異なるポートの可能性があります。ポートを変更するには、「Scout の構成」を参照してください。
  - ネットワーク接続が正しく動作していること（ファイアウォールが正しく構成されていることの確認も含まれる場合があります）。

バージョンの互換性

本バージョンの Scout（3.x）は、Citrix Virtual Apps and Desktops（または 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、バージョン 7.14 より前の XenApp および XenDesktop 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
Citrix Virtual Apps and Desktops（と XenApp および XenDesktop 7.14～7.18）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
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（Telemetry Service をインストール済みのすべてのマシン）
ヘルスチェック	いいえ	はい

インストールとアップグレード

デフォルトでは、Scout は VDA または Controller のインストールまたはアップグレード時に Citrix Telemetry Service の一部として自動でインストールまたはアップグレードされます。

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、Citrix Virtual Apps and Desktops のインストールメディアに含まれる`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。

マシンが実行する Citrix Telemetry Service のバージョンが古い場合には、［収集］または ［トレースおよび再現］アクションを選択したときに、その旨を知らせるメッセージが表示されます。シトリックスではサポートされている最新バージョンを使用することをお勧めします。Telemetry Service をアップグレードしていないマシンは、［収集］と ［トレースおよび再現］の対象になりません。Telemetry Service をアップグレードするには、インストールと同じ手順を実行します。

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の ［収集］または ［トレースおよび再現］でも使用するには、［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 を構成します。または、プロキシサーバーの IP アドレスとポート番号を指定できます。

手動でのマシンの追加

Scout が検出した Controller と VDA の一覧が表示されたら、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなどの展開にある他のマシンを手動で追加できます。

ヘルスチェックの実行時には、以下のようになります:

- ドメイン内の Citrix ライセンスサーバーは自動検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンの一覧が表示されている Scout のページで、［**+** マシンの追加］をクリックします。追加するマシンの完全修飾ドメイン名を入力し、［続行］をクリックします。必要に応じて、他のマシンの追加を繰り返します。（FQDN の代わりに DNS エイリアスを入力しても有効に見える場合がありますが、ヘルスチェックは失敗する可能性があります）

手動で追加したマシンは、常に、マシンの一覧の上部、検出されたマシンの上に表示されます。

手動で追加したマシンを簡単に識別する方法は、行の右端にある赤い削除ボタンです。手動で追加したマシンにだけこのボタンがあります。検出されたマシンにはありません。

手動で追加したマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。手動で追加した他のマシンの削除を繰り返します。

Scout は、削除されるまで、手動で追加されたマシンを覚えています。Scout を閉じてから再び開くと、手動で追加したマシンはそのまま一覧の一番上に表示されています。

StoreFront サーバーでトレースおよび再現を使用しているときは、CDF トレースは収集されません。ただし、他のすべてのトレース情報は収集されます。

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。

1. Scout を起動します。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。
2. マシンを選択します。［マシンの選択］ページに、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。

   StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。

   選択した各マシン上で Scout が確認テストを自動で開始し、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します。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。

3. 診断情報を収集します。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。
   - 診断情報を再度収集するには、そのマシンの ［アクション］列で ［再度収集する］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。
   - 選択した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。（クリックすると、収集した情報は失われます）

   収集が完了したら、［続行］をクリックします。

4. 収集情報を保存またはアップロードします。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 にアップロードできます。CTX136396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。

5. アップロードの認証を行い、任意でプロキシを指定します。詳しくは、「アップロードの認証」を参照してください。

   - Scout で認証を行っていない場合、以下の手順を実行します。
   - Scout で認証を行っている場合は、デフォルトで保存済みの認証トークンが使用されます。それでよい場合には、このオプションを選択して ［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取得する場合は、［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。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。

6. アップロードの情報を入力します。

   - ［名前］フィールドには、収集した診断情報の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、トレースを開始し、問題を再現し、診断情報の収集を完了してから、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。すべての診断情報には AOT トレース情報が含まれています。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。

1. Scout を起動します。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。

2. マシンを選択します。［マシンの選択］ページに、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ます。次に、［続行］をクリックします。

   StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。

   選択した各マシン上で Scout が確認テストを自動で開始し、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します。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および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。

3. トレースを開始します。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。

4. マシンの診断情報を収集します。［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。
   - マシンから診断情報を再度収集するには、そのマシンの ［アクション］列で ［再度収集する］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。
   - 選択した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。（クリックすると、収集した情報は失われます）

   収集が完了したら、［続行］をクリックします。

5. 収集情報を保存またはアップロードします。ファイルを Citrix にアップロードするか、ローカル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。注意: ファイルは後でシトリックスからアップロードできます。Citrix Insight Services の場合はCTX136396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。

6. アップロードの認証を行い、任意でプロキシを指定します。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。

   - Scout で認証を行っていない場合、以下の手順を実行します。
   - Scout で認証を行っている場合は、デフォルトで保存済みの認証トークンが使用されます。それでよい場合には、このオプションを選択して ［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取得する場合は、［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。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 Web 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。

7. アップロードの情報を入力します。

   アップロードの詳細を入力します。

   - ［名前］フィールドには、収集した診断情報の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

> 注:
>
> 収集機能についてはスケジュールを指定して実行することができますが、現時点ではヘルスチェックでスケジュールを指定することはできません。

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。詳しくは、「Citrix Call Home」を参照してください）。

1. Scout を起動します。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。
2. マシンを選択します。サイト内のすべての VDA とコントローラー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 およびコントローラーをインストールした場合、Call Home スケジュールを設定すると（「Citrix Call Home」を参照）、Scout ではデフォルトで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。

   コンポーネントのインストール時に Call Home をマシンごとに有効化または無効化しても、Scout で設定されたスケジュールは選択したすべてのマシンに影響します。

   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。

   StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。

   選択した各マシン上で Scout が確認テストを自動で開始し、各マシンが「確認テスト」の基準を満たしているか確認します。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。

3. スケジュールを設定します。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。曜日を選択します。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。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。

4. アップロードの認証を行い、任意でプロキシを指定します。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。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。

   収集中、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。

ヘルスチェックの実行

ヘルスチェックはマシンの選択、チェックの開始、結果レポートの確認の各手順から構成されます。

1. Scout を起動します。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 ［ヘルスチェック］をクリックします。

2. マシンを選択します。［マシンの選択］ページには、サイト内にあるすべての VDA、Delivery Controller、ライセンスサーバー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。

   他のタイプのコンポーネント（StoreFront サーバーなど）を追加するには、「手動でのマシンの追加」を参照してください。Citrix Provisioning サーバーやライセンスサーバーを手動で追加することはできません。

   選択した各マシン上で Scout が確認テストを自動で開始し、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します。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）。そのマシンのヘルスチェックは実行されません。

   確認テストが完了したら、［続行］をクリックします。

3. 選択したマシンのヘルスチェックを実行します。概要に、ヘルスチェックが実行されるマシン（選択し、確認テストに合格したマシン）が一覧表示されます。［チェックの開始］をクリックします。

   確認中および確認後の状態：

   - ［状態］列には、マシンの現在のチェック状態が表示されます。
   - 進行中のチェックをすべて停止するには、ページの右下隅にある ［チェックの停止］をクリックします。（ヘルスチェックの取り消しはチェック対象のマシン全台に適用されます。マシン単体を選んで取り消すことはできません。チェックが完了したマシンからの情報は保持されます。
   - すべての選択したマシンでチェックが完了すると、右下隅にある ［チェックの停止］が ［完了］に変わります。
   - チェックが失敗した場合は、［操作］列の ［再試行］をクリックできます。
   - チェックが完了しても問題が見つからなかった場合は、［操作］列には何も表示されません。
   - チェックで問題が見つかった場合は、［詳細の表示］で結果を確認できます。
   - すべてのマシンでチェックが完了した後に、［戻る］をクリックしないでください。（クリックすると、チェック結果は失われます）

4. チェックが終了したら、［完了］をクリックして Scout の開始ページに戻ります。

ヘルスチェックの結果

Citrix がチェックするレポート生成には、次の情報が含まれます：

- 結果レポートが生成された日時
- チェックが行われたマシン
- チェック対象のマシンで検索する条件

データマスキング

Citrix Scout を使用して収集した診断情報は、セキュリティ上の機密情報が含まれている場合があります。Citrix Scout のデータマスキング機能を使用すると、シトリックスにアップロードする前に診断ファイル内の機密データをマスキングすることができます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、SID をマスキングするように構成されます。

> 注:
>
> CDF トレースは暗号化されており、マスキングすることはできません。
>
> Linux VDA ログは`.tar.gz2`形式で圧縮されており、マスキングすることはできません。

新しい診断情報の収集およびデータマスキングの実行

Citrix Scout のデータマスキング機能を使用するには、コマンドラインで Scout を起動します。

1. Windows で、管理者としてコマンドプロンプトを開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scout を起動します: `ScoutUI.exe datamasking`。
4. [収集] または [トレースと再現] をクリックして診断情報を収集します。
5. 収集の完了後、[データマスキングを有効にする] を選択します。このオプションは、デフォルトで有効になっています。
6. データマスキングを構成します。デフォルトの規則を使用するか、規則をカスタマイズできます。
7. 収集した診断情報をアップロードするか保存するかを選択します。
   - [収集した診断情報を **Citrix** にアップロードする] を選択した場合、マスキングされた診断情報ファイルがシトリックスにアップロードされます。
   - [収集した診断情報をローカルマシンに保存する] を選択した場合、元の診断情報とマスキングされた診断情報の両方が指定された場所に保存されます。

既存の診断情報でデータマスキングを実行

1. Windows で、管理者としてコマンドプロンプトを開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードで Scout を直接起動します: `ScoutUI.exe datamasking filePath`。
4. [データマスキングを有効にする] を選択して続行します。このオプションは、デフォルトで有効になっています。
5. データマスキングを構成します。デフォルトの規則で、または規則をカスタマイズしてデータマスキングを実行できます。

6. 収集した診断情報をアップロードするか保存するかを選択します。
    - ［収集した診断情報を **Citrix** にアップロードする］を選択した場合、マスキングされた診断情報ファイルがシトリックスにアップロードされます。
    - ［収集した診断情報をローカルマシンに保存する］を選択した場合、元の診断情報とマスキングされた診断情報の両方が指定された場所に保存されます。

マスキングされたデータファイルとマッピングファイルの場所

診断情報をアップロードまたは保存したあと、リンクをクリックして元の診断情報やマスキングされた診断情報を開いたり、マッピング情報ファイルを開いたりできます。

監視

April 26, 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、Citrix Virtual Apps and Desktops 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」を参照してください。

構成ログ

構成ログでは、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］ビューで確認し、構成変更についての通知を提供することもできます。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
- 障害が発生したシングルセッションマシン
- 障害が発生したマルチセッションマシン

構成ログ機能の有効化と構成方法について詳しくは、「構成ログ」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

Citrix Virtual Apps and Desktops 内のサービスは、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。

構成ログ

April 26, 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。構成ログサービスは、サイト内のすべての Controller 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。

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。通常ログに記録される構成の変更や管理作業は、構成ログデータベースへの書き込みが可能になるまで許可されません。必須ログ機能は、構成ログが有効な場合（［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

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。有効な形式については「データベースのアドレス形式」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。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）。
7. データベースを手動で作成する場合は、［データベーススクリプトの生成］をクリックします。生成されるスクリプトにはデータベースを手動で作成するためのコマンドが記述されます。スキーマをアップロードする前

に、データベースが空であること、および 1 人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

変更前のデータベース内の構成ログデータは変更後のデータベースにインポートされません。構成ログデータベースの場所を変更する場合、変更前のデータベースの内容は集約されなくなります。変更後の構成ログデータベースの最初にデータベースの変更を示すログが記録されますが、変更前のデータベースの場所は記録されません。

構成ログの内容の表示

管理者が構成の変更などの管理作業を開始すると、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。ペインの上部で高レベル操作を選択すると、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、データベースでログ操作が完結しない場合があります。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です。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。次の操作を実行できます:

- 列の見出しで表示を並べ替える。
- 日間隔を指定したり、［検索］ボックスにテキストを入力したりして、表示をフィルタリングします。検索を使用した後で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。

レポートの生成

構成ログデータを CSV および HTML 形式のレポートとして書き出すことができます。

- CSV 形式のレポートには、指定した期間のすべてのログデータが書き込まれます。データベースの階層データが単一の CSV テーブルとして出力されます。データの特定の要素に基づいて並べ替えられたものではありません。書式も適用されず、読み取りやすさについても考慮されていません。レポートファイル（MyReport）には、汎用的な書式でデータが書き出されます。CSV ファイルはデータのアーカイブ化や、レポート機能または Microsoft Excel などデータ操作ツールのデータソースとして使用されます。
- HTML 形式のレポートには、指定した期間のログデータが判読可能な形式で書き込まれます。変更内容の確認が容易な、構造的でナビゲーション可能なレポートです。HTML レポートでは、概要（Summary）および詳細（Details）の 2 つのファイルが生成されます。概要レポートには、各操作の実行日時、操作主、および操作結果など、より高レベルな情報が一覧で表示されます。各操作項目の横にある［詳細］リンクをクリックすると詳細ファイルが開き、より低いレベルの操作に関する情報を参照できます。

構成ログレポートを生成するには、Studio のナビゲーションペインで ［ログ］ノードを選択し、［操作］ペインの［カスタムレポートの作成］を選択します。

- レポートの日付の範囲を選択します。
- レポート形式として、［CSV ファイル］、［HTML］、または［両方］を選択します。
- レポートを保存する場所を参照します。

構成ログの内容の削除

構成ログを削除するには、特定の委任管理権限および SQL Server データベース権限が必要です。

- 委任管理：展開構成を読み取ることができる委任管理の役割が必要です。すべての管理権限を実行できる管理者には、この権限があります。カスタムの役割では、［そのほかの権限］カテゴリで［読み取り専用］または［管理］権限を選択する必要があります。

  構成ログデータを削除する前にバックアップを作成するには、［ログ］カテゴリで［読み取り専用］または［管理］権限を選択する必要もあります。

- **SQL Server** データベース：データベースからレコードを削除するための権限を持つ SQL Server のログインアカウントが必要です。次のいずれかの方法を使用します：

  - データベースに対するすべての権限を持つ sysadmin サーバーロールを持つ SQL Server データベースログインを使用します。また、serveradmin または setupadmin サーバーロールでも削除操作を実行できます。

  - 高度なセキュリティが必要な環境では、データベースからレコードを削除する権限を持つデータベースユーザーにマップされた非 sysadmin データベースログインを使用します。

    1. SQL Server Management Studio で、sysadmin 以外のサーバーロールを持つ SQL Server ログインを作成します。
    2. 作成したログインをデータベースのユーザーにマップします。SQL Server により、ログインと同じ名前のユーザーがデータベースに作成されます。
    3. データベースロールのメンバーシップとして、このデータベースユーザーに ConfigurationLoggingSchema_ROLE または db_owner のロールを指定します。

    詳しくは、SQL Server Management Studio のドキュメントを参照してください。

構成ログを削除するには、以下の手順に従います：

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

April 24, 2021

次の記事には、Citrix Virtual Apps and Desktops に含まれる各種サービスで記録できるイベントの一覧と説明が記載されています。

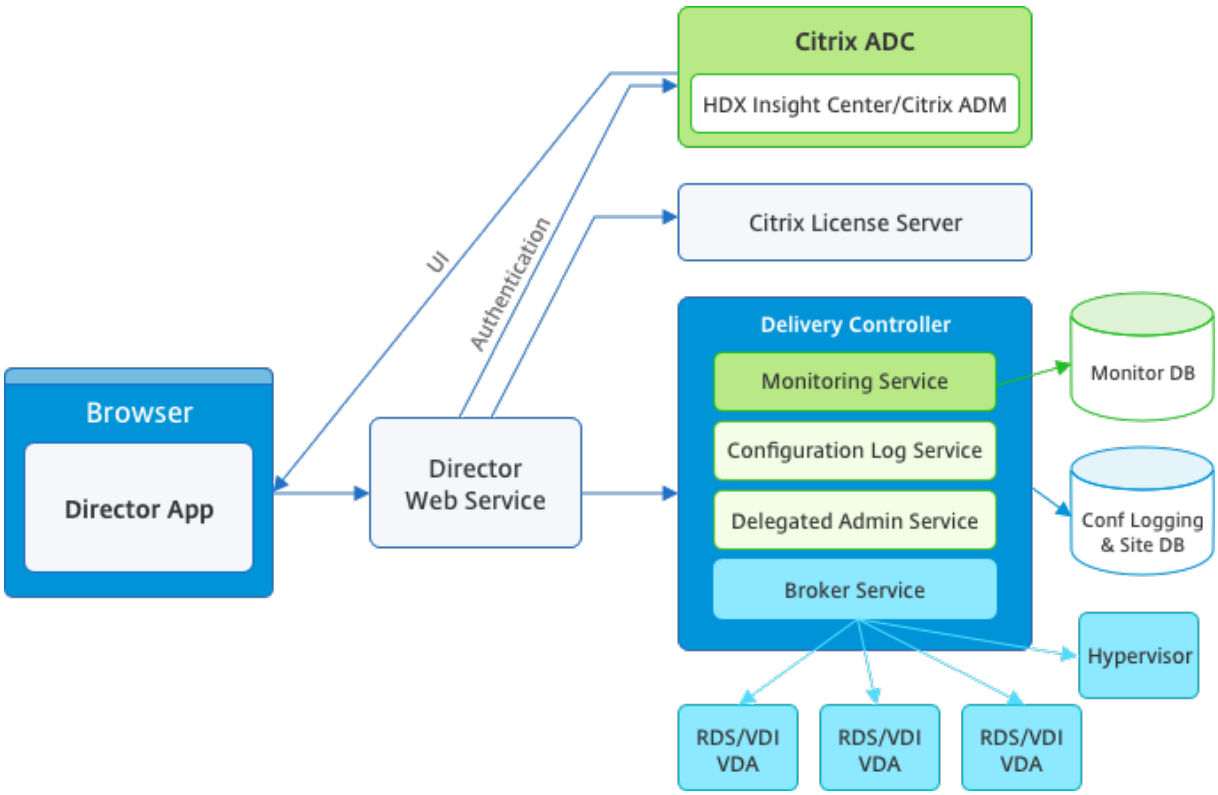
この情報は包括的ではありません。個別の特集記事で、追加のイベント情報を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- Citrix Configuration Service イベント
- Citrix Delegated Administration Service イベント

Director

April 26, 2021

Director は、Citrix Virtual Apps and Desktops の監視およびトラブルシューティングのためのコンソールです。



Director では、以下の情報にアクセスできます。

- Broker Agent からのリアルタイムデータ。Analytics、Performance Manager、および Network Inspector の機能が統合されたコンソールを使用します。
  - Analytics には、ヘルスおよびキャパシティのチェック機能と、Citrix ADM 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、Citrix Virtual Apps and Desktops 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。
- Citrix ADM を使用した Citrix Gateway からの ICA データ。
  - Citrix Virtual Apps または Desktops 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。
  - Citrix Virtual Desktop 7 Director の監視ツールに統合されています。

Director では、Citrix Virtual Apps または Desktops 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、「機能の互換性マトリックス」を参照してください。

> 注:
>
> Meltdown および Spectre の投機的実行のサイドチャネルの脆弱性に関する発表を受けて、Citrix では、問題を軽減する適切なパッチをインストールすることをお勧めしています。これらのパッチは SQL Server のパフォーマンスに影響する可能性があることに注意してください。詳しくは、Microsoft 社のサポート記事「スペクターおよびメルトダウンのサイドチャネルの脆弱性に対する攻撃から SQL Server を保護する」を参照してください。実稼働環境でパッチを展開する前にスケールをテストし、ワークロードを計画することをお勧めします。

Director は、Delivery Controller 上の Web サイトとしてデフォルトでインストールされます。必須要件およびそのほかの詳細については、このリリースのドキュメントの「システム要件」を参照してください。Director のインストールと設定の詳細については、「Director のインストールと設定」を参照してください。

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://<Server FQDN>/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 PIV スマートカード認証の使用

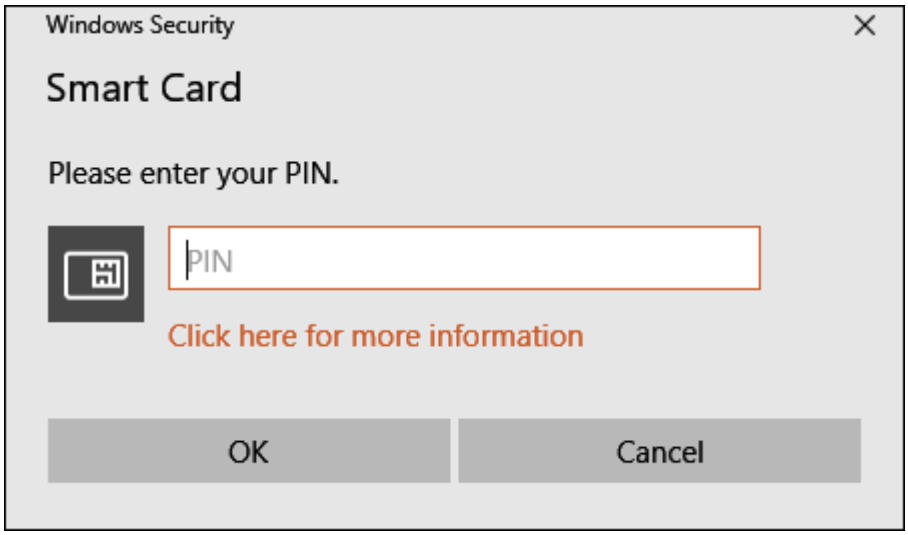
Director で、ログオンのために Personal Identity Verification（PIV）ベースのスマートカード認証がサポートされるようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関に役立ちます。

スマートカード認証には、Director サーバーと Active Directory での特定の構成が必要となります。設定手順については「PIV スマートカード認証の構成」で説明しています。

> 注:
>
> スマートカード認証は、同じ Active Directory ドメインからのユーザーに対してのみサポートされています。

必要な構成を実行した後は、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. Web ブラウザーを開き、Director の URL（`https://<directorfqdn>/Director`）に移動します。
3. 表示された一覧から有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



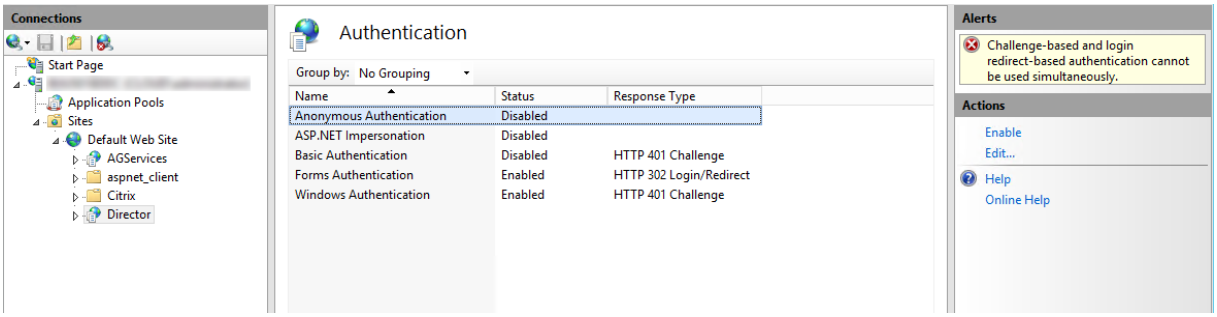
5. 認証されると、Director ログオンページで追加の資格情報を入力せずに Director にアクセスできます。

Director での統合 Windows 認証の使用

統合 Windows 認証（IWA）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。

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 でのさまざまな役割とその権限について詳しくは、「委任管理と Director」を参照してください。

Google Analytics による利用状況データ収集

Director がインストールされると、Director サービスは Google Analytics を使った利用状況データの収集を匿名で開始します。［傾向］ページと OData API 呼び出し分析の使用状況に関する統計が収集されます。Analytics のコレクションは、Citrix プライバシーポリシーに準拠しています。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 のデータ収集をオプトアウトするには、Director がインストールされているマシンで以下のようにレジストリキーを編集します。レジストリキーがまだ存在していない場合は、作成して目的の値に設定します。レジストリキー値を変更した後、Director インスタンスを更新します。

注意：レジストリエディターを誤って使用す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。変更前に Windows レジストリのバックアップを作成してください。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

値の名前：DisableGoogleAnalytics

値：0 = 有効（デフォルト）、1 = 無効

次の PowerShell コマンドレットを使用して、Google Analytics によるデータ収集を無効にすることができます。

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2
3 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
     DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Director には、最新バージョンでリリースされた新機能に関する情報を提供する製品内ガイドがあります。このガイドは、簡単な概要と適切な製品内メッセージを組み合わせているため、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Director がインストールされているマシンで以下のようにレジストリキーを編集します。レジストリキーがまだ存在していない場合は、作成して目的の値に設定します。レジストリキー値を変更した後、Director インスタンスを更新します。

注意：レジストリエディターを誤って使用す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。変更前に Windows レジストリのバックアップを作成してください。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

値の名前：DisableGuidedHelp

値：0 = 有効（デフォルト）、1 = 無効

次の PowerShell コマンドレットを使用して、製品内ガイドを無効にできます：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

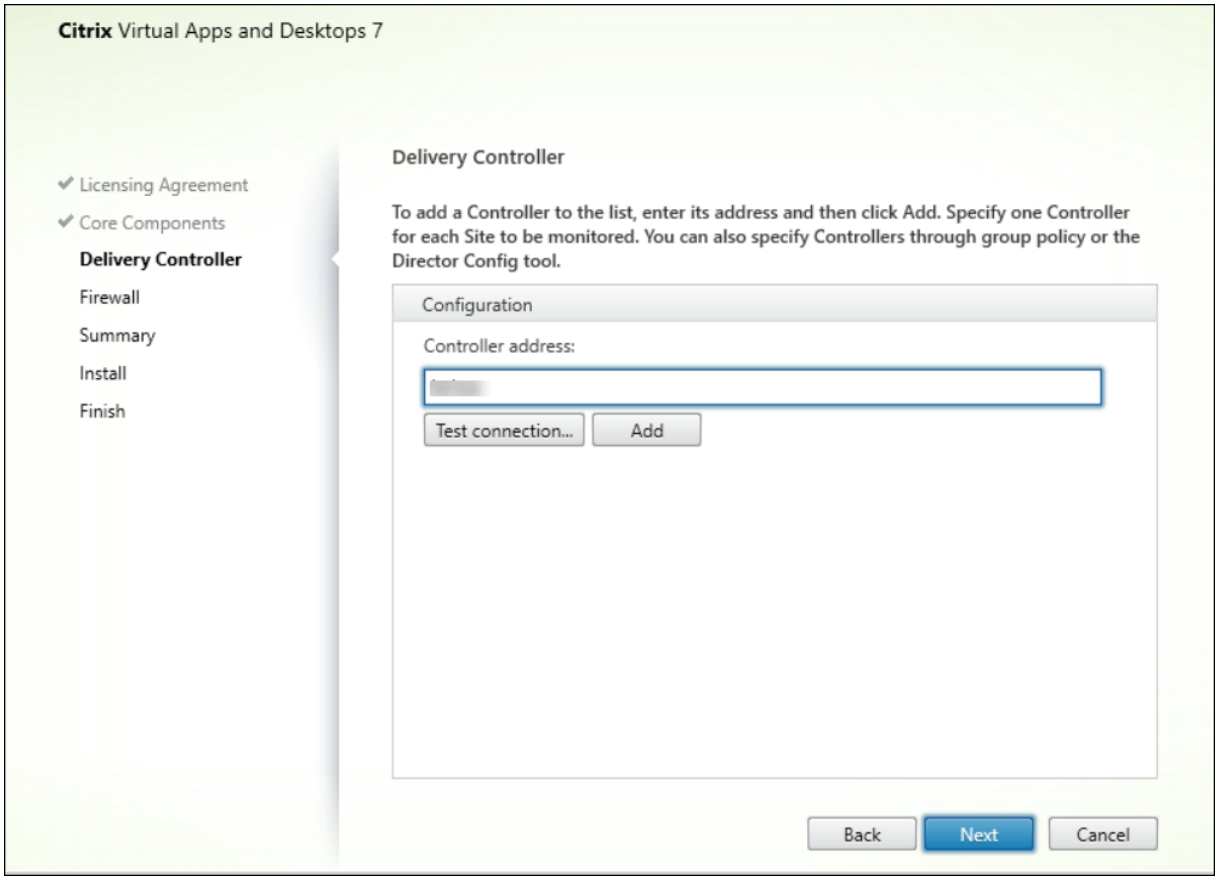
インストールと構成

April 26, 2021

Director のインストール

Director のインストールは、Citrix Virtual Apps and Desktops 用の全製品 ISO インストーラーを使って行います。このインストーラーは、前提条件をチェックして不足しているコンポーネントをすべてインストールし、Director の Web サイトをセットアップして、基本的な構成を行います。必須要件およびそのほかの詳細については、このリリースのドキュメントの「システム要件」を参照してください。このリリースの Director には、Virtual Apps 6.5 以前の環境または Virtual Desktops 7 以前の環境との互換性はありません。
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。この手順については、Microsoft IIS のドキュメントを参照してください。Director 側では、TLS を有効にするために何らかの構成を行う必要はありません。

Director の展開と構成

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。

> 重要:
>
> ユーザー名とパスワードがプレーンテキストで送信されないように、Director 接続では HTTP ではなく HTTPS での接続のみを許可することを強く推奨します。特定のツールを使用すると、HTTP（非暗号化）ネットワークパケット内のプレーンテキストのユーザー名やパスワードを読み取ることができるため、ユーザーにとってセキュリティ上のリスクとなる場合があります。

権限を構成する

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（「詳細な構成」を参照）
- 構成済みの委任管理者ロール（「委任管理と 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。

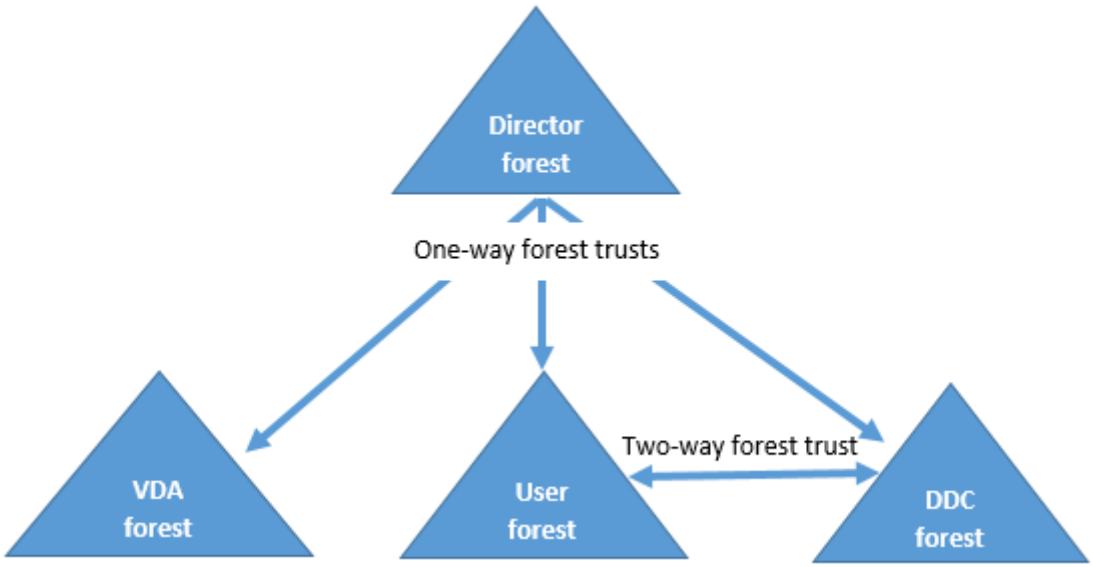
詳細な構成

April 24, 2021

Director は、ユーザー、Delivery Controller（DC）、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 Delivery Controller の問題をトラブルシューティングできます。

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。
5. 新しい設定を追加するには ［追加］をクリックします。

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。次のアプリケーション設定を IIS マネージャーの Director Web サイトに構成します:

```
1 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:

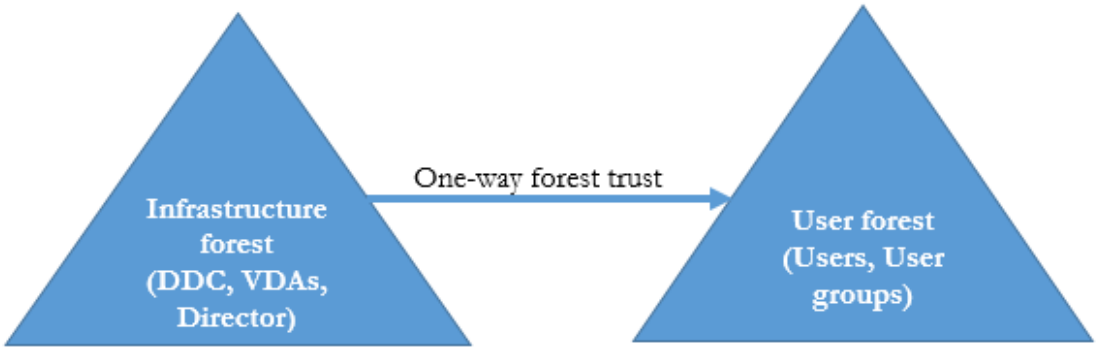
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

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。

ドメインローカルグループの設定

ほとんどの Citrix Service Provider（CSP）は、Infrastructure フォレストと呼ばれるところに、VDA、DC、および Director で構成される同様の環境設定を備えています。ただし、ユーザーまたはユーザーグループのレコードは Customer フォレストに属しています。Infrastructure フォレストから Customer フォレストへの一方向の送信の信頼が存在します。

CSP 管理者は、通常、Infrastructure フォレスト内にドメインローカルグループを作成し、Customer フォレスト内のユーザーまたはユーザーグループをこのドメインローカルグループに追加します。



Director は、このようなマルチフォレストの設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. 次のアプリケーション設定を IIS マネージャーの Director Web サイトに追加します:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true Connector.
       ActiveDirectory

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domain1><domain2> は、ドメインローカルグループが存在するフォレストの名前です。

2. Citrix Studio でドメインローカルグループをデリバリーグループに割り当てます。

3. 変更を有効にするには、IIS を再起動して Director に再度ログオンします。これで、Director でこれらのユーザーのセッションを監視して表示できます。

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
<!--NeedCopy-->
```

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。

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。
   次の設定で値を変更します:
   UI.TaskManager.EnableApplications = false

> 重要:
>
> 実行中のアプリケーションの表示を無効にするには、これらの両方の値を変更して、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。

PIV スマートカード認証の構成

April 26, 2021

この記事では、スマートカード認証機能を有効にするために Director サーバーと Active Directory で必要な構成について説明します。

> 注:
> スマートカード認証は、同じ Active Directory ドメインからのユーザーに対してのみサポートされています。

Director サーバー構成

Director サーバーで、次の構成手順を実行します。

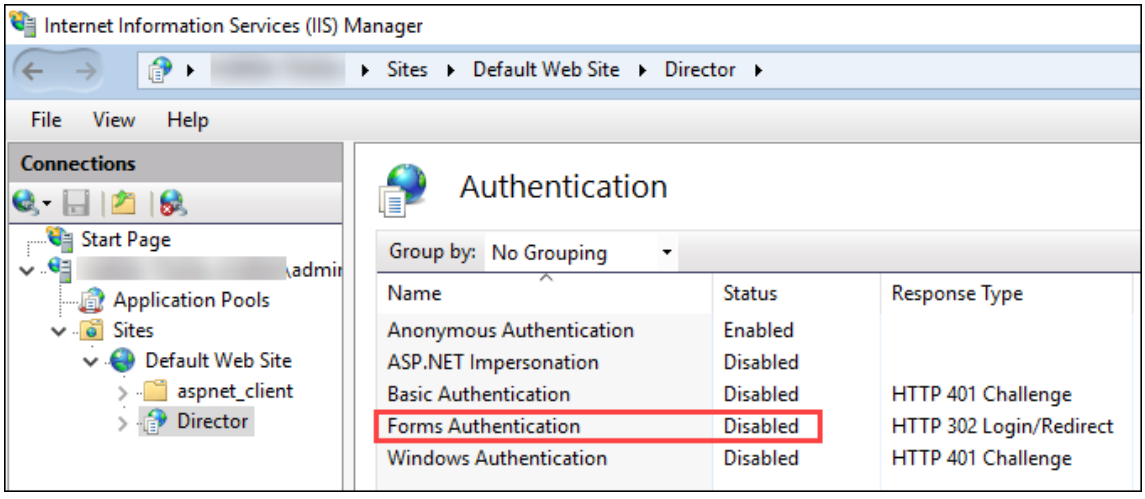
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoft のドキュメント「Client Certificate Mapping Authentication」の「**Client Certificate Mapping authentication using Active Directory**」の説明に従います。
2. Director サイトでフォーム認証を無効にします。

   IIS マネージャーを起動します。

   [サイト] > [既定の **Web** サイトのホーム] > [**Director**] に移動します。

   [認証] を選択します。

   [フォーム認証] を右クリックし、[無効化] を選択します。



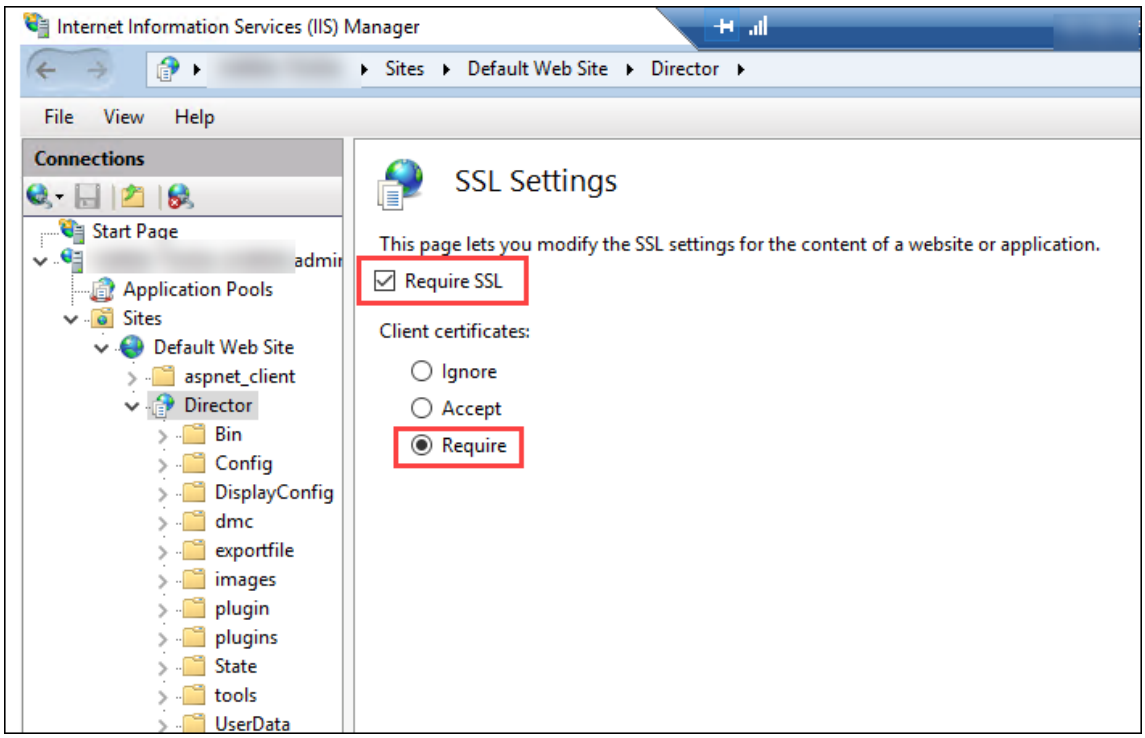
3. クライアント証明書認証として、Director URL に、より安全な https プロトコル（http ではなく）を設定します。

   a) IIS マネージャーを起動します。

   b) ［サイト］>［既定の **Web** サイトのホーム］>［**Director**］に移動します。

   c) ［**SSL** 設定］を選択します。

   d) ［**SSL** を必須にする］および ［クライアント証明書］>［必須］を選択します。



4. web.config を更新します。テキストエディターを使用して web.config ファイル(c:\inetpub\wwwroot\Director にある）を開きます。

<system.webServer>親要素の下で、最初の子要素として次のスニペットを追加します:

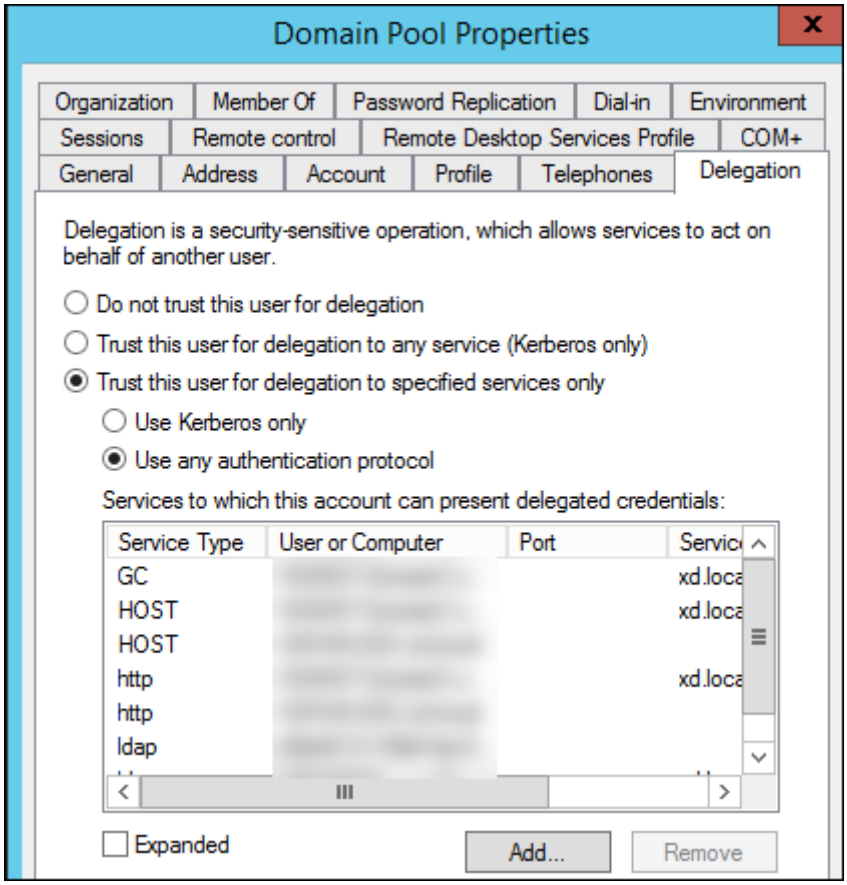
```
<defaultDocument>
<files>
<add value="LogOn.aspx"/>
</files>
</defaultDocument>
```

Active Directory 構成

デフォルトでは、Director アプリケーションは、アプリケーションプール ID プロパティを使用して実行されます。スマートカード認証には委任が必要であり、この委任には、Director アプリケーション ID にサービスホスト上の TCB（Trusted Computing Base）特権が必要となります。

アプリケーションプール ID 用に別個のサービスアカウントを作成することを Citrix ではお勧めします。Microsoft の MSDN の記事「制約付き委任を使用したプロトコル移行テクニカルサプリメント」内の説明に従って、サービスアカウントを作成し、TCB 特権を割り当てます。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント Domain Pool のプロパティダイアログです。

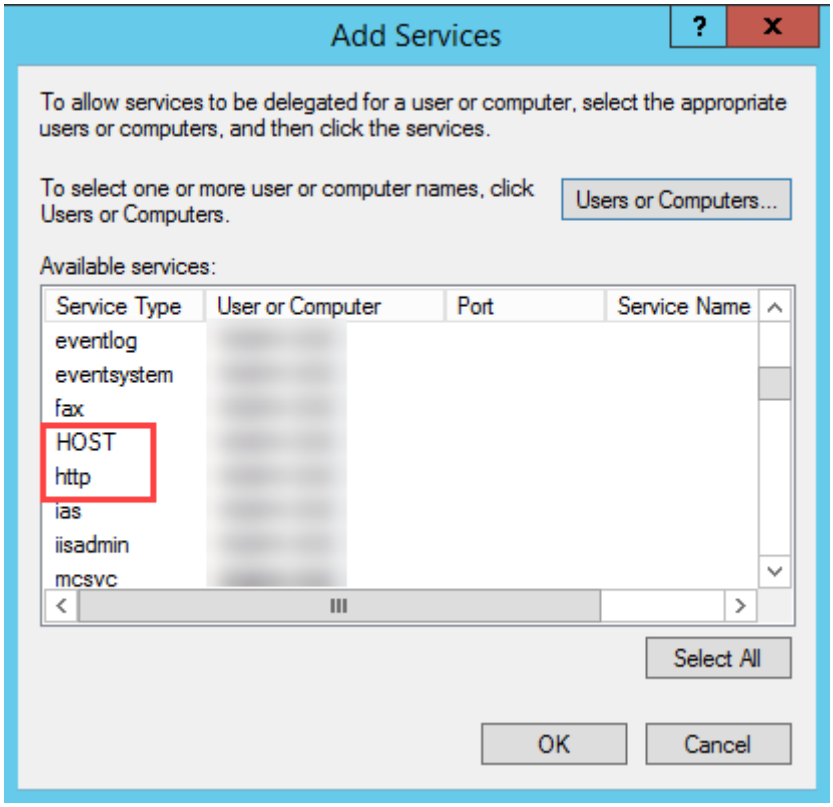


このアカウント用に以下のサービスを構成します：

- Delivery Controller：HOST、http
- Director：HOST、http
- Active Directory：GC、LDAP

これを行うには、次のようにします。

1. ユーザーアカウントのプロパティダイアログで、［追加］をクリックします。
2. ［サービスの追加］ダイアログで、［ユーザーまたはコンピューター］をクリックします。
3. Delivery Controller ホスト名を選択します。
4. ［使用可能なサービス］一覧から、［HOST］および［http］サービスタイプを選択します。



同様に、**Director** および **Active Directory** のホストのサービスタイプを追加します。

Firefox ブラウザー構成

Firefox ブラウザーを使用するには、OpenSC 0.17.0で使用可能な PIV ドライバーをインストールします。詳しくは、「OpenSC のインストール PKCS#11 Firefox のモジュール、ステップバイステップ」を参照してください。Director でスマートカード認証機能を使用する方法については、Director の記事で「Director での PIV スマートカード認証の使用」のセクションを参照してください。

ネットワーク分析機能の構成

April 26, 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、Citrix ADM との統合により、次のようなネットワーク分析機能と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、Citrix ADM の HDX Insight を使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。こ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:

- [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 に Citrix ADM をインストールし、構成する必要があります。Director には、Citrix ADM Version 11.1 Build 49.16 以降が必要です。NetScaler 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、Citrix ADMのドキュメントを参照してください。

> 注:
> Citrix NetScaler Insight Center のメンテナンスは、2018 年 5 月 15 日時点で終了しました。「シトリックスの製品マトリクス」を参照してください。ネットワーク分析機能を利用するには、Director を Citrix ADM と統合してください。NetScaler Insight Center から Citrix ADM に移行するには、「NetScaler Insight Center から Citrix ADM への移行」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、Citrix ADM 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、および接続の種類として HTTPS（HTTP よりも望ましい）を入力して、Citrix ADM 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。

委任管理と **Director**

April 26, 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。シングルセッション 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。マルチセッション 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	[マシン詳細] ページ（マシンベースの検索）にのみアクセスできます。
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

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:

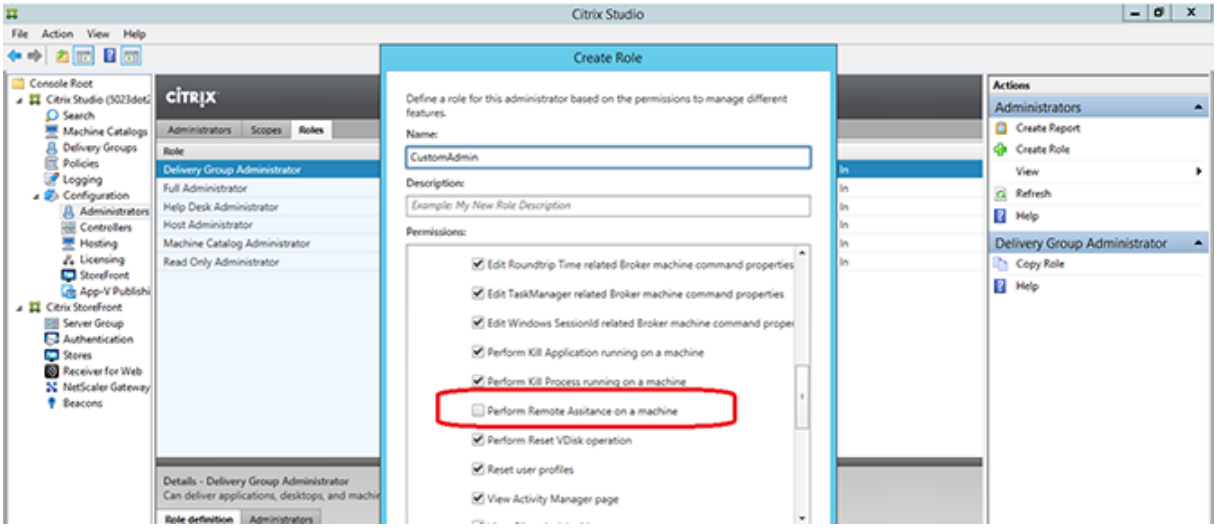
- Director にログオンするための Delivery Controller 権限 - 少なくとも管理者ノードでの読み取り専用アクセス
- デリバリーグループのデータを Director で閲覧するための権限 - 少なくとも読み取り専用アクセス

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

April 26, 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、Citrix ADC との通信を保護する必要があります。

Director と Citrix Virtual Apps and Desktops サーバー間の（監視機能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 Citrix ADC の（Citrix 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。

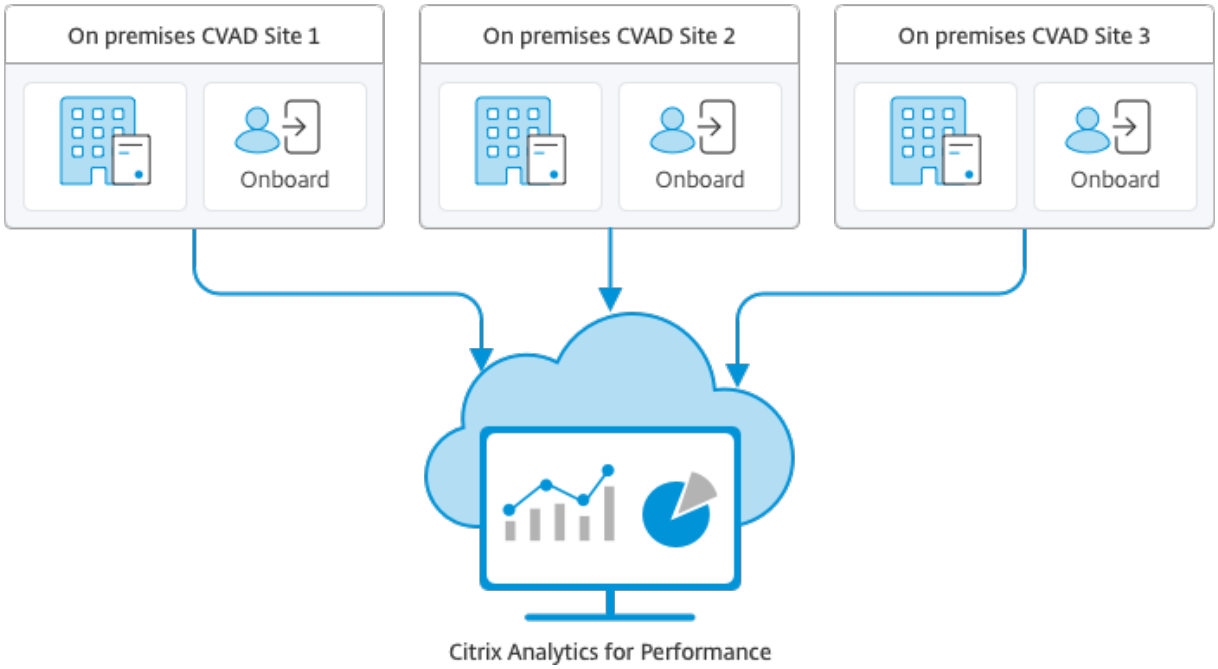
Citrix Analytics for Performance を使用したオンプレミスサイトの構成

April 26, 2021

Citrix Analytics for Performance（パフォーマンス分析）は、Citrix Analytics クラウドサービスの包括的なパフォーマンス監視ソリューションです。パフォーマンス分析は、パフォーマンスメトリックに基づいて構築された高度な洞察と分析を提供します。パフォーマンス分析は、組織内の 1 つまたは複数の Citrix Virtual Apps and Desktops サイトの使用状況とパフォーマンスメトリックを監視および表示するのに役立ちます。

パフォーマンス分析について詳しくは、「パフォーマンス分析の記事」を参照してください。

パフォーマンスデータをサイトから Citrix Cloud 上の Citrix Analytics for Performance に送信して、高度なパフォーマンス分析機能を活用できます。パフォーマンス分析を表示して使用するには、まず **Director** の［**Analytics**］タブから、Citrix Analytics for Performance でオンプレミスサイトを構成する必要があります。



パフォーマンス分析は安全な方法でデータにアクセスし、Citrix Cloud からオンプレミス環境にデータが転送されることはありません。

前提条件

Director からパフォーマンス分析を構成するには、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認します:

- Delivery Controller と Director のバージョンは 1909 以降を使用しています。詳しくは、「機能の互換性マトリックス」を参照してください。
- この構成を実行するための［**Analytics**］タブには、すべての管理権限を実行できる管理者のみがアクセスできます。
- パフォーマンス分析でパフォーマンスメトリックにアクセスする場合、アウトバウンドインターネットアクセスは、すべての Delivery Controller、および Director がインストールされているマシンで利用できます。具体的には、次の URL にアクセスできるようにしてください。
  - Citrix キーの登録: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`
- Delivery Controller と Director マシンがイントラネット内にあり、送信用のインターネットアクセスがプロキシサーバーを経由している場合、以下を確認してください:
  - プロキシサーバーは、前述の URL 一覧をホワイトリストに登録する必要があります。

- Director の web.config ファイルと Monitor.exe.config ファイルに次の構成を追加します:

```
<system.net>
<defaultProxy>
<proxy  usesystemdefault = "false"  proxyaddress = "http://
    proxyserver:80" bypassonlocal = "true"  />
<bypasslist>
<add address="http://[a-z]+\.abc \.com/" />
</bypasslist>
</defaultProxy>
</system.net>
```

この設定は Microsoft によって IIS で提供されます。詳しくは、「https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration」を参照してください。

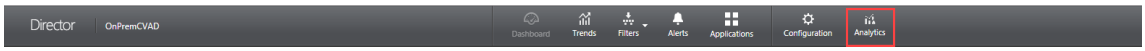
構成ファイルの **defaultproxy** フィールドは、Director およびモニターサービスの送信アクセスを制御します。パフォーマンス分析の構成および通信で、**defaultproxy** フィールドを **true** に設定する必要があります。適用されるポリシーでこのフィールドを false に設定することもできます。この場合、フィールドを手動で true に設定する必要があります。変更を加える前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller の Monitoring Service を再起動します。

- アクティブなパフォーマンス分析用 Citrix Cloud 使用権があります。
- Citrix Cloud アカウントは、製品登録操作の権限を持つ管理者アカウントです。管理者権限について詳しくは、「管理者権限の変更」を参照してください。

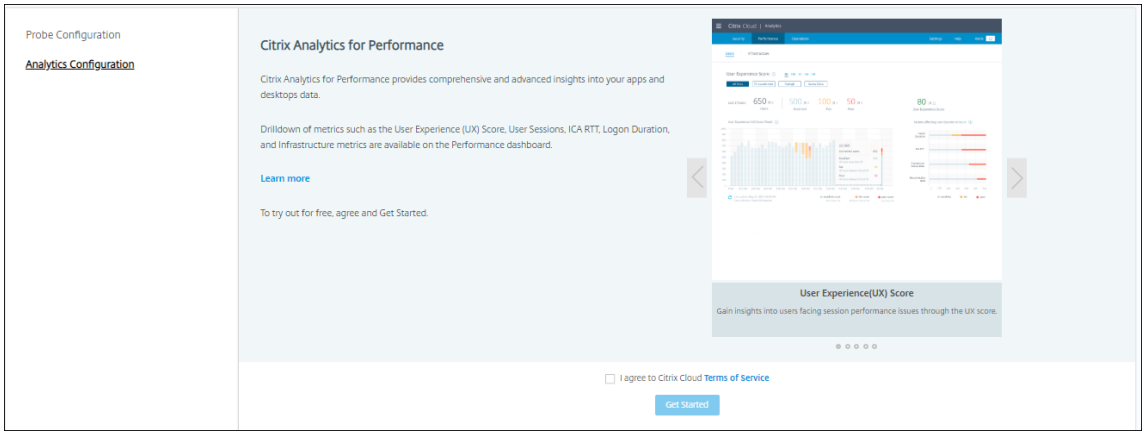
構成の手順

前提条件を確認したら、次の操作を行います:

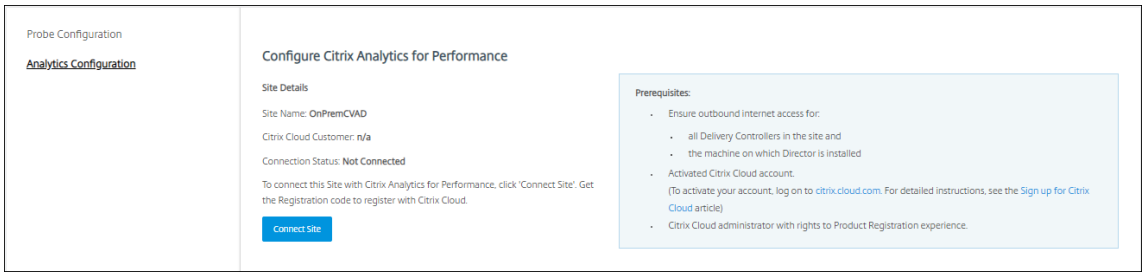
1. すべての管理権限を実行できる管理者として Director にログオンし、パフォーマンス分析で構成するサイトを選択します。
2. [**Analytics**] タブをクリックします。[構成] ページが表示されます。



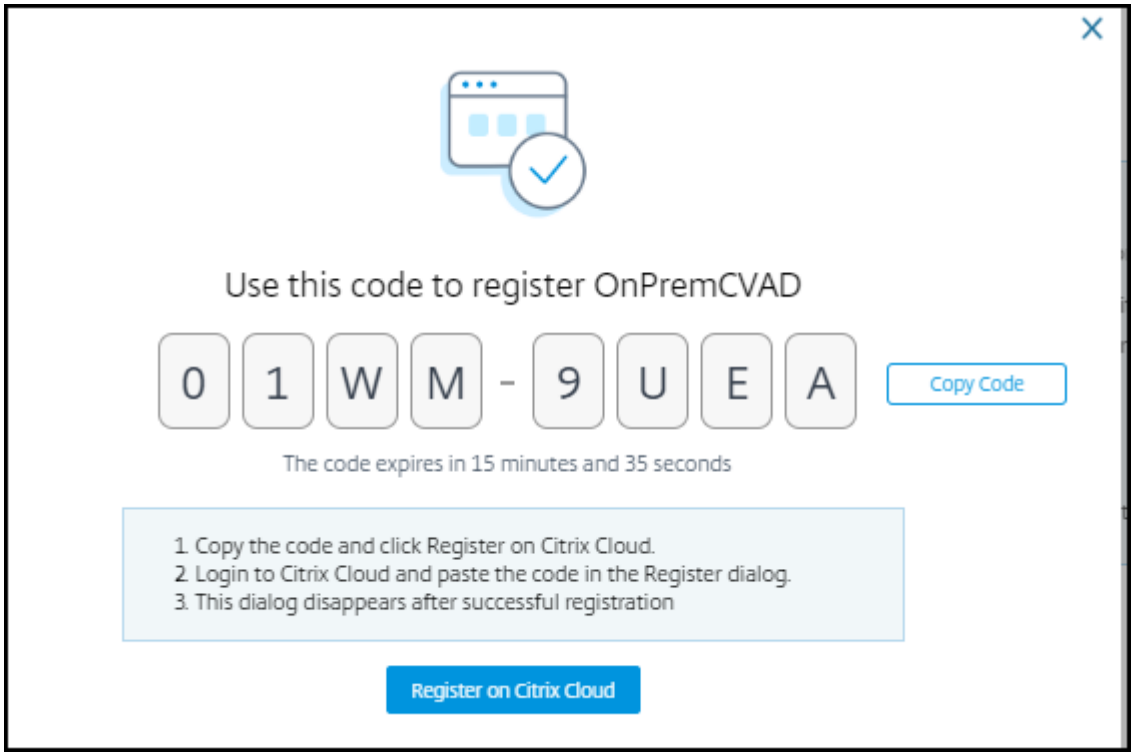
3. 手順を確認し、サービス利用規約を選択し、[導入] をクリックします。



4. 前提条件を確認し、それらが満たされていることを確認します。サイトの詳細を確認します。
5. ［サイトを接続する］をクリックして、構成プロセスを開始します。

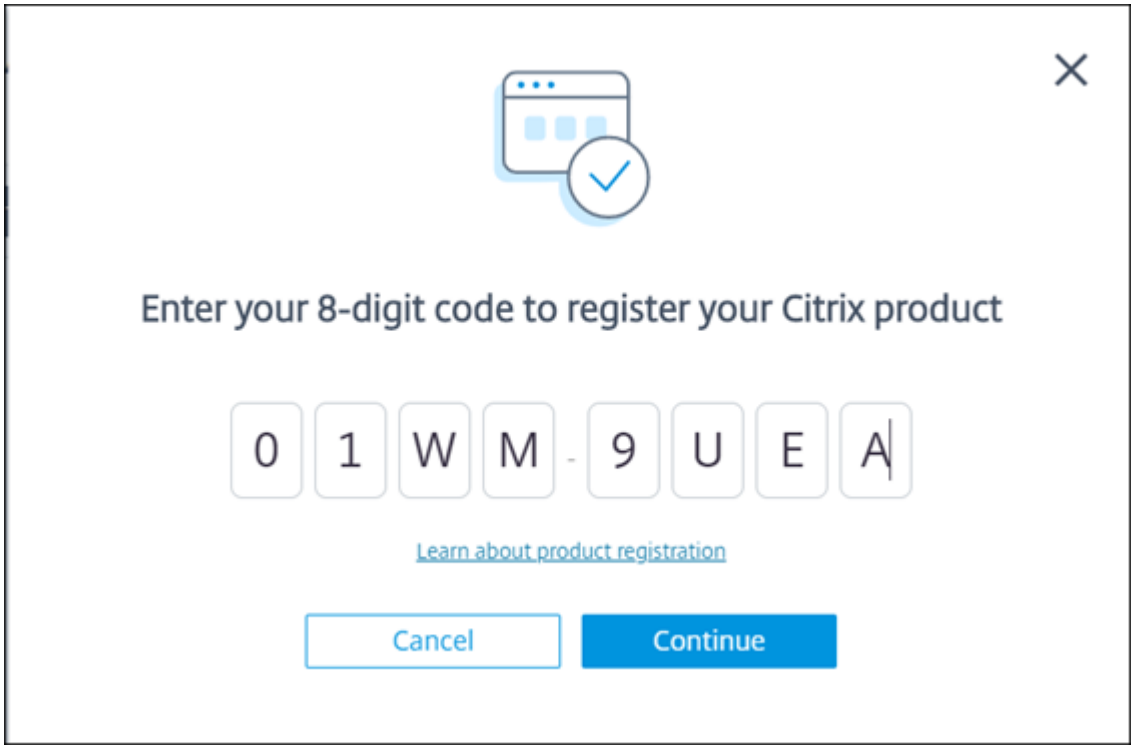


6. 本サイトを Citrix Cloud に登録するために使用する一意の 8 桁の登録コードが生成されます。

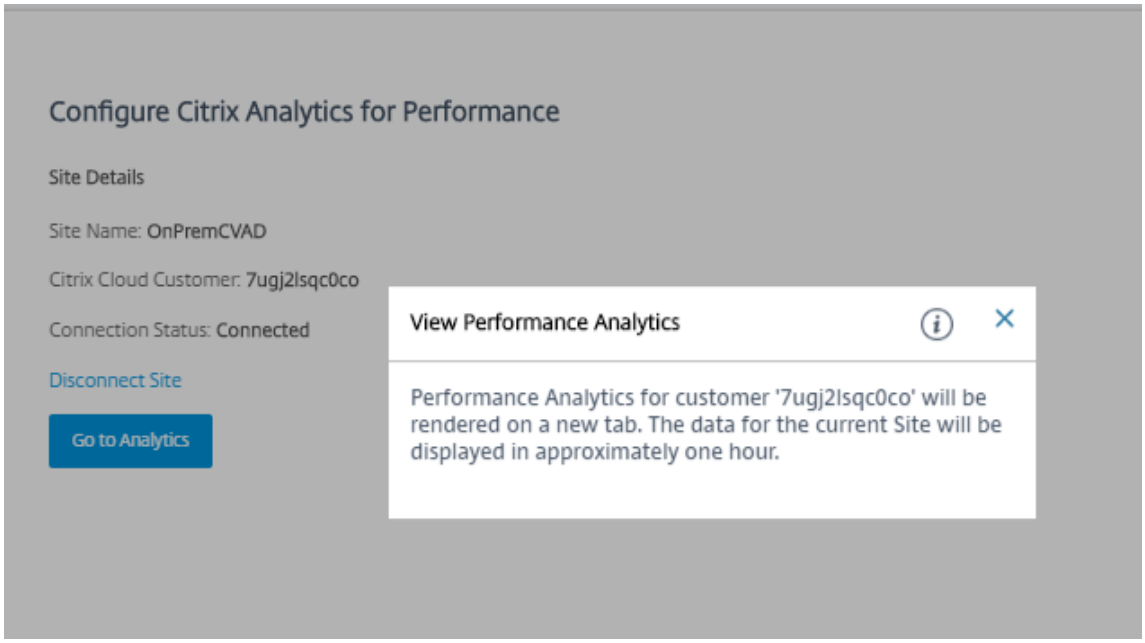


7. ［コードのコピー］をクリックしてコードをコピーし、［**Citrix Cloud** に登録］をクリックします。

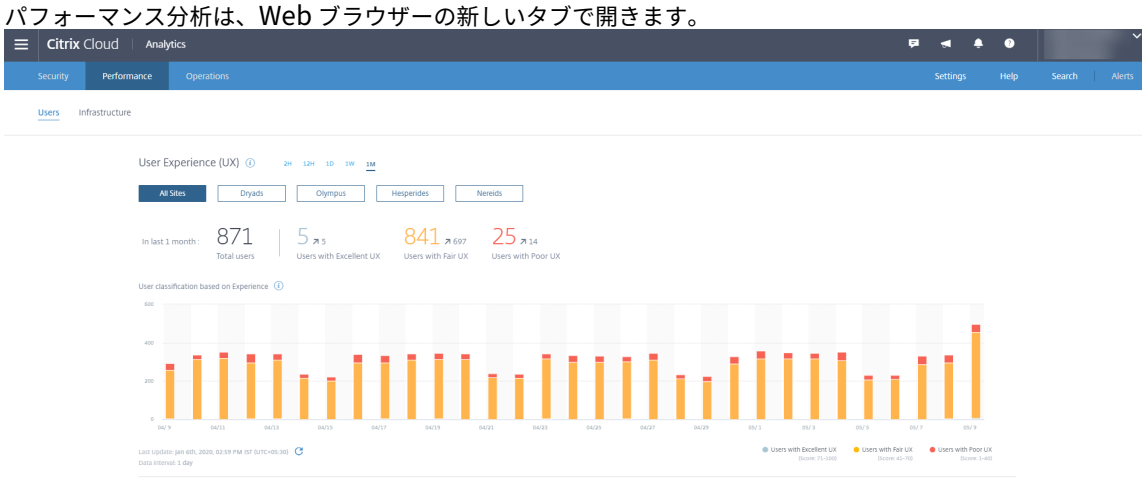
8. Citrix Cloud の登録 URL にリダイレクトされます。Citrix Cloud の資格情報でログインし、顧客を選択します。
9. コピーした登録コードを Citrix Cloud の［製品の登録］ページに貼り付けます。［続行］をクリックして登録します。登録の詳細を確認してから、［登録］をクリックします。



10. オンプレミスサイトが Citrix Cloud に登録されます。次に、**Director** から［**Analytics**］タブで［**Analytics** に移動］をクリックします。



11. パフォーマンス分析は、Web ブラウザーの新しいタブで開きます。



Citrix Cloud セッションの有効期限が切れている場合、Citrix.com または My Citrix アカウントのログオンページにリダイレクトされることがあります。

12. 複数のサイトをパフォーマンス分析に登録するには、Director のサイトごとに前述の構成手順を繰り返します。すべての構成済みサイトのメトリックは、パフォーマンス分析ダッシュボードに表示されます。

    サイトごとに複数の Director インスタンスが実行されている場合は、任意の Director インスタンスから構成します。サイトに接続されている他のすべての Director インスタンスは、構成プロセス後の次回の更新時に更新されます。

13. Citrix Cloud からサイトを切断するには、［サイトを切断する］をクリックします。このオプションは、既存の構成を削除します。

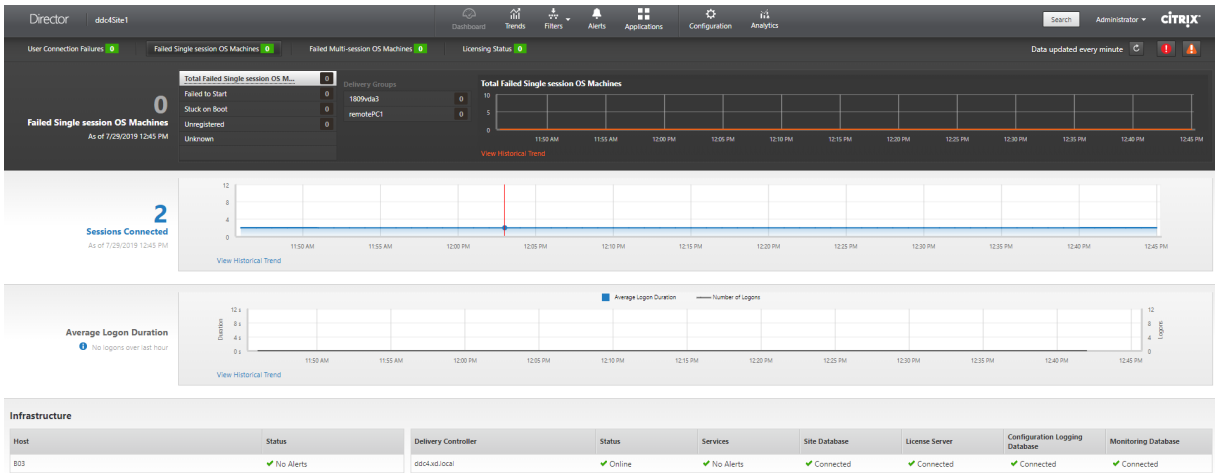
    > 注:
    >
    > サイトを初めて構成するときに、サイトからのイベントの処理に多少の時間（約 1 時間）がかかる場合があります。このため、Performance Analytics ダッシュボードでのメトリックの表示に遅延が生じます。その後、イベントは定期的に更新されます。
    >
    > 切断すると、新しいアカウントからのイベントが転送されるまで、古いアカウントからのデータ送信がしばらく継続されます。データ送信が停止してから約 1 時間、古いアカウントに関連する分析がパフォーマンス分析ダッシュボードに表示されたままになります。
    >
    > Citrix Analytics サービスの使用権限の有効期限が切れると、パフォーマンス分析へのサイトメトリックの送信を停止するまでに 1 日ほどかかります。

サイト分析

April 26, 2021

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。

Director のダッシュボードのパネル

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」を参照してください。

失敗したシングルセッション **OS** マシンまたは失敗したマルチセッション **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。マルチセッション OS マシンの場合は、最大負荷に達しているマシンも含まれます。

ライセンスの状態

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートメッセージとそのアラートを解決するための操作が表示されます。ライセンスサーバー 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。［**Delivery Controller**］ > ［詳細］ > ［製品エディション］ > ［**PLT**］の画面に表示されるライセンスステータスは ［**Premium**］です（[**Platinum**］ではありません）。

猶予期間の状態

Director は、次のいずれかの猶予期間の状態を表示します。この情報は、Delivery Controller から取得します。

1. 非アクティブ：どの種類の猶予期間にも該当しません。通常のライセンス制限が適用されます。
2. 購入時猶予期間：新しいインストール後、ライセンスのないライセンスサーバーを参照した場合に、最初の 30 日間 10 接続が提供されます。
3. 追加猶予期間：すべてのライセンスが消費されると新しいライセンスが追加されるまで、または消費数が少なくなるまでビジネス継続性のために 15 日間の猶予期間が提供されます。追加猶予期間中は、無制限の接続が許可されます。ユーザーは影響を受けません。追加猶予期間が期限切れになるまで、またはリセットされるまで Director で表示された警告は破棄できません。
4. 緊急猶予期間：ライセンスサーバーに到達できない場合、または接続の仲介中ライセンス情報が取得できない場合に有効になります。緊急猶予期間は 30 日間有効です。ユーザーは影響を受けません。ライセンスサーバーに到達できるようになるまで、Director で表示されたエラーは破棄できません。
5. 猶予期間の期限切れ：緊急猶予期間または追加猶予期間が期限切れになりました。

詳しくは、「ライセンスの超過使用保護」および「追加猶予期間」を参照してください。

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覧 - ホストおよびコントローラー。Citrix Hypervisor または VMware のインフラストラクチャで、パフォーマンスアラートを表示できます。たとえば、XenCenter では、サーバーまたは仮想サーバーの CPU、ネットワーク I/O、またはディスク I/O の使用量が特定のしきい値を超えた場合にパフォーマンスアラートが発せられるように構成できます。アラートの送信間隔はデフォルトで 60 分ですが、必要に応じて変更できます。詳しくは、Citrix Hypervisor 製品ドキュメントの 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］ビューの ［セッション］タブを選択して、長期間の接続セッションと切断セッション（つまり直近の 60 分よりも前のすべてのセッション）に関する使用状況データを詳細に確認できます。この情報を表示するには、［履歴傾向の表示］をクリックします。

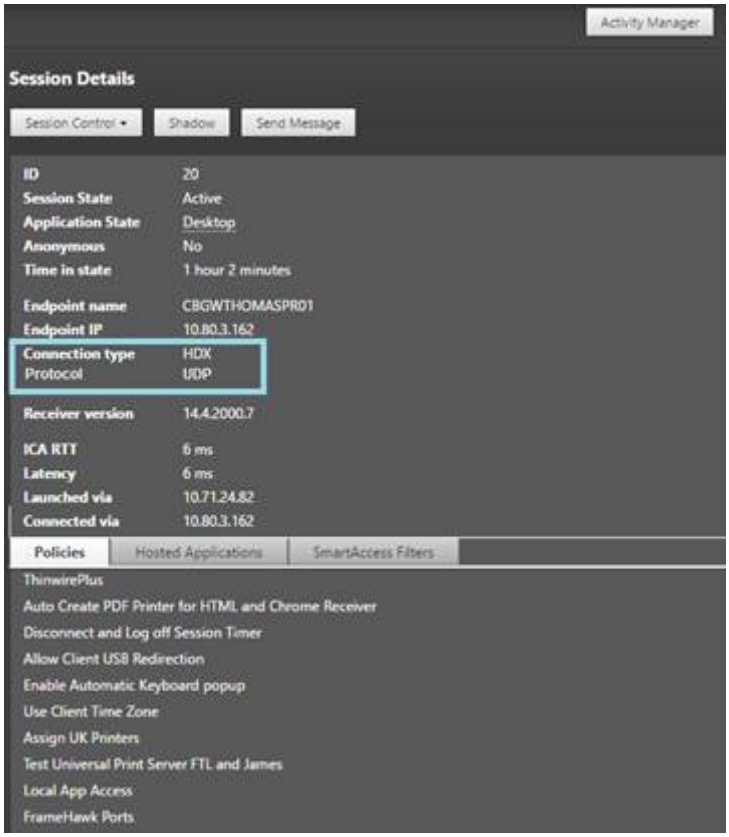
> 注:
> Virtual Delivery Agent 7 より前のバージョンの VDA、または Linux VDA を実行する場合、セッションに関する一部の情報が Director に表示されません。代わりに、利用できる情報がないというメッセージが表示されます。

デスクトップ割り当て規則の制限:
Citrix Studio では、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront では、ログインしているユーザーの DAR に従って、割り当て済みのデスクトップが、対応する表示名とともに表示されます。ただし、Director では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、Director で特定のデスクトップをマシンにマッピングすることはできません。
StoreFront に表示されている割り当て済みデスクトップを、Director に表示されているデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "\<Name on StoreFront\>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

セッショントランスポートプロトコル

[セッション詳細] パネルには、現在のセッションの HDX 接続の種類で使用されているトランスポートプロトコルが表示されます。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。

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. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimit フィールドの設定を編集または追加します。

［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大きい値に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シングルセッション OS マシンに対して実行できますが、マルチセッション OS マシンに対しては使用できないことがあります。

> 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。
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。

コマンド	機能
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。

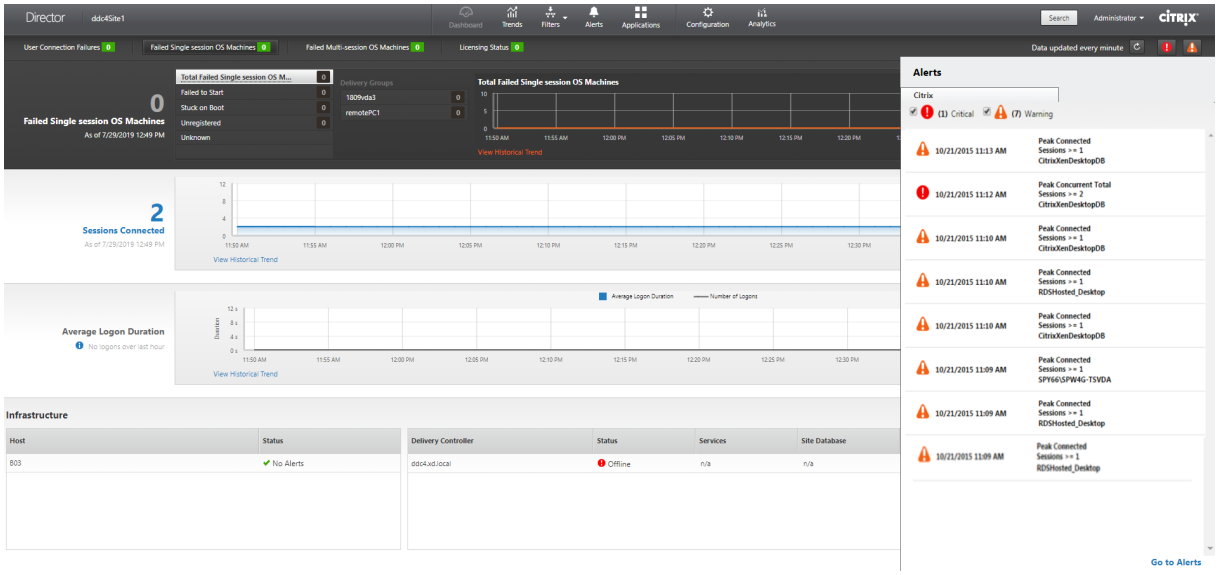
アプリケーション分析

［アプリケーション］タブには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つアプリケーションごとの分析結果が、単一の統合ビューで表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な識見を得ることができます。プローブの結果、アプリケーションごとのインスタンス数、公開アプリケーションに関連する障害およびエラーなどのメトリックが表示されます。詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーション分析」セクションを参照してください。

アラートおよび通知

April 26, 2021

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、**Premium** 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。

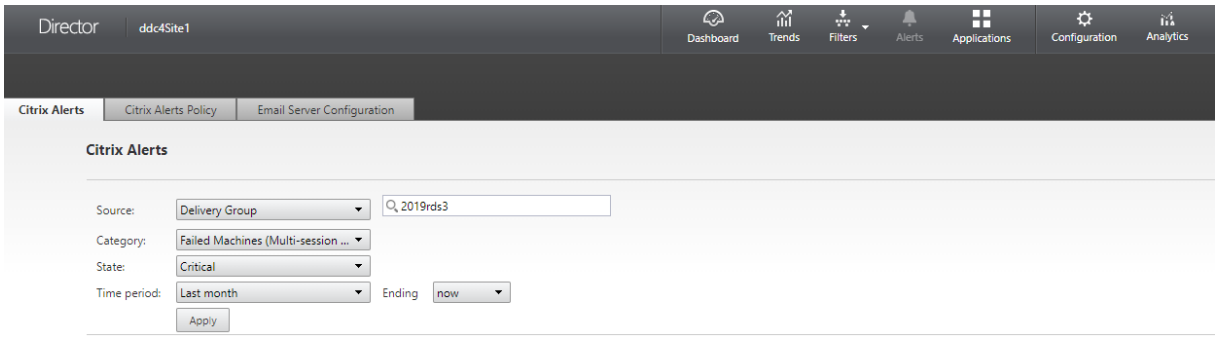


警告アラート（黄色の三角形）は、条件の警告しきい値以上になっていることを示します。

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マルチセッション 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

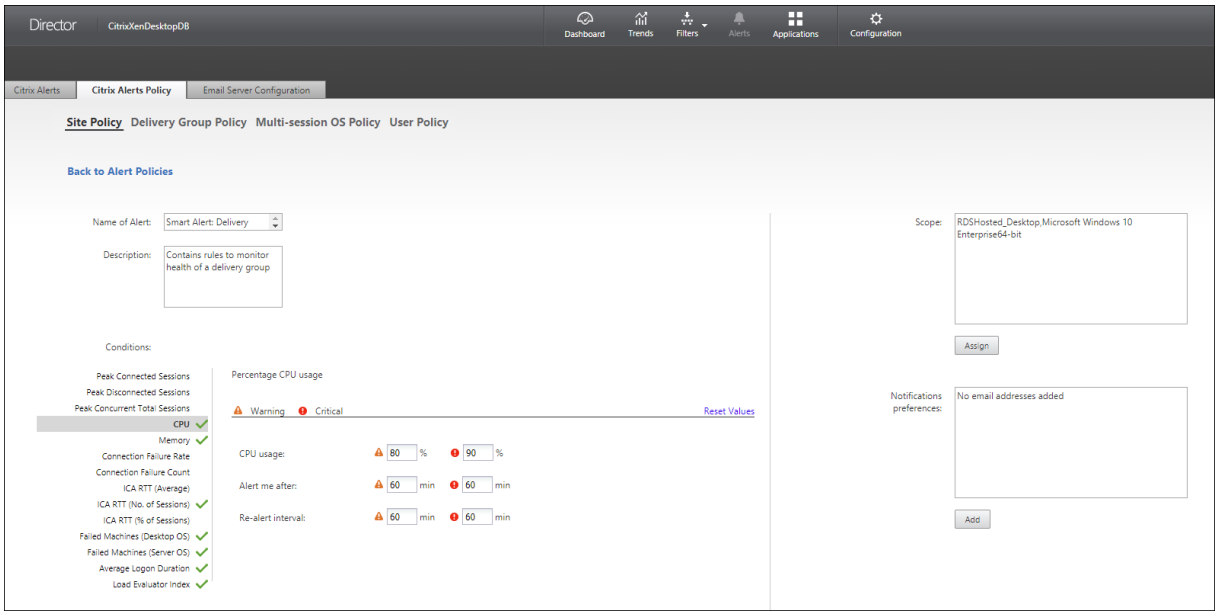
Citrix アラートは、Citrix コンポーネントで発生し、Director で監視されるアラートです。Citrix アラートは、Director 内で［アラート］>［**Citrix** アラートポリシー］の順に選択して構成できます。この構成では、設定したしきい値を超過した場合のアラートに関して、ユーザーおよびグループにメール送信する通知を設定できます。Citrix アラートのセットアップについて詳しくは、「アラートポリシーの作成」を参照してください。

スマートアラートポリシー

定義済みのしきい値を持つ組み込みアラートポリシーのセットは、デリバリーグループおよびマルチセッション OS VDA スコープで使用できます。この機能には、Delivery Controller バージョン 7.18 以降が必要です。［アラート］>［**Citrix** アラートポリシー］で、組み込みアラートポリシーのしきい値パラメーターを変更できます。
これらのポリシーは、少なくとも 1 つのアラートターゲット（サイト内に定義されているデリバリーグループまたはマルチセッション OS VDA）が存在する場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッション OS VDA に自動的に追加されます。

Director とサイトをアップグレードする場合、以前の Director インスタンスのアラートポリシーが引き継がれます。対応するアラートルールが監視データベースに存在しない場合にのみ、組み込みアラートポリシーが作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」を参照してください。

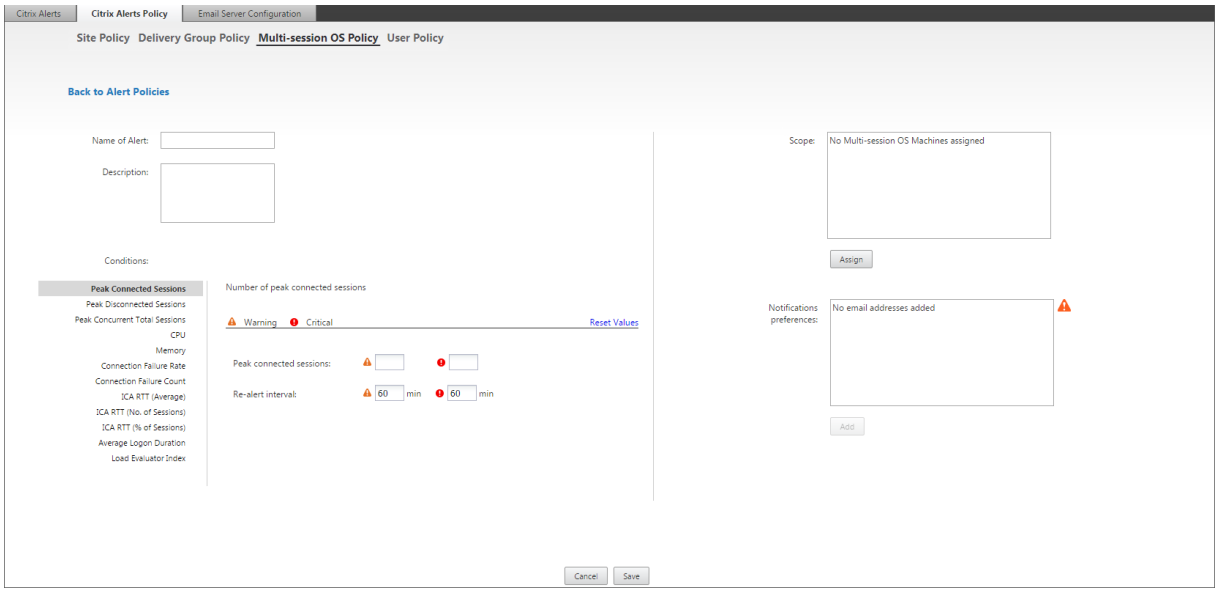


SCOM アラート

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 アラート統合の構成」セクション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、[マルチセッション 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。

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

アラートカテゴリ、アラートを緩和するための推奨アクション、および定義されている場合は組み込みポリシーの条件を以下に示します。組み込みアラートポリシーは、60 分のアラートおよび再アラートの間隔で定義されています。

最大接続セッション数

- 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

- 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。

合計最大同時セッション数

- Director セッションの傾向ビューで、最大同時セッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。
- 必要に応じ、切断されたセッションからログオフします。

CPU

CPU 使用率は、プロセスも含めた VDA の全体的な CPU の消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによる CPU 使用率に関する情報を表示できます。

- ［マシンの詳細］**>** ［履歴使用率の表示］**>** ［上位 **10** 位のプロセス］に移動して、CPU を消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 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 とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

スマートポリシーの条件:

- スコープ: デリバリーグループ、マルチセッション OS スコープ
- しきい値: 警告 - 80%、重大 - 90%

メモリ

メモリ使用率は、プロセスも含めた VDA の全体的なメモリの消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによるメモリ使用率に関する情報を表示できます。

- ［マシンの詳細］**>**［履歴使用率の表示］**>**［上位 **10** 位のプロセス］に移動して、メモリを消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 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 とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

スマートポリシーの条件:

- スコープ: デリバリーグループ、マルチセッション OS スコープ
- しきい値: 警告 - 80%、重大 - 90%

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。

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

- Citrix ADM で ICA RTT のブレークダウンをチェックして、原因を特定します。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM 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 および遅延をチェックして、これがネットワークの問題か、それともアプリケーションやデスクトップの問題かを特定します。

ICA 往復時間（セッション数）

ICA 往復時間を超過しているセッションの数。

- Citrix ADM 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、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、ネットワークチームと協力して原因を特定してください。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 5 つ以上のセッションで 300ms、重大 - 10 以上のセッションで 400ms

ICA 往復時間（セッションの**%**）

平均 ICA 往復時間を超過しているセッションの割合。

- Citrix ADM 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、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、ネットワークチームと協力して原因を特定してください。

ICA RTT（ユーザー）

特定のユーザーによって開始されたセッションに適用された ICA 往復時間。1 つ以上のセッションで ICA RTT がしきい値よりも高い場合は、アラートがトリガーされます。

障害が発生したマシン（シングルセッション **OS**）

障害が発生したシングルセッション OS マシンの数。Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。

- Citrix Scout 診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

  スマートポリシーの条件：

- スコープ：デリバリーグループスコープ
- しきい値：警告 - 1、重大 - 2

障害が発生したマシン（マルチセッション **OS**）

失敗したマルチセッション OS マシンの数。Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。

- Citrix Scout 診断を実行して、原因を特定します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 1、重大 - 2

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、ログオン処理時間に関する最新の測定基準を取得します。短時間のうちに多数のユーザーがログインするとログオン処理時間が長引くことがあります。
- 原因を絞り込むため、ログオンのベースラインおよび内訳をチェックします。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 45 秒、重大 - 60 秒

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マルチセッション OS マシンをチェックします。ダッシュボード（失敗）および負荷評価基準インデックス傾向レポートを表示します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 80%、重大 - 90%

ハイパーバイザーアラートの監視

Director では、ハイパーバイザーの正常性を監視するアラートが表示されます。Citrix Hypervisor と VMware vSphere のアラートは、ハイパーバイザーのパラメーターと状態を監視するのに役立ちます。ハイパーバイザーへの接続状態も監視され、クラスターまたはホストのプールが再起動された場合、または使用できなくなった場合にアラートが出されます。

ハイパーバイザーアラートを受信するには、Citrix Studio でホスト接続が作成されている必要があります。詳しくは、「接続とリソース」を参照してください。ハイパーバイザーアラートではこれらの接続のみが監視されます。次の表に、ハイパーバイザーアラートのさまざまなパラメーターと状態を示します。

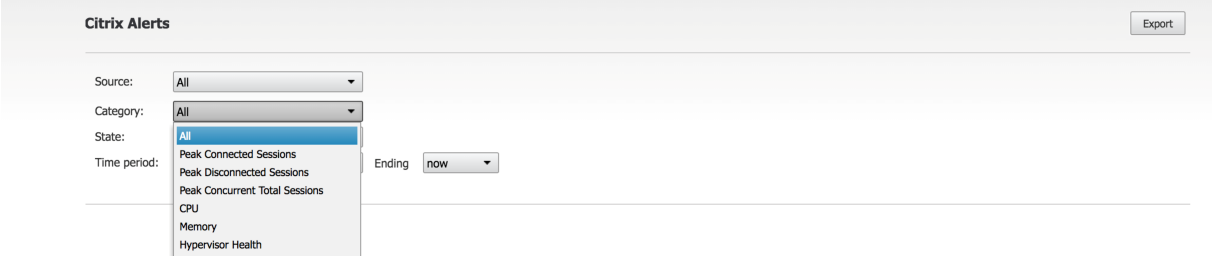
アラート	サポートされるハイパーバイザー	トリガー元	条件	構成
CPU 使用率	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	CPU 使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
メモリ使用率	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	メモリ使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ネットワーク使用状況	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	ネットワーク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ディスク使用率	VMware vSphere	ハイパーバイザー	ディスク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ホスト接続や電源の状態	VMware vSphere	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、または利用できない	アラートは VMware vSphere にあらかじめ組み込まれています。追加の構成は必要ありません。

アラート	サポートされるハイパーバイザー	トリガー元	条件	構成
使用不可のハイパーバイザー接続	Citrix Hypervisor、VMware vSphere	Delivery Controller	ハイパーバイザー（プールまたはクラスター）への接続が失われるか、電源がオフになるか、再起動されます。このアラートは、接続が利用できない間、1 時間ごとに生成されます。	アラートは Delivery Controller にあらかじめ組み込まれています。追加の構成は必要ありません。

> 注:
>
> アラートの構成について詳しくは、「Citrix XenCenter のアラート」および VMware vCenter のアラートを参照してください。

メール通知設定は、[**Citrix** アラートポリシー] **>** [サイトポリシー] **>** [ハイパーバイザーの正常性] から設定できます。Hypervisor のアラートポリシーのしきい値条件は、Director からではなくハイパーバイザーからのみ設定、編集、無効化、または削除できます。ただし、メール設定の変更とアラートの解除は Director で行うことができます。

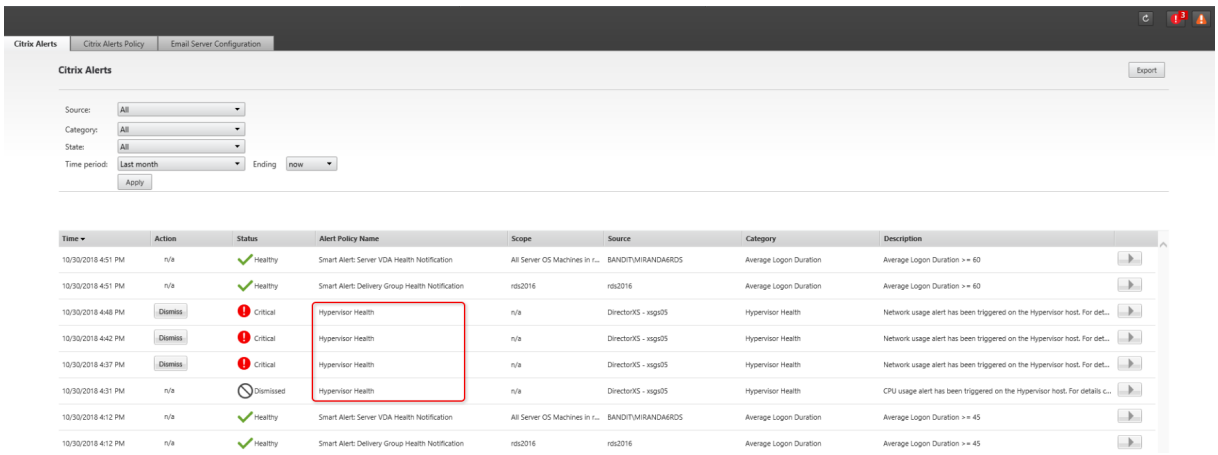
> 重要:
>
> - アラートは Hypervisor により取得され、Director に表示されます。ただし、Hypervisor のアラートのライフサイクルや状態に対する変更は、Director には反映されません。
> - 正常状態のアラートや Hypervisor コンソールで破棄または無効化したアラートであっても、Director には表示され続けるため、Director で明示的に破棄する必要があります。
> - アラートを Director で破棄しても、Hypervisor コンソールで自動的に破棄されることはありません。



ハイパーバイザーアラートのみをフィルタリングできるように、「ハイパーバイザーの正常性」という新しいアラートカテゴリが追加されました。これらのアラートは、しきい値に達するか超過すると表示されます。ハイパーバイザーのアラートには次のものがあります:

- 重大—ハイパーバイザーアラームポリシーの重大しきい値に達したか超過した
- 警告—ハイパーバイザーアラームポリシーの警告しきい値に達したか超過した

- 解除—アラートはアクティブなアラートとして表示されなくなる



この機能の使用には、Delivery Controller バージョン 7 1811 以降が必要です。サイトの 7 1811 以降で古いバージョンの Director を使用している場合は、ハイパーバイザーアラート数のみが表示されます。アラートを表示するには、Director をアップグレードする必要があります。

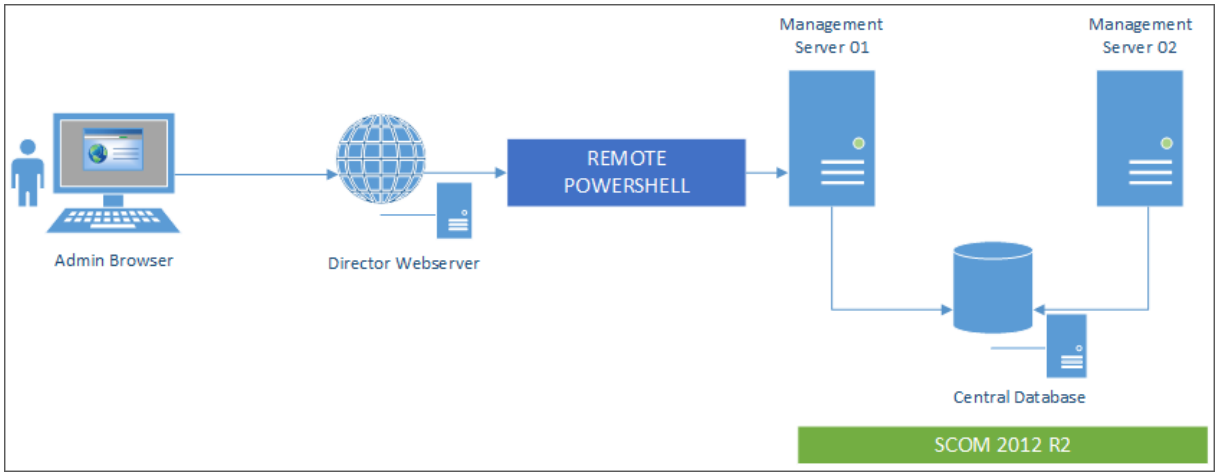
SCOM アラート統合の構成

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。

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。

これに加えて、最適なパフォーマンスを得るために、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:
   - 最新の TrustedHosts 一覧を取得します。

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - SCOM 管理サーバーの FQDN を、TrustedHosts の一覧に追加します。<Old Values> は、Get-Item コマンドレットから返された既存エントリのセットを表します。

     Set-Item WSMAN:\localhost\Client\TrustedHosts -Value “<FQDN SCOM Management Server>,<Old Values>”
3. DirectorConfig ツールを使用して、SCOM を構成します。

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

SCOM 管理サーバーで、以下を実行します:

1. SCOM 管理者の役割に、Director 管理者を割り当てます。
   a) SCOM 管理コンソールを開き、［管理］>［セキュリティ］>［ユーザーロール］の順に選択します。
   b) ［ユーザーロール］では、新しいユーザー役割を作成するか、または既存のユーザー役割を変更することができます。SCOM データへのアクセス方法を定義する SCOM オペレーターの役割には 4 つのカテゴリがあります。たとえば、読み取り専用の役割には、［管理］ペインが表示されず、規則、マシン、アカウントを検出または管理することができません。オペレーターの役割は、すべての管理権限を実行できる管理者の役割です。

> 注:
>
> Director 管理者がオペレーター以外の役割に割り当てられている場合、以下の操作を実行できません:
>
> - 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<!--NeedCopy-->
```

b) MaxShellsPerUser の変更:

CLI:

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--NeedCopy-->
```

PS:

“‘Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1. MaxMemoryPerShellMB の 変 更:

   CLI:
```


```

```
4
5   ```winrm set winrm/config/winrs @{
6   MaxMemoryPerShellMB="1024" }
7   <!--NeedCopy-->
```

```
1  PS:
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--NeedCopy-->
```

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、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。

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。

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

April 26, 2021

[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したりすると、[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。シングルセッション OS マシンまたはマルチセッション OS マシンを選択します。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、［マルチセッション 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、サーバーおよびシングルセッション OS VDA 上における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、マルチセッション OS 対応 VDA のアプリケーションインスタンスに利用できます。

> 注:
>
> Windows 10 1809 コンピューターにインストールされた VDA でデスクトップセッションを起動した場合、実際にはバックグラウンドで実行されている Microsoft Edge と Office が、Director のアクティビティマネージャー上ではアクティブ状態のアプリケーションとして表示されることがあります。

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. データを CSV 形式のファイルにエクスポートするには、［エクスポート］をクリックします。最大 100,000 レコードのデータをエクスポートできます。この機能は、Delivery Controller バージョン 1808 以降で使用できます。
9. ［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。
10. ［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。

11. ［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。
12. ［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。アプリケーションインスタンスのフィルターページと、セッションのフィルターページにあるアイドル時間の測定値は、Citrix Director、Delivery Controller、および VDA の各バージョンが 7.13 以降である場合に使用可能です。

> 注:
> Citrix Studio では、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）を、デリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront では、ログインしているユーザーの DAR に従って、割り当て済みのデスクトップが、対応する表示名とともに表示されます。ただし、Director では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、Director で特定のデスクトップをマシンにマッピングすることはできません。StoreFront に表示されている割り当て済みデスクトップを Director に表示されているデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

サイト全体の履歴傾向の監視

April 26, 2021

［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:

- Premium 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。
- Advanced 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。
- Premium Edition 以外や Advanced Edition 以外のユーザーは、過去 7 日間の傾向レポートを利用できます。

> 注:
>
> - すべての Director 展開環境で、セッション、障害、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るのは、期間を ［先月（現時点まで)］以下に設定した場合です。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。
> - Monitor Service の保持値をグルーミングすることで、傾向データの可用性を制御できます。デフォルト値は「データの粒度と保持」に記載されています。Premium 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。
> - IIS マネージャーの次のパラメータは、カスタマイズでき、選択可能なカスタム終了日の範囲を制御します。ただし、選択した日付のデータ可用性は、測定されている特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

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。

［セッションの自動再接続］列はセッション内で自動的に再接続を行う回数を表します。自動再接続は、［セッション画面の保持］ポリシーまたは［クライアントの自動再接続］ポリシーが有効な場合に実行されます。エンドポイントでネットワークの接続が中断された場合は、次のポリシーが有効になります:

- セッション画面の保持ポリシーが有効になり、デフォルトで 3 分間の持続時間に Citrix Receiver または Citrix Workspace アプリが VDA への接続を試みます。
- クライアントの自動再接続ポリシーが有効になり、3〜5 分間の持続時間にクライアントが VDA への接続を試みます。

どちらの場合も再接続の情報は記録され、ユーザーが確認できるようになっています。この情報が Director UI に表示されるまでには、再接続が施行されてから最大 5 分ほどかかることがあります。

自動再接続の情報は中断が発生したネットワーク接続の確認やトラブルシューティングに役立つだけでなく、シームレスなネットワークの分析にも活用できます。再接続数はデリバリーグループを指定したり、フィルターで特定の期間に絞り込んだりしたうえで表示することができます。ドリルダウンではセッション画面の保持やクライアントの自動再接続、タイムスタンプ、エンドポイントの IP、Workspace アプリがインストールされているマシンのエンドポイント名などの詳しい情報を確認できます。デフォルトでは、ログはイベントが起きたタイムスタンプに従って降順で並び替えられます。この機能は、Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Citrix Receiver for Windows、および Citrix Receiver for Mac で使用できます。使用するには Delivery Controller バージョン 7 1906 以降および VDA のバージョン 1906 以降が必要です。セッションの再接続について詳しくは、「セッション」を参照してください。ポリシーについて詳しくは、「クライアントの自動再接続のポリシー設定」および「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。

次の理由により、自動再接続データが Director に表示されない場合があります:

- Workspace アプリから VDA に自動再接続データが送信されていない。
- VDA から監視サービスにデータが送信されていない。
- 対応するセッションがない可能性があるため、VDA ペイロードが Delivery Controller によって破棄される。

> 注:
>
> 特定の NSG ポリシーが設定されていると、クライアント IP アドレスが正しく取得できない場合があります。

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:［失敗したシングルセッション OS マシン］タブまたは［失敗したマルチセッション 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、マルチセッション 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、マルチセッション 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。

シングルセッション **OS** およびマルチセッション **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シングルセッション 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、およびマシン別のマルチセッション 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［シングルセッション OS マシン］または［マルチセッション 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し、サイトの容量ニーズにすばやく対処することができます。
シングルセッション OS の可用性 - シングルセッション 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。
マルチセッション OS の可用性 - マルチセッション 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。

> 注：
> 使用可能カウンターに表示されるマシンの数には、保守モードのマシンが含まれます。

リソース使用の表示：［リソース使用］タブで［シングルセッション OS マシン］または［マルチセッション OS マシン］を選択して、各 VDI マシンの CPU とメモリ使用量、および IOPS とディスク遅延に関する履歴傾向を取得し、容量の計画に役立てることができます。
この機能の使用には、Delivery Controller および VDA の バージョン **7.11** 以降が必要です。
平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、および最大同時セッション数を表示するグラフです。マシンにドリルダウンして、CPU を消費している上位 10 のプロセスに関するデータとチャートを表示できます。デリバリーグループ別および期間別でフィルターできます。過去 2 時間、24 時間、7 日間、月、年の CPU、メモリ使用量、最大同時セッション数のグラフを入手できます。平均 IOPS とディスク遅延は、過去 24 時間、月、年のグラフが入手可能です。

> 注：
>
> - データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］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。詳しくは、「監視のポリシー設定」を参照してください。
> - 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。この機能により、Director は Citrix ADM の 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 以降が動作するシングルセッション OS VDA、および Windows Server 2008 以降が動作するマルチセッション OS 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、マルチセッション OS 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。

アプリケーションプローブの結果を表示する：［アプリケーションプローブの結果］タブには、［構成］ページでプロービングが設定されているアプリケーションのプローブの結果が表示されます。そこには、アプリケーションの起動に失敗した起動の段階が記録されています。

この機能の使用には、Delivery Controller および VDA の バージョン **7.18** 以降が必要です。詳しくは、「アプリケーションプロービング」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、［実行してダウンロード］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。

> 注：
> OData クエリを使用して生成したレポートのプレビューとエクスポートでは、列名はローカライズされず、英語で表示されます。

また、重要なイベントやアクションの発生は、フラグアイコンで示されます。フラグをクリックすると、発生したイベントまたはアクションが表示されます。

> 注:
>
> - 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。

展開のトラブルシューティング

April 24, 2021

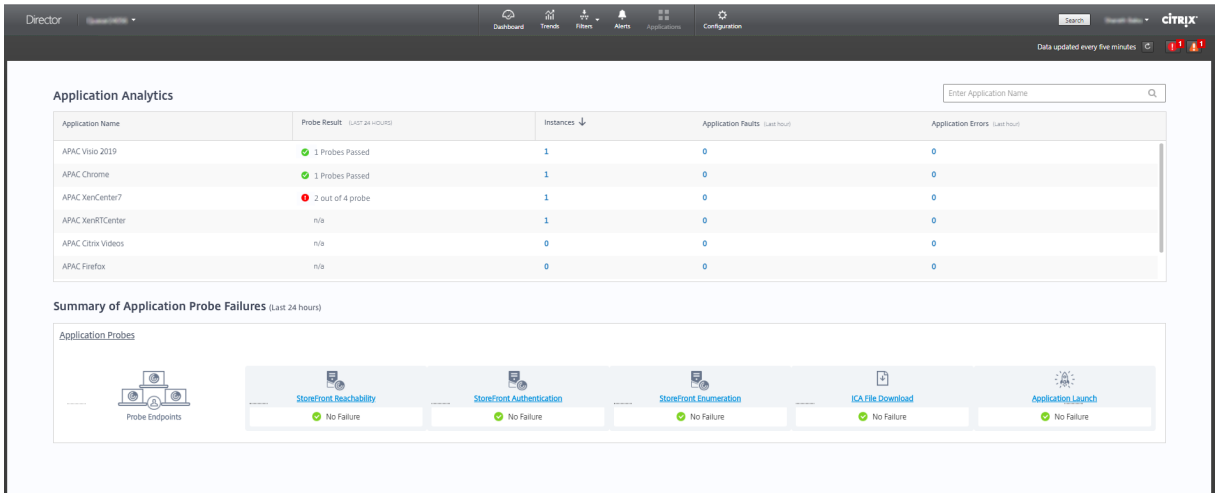
ヘルプデスク管理者は、問題を報告したユーザーを検索して、そのユーザーに関連付けられているセッションまたはアプリケーションの詳細を確認できます。同様に、問題が報告されたマシンやエンドポイントも検索できます。関連するメトリックを監視し、適切な対処法を実行することで、問題を迅速に解決できます。考えられる対処法としては、応答しないアプリケーションやプロセスの終了、ユーザーマシン上の操作のシャドウ、応答しないセッションからのログオフ、マシンの再起動、マシンのメンテナンスモードへの切り替え、ユーザープロファイルのリセットなどがあります。

アプリケーションのトラブルシューティング

April 26, 2021

アプリケーション分析

［アプリケーション］ビューには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つ、単一の統合ビューにアプリケーションベースの分析が表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な識見を得ることができます。デフォルトのビューは、よく実行されているアプリケーションを識別するのに役立ちます。
この機能の使用には、Delivery Controller バージョン 7.16 以降および VDA のバージョン 7.15 以降が必要です。



［プローブの結果］列には、過去 24 時間に実行されたアプリケーションプロービングの結果が表示されます。［傾向］>［アプリケーションプローブの結果］ページで詳細を表示するには、プローブの結果のリンクをクリックします。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションプロービング」を参照してください。

［インスタンス］列には、アプリケーションの使用状況が表示されます。現在実行中のアプリケーションインスタンス（接続インスタンスと切断インスタンスの両方）の数を示します。詳細なトラブルシューティングを行うには、［インスタンス］フィールドをクリックして、対応する ［アプリケーションインスタンス］フィルターページを表示します。ここでは、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> 注:
>
> カスタムスコープ管理者の場合、Director はアプリケーショングループに作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、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、Knowledge Center の記事CTX256001を参照してください。

［アプリケーション障害］列と ［アプリケーションエラー］列を使用して、サイト内の公開アプリケーションの正常性をモニターします。これらの列には、過去 1 時間以内に対応するアプリケーションを起動している間に発生した障害とエラーの合計数が表示されます。［アプリケーション障害］または ［アプリケーションエラー］フィールドをクリックすると、選択したアプリケーションに対応する ［傾向］ > ［アプリケーション障害］ページに障害の詳細が表示されます。

アプリケーション障害ポリシーの設定では、障害やエラーの可用性と表示を管理します。ポリシーとその変更方法について詳しくは、「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。

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。

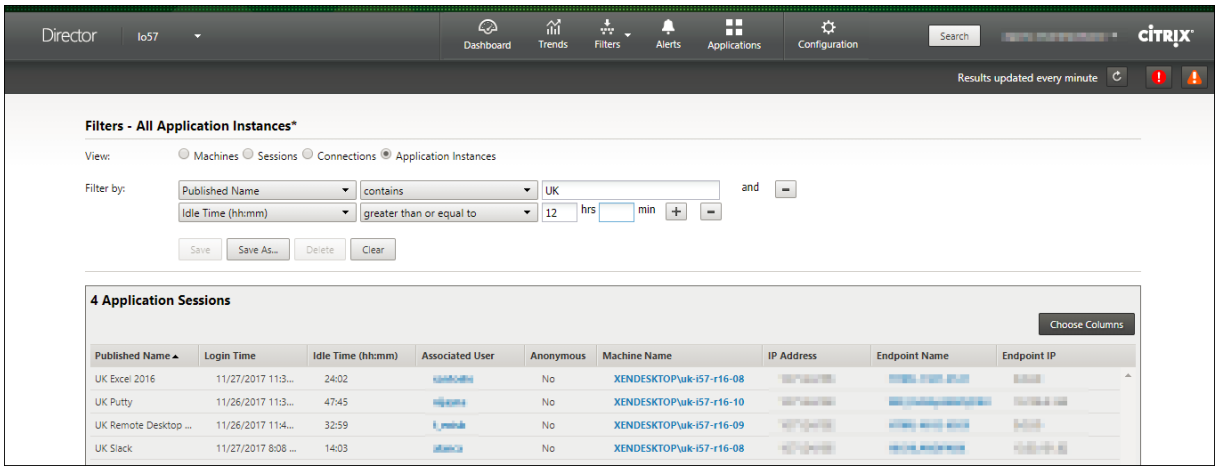
アプリケーションベースのトラブルシューティングの一般的な用途は、ヘルスケアのセクターです。このセクターでは、従業員間でアプリケーションライセンスが共有されています。このため、Citrix Virtual Apps and Desktops

の環境の削除、パフォーマンスの低いサーバーの再構成、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、サーバー上とシングルセッション 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マルチセッション OS 対応 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。

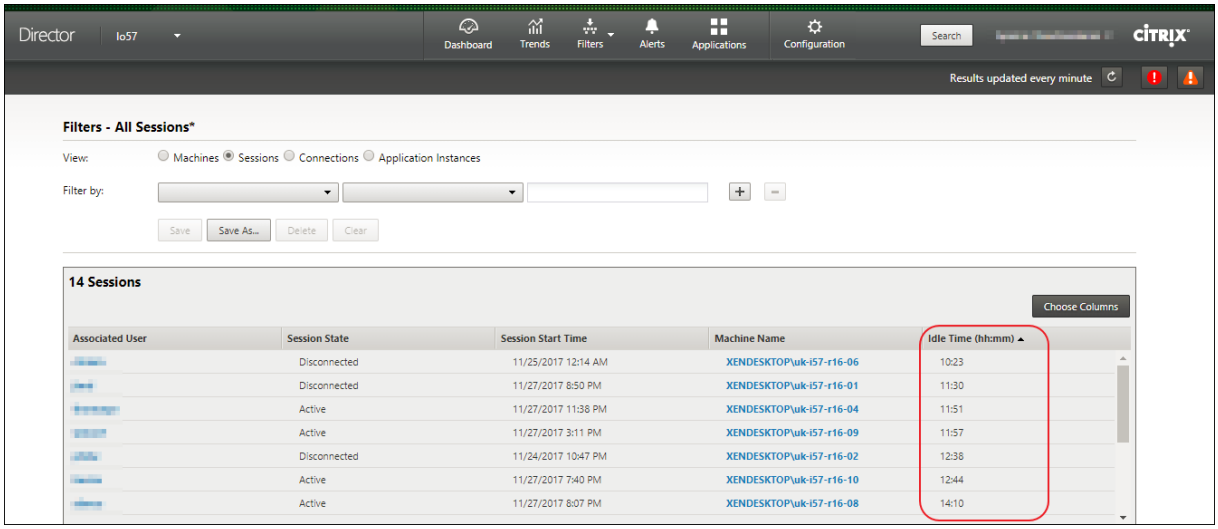
一定時間以上アイドル状態になっているアプリケーションインスタンスを識別して、必要に応じてログオフするか接続を切断するためにこの情報を使用します。これを行うには、［フィルター］**>**［アプリケーションインスタンス］の順に選択し、保存済みのフィルターを選択するか ［すべてのアプリケーションインスタンス］を選択し、独自のフィルターを作成します。



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マルチセッション OS 対応 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
- シングルセッション 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

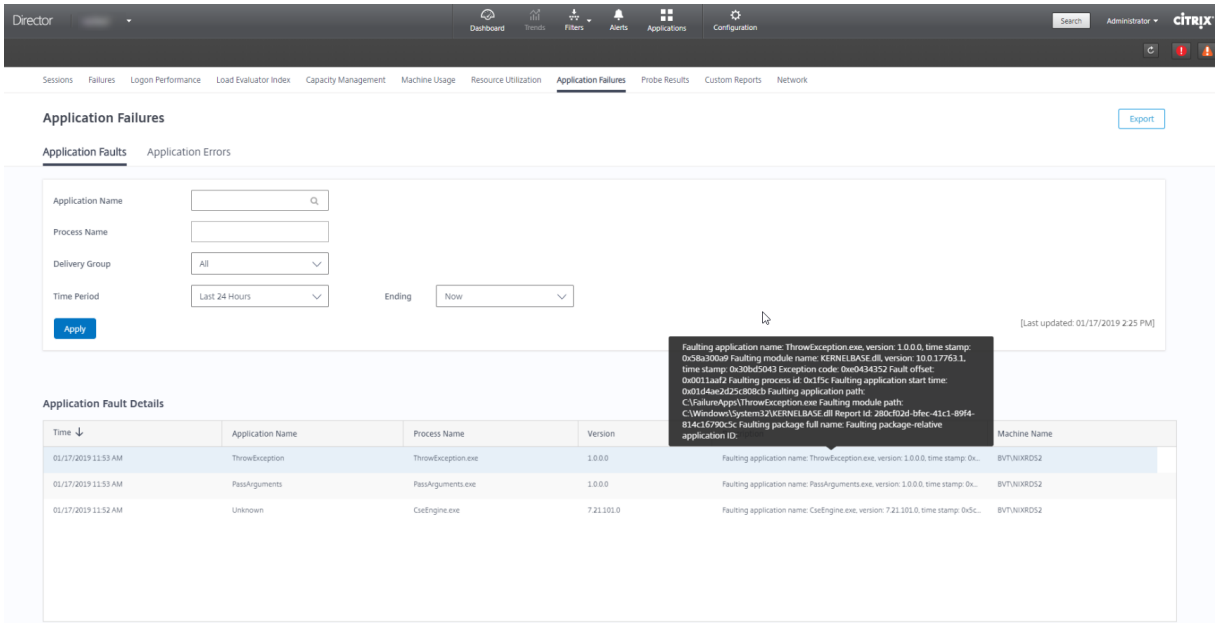
アプリケーション障害履歴の監視

［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、Premium および Advanced 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、Premium Edition も Premium Edition 以外も、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:

```
PowerShell command Set-MonitorConfiguration -<setting name> <value> <!--
NeedCopy-->
```

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、マルチセッション OS 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、シングルセッション OS 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。

［傾向］>［アプリケーションプローブの結果］ページには、そのサイトで過去 24 時間および 7 日間に実行されたアプリケーションプロービングの結果が表示されます。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションプロービング」を参照してください。

アプリケーションプロービング

April 24, 2021

アプリケーションプロービングでは、サイトに公開されている Citrix Virtual Apps の状態チェックプロセスが自動化されます。アプリケーションプロービングの結果は Director で使用できます。

要件:

- Delivery Controller はバージョン 7.18 以降で動作します。
- プローブエージェントが実行されるエンドポイントマシンは、Citrix Receiver for Windows バージョン 4.8 以降または Windows 向け Citrix Workspace アプリ（旧称 Citrix Receiver for Windows）バージョン 1808 以降がインストールされたマシンのみです。統合 Windows プラットフォーム（UWP）向けの Workspace アプリはサポートされていません。
- Director と StoreFront はデフォルトのフォームベース認証のみをサポートしています。Director は、シングルサインオン（SSO）認証をサポートしていません。
- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認します。

Application Probing を実行するために必要なユーザーアカウント/権限:

- 各エンドポイントマシンで調査するための固有の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理コンテキストで実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび設定するための Windows 管理者権限を持つユーザーアカウント
- 次の権限を持つ完全な管理者ユーザーアカウントまたはカスタムロール。アプリケーションプロービングに既存のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションがログオフされる可能性があります。
  - デリバリーグループの権限:
    - Read-only
  - Director の権限:
    - アラートメールサーバー構成の作成\編集\削除 - メールサーバーがまだ構成されていない場合
    - プローブ構成の作成\編集\削除
    - 構成ページの表示
    - 傾向ページの表示

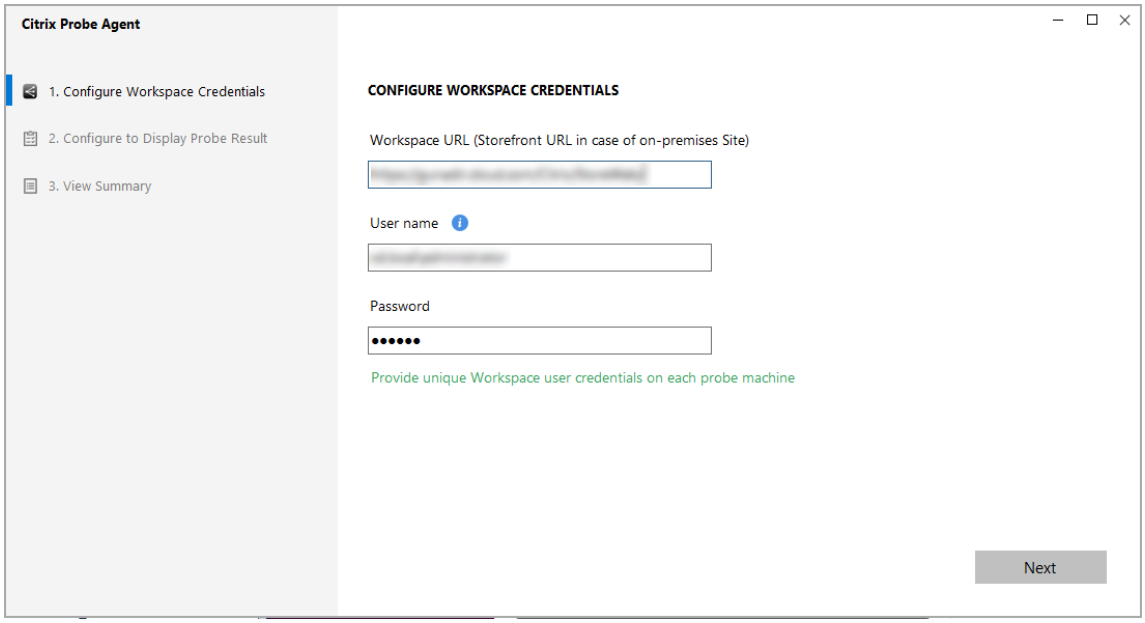
アプリケーションプロービングの構成

アプリケーションプローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。包括的なプローブの結果は、アプリケーション、ホストマシン、または接続に関連する問題を、ユーザーが経験する前にトラブルシューティングするのに役立ちます。

手順 **1**: **Citrix Probe Agent** をインストールして構成する

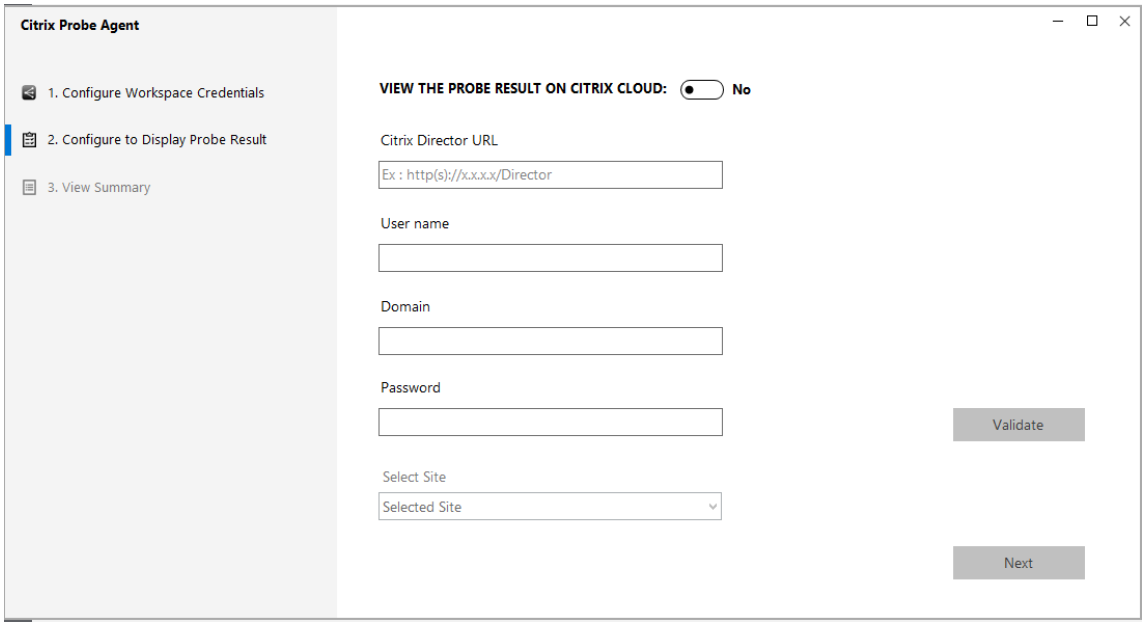
Citrix Probe Agent は、StoreFront を介したユーザーの実際のアプリケーション起動をシミュレートする Windows 実行可能ファイルです。Director で構成したアプリケーション起動をテストし、結果を Director に報告します。

1. アプリケーションプロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、Citrix Probe Agent をエンドポイントマシンにインストールして設定することができます。次の場所にある Citrix Probe Agent 実行可能ファイルをダウンロードします: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. エージェントを起動し、StoreFront Receiver for Web の認証情報を構成します。各エンドポイントマシンで固有の StoreFront ユーザーを構成します。資格情報は暗号化され、安全に保管されます。



> 注:
>
> - ネットワーク外からプローブされるサイトにアクセスするには、StoreFront URL フィールドに Citrix Gateway のログイン URL を入力します。Citrix Gateway は、対応するサイトストアフロント URL に要求を自動的にルーティングします。この機能は、Citrix Gateway バージョン 12.1 以降（RfWebUI テーマ）および Delivery Controller 1811 以降で使用できます。
> - ユーザー名フィールドのドメイン名として NetBIOS を使用します。例: NetBIOS/ユーザー名。

4. [プローブ結果の表示構成] タブで、Director の資格情報を入力し、[検証] をクリックします。

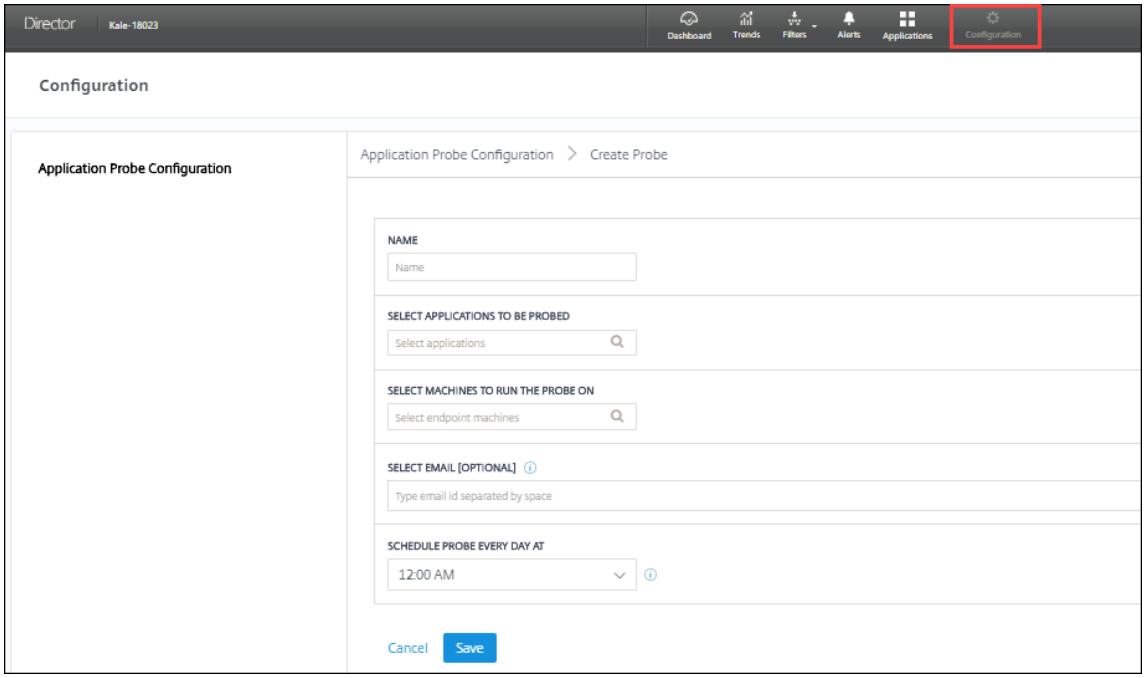


5. サイトを選択して ［次へ］をクリックします。

手順 **2**：**Director** でアプリケーションプロービングを設定する

1. ［構成］>［アプリケーションプローブの構成］を選択します。
2. プローブを作成し、以下を選択します:
   - プローブされるアプリケーション、
   - プローブを実行する必要があるエンドポイントマシン、
   - プローブのエラー結果が送信されるメールアドレス（［アラート］>［メールサーバーの構成］でメールサーバーを構成する）、および
   - プローブを実行する必要がある時刻（エンドポイントマシンのローカルタイムゾーンに従う）。

   Director での構成後、エージェントがプロービングを開始する準備を整えるまでに 10 分かかります。その後、次の 1 時間に開始する構成済みのプローブを実行します。



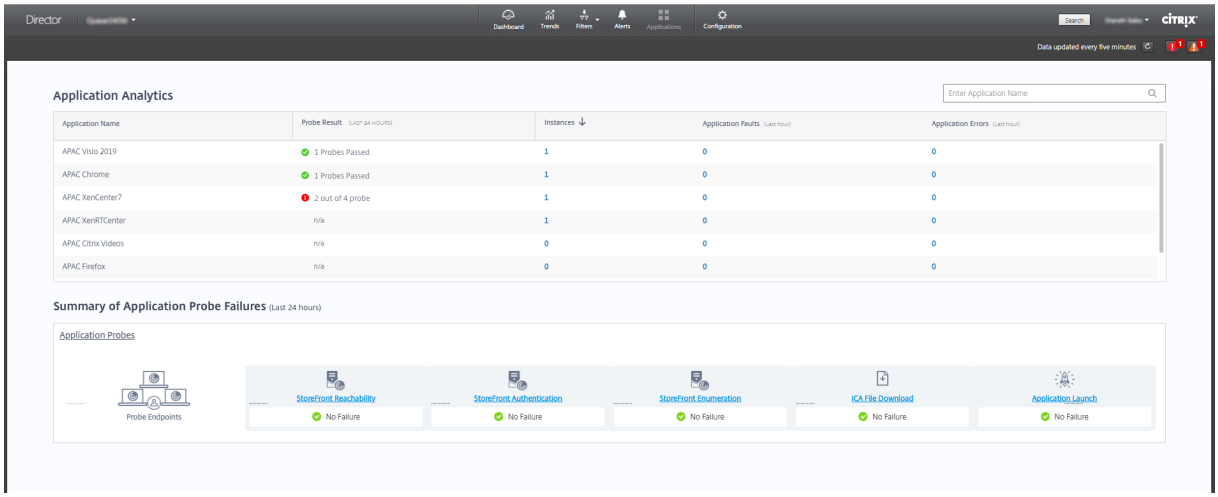
手順 **3**：プローブの実行

エージェントは、Director から定期的にフェッチするプローブ構成に従ってアプリケーションプロービングを実行します。StoreFront を使用して、選択したアプリケーションを連続して起動します。エージェントは、監視データベースを介して Director に結果を報告します。エラーは、以下の 5 つの特定の段階で報告されます：

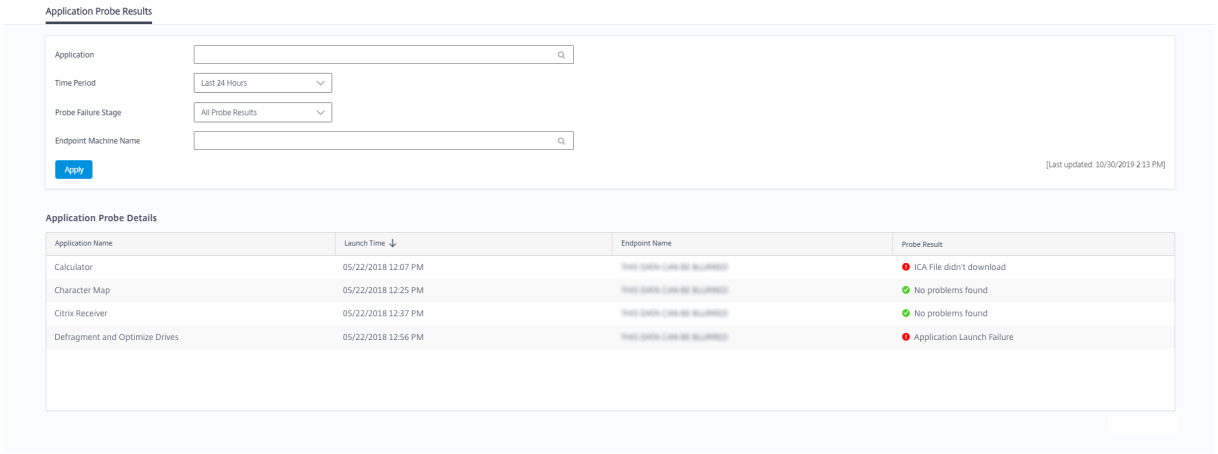
- **StoreFront** の到達可能性 - 構成済みの StoreFront URL に到達できません。
- **StoreFront** の認証 - 構成された StoreFront 資格情報が無効です。
- **StoreFront** の列挙 - StoreFront で列挙されるアプリケーションの一覧には、調査対象のアプリケーションが含まれていません。
- **ICA** のダウンロード - ICA ファイルは使用できません。
- アプリケーションの起動 - アプリケーションを起動できませんでした。

手順 **4**：プローブの結果を表示する

最新のプローブ結果は、［アプリケーション］ページで確認できます。



さらにトラブルシューティングするには、プローブの結果のリンクをクリックして、［傾向］>［アプリケーションプローブの結果］ページで詳細を表示します。



統合されたプローブの結果データは、このページの過去 24 時間または過去 7 日間の期間に使用できます。プローブが失敗した段階がわかります。特定のアプリケーション、プローブ障害段階、またはエンドポイントマシンの表をフィルタリングできます。

デスクトッププロービング

April 24, 2021

デスクトッププロービングでは、サイトに公開されている Citrix Virtual Desktops の状態チェックプロセスが自動化されます。デスクトッププロービングの結果は Director で確認できます。

Director の［構成］ページで、プローブするデスクトップ、プローブを実行するエンドポイントマシン、およびプローブ時間を設定します。エージェントは、選択したデスクトップの起動を StoreFront を使用してテストし、その結果を Director に報告します。プローブの結果は Director UI に表示されます。［アプリケーション］ページに

アプリケーションの過去 24 時間のデータが表示され、［傾向］>［プローブの結果］>［デスクトッププローブの結果］ページにプローブの履歴データが表示されます。ここでは、プローブ障害がどの段階（StoreFront の到達可能性、StoreFront の認証、StoreFront の列挙、ICA ダウンロード、またはデスクトップの起動）で発生したかを確認できます。障害レポートは、設定されているメールアドレスに送信されます。デスクトッププローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。包括的なプローブの結果は、デスクトップ、ホストマシン、または接続に関連する問題が生じてユーザーに影響が出る前に、予防的にトラブルシューティングするのに役立ちます。デスクトッププロービングは、Premium ライセンスを持つユーザーが使用できます。使用するには Delivery Controller バージョン 7 1906 以降および Probe Agent のバージョン 1903 以降が必要です。

要件:

- Delivery Controller はバージョン 1906 以降で動作します。
- プローブエージェントが実行されるエンドポイントマシンは、Citrix Receiver for Windows バージョン 4.8 以降または Windows 向け Citrix Workspace アプリ（旧称 Citrix Receiver for Windows）バージョン 1906 以降がインストールされたマシンのみです。統合 Windows プラットフォーム（UWP）向けの Workspace アプリはサポートされていません。
- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認します。
- Director と StoreFront はデフォルトのフォームベース認証のみをサポートしています。Director は、シングルサインオン（SSO）認証をサポートしていません。

デスクトッププロービングを実行するために必要なユーザーアカウントまたは権限:

- 各エンドポイントマシンで調査するための固有の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理コンテキストで実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび設定するための Windows 管理者権限を持つユーザーアカウント
- 次の権限を持つ完全な管理者ユーザーアカウントまたはカスタムロール。デスクトッププロービングに通常のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションがログオフされる可能性があります。
  - デリバリーグループの権限:
    - Read-only
  - Director の権限:
    - アラートメールサーバー構成の作成、編集、削除 - メールサーバーがまだ構成されていない場合
    - プローブ構成の作成、編集、削除
    - 構成ページの表示
    - 傾向ページの表示

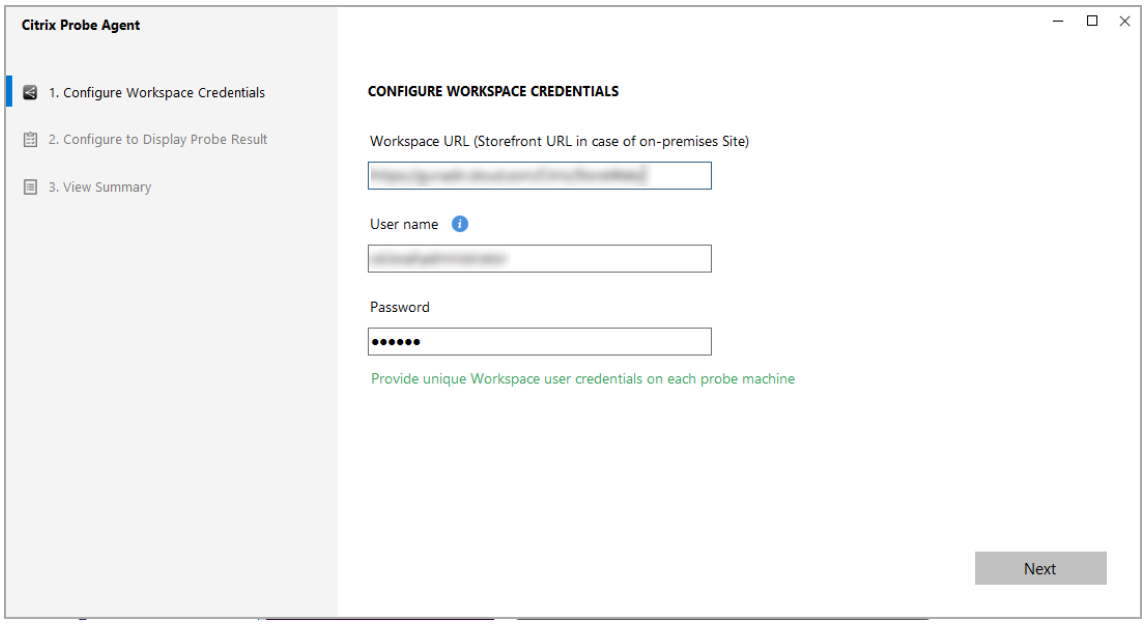
デスクトッププロービングの設定

デスクトッププローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。包括的なプローブの結果は、デスクトップ、ホストマシン、または接続に関連する問題が生じてユーザーに影響が出る前にトラブルシューティングするのに役立ちます。

手順 **1**：**Citrix Probe Agent** をインストールして構成する

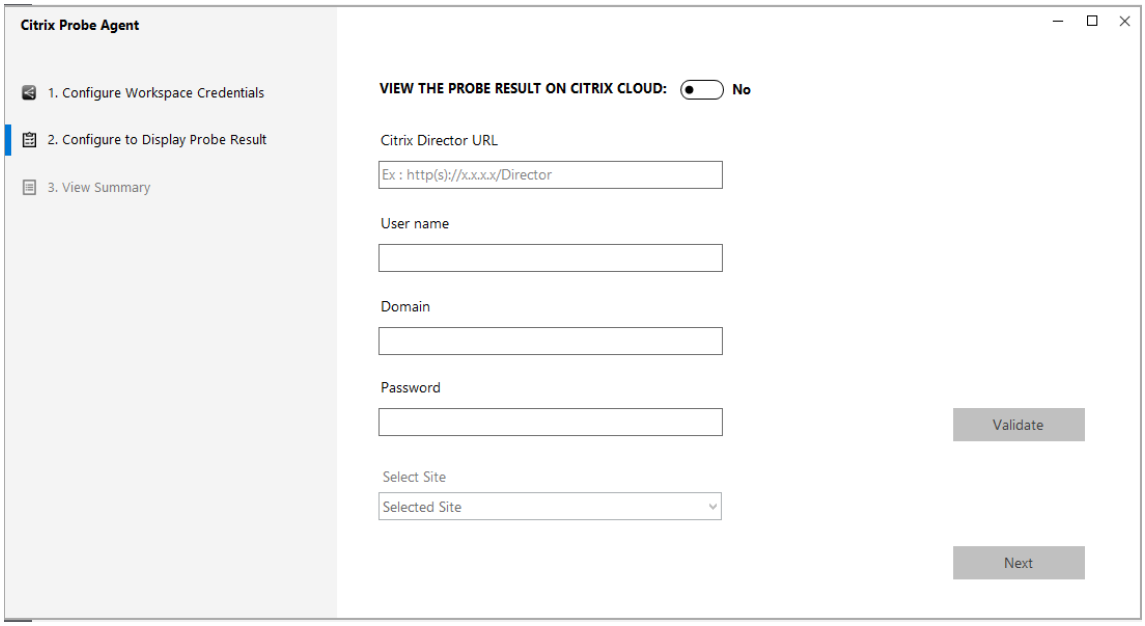
Citrix Probe Agent は、StoreFront を介したユーザーの実際のデスクトップ起動をシミュレートする Windows 実行可能ファイルです。Director で構成したデスクトップ起動をテストし、結果を Director に報告します。

1. デスクトッププロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、Citrix Probe Agent をエンドポイントマシンにインストールして設定することができます。次の場所にある Citrix Probe Agent 実行可能ファイルをダウンロードします：https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. エージェントを起動し、StoreFront Receiver for Web の認証情報を構成します。各エンドポイントマシンで固有の StoreFront ユーザーを構成します。資格情報は暗号化され、安全に保管されます。



> 注：
>
> - プローブ対象のサイトにネットワーク外からアクセスするには、StoreFront URL フィールドに Citrix Gateway のログインページの URL を入力します。Citrix Gateway は、対応するサイトストアフロント URL に要求を自動的にルーティングします。この機能は、Citrix Gateway バージョン 12.1 以降および Delivery Controller 1811 以降で使用できます。
> - ユーザー名フィールドのドメイン名として NetBIOS を使用します。例：NetBIOS/ユーザー名。

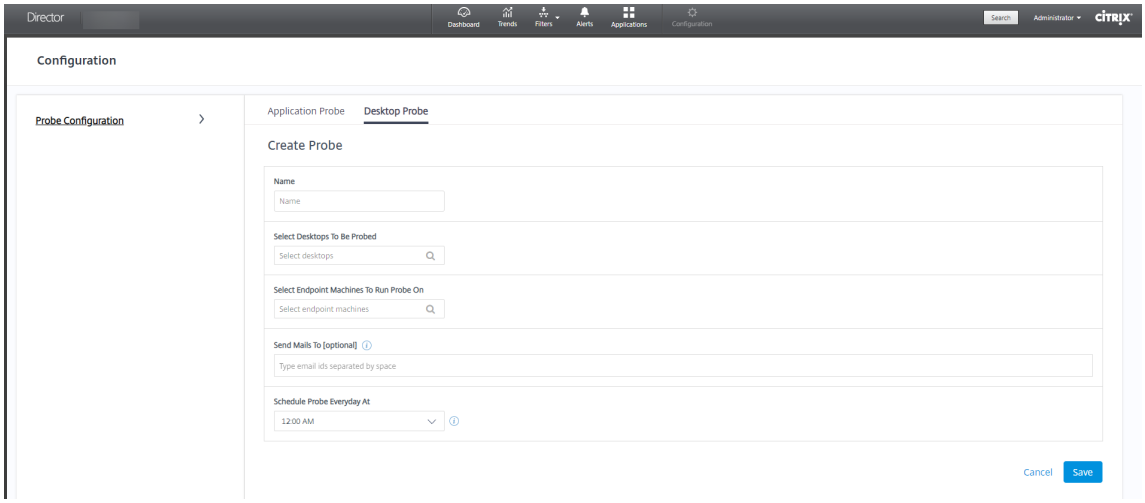
4.［プローブ結果の表示構成］タブで、Director の資格情報を入力し、［検証］をクリックします。



5. サイトを選択して ［次へ］をクリックします。

手順 **2**：**Director** でデスクトッププロービングを設定する

1. ［構成］ > ［デスクトッププローブの構成］を選択します。
2. プローブを作成するには、詳細を入力して ［保存する］をクリックします。



> 注:
>
> ［アラート］ > ［メールサーバー構成］でメールサーバーを構成してください。

デスクトッププロービングの構成後、エージェントがプロービングを開始する準備を整えるまでに 10 分かかります。その後、次の 1 時間に開始する構成済みのプローブを実行します。

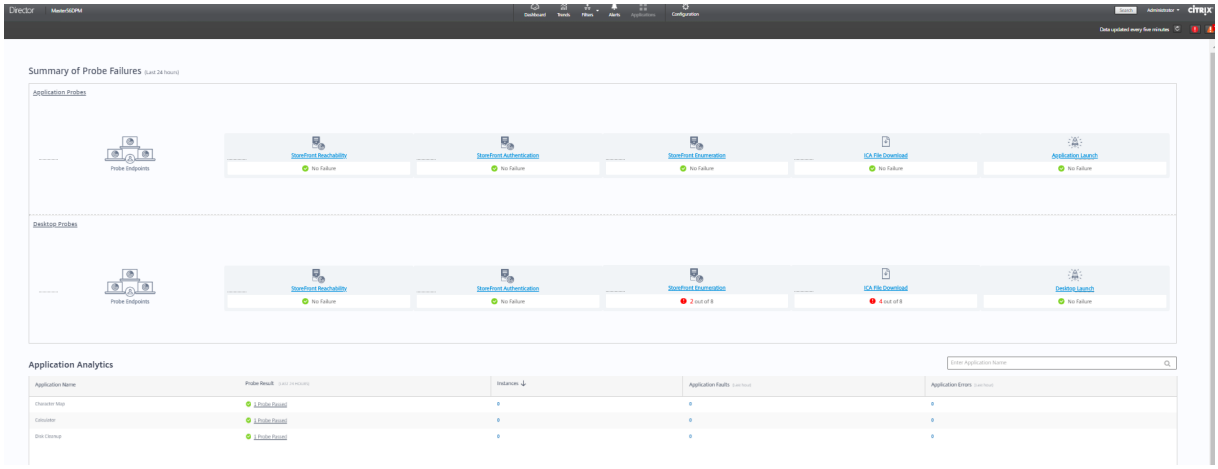
手順 **3**：プローブの実行

エージェントは、Director から定期的にフェッチするプローブ構成に従ってデスクトッププロービングを実行します。StoreFront を使用して、選択したデスクトップを連続して起動します。エージェントは、監視データベースを介して Director に結果を報告します。エラーは、以下の 5 つの特定の段階で報告されます：

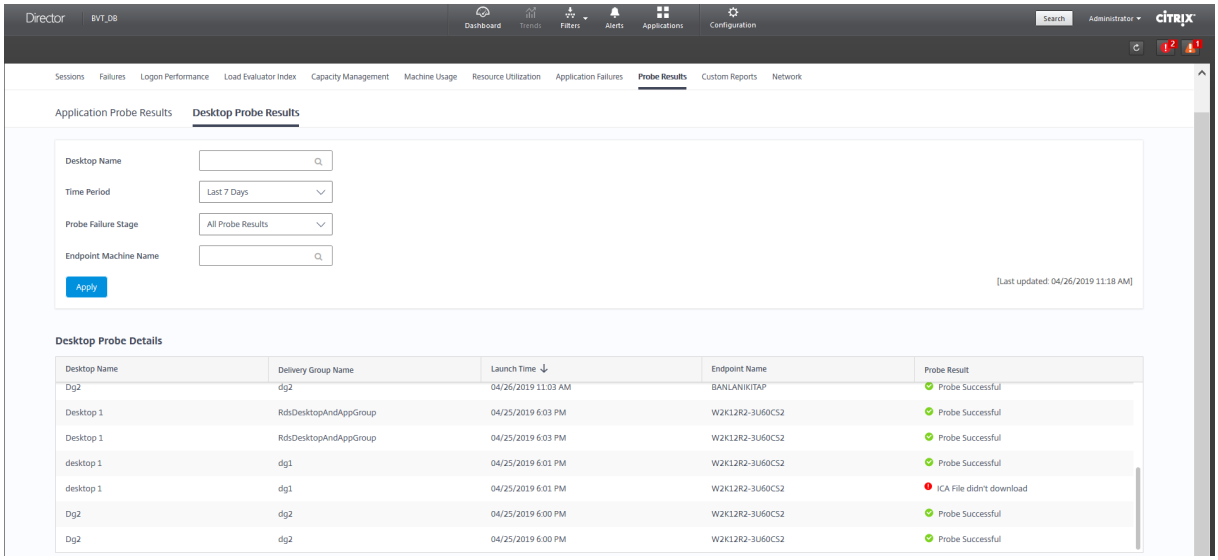
- **StoreFront** の到達可能性 - 構成済みの StoreFront URL に到達できません。
- **StoreFront** の認証 - 構成された StoreFront 資格情報が無効です。
- **StoreFront** の列挙 - StoreFront で列挙されるデスクトップの一覧には、調査対象のデスクトップが含まれていません。
- **ICA** のダウンロード - ICA ファイルは使用できません。
- デスクトップ起動 - デスクトップを起動できません。

手順 **4**：プローブの結果を表示する

最新のプローブ結果は、［デスクトップ］ページで確認できます。



さらにトラブルシューティングするには、プローブの結果のリンクをクリックして、［傾向］ > ［プローブの結果］ > ［デスクトッププローブの結果］ページで詳細を表示します。



集約されたプローブの結果データをこのページで確認できる期間は、過去 24 時間または過去 7 日間の間です。プローブが失敗した段階がわかります。この表をフィルタリングして、特定のデスクトップ、プローブの障害が発生した段階、またはエンドポイントマシンを確認することができます。

マシンのトラブルシューティング

April 26, 2021

> 注:
> **Citrix Health Assistant** は、未登録の VDA の構成に関する問題をトラブルシューティングするためのツールです。このツールは、いくつかのヘルスチェックを自動化して、セッションの起動やタイムゾーンリダイレクトの構成での VDA の登録の失敗や問題の根本原因を特定します。Knowledge Center の記事「Citrix Health Assistant - VDA の登録とセッションの起動のトラブルシューティング」には、**Citrix Health Assistant** ツールのダウンロード方法と使用方法が記載されています。

Director コンソールの ［フィルター］ **>** ［マシン］ビューには、そのサイトに構成されているマシンが表示されます。また、［マルチセッション 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。

登録に失敗したマシンの ［失敗の理由］列をクリックすると、失敗の詳細な説明とその失敗をトラブルシューティングするための推奨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。

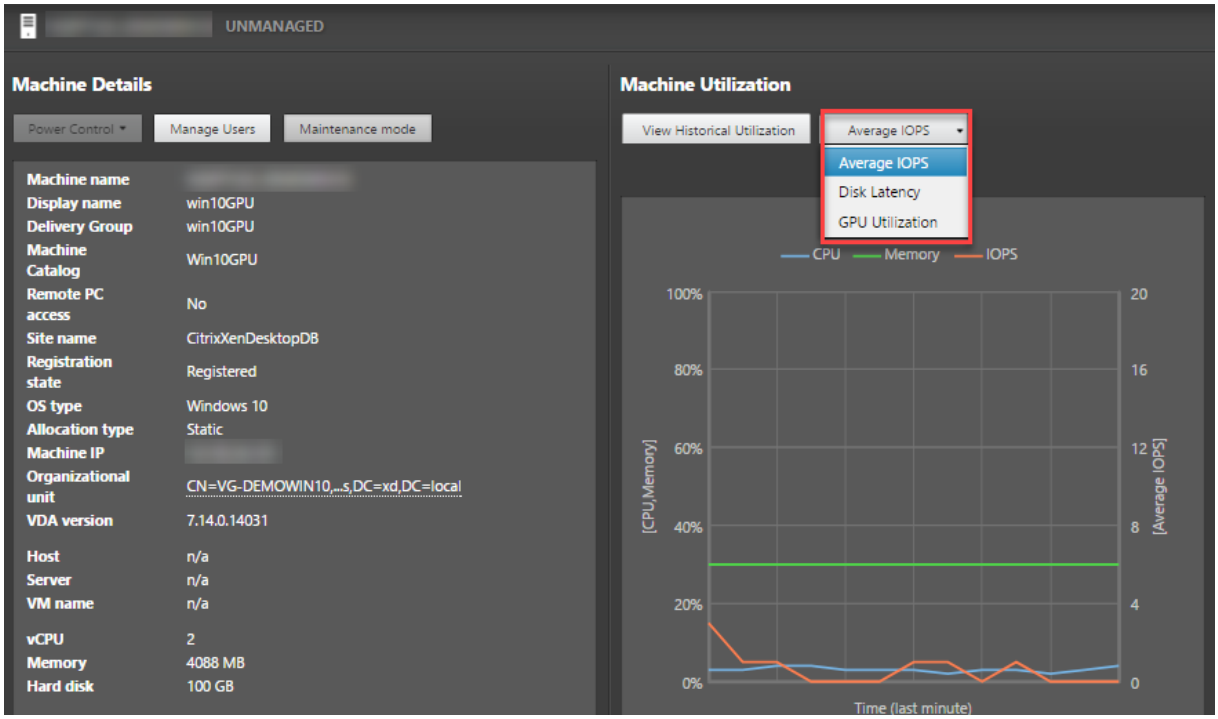
マシン名のリンクをクリックし、［マシンの詳細］ページに移動します。

［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、サーバーまたはシングルセッション OS 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 シングルセッション OS のための GPU アクセラレーション」および「Windows マルチセッション 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。

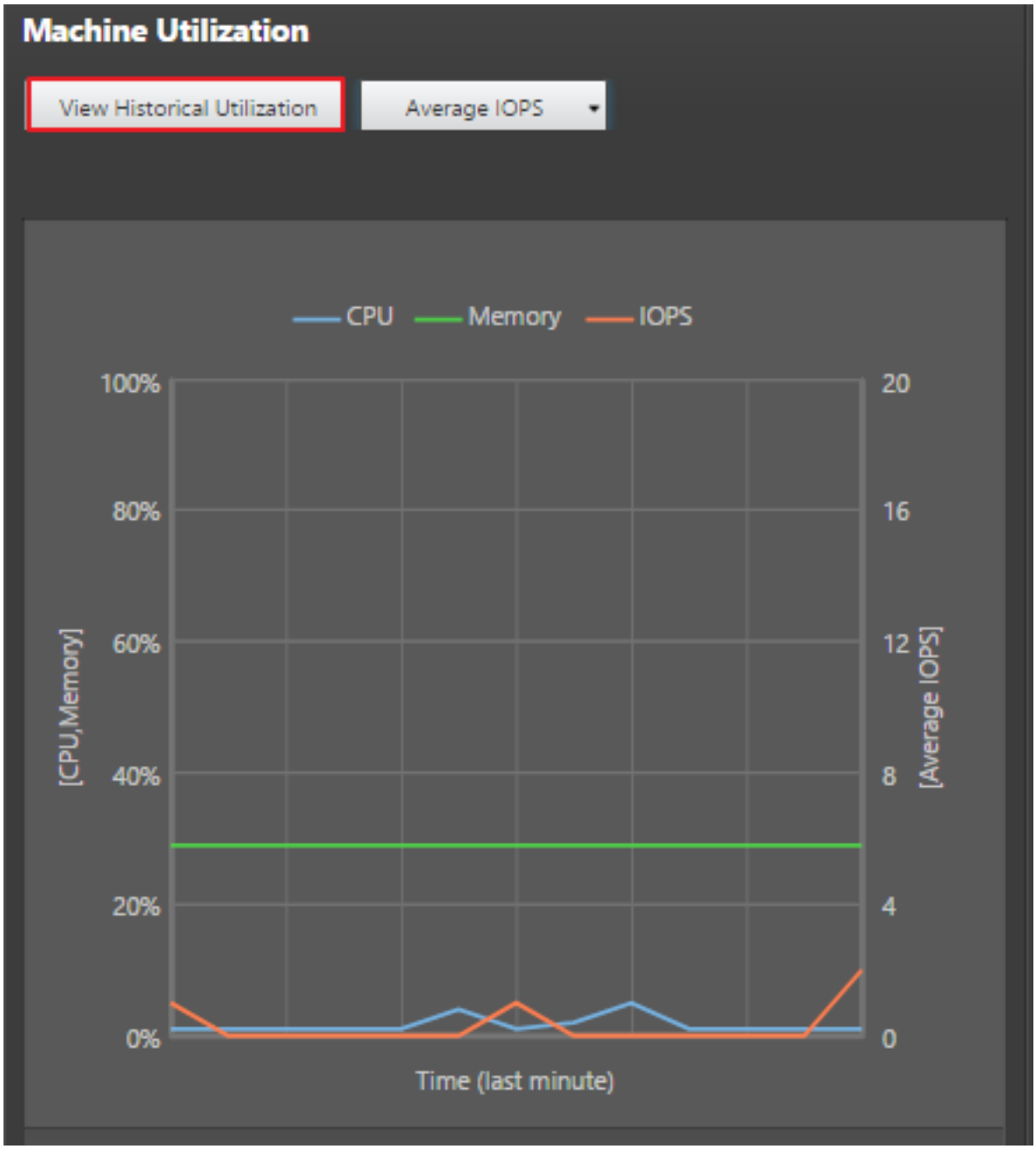
マシンごとの過去のリソース使用状況

［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 位のプロセス］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。

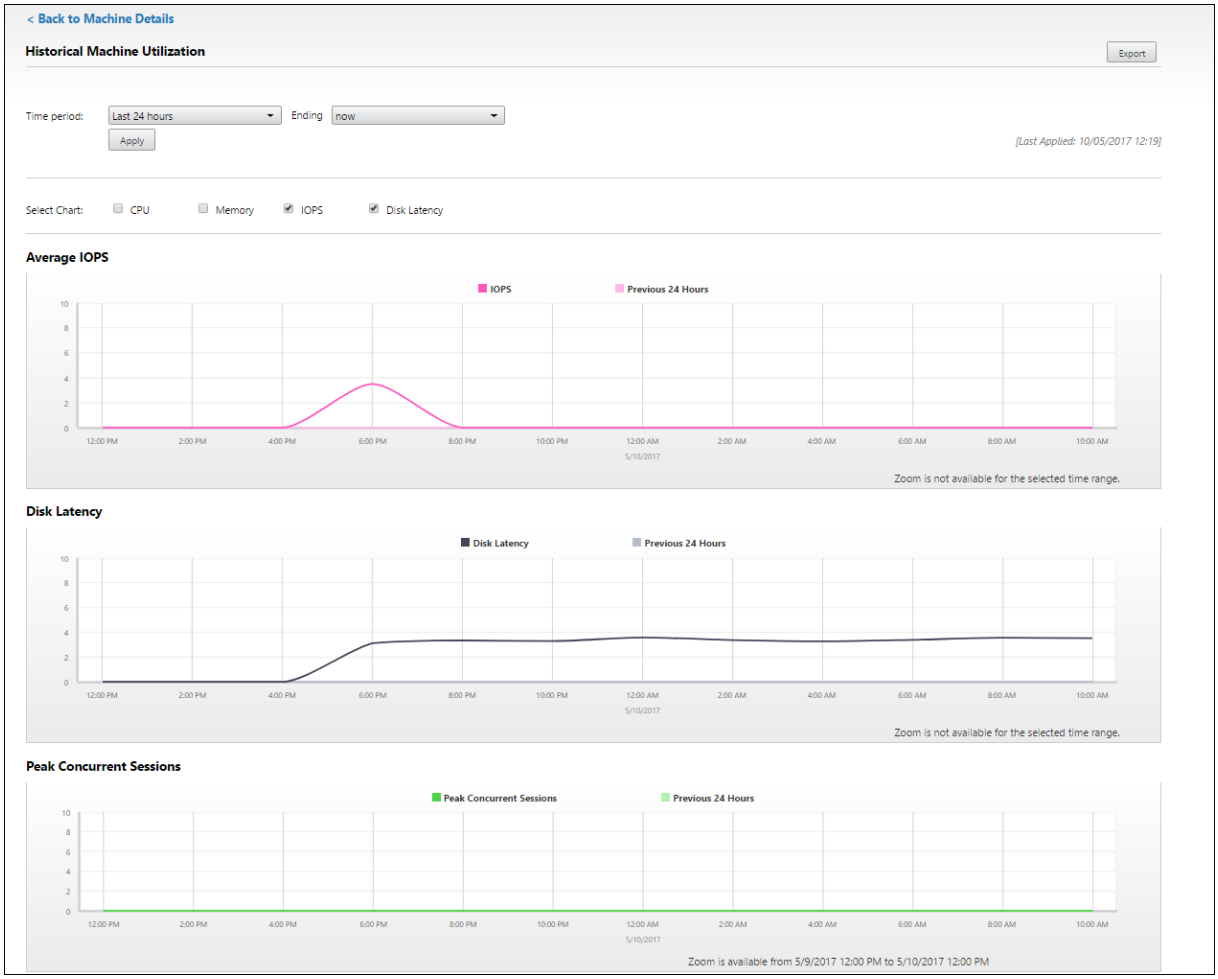
デフォルトでは、CPU とメモリの使用率、平均 IOPS、ディスク遅延に関するデータが収集されます。この収集は、［リソースの監視を有効にします］ポリシー設定で無効にできます。



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。
2. ［マシン使用率の履歴］ページで、［期間］で、使用率を表示する期間を過去 2 時間、過去 24 時間、過去 7 日間、過去 30 日間、または過去 1 年から選択します。

   > 注:
   > 現在、平均 IOPS とディスク遅延のデータについては、過去 24 時間、過去 30 日間、過去 1 年についてのみ表示できます。カスタムの終了時刻は使用できません。

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。

1. 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。
2. 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。

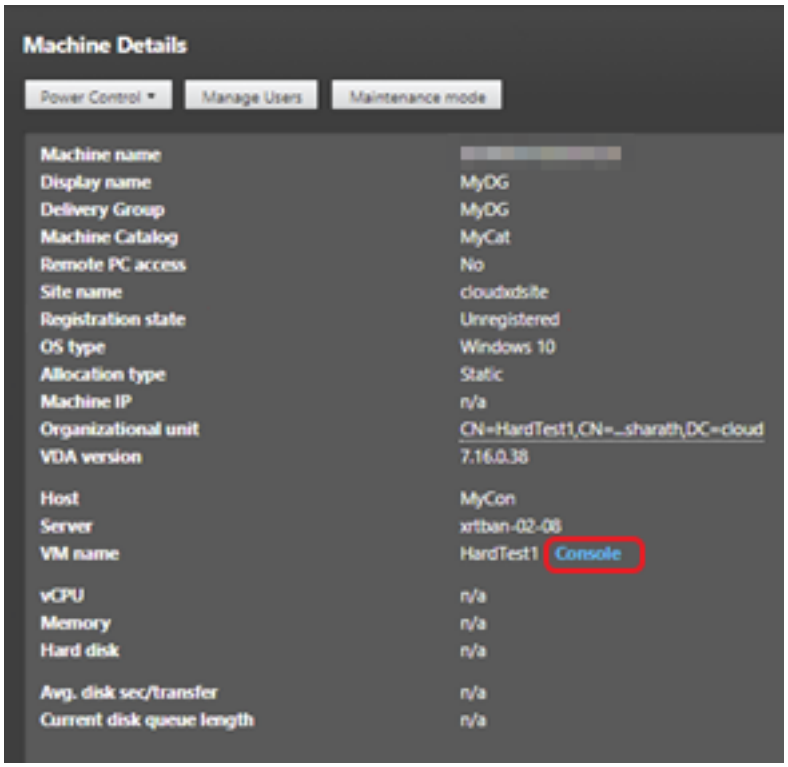
> 注:
> システムプロセスのセッション ID は「0000」と表示されます。

3. 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。

マシンコンソールへのアクセス

XenServer Version 7.3 以降でホストされているシングルセッション OS マシンおよびマルチセッション OS マシンのコンソールに、Director から直接アクセスできます。このため、XenServer がホストする VDA での問題を解決するために XenCenter を使用する必要はありません。この機能を利用できるようにするには:

- バージョン 7.16 以降の Delivery Controller が必要です。
- マシンをホストする XenServer は、バージョン 7.3 以降である必要があり、Director UI からアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応する［マシンの詳細］パネルで［コンソール］リンクをクリックします。提供したホスト資格情報が認証されると、Web ベースの VNC クライアントである noVNC を使用して、別のタブでマシンコンソールが開きます。これで、キーボードとマウスでコンソールにアクセスできるようになりました。

> 注:
>
> - この機能は、Internet Explorer 11 ではサポートされていません。
> - マシンコンソール上のマウスポインターの位置がずれている場合は、CTX230727で、問題を解決する手順を参照してください。
> - Director は、新しいタブでコンソールアクセスを起動し、Web ブラウザー設定でポップアップが許可されていることを確認します。
> - セキュリティ上の理由から、Web ブラウザーに SSL 証明書をインストールすることを Citrix ではお勧めします。

Microsoft RDS ライセンスの正常性

マルチセッション OS マシンの ［マシンの詳細］ページと ［ユーザーの詳細］ページの［マシンの詳細］パネルに、Microsoft RDS（Remote Desktop Services）のライセンスの状態を表示できます。

次のいずれかのメッセージが表示されます：

- ライセンスを使用できます
- 正しく構成されていません（警告）
- ライセンスエラー（エラー）
- 非互換 VDA バージョン（エラー）

> 注：
> 有効なライセンスのある猶予期間中のマシンの RDS ライセンス正常性の状態には、［ライセンスを使用できます］のメッセージが緑色で表示されます。有効期限が切れる前にライセンスを更新してください。

警告メッセージとエラーメッセージの場合、情報アイコンの上にカーソルを置くと、次の表に示す詳細情報が表示さ

れます。

メッセージの種類	Director でのメッセージ
エラー	VDA バージョン 7.16 以降で使用可能
エラー	新しい RDS 接続は許可されていません。
エラー	RDS ライセンスの猶予期間が終わりました。
エラー	ライセンスサーバーが、クライアントアクセスライセンス（接続デバイス数）の種類で必要な OS レベル用に構成されていません。
エラー	構成されたライセンスサーバーは、クライアントアクセスライセンス（接続デバイス数）の RDS ホスト OS レベルと互換性がありません。
警告	パーソナルターミナルサーバーは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	管理用リモートデスクトップは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	RDS ライセンスの種類は構成されていません。
警告	RDS クライアントアクセスライセンス（接続ユーザー数）の種類では、ドメインコントローラーまたはライセンスサーバーに接続できません。
警告	ライセンスの種類がクライアントアクセス（接続デバイス数）の場合、必要な OS レベルのライセンスサーバーに接続できないため、クライアントデバイスライセンスを確認できません。

> 注:
> この機能は、Microsoft RDS CAL（クライアントアクセスライセンス）にのみ適用されます。

ユーザーの問題のトラブルシューティング

April 26, 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
セッションの開始に時間がかかる。断続的もしくは繰り返し失敗する	セッション開始時の問題の診断
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、診断からさらなる分析情報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、Citrix Virtual Apps and Desktops のコンポーネントと一緒にインストールされます。Windows のバージョンによっては、Citrix Virtual Apps and Desktops をインストールするかこれにアップグレードすると、Scout が Windows のスタートメニューまたはスタート画面に表示されるようになります。

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。

セッション開始時の問題の診断

April 26, 2021

Director には「ユーザーログオンの問題の診断」セクションに記載されているログオンプロセスのフェーズだけでなく、セッション開始時の実行時間も表示されます。これは ［ユーザーの詳細］ページの［セッション開始時の Workspace アプリの実行時間］と、［マシンの詳細］ページの［セッション開始時の VDA の実行時間］に分かれます。この 2 つの時間にはフェーズの情報も含まれていて、各フェーズの実行時間も確認できます。このデータはセッションの開始時間が長い場合に問題を把握し、トラブルシューティングを行うのに役立ちます。また、セッションの開始プロセスを構成する各フェーズの実行時間の情報は、それぞれのフェーズに関連する問題のトラブルシューティングに有効です。たとえばドライブマッピングの時間が長い場合は、有効なすべてのドライブが GPO に正しくマップされているかを確認するか、スクリプトを確認するという対処ができます。この機能は、Delivery Controller バージョン 7 1906 以降および VDA 1903 以降で使用できます。

前提条件

セッションの開始時間を表示するには、以下の条件を満たしている必要があります:

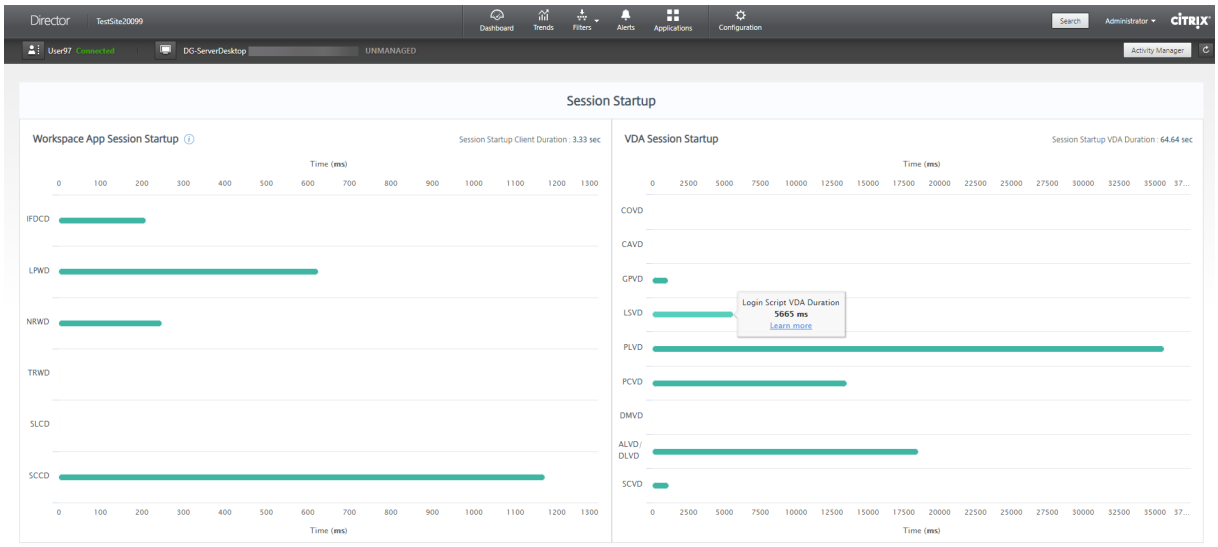
- Delivery Controller のバージョン 7 1906 以降。
- VDA のバージョン 1903 以降。
- EUEM（End User Experience Monitoring：エンドユーザー状況監視）サービスが VDA で実行されている。

制限事項

Director でセッションの開始時間を表示する場合は、以下の制限が適用されます。

- セッションの開始時間は HDX セッションでのみ確認できます。
- iOS および Android OS から開始したセッションについては、セッション開始時の VDA の実行時間のみ確認できます。
- IFDCD は、Web ブラウザーからの起動時に Workspace アプリが検出された場合にのみ使用できます。
- Mac OS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。
- Windows OS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。それ以前のバージョンで IFDCD を表示するには、Workspace アプリが検出された状態で Web ブラウザーからアプリを起動する必要があります。

> 注:
>
> - 条件が整っているにもかかわらずセッションの開始時間を表示するのに問題がある場合は、CTX130320の記事を参考にして Director サーバーのログと VDA のログを確認してください。
>   共有セッション（複数のアプリケーションが同一セッションで起動された状態）では、Workspace アプリの開始メトリックには最新の接続または最新のアプリケーション起動についての情報が表示されます。
> - VDA セッションの開始では、再接続時には適用されないメトリックがあります。その場合はメッセージが表示されます。



Workspace アプリでのセッションの開始フェーズ

セッション開始時のクライアントの実行時間（**SSCD**）

このメトリックの値が高い場合は、開始時間が長くなる要因がクライアント側にあることを示しています。問題の根本的な原因を特定するには、後に続くメトリックを調査します。これは要求が発生した瞬間に可能な限り近いタイミング（マウスのクリック）を起点とし、クライアントデバイスと VDA をつなぐ ICA 接続が確立されたタイミングを終点とする範囲が対象となります。共有セッションの場合は、サーバーとの接続を新たに確立するときのセットアップコストがそれほど生じないため、この時間は大幅に短くなります。次のレベルではいくつかの詳しいメトリックを利用できます。

ICA ファイルのダウンロード実行時間（**IFDCD**）

これはクライアントがサーバーから ICA ファイルをダウンロードするのにかかった時間を表します。このプロセスの全容は、以下のとおりです：

1. ユーザーが Workspace アプリでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. Citrix Gateway が構成されている場合は、それを介してユーザーの要求が StoreFront に送信されます。要求は StoreFront から Delivery Controller に送信されます。
3. Delivery Controller は要求を処理できるマシンを探し、そのマシンの情報などの詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority にワンタイムチケットを要求し、これを受信します。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCD はこのプロセス（ステップ 1～4）が完了するまでにかかる時間を表します。クライアントが ICA ファイルを受信すると、IFDCD のカウントが停止します。

LPWD は、このプロセスにおける StoreFront のコンポーネントです。

IFDCD の値が高い（ただし LPWD の値は普通である）場合、サーバー側の開始処理は正常ですが、クライアントデバイスと StoreFront との間の通信に問題があったことを示しています。これは 2 台のマシンをつなぐネットワーク上の問題によるものです。これがわかれば、最初にネットワークの潜在的な問題に対処することができます。

ページ開始時の **Web** サーバーの実行時間（**LPWD**）

これは StoreFront の起動ページ（launch.aspx）の処理にかかる時間を表します。LPWD の値が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです：

- StoreFront の高負荷 Internet Information Services（IIS：インターネットインフォメーションサービス）のログ、監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して速度低下の原因を特定します。

- StoreFront で Delivery Controller などの他のコンポーネントとの通信に問題が生じています。StoreFront と Delivery Controller との間のネットワーク接続が遅くなっていないか、または停止や過負荷の状態になっている Delivery Controller がないかを確認してください。

名前解決時の **Web** サーバーの実行時間（**NRWD**）

これは Delivery Controller が公開アプリケーションまたは公開デスクトップの名前を VDA マシンの IP アドレスに解決するのにかかる時間を表します。

このメトリックの値が高い場合、Delivery Controller が公開アプリケーションの名前を IP アドレスに解決するのに時間がかかっていることを示しています。この原因としては、クライアントの問題、Delivery Controller の問題（過負荷など）、クライアントと Delivery Controller をつなぐネットワークリンクの問題などが考えられます。

チケット応答時の **Web** サーバーの実行時間（**TRWD**）

これはチケットが必要な場合に、Secure Ticket Authority（STA）サーバーまたは Delivery Controller からチケットを取得するのにかかる時間を表します。この時間が長い場合は、STA サーバーまたは Delivery Controller が過負荷になっていることを示しています。

セッション検索時のクライアントの実行時間（**SLCD**）

これは要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。この照会処理は既存のセッションでアプリケーションの起動要求を処理できるかどうかを判断するために、クライアント上で実行されます。新規セッションか共有セッションかによって異なる手法が使用されます。

セッション作成時のクライアントの実行時間（**SCCD**）

これはセッションの作成にかかった時間です。具体的には wfica32.exe ファイルが実行されてから接続が確立されるまでの時間を表しています。

VDA セッションの開始フェーズ

セッション開始時の **VDA** の実行時間（**SSVD**）

この時間は VDA が開始処理の全体を実行するのに要する時間を含めた、サーバー側の接続開始時の高レベルメトリックを表します。このメトリックの値が高い場合は、セッション開始までの時間が長くなる要因が VDA 側にあることを示しています。VDA が開始処理全体の実行にかかった時間は、この値に含まれます。

アカウント情報取得時の **VDA** の実行時間（**COVD**）

VDA がユーザーの資格情報を取得するのにかかった時間を表します。

この時間はユーザーが資格情報を適宜入力しなければいくらでも増加する可能性があるため、VDA の開始時間には含まれません。この時間が意味を持つと考えられるのは、ログイン操作が必要かつサーバー側で資格情報の入力を求めるダイアログボックスが表示される場合（またはログイン前に法律上の注意点が表示される場合）に限られます。

アカウント情報認証時の **VDA** の実行時間（**CAVD**）

これは VDA が認証プロバイダーを照会してユーザーの資格情報を認証するのにかかる時間を表します。認証プロバイダーは Kerberos、Active Directory、Security Support Provider Interface（SSPI）のいずれかになります。

グループポリシーの **VDA** の実行時間（**GPVD**）

これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間を表します。

ログインスクリプト実行時の **VDA** の実行時間（**LSVD**）

これは VDA がユーザーのログインスクリプトを実行するのにかかる時間を表します。

ユーザーまたはグループのログインスクリプトの実行を非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロード時の **VDA** の実行時間（**PLVD**）

これは VDA がユーザーのプロファイルを読み込むのにかかる時間を表します。

この時間が長い場合は、ユーザープロファイルの設定を見直してください。移動プロファイルのサイズと保存場所によってはセッションの開始が遅くなります。ユーザーがターミナルサービスの移動プロファイルとホームフォルダーが有効になっているセッションにログオンすると、移動プロファイルの内容とホームフォルダーへのアクセスがログオン時にマップされるため、その分だけリソースが必要になります。場合によっては CPU 使用率が著しく高くなることもあります。この問題による影響を軽減するには、ターミナルサービスのホームフォルダーと、リダイレクトされた個人用フォルダーの使用を検討してください。通常 Citrix 環境でユーザープロファイルを管理する場合は、Citrix Profile Management を使用することを検討してください。Citrix Profile Management を使用していてログオン時間が遅くなる場合は、アンチウイルスプログラムが Citrix Profile Management ツールをブロックしていないかを確認してください。

プリンター作成時の **VDA** の実行時間（**PCVD**）

これは VDA がユーザーのクライアントプリンターを同期的にマップするのにかかる時間を表します。プリンターの作成を非同期で実行するように設定している場合は、セッションの開始処理の完了に影響しないため、PCVD の値は記録されません。

プリンターのマッピングの時間が長くなるのは、多くの場合プリンターの自動作成ポリシーの設定に原因があります。ユーザーのクライアントデバイスにローカルで追加されたプリンターの台数と印刷設定は、セッションの開始時間に

直接影響を及ぼす可能性があります。Citrix Virtual Apps and Desktops はセッションが開始されると、ローカルにマップされたすべてのプリンターをクライアントデバイス上に作成する必要があります。特にユーザーの設定で多数のローカルプリンターが存在する場合は、印刷ポリシーを設定しなおして、作成するプリンターの台数を減らすことを検討してください。これを行うには、Delivery Controller と Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピング時の **VDA** の実行時間（**DMVD**）

これは VDA がユーザーのクライアントドライブ、デバイス、ポートをマップするのにかかる時間です。

ICA プロトコルを最適化し、セッション全体のパフォーマンスを向上させるには、基本ポリシーにオーディオや COM ポートマッピングなどの未使用の仮想チャネルを無効にする設定が指定されていることを確認してください。

アプリケーション/デスクトップ起動時の **VDA** の実行時間（**ALVD/DLVD**）

このフェーズは UserInit と Shell の実行時間を合わせたものです。ユーザーが Windows マシンにログオンすると、Winlogon は userinit.exe を実行します。Userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Windows ユーザーインターフェイスである Explorer.exe を起動します。Userinit は、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。Shell の実行時間は、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。

セッション作成時の **VDA** の実行時間（**SCVD**）

この時間には VDA でのセッション作成時における各種の遅延時間が含まれます。

ユーザーログオンの問題の診断

April 26, 2021

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。

ログオン処理時間は、HDX を使用するデスクトップまたはアプリに初めて接続する場合のみ測定されます。このデータには、リモートデスクトッププロトコルを使用して接続しようとするユーザーや、切断されたセッションから再接続するユーザーは含まれません。具体的には、ユーザーが最初に HDX 以外のプロトコルを使用して接続してから、HDX を使用して再接続するときは、ログオン処理時間は測定されません。

[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 Citrix Virtual Apps and Desktops にログオンすると、Monitor Service により、ユーザーが Citrix Workspace アプリ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。処理時間の情報は秒単位（または秒の小数単位）まで表示されます。

前提条件

ログオン期間データとドリルダウンが表示されるようにするには、次の前提条件を満たす必要があります:

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールする。
2. Citrix Profile Management Service が実行されている。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 ［従来の実行リストを処理しない］を無効にします。
4. 対話型セッションのドリルダウンでは、監査プロセスの追跡を有効にする必要があります。
5. GPO ドリルダウンの場合は、グループポリシーの操作ログのサイズを大きくします。

> 注:
>
> - ログオン期間は、デフォルトの Windows シェル（explorer.exe）でのみサポートされ、カスタムシェルではサポートされません。
> - リモート PC アクセスのログオン期間は、リモート PC インストール中に **Citrix User Profile Manager** および **Citrix User Profile Manager WMI Plugin** が追加のコンポーネントとしてインストールされる場合のみ利用できます。詳しくは、「リモート PC アクセスの構成の順序」の手順 4 を参照してください。

ユーザーログオンの問題のトラブルシューティング手順

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

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

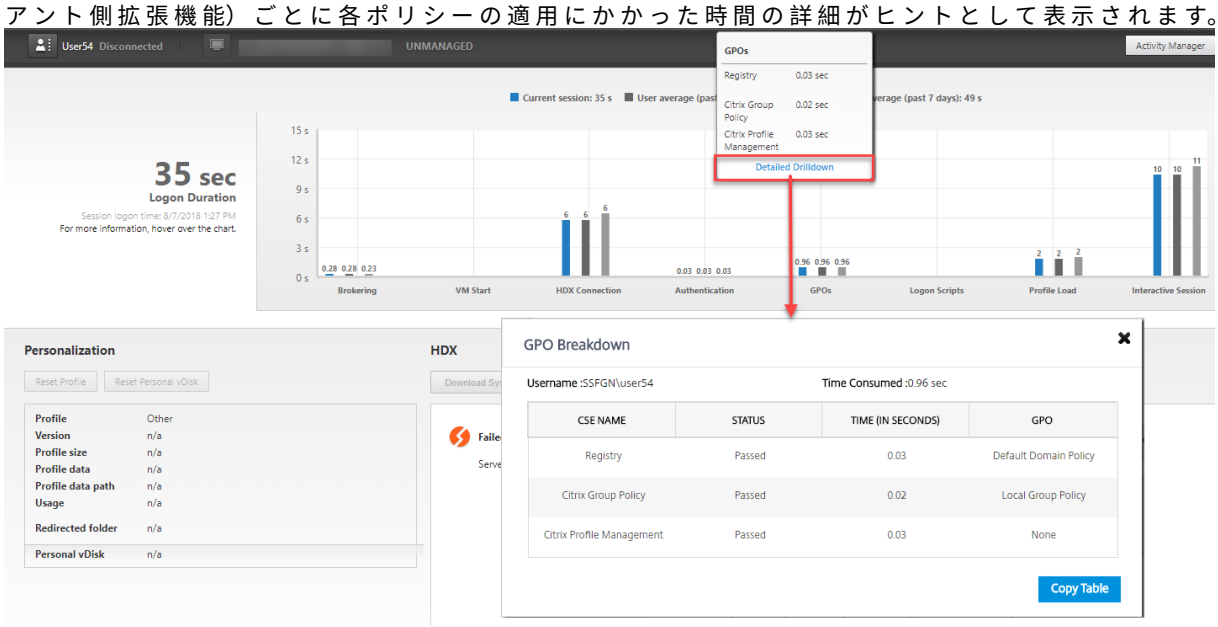
クライアントから仮想マシンへの HDX 接続の設定で必要な手順を実行するためにかかった時間です。

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。

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に、ログオン中に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。GPO バーにマウスカーソルを重ねると、CSE（クライアント側拡張機能）ごとに各ポリシーの適用にかかった時間の詳細がヒントとして表示されます。



[詳細なドリルダウン] をクリックすると、ポリシーの状態と対応する GPO 名を示すテーブルが表示されます。ドリルダウンの期間は CSE 処理時間のみを表し、合計 GPO 時間には加算されません。ドリルダウンテーブルは、詳細なトラブルシューティングやレポートで使用するためにコピーできます。各ポリシーの GPO 時間は、イベントビューアーのログから取得されます。操作ログに割り当てられているメモリ（デフォルトサイズは 4MB）によっては、このログは上書きされる可能性があります。操作ログのログサイズを増やす方法について詳しくは、「Configuring the Event Logs」を参照してください。

ログオンスクリプト

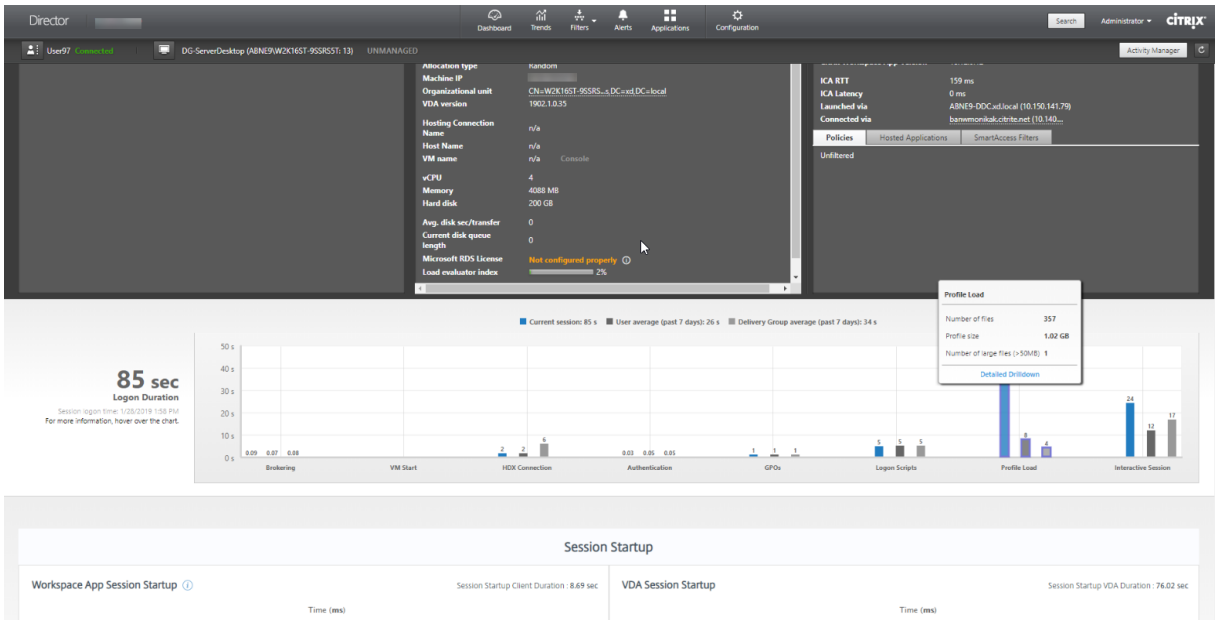
セッションでログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。

プロファイルのロード

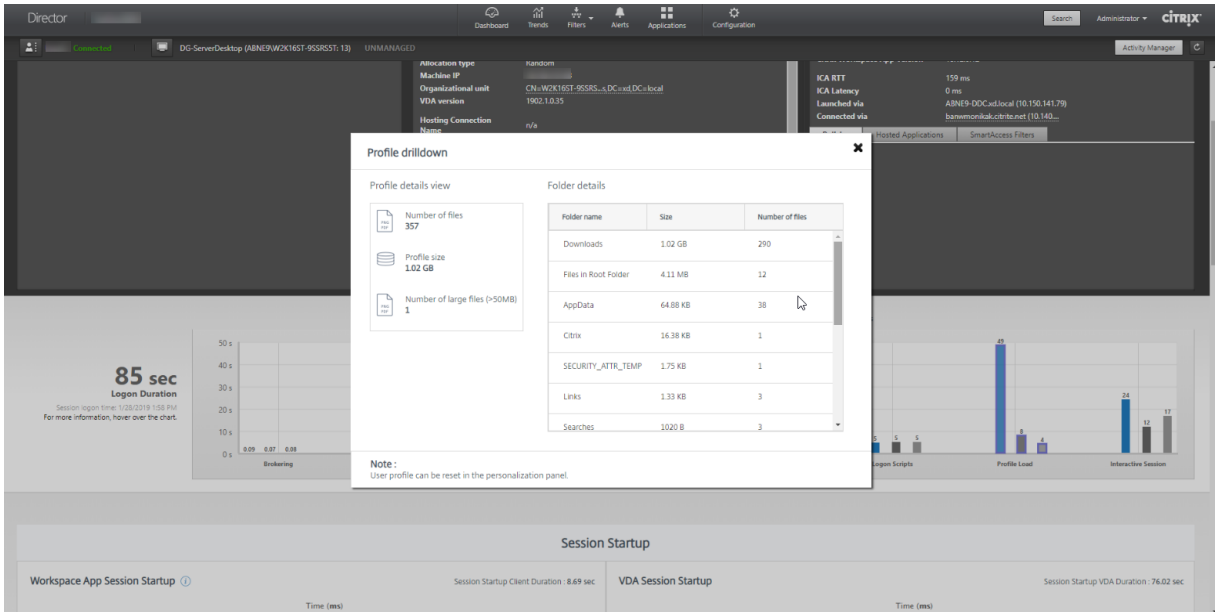
ユーザーまたは仮想マシンに対してプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。

Citrix Profile Management が構成されている場合、［プロファイルロード］バーに表示されるのは Citrix Profile Management がユーザープロファイルの処理に要する時間です。この情報は、管理者が処理に時間がかかる問題をトラブルシューティングするために役立ちます。Profile Management が構成されている場合、［プロファイルロード］バーに表示される処理時間が長くなります。この処理時間の増加は機能を拡張した結果であり、パフォーマンスが低下したわけではありません。この機能拡張は、VDA 1903 以降で利用できます。

［プロファイルのロード］バーの上にカーソルを置くと、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



［詳細なドリルダウン］をクリックすると、プロファイルのルートフォルダー（C:/Users/username など）内の個別のフォルダー、そのサイズとファイル数（サブフォルダー内のファイルを含む）に詳細にドリルダウンできます。



プロファイルのドリルダウンは、Delivery Controller バージョン 7 1811 以降および VDA 1811 以降で使用できます。プロファイルドリルダウン情報を使用すると、長いプロファイルロード時間に関連する問題を解決できます。次の操作を実行できます:

- ユーザープロファイルをリセットする
- 大きな不要ファイルを削除してプロファイルを最適化する
- ファイル数を減らしてネットワーク負荷を軽減する
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルのルートフォルダー内にあるすべてのフォルダーがドリルダウンに表示されます。フォルダーを非表示にするには、VDA マシンの以下のレジストリ値を編集します:

> 警告:
>
> レジストリの追加や編集を誤ると、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。

1. VDA で、HKEY_LOCAL_MACHINE\Software\Citrix\Director に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。\
2. 値を 1 に設定します。この値は、DWORD（32 ビット）値である必要があります。フォルダ名の表示が無効になりました。
3. フォルダ名を再度表示するには、値を 0 に設定します。

> 注:
> GPO または PowerShell コマンドを使用して、複数のマシンでレジストリ値の変更を適用できます。GPO を使用してレジストリの変更を展開する方法について詳しくは、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内の NTUser.dat ファイルは、エンドユーザーに表示されないことがあります。ただし、これらはプロファイルのドリルダウンに含まれ、ルートフォルダー内のファイルのリストに表示されます。
- AppData フォルダーの一部の隠しファイルは、プロファイルドリルダウンに含まれません。
- ファイル数およびプロファイルサイズに関するデータは、Windows の制限事項が原因で［個人設定］パネルのデータと一致しないことがあります。

対話型セッション

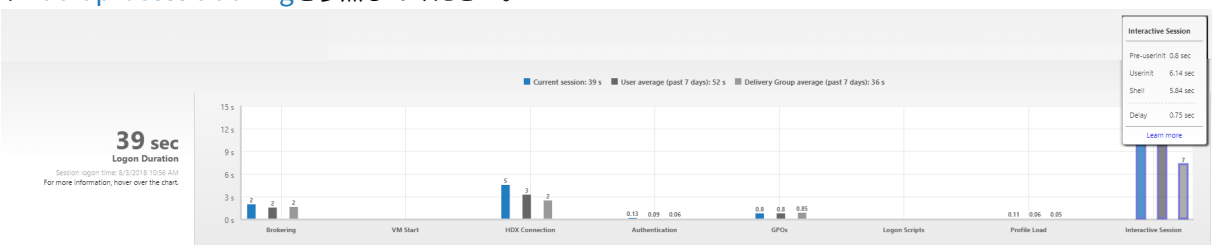
これは、ユーザープロファイルのロード後、キーボードやマウスの制御をユーザーに「渡す」までにかかった時間です。通常、ログオンプロセスのすべてのフェーズで最も長い時間であり、次のように計算されます：対話型セッションの処理時間 **=** デスクトップ準備完了イベントのタイムスタンプ（**VDA** の **EventId 1000**）**-** ユーザープロファイルロード完了イベントのタイムスタンプ（**VDA** の **EventId 2**）対話型セッションには、userinit 実行前、userinit、Shell の 3 つのサブフェーズがあります。［対話型セッション］上にマウスカーソルを置くと、サブフェーズ、各サブフェーズの所要時間、サブフェーズ間の総累積遅延時間、ドキュメントへのリンクを示すヒントが表示されます。

> 注：
>
> この機能は VDA バージョン 1811 以降で使用できます。7.18 より前のバージョンのサイトでセッションを開始してから 7.18 以降にアップグレードした場合、「サーバーエラーのためドリルダウンを使用できません。」というメッセージが表示されます。アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、仮想マシン（VDA ）でプロセス追跡の監査を有効にします。プロセス追跡の監査が無効（デフォルト）の場合、表示されるのは userinit 実行前の時間と、Userinit と Shell の合計時間になります。以下の手順により、グループポリシーオブジェクト（GPO）を使用してプロセス追跡の監査を有効化できます：

1. 新しい GPO を作成し、GPO エディターで編集します。
2. ［コンピューターの構成］> ［Windows の設定］> ［セキュリティの設定］> ［ローカルポリシー］> ［監査ポリシー］の順に移動します。
3. 右側のペインで、［プロセス追跡の監査］をダブルクリックします。
4. ［成功］チェックボックスをオンにして、［OK］をクリックします。
5. この GPO を目的の VDA やグループに適用します。

プロセス追跡の監査の詳細とこの機能の有効化および無効化の切り替え方法については、Microsoft のドキュメントAudit process trackingを参照してください。



［ユーザーの詳細］ビューの［ログオン処理時間］パネル。

- 対話型セッション – **userinit** 実行前：対話型セッションの所要時間のうち、グループポリシーオブジェクトおよびスクリプトの適用にかかった時間です。このサブフェーズは、GPO とスクリプトを最適化することで短縮できます。
- 対話型セッション – **userinit**： Windows マシンにユーザーがログオンすると、Winlogon により userinit.exe が実行されます。Userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Windows ユーザーインターフェイスである Explorer.exe を起動します。この対話型セッションのサブフェーズは、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。
- 対話型セッション – **Shell**：前のサブフェーズで、userinit により Windows ユーザーインターフェイスの初期化が開始されます。Shell サブフェーズは、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。
- 遅延： **userinit** 実行前および **userinit** と **userinit** および **Shell** の各サブフェーズ間の累積遅延時間です。

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、一部のフェーズは並行して発生するほか、フェーズによっては追加処理が発生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。総ログオン処理時間には、ICA ファイルのダウンロードとアプリケーションでの ICA ファイルの起動までの時間に相当する、ICA アイドル時間は含まれません。
アプリケーション起動時に ICA ファイルを自動的に開くようにするは、ICA ファイルをダウンロード時に自動で開くようにお使いの Web ブラウザーを構成します。詳しくは、「CTX804493」を参照してください。

> 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。

ユーザーのシャドウ

April 26, 2021

Director のユーザーのシャドウ機能を使用すると、ユーザーの仮想マシン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。Windows と Linux VDA の両方をシャドウできます。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。

Director は新しいタブでシャドウを開始し、Director URL からのポップアップを許可するように Web ブラウザーの設定を更新します。

［ユーザーの詳細］ビューからシャドウ機能にアクセスします。ユーザーセッションを選択し、［アクティビティマネージャー］ビューまたは［セッション詳細］パネルで、［シャドウ］をクリックします。

Linux VDA のシャドウ

シャドウは、RHEL7.3 または Ubuntu バージョン 16.04 Linux ディストリビューションを実行する Linux VDA バージョン 7.16 以降で使用できます。

> 注:
>
> - シャドウが機能するには、Director UI から VDA にアクセスできる必要があります。したがって、シャドウは Director クライアントと同じイントラネット内の Linux VDA に対してのみ実行できます。
> - Director は完全修飾ドメイン名を使用してターゲットの Linux VDA に接続します。Director クライアントが Linux VDA の完全修飾ドメイン名を解決できるようにしてください。
> - VDA には、python-websockify パッケージと x11vnc パッケージがインストールされている必要があります。
> - VDA への noVNC 接続は、WebSocket プロトコルを使用します。デフォルトでは、**ws://** WebSocket プロトコルが使用されます。セキュリティ上の理由からセキュリティ保護された **wss://** プロトコルを使用することをお勧めします。各 Director クライアントおよび Linux VDA に SSL 証明書をインストールします。

VDA をシャドウ用に設定するには、「セッションのシャドウ」の手順に従います。

1. ［シャドウ］をクリックすると、シャドウ接続が初期化され、確認プロンプトがユーザーデバイスに表示されます。

2. 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。
3. 管理者は、シャドウセッションのみを表示できます。

Windows VDA のシャドウ

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDA のインストール中にユーザーの Windows リモートアシスタンス機能を有効にします。詳しくは、「VDA のインストール」の「機能を有効または無効にする」セクションを参照してください。

1. ［シャドウ］をクリックするとシャドウ接続が初期化されます。これにより、.msrc インシデント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。
2. 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。
3. 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。
4. 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。

ユーザーへのメッセージの送信

April 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。

ユーザーにメッセージを送信するには、次の手順を実行します：

1. ［監視］ > ［フィルター］ > ［マシン］ > ［すべてのマシン］と移動します。
2. メッセージの送信先のマシンを選択し、［メッセージの送信］をクリックします。
3. 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。

アプリケーション障害の解決

April 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。

マルチセッション OS マシンおよびシングルセッション 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	シングルセッション 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。マルチセッション 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。

デスクトップ接続の復元

April 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。

セッションの復元

April 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、仲介されたマルチセッション 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。

HDX チャネルシステムレポートの実行

April 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。

ユーザープロファイルのリセット

April 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。

これまでの手順では、Citrix Virtual Desktops（デスクトップ VDA）を使用している前提になっています。Citrix Virtual Desktops（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。

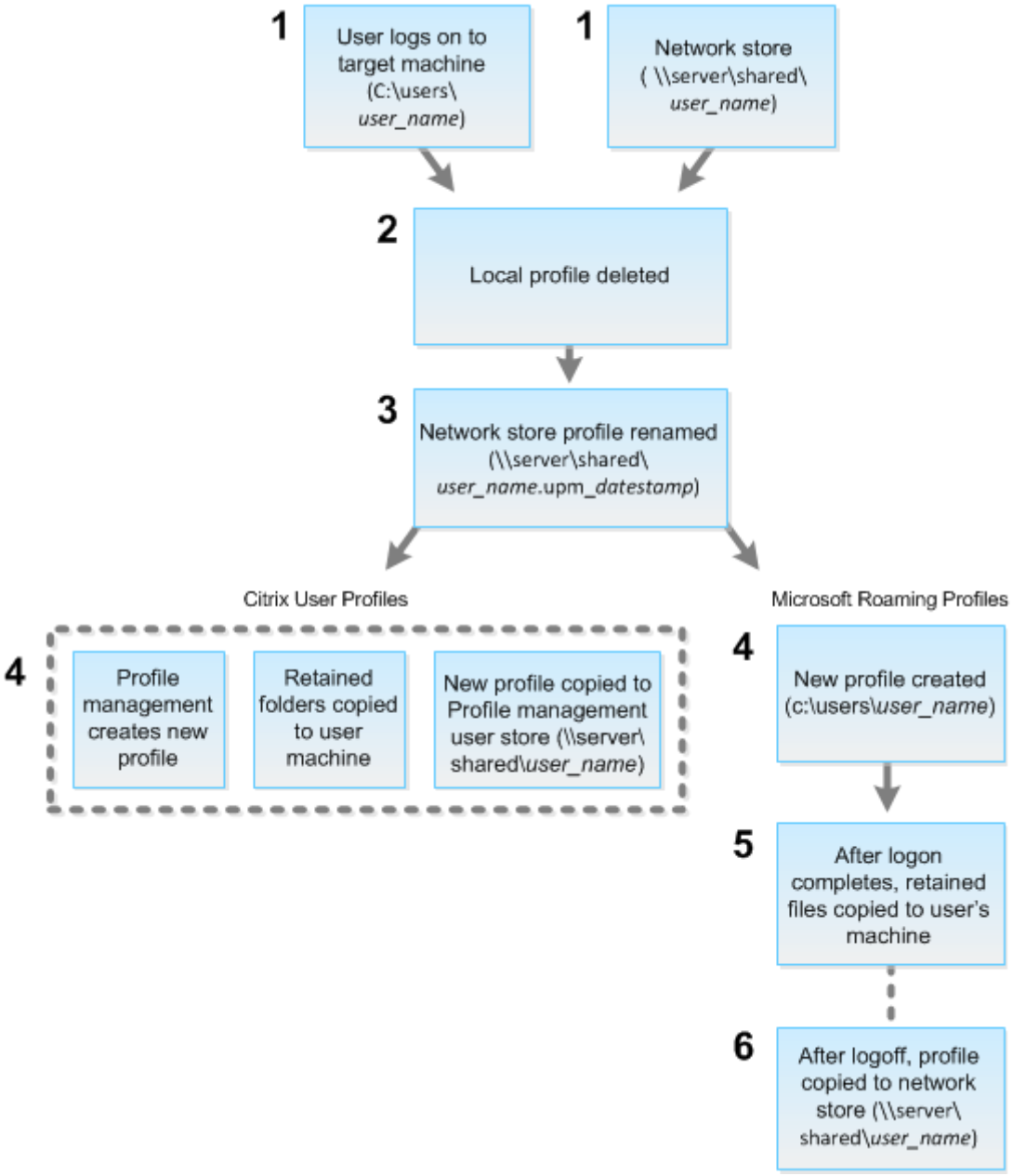
- デスクトップ
- Cookies
- お気に入り
- ドキュメント
- ピクチャ
- ミュージック
- ビデオ

> 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、ユーザープロファイルがリセットされた場合の処理を説明した図です。



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）。

1. ローカルプロファイルがある場合は削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 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。必要な場合は、テンプレートプロファイルが移動プロファイルよりも優先されるように Profile Management を構成することもできます。

Microsoft 移動プロファイルの場合、Windows により新しいプロファイルが作成され、ユーザーがログオンするとフォルダーがユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルがネットワークストアにコピーされます。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーに、すべてのセッションからログオフするように指示します。
2. ローカルプロファイルが存在する場合は削除します。
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。

PowerShell SDK を使用してプロファイルをリセットするには

Broker PowerShell SDK を使用してプロファイルをリセットできます。

New-BrokerMachineCommand

特定のユーザー、セッション、またはマシンに配信するためのキューに登録されたコマンドを作成します。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-BrokerMachineCommand/を参照してください。

例

PowerShell コマンドレットを使用してプロファイルをリセットする方法の詳細については、以下の例を参照してください:

Profile Management プロファイルのリセット

- user1 のプロファイルをリセットしたいとします。PowerShell コマンドの New-BrokerMachineCommand を使用します。例:
  - ```
    New-BrokerMachineCommand -Category UserProfileManager -CommandName
    "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger
     logon -user domain1\user1
    ```


    ```

> 重要:
>
> `CommandData $byteArray`を使用する際は、`<SID>[,<backup path>]`の形式にする必要があります: バックアップパスを指定しない場合、Profile Management により現在の日付と時刻で名前が付けられたバックアップフォルダが生成されます。

Windows 移動プロファイルのリセット

- user1 の移動プロファイルをリセットしたいとします。PowerShell コマンドの New-BrokerMachineCommand を使用します。例:
  - ```
    New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1
    ```

セッションの録画

April 26, 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［セッションレコーディング］を構成するには、「録画ポリシーの作成とアクティブ化」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 ポリシーコンソールによる 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

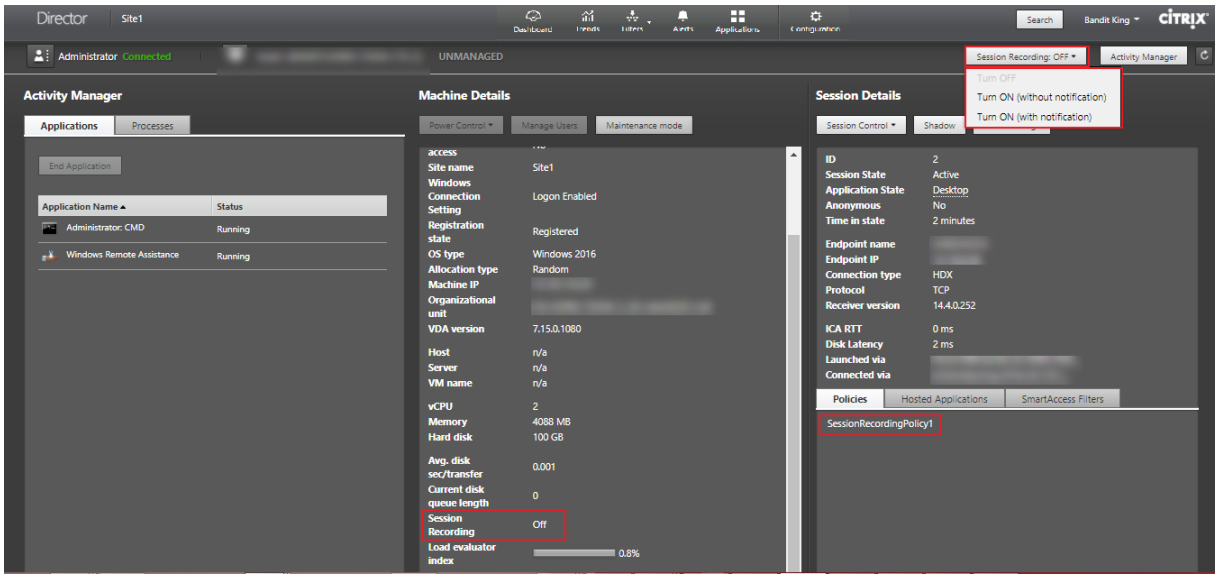
［アクティビティマネージャー］または［ユーザーの詳細］画面で、特定のユーザーに対して Session Recording を有効にできます。サポートされるすべてのサーバーで特定のユーザーに対して以降のセッションが録画されます。

次の操作を実行できます:

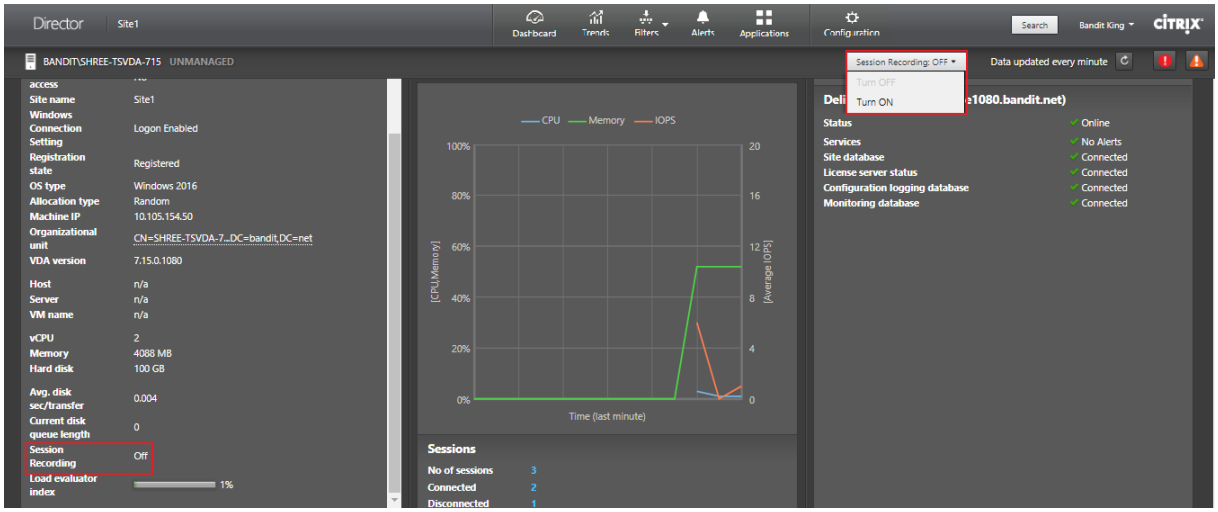
- オンにする（通知あり）- ICA セッションへのログオン時に録画されているセッションについてユーザーに通知されます。
- オンにする（通知なし）- ユーザーに通知されることなく、セッションは録画されます。
- オフにする - ユーザーのセッションの録画を無効にします。


    ```

［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。




## 機能の互換性マトリックス

April 26, 2021

Citrix Director 7 2003 は以下の製品と互換性があります:

- Citrix Virtual Apps and Desktops 7 1912 以降
- XenApp および XenDesktop バージョン 7.15 LTSR

各サイトでは、Delivery Controller の以前のバージョンとともに Director 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。Director、Delivery Controller、VDA は同じバージョンを使用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。

Director のアップグレード後に初めてログオンすると、設定されたサイトでバージョンチェックが実行されます。いずれかのサイトで Director のバージョンよりも前のバージョンの Controller が実行されている場合は、Director のコンソールにメッセージが表示され、サイトのアップグレードが推奨されます。さらに、サイトのバージョンが Director のバージョンより古い限り、この不一致を示すメモが Director のダッシュボードに引き続き表示されます。

Director の特定の機能と、Delivery Controller（DC）、VDA、およびライセンスエディションとともに必要なその他の従属コンポーネントの最小バージョンを次に示します。

| **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 |
|---|---|---|---|
| 1909 | Citrix Analytics for Performance を使用したオンプレミスサイトの構成 | DC 7 1906 および VDA 1906 | すべて |
| 1906 | セッションの自動再接続 | DC 7 1906 および VDA 1906 | すべて |
| 1906 | セッションの開始時間 | DC 7 1906 および VDA 1903 | すべて |
| 1906 | デスクトッププロービング | DC 7 1906 および Citrix Probe Agent 1903 | Premium |
| 7.9 以降 | Citrix Profile Management のプロファイルのロード時間 | VDA 1903 | すべて |
| 1811 | プロファイルのドリルダウン | DC 7 1811 および VDA 1811 | すべて |
| 1811 | ハイパーバイザーアラートの監視 | DC 7 1811 | Premium |
| 1811 | アプリケーションプロービング | DC 7 1811 および Citrix Application Probe Agent 1811 | Premium |

| **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 |
|---|---|---|---|
| 1811 | Microsoft RDS ライセンスの正常性 | DC 7 1811 および VDA 7.16 | すべて |
| 1811 | RTOP の主要データの表示 | DC 7 1811 および VDA 1808 | Premium |
| 1808 | フィルターデータのエクスポート | DC 7 1808 | すべて |
| 1808 | 対話型セッションのドリルダウン | DC 7 1808 および VDA 1808 | すべて |
| 1808 | GPO のドリルダウン | DC 7 1808 および VDA 1808 | すべて |
| 1808 | OData API を使用したマシン履歴データの取得 | DC 7 1808 | すべて |
| 7.18 | アプリケーションプロービング | DC 7.18 | Premium（旧称 Platinum） |
| 7.18 | スマートアラートポリシー | DC 7.18 | Premium（旧称 Platinum） |
| 7.18 | Health Assistant リンク | なし | すべて |
| 7.18 | 対話型セッションのドリルダウン | なし | すべて |
| 7.17 | PIV スマートカード認証 | なし | すべて |
| 7.16 | アプリケーション分析 | DC 7.16 および VDA 7.15 | すべて |
| 7.16 | OData API V.4 | DC 7.16 | すべて |
| 7.16 | Linux VDA ユーザーのシャドウ | VDA 7.16 | すべて |
| 7.16 | ドメインローカルグループのサポート | なし | すべて |
| 7.16 | マシンコンソールへのアクセス | DC 7.16 | すべて |
| 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 |

| **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 |
|---|---|---|---|
| 7.14 | 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 | Premium（旧称 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 |
| 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 | Premium（旧称 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 ADM 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 | Premium（旧称 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 | Premium（旧称 Platinum） |
| 7.7 | SCOM 統合 | DC 7.7、VDA 7.x、SCOM 2012 R2、および PowerShell 3.0 | Premium（旧称 Platinum） |

| **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 |
|---|---|---|---|
| 7.7 | Windows 認証の統合 | DC 7.x および VDA 7.x | すべて |
| 7.7 | シングルセッション OS およびマルチセッション OS の使用 | DC 7.7 および VDA 7.x | Premium（旧称 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 | Premium（旧称 Platinum） |
| 7 | HDX Insight 統合 | DC 7.6、VDA 7.x、および Citrix ADM | Premium（旧称 Platinum） |

## データの粒度と保持

April 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。Premium 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-->
```

	設定名	対象データ	デフォルト値（Premium、日数）	デフォルト値（Premium 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	GroomFailuresReten	MachineFailureLog レコードおよび ConnectionFail-ureLog レコード	90	7
3	GroomLoadIndexe	LoadIndex レコード	90	7

	設定名	対象データ	デフォルト値（Premium、日数）	デフォルト値（Premium 以外、日数）
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
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

	設定名	対象データ	デフォルト値（Premium、日数）	デフォルト値（Premium 以外、日数）
10	GroomNotificationLogRetentionDays	通知ログ	90	
11	GroomResourceUs	リソース使用率データ（生データ）	3	3
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）	90	7
19	GroomSessionMet	セッションメトリックデータ	1	1
20	GroomMachineMetricDataRetentionDays	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。

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。

サードパーティ製品についての通知

April 24, 2021

Citrix Virtual Apps and Desktops のこのリリースには、次のドキュメントで規定された条件の元でライセンス提供されている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:

- Citrix Virtual Apps and Desktops サードパーティ製品についての通知 （PDF のダウンロード）

- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0)（PDF のダウンロード）
- FlexNet Publisher Documentation Supplement Third Party および FlexNet Publisher 11.15.0 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）

SDK および API

April 24, 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 Citrix Virtual Apps and Desktops 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、Citrix Virtual Apps または Citrix Virtual Desktops 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。

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。

> 注:
>
> 最新の SDK は、PowerShell スナップインと PowerShell モジュールの両方としてインストールされ

> ます。
>
> モジュール機能の追加により、この SDK のコマンドレットを先行コマンドレット`Add-PSSnapin`（または`asnp`）なしで使用できます。
>
> スナップインとしてのみインストールされる関連コンポーネントの SDK（Citrix ライセンスサーバー、Citrix Provisioning、StoreFront など）でコマンドレットを使用するには、先行コマンドレット`Add-PSSnapin`（または`asnp`）が必要です。
>
> スナップインからこの SDK を使用する場合、次の手順に進みます。

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 と V2 は、スナップインのバージョンを示します。XenDesktop 5 スナップインはバージョン 1 です。Citrix Virtual Apps and Desktops、およびそれ以前の XenDesktop 7 バージョンのスナップインはバージョン 2 です。たとえば、Citrix Virtual Apps and Desktops スナップインをインストールするには、「`Add-PSSnapin Citrix.ADIdentity.Admin.V2`」と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

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。

最新の Citrix Virtual Apps and Desktops PowerShell コマンドレットヘルプを確認するには、次の手順に従います:

1. PowerShell コンソールから Citrix スナップイン: `Add -PSSnapin Citrix.*.Admin.V*`。
2. Windows PowerShell ISEの手順に従ってください。

グループポリシー **SDK**

Group Policy SDK を使用するには、Studio または Citrix Virtual Apps and Desktops 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、「`Add-PSSnapin citrix.common.grouppolicy`」と入力します。（ヘルプにアクセスするには、次を入力します: `help New-PSDrive -path localgpo:/`）

仮想ドライブを作成して設定を読み込むには、`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。

Monitor Service OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズした監視ダッシュボードおよびレポートダッシュボードを作成できます。OData V.4 は、ASP.NET Web APIに基づいており、アグリゲーションクエリをサポートしています。詳しくは「Monitor Service OData API」を参照してください。

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